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

Gérard Leloup

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

G. LELOUP

Abstract. In order to study simple extensions of valued fields, notions of key polynomials were developed. Model theoretical properies of extensions of valued fields were also studied. The properties of valuations used in model theory shed a new light on key polynomials and they make it possible to obtain underlying properties of these extensions. Key polynomials are used for defining separate valuations which approximate a valuation on an extension $K(\chi)$. A valuation ν_λ on $K(\chi)$ is separate if there is a K-basis $\mathcal{B}_\lambda$ of $K[\chi]$ such that ν_λ is determined by its restrictions to K and $\mathcal{B}_\lambda$. For every valuation ν the aim is to find a family of monic polynomials of $K[\chi]$, which are called key polynomials, and a family ν_λ of separate valuations such that for every λ the elements of $\mathcal{B}_\lambda$ are products of key polynomials, and, for every $f \in K[\chi]$, $\nu(f)$ is the maximum of the family $(\nu_\lambda(f))$. The approach of the present paper shows the links between some properties of valuations used in model theory and the key polynomials. The existence of a family of separate valuations as above follows in a natural way. Our definitions rely on euclidean division of polynomials, on bases of vector spaces and on classical properties of valuations.

[1] The purpose of this work is twofold. On the one hand, it is to show the links between the model theoretical study of extensions of valued fields of W. Baur, F. Delon and the author (see [B 81], [B 82], [D 82], [D 88], [D 91], [L 89], [L 03]) and the study of simple extensions of valued fields of S. Maclane ([ML 36a], [ML 36b]), M. Vaquié ([V 07]), F. J. Herrera Govantes, W. Mahloud, M. A. Olalla Acosta, M. Spivakovsky ([HOS 07], [HMOS 14]) and others. These last authors made this study with algebraic geometrical purposes. On the other hand, it is to give a different approach to the study of key polynomials. This approach relies on euclidean division of polynomials, basis of vector spaces and the notions of separate and immediate extensions used in model theoretical study of extensions of valuations. In the following, we use the word "module" which is shorter than "vector space". As much as possible, we try to use only elementary properties of valuations. Furthermore, we try to make clear that some valuations that we define are only K-module valuations (see definition below). However, we use an approximation theorem of Ribenboim in one proof, pseudo-Cauchy sequences in two subsections dedicated to immediate extensions, and the graded algebra associated to a valuation in two proofs (all the definitions will be given below). On the one side, pseudo-Cauchy sequence play an important role in the study of immediate extensions. On the other side graded algebras are a good tool for providing nice proofs of some properties of separate extensions. This work is self-contained and when we use results on key polynomials of preceding papers, we generally give a proof.

S. MacLane introduced key polynomials to define families of separate valuations which approximate an extension of ν to the field $K(\chi)$, where χ is algebraic or transcendental over K. They are also used for defining the different extensions of a fixed valuation to a given simple algebraic extension of a field. Here we will focus on the first purpose. S. MacLane gave a definition of a key polynomial for a valuation, but with this definition Φ is a key polynomial for the generalized Gauss valuation ν_Φ that we will define in Proposition 3.15 and Notations 3.16, but not for ν in general. In the works of S. MacLane and of M. Vaquié, the key polynomials Φ are constructed by induction, starting from the degree 1 key polynomials. In [HOS 07] the authors do not define key polynomials but families of key polynomials, by means of properties that these families have to satisfy. Then they construct such families by induction, starting from the degree 1, in a different way from the constructions of S. MacLane and M. Vaquié. Here, we give a general 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). In Proposition 3.23 we show that Φ being a key polynomial for ν is equivalent to being a MacLane key polynomial for the generalized Gauss valuation ν_Φ. However, we only need a family of key polynomials that we call strict key polynomials. With our definition, it is not necessary to construct the families of key polynomials by induction on the degree, but we construct independently the key polynomials of each degree, if any (Definition 4.9). Next we deduce a family (ν_λ) of K-module valuations (where λ runs over a partially ordered set) and we prove in a natural way that, for every $f \in K[\chi]$, $\nu(f)$ is the maximum of the family $\nu_\lambda(f)$, and that, if the family of λ's is infinite, there are infinitely many λ's such that $\nu_\lambda(f) = \nu(f)$ (Theorem 4.11).

Date: September 18, 2018.

[1]2010 *Mathematics Subject Classification.* 12J10, 12J20, 12F99.

Keywords: simple extension, valuation, key polynomial.

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*. 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 field of the valuation ring by the maximal ideal 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 $\mathrm{char}K_\nu=0\Rightarrow \mathrm{char}K=0$ and $\mathrm{char}K>0\Rightarrow \mathrm{char}K_\nu=\mathrm{char}K$. 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 $\{\nu(x)\mid x\in M,\ x\neq 0\}$.

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. For $n\in\mathbb{N}^*$, we denote by $K_n[\chi]$ the K-submodule of $K[\chi]$ of all polynomials of degree at most n, where χ is algebraic or transcendental over K. We let $K_0[\chi]=K$ and if χ is transcendental over K, then we let $K_\infty[\chi]=K[\chi]$. 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 and $\nu K(\chi)$ have countable cofinality. If the rank is 1, then νK embeds in the ordered group $(\mathbb{R},+)$; we also say that ν is *archimedean*.

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 $x\in K$: $\nu(y_1)=\infty\Leftrightarrow y_1=0$, $\nu(y_1+y_2)\geq\min(\nu(y_1),\nu(y_2))$, $\nu(xy_1)=\nu(x)+\nu(y_1)$ (it follows that its restriction to K is a valuation of field).

Separate and immediate extensions.

Assume that ν is a K-module valuation on M. In general, for every $x_1,\dots,x_n$ in K, pairwise distinct $y_1,\dots,y_n$ in M, $\nu(x_1y_1+\cdots+x_ny_n)$ is at least equal to $\min(\nu(x_1y_1),\dots,\nu(x_ny_n))$, and it can be arbitrarily large. The K-module valuation ν is said to be *separate* if there exists a basis $\mathcal{B}$ of M such that for every $x_1,\dots,x_n$ in K, pairwise distinct $y_1,\dots,y_n$ in $\mathcal{B}$, $\nu(x_1y_1+\cdots+x_ny_n)=\min(\nu(x_1y_1),\dots,\nu(x_ny_n))$. If this holds, then the basis $\mathcal{B}$ is said to be *ν-separate* (in short *separate*). Note that if $\mathcal{B}$ is a basis of L, then we can define a separate K-module valuation ν' by setting, for every $x_1,\dots,x_n$ in K, pairwise distinct $y_1,\dots,y_n$ in $\mathcal{B}$, $\nu'(x_1y_1+\cdots+x_ny_n)=\min(\nu(x_1y_1),\dots,\nu(x_ny_n))$. If ν is separate, then one can compute the valuation of any element of M by means of the restrictions of ν to K and $\mathcal{B}$.

We will see in Proposition 2.19 that for $d\in\mathbb{N}\cup\{\infty\}$ such that $0<d\leq[K[\chi]:K]-1$, the extension $(K_d[\chi]|K,\nu)$ is separate if, and only if, for every integer n, $1\leq n\leq d$, $\nu(\chi^n-K_{n-1}[\chi])=\{\nu(\chi-y)\mid y\in K_{n-1}[\chi]\}$ has a maximal element. Futhermore, if χ is transcendental over K, and ν is a field valuation on $K(\chi)$, then $(K(\chi)|K,\nu)$ is separate if, and only if, for every $n\in\mathbb{N}^*$, $\nu(\chi^n-K_{n-1}[\chi])$ has a maximal element.

Let $M\subset N$ be K-submodules of L. We say that the K-module N is *immediate* over M if for every $l\in N$, the set $\nu(l-M)=\{\nu(l-x)\mid x\in M\backslash\{l\}\}$ is a subset of νM and it has no maximal element. We say that it is *dense* over M if for every $l\in N$, the set $\nu(l-M)$ is equal to νM. One can prove that saying that the extension of valued field $(L|K,\nu)$ is immediate is equivalent to saying that $\nu L=\nu K$ and $L_\nu=K_\nu$. We will show in Proposition 1.7 that for d, d' in $\mathbb{N}\cup\{\infty\}$ such that $0\leq d<d'\leq[K[\chi]:K]-1$, (that is, if χ is algebraic over K, then $d'<[K[\chi]:K]$), the extension $(K_{d'}[\chi]|K_d[\chi],\nu)$ is immediate if, and only if, for every $n\in\{d+1,\dots,d'\}$, $\nu(\chi^n-K_{n-1}[\chi])$ has no maximal element. Furthermore, if ν is a field valuation and $\nu K[\chi]$ is a group, then it is dense if, and only if, for every $n\in\{d+1,\dots,d'\}$, $\nu(\chi^n-K_{n-1}[\chi])=\nu K$. The sets $\nu(\chi^n-K_{n-1}[\chi])$, which appear in Propositions 1.7 and 2.19, will be used in the definitions of key polynomials, and in the construction of families of key polynomials.

Families of key polynomials.

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 $f(\chi)$. S. MacLane defined families (ν_i) of separate K-module valuations to approximate ν (where i runs over a well-ordered set). Note that if $\mathcal{B}_i$ is a separate basis for ν_i, and the restrictions of ν and ν_i to K and $\mathcal{B}_i$ are equal, then for every $f\in K[\chi]$ we have $\nu_i(f)\leq\nu(f)$ (in short, $\nu_i\leq\nu$). Assume that χ is algebraic (so that $K(\chi)=K[\chi]$), and that there exists $f\in K[\chi]$ such that $\nu_i(f)<\nu(f)$. Since $\nu_i\leq\nu$, 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 3.15 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.

If for every f, g in $K[\chi]$ such that $\deg(f)+\deg(g)<[K[\chi]:K]$ we have $\nu(fg)=\nu(f)+\nu(g)$, then we say that ν is *partially multiplicative*, or a *p-m valuation*. In the case where $[K[\chi]:K]=\infty$, 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*.

Let Φ be a monic polynomial of degree d. We say that Φ is a *strict key polynomial* if, for every f, g in $K_{d-1}[\chi]$ with $\deg(f)+\deg(g) < [K[\chi]:K]$, $\nu(fg)=\nu(r)<\nu(q\Phi)$, where $fg=q\Phi+r$ is the euclidean division. A positive integer d is said to be a *strict key degree* if there is a strict key polynomial of degree d. Trivially, 1 is a strict key degree, and we see that any strict key polynomial is irreducible. Let $d_1=1<d_2<\cdots<d_n$ be the first n strict key degrees. For $i\leq n$, let Φ_{d_i} be a strict key polynomial of degree d_i, and $d_{n+1}=[K(\chi):K]$. We let $\mathcal{B}$ be the family of the $\Phi_{d_1}^{e_1}\cdots\Phi_{d_n}^{e_n}$, where, for $1\leq j\leq n$, $e_1+e_2d_2+\cdots+e_jd_j<d_{j+1}$. Since the degree mapping is one-to-one from $\mathcal{B}$ onto $[0,[K(\chi):K][$, $\mathcal{B}$ is indeed a basis of the K-module $K[\chi]$. We let $\nu_{\Phi_{d_1},\ldots,\Phi_{d_n}}$ be the separate K-module valuation defined by this basis. Then, for every $f\in K[\chi]$, all the $\nu_{\Phi_{d_1},\ldots,\Phi_{d_n}}(f)$ are bounded above by $\nu(f)$. We prove that there exists a family $\mathcal{F}$ of strict key polynomials such that, for every $f\in K[\chi]$, by letting d_n be the greatest strict key degree which is at most equal to $\deg(f)$, there exist $\Phi_{d_1},\ldots,\Phi_{d_n}$ in $\mathcal{F}$ such that $\nu_{\Phi_{d_1},\ldots,\Phi_{d_n}}(f)=\nu(f)$.

The family $\mathcal{F}$ is defined in the following way. Let d be a strict key degree. We say that d is a *separate* key degree if the set $\nu(\chi^d-K_{d-1}[\chi])$ has a maximal element. We will show in Proposition 3.26 that every monic polynomial Φ_d of degree d such that $\nu(\Phi_d)=\max\nu(\chi^d-K_{d-1}[\chi])$ is a strict key polynomial. We say that d is an *immediate* key degree if the set $\nu(\chi^d-K_{d-1}[\chi])$ has no maximal element. We will show in Proposition 3.26 that there exists a sequence $(\Phi_{d,n})$ of key polynomials of degree d such that the sequence $(\nu(\Phi_{d,n}))$ is increasing and cofinal in $\nu(\chi^d-K_{d-1}[\chi])$. Now, let $1=d_1<d_2<\cdots$ be the sequence of strict key degrees. If d_i is a separate key degree, then we let Φ_{d_i} be a strict key polynomial such that $\nu(\Phi_{d_i})=\max\nu(\chi^{d_i}-K_{d_i-1}[\chi])$. For notational convenience, for every non-negative integer n we set $\Phi_{d_i,n}=\Phi_{d_i}$. If d_i is an immediate key degree, then we let $(\Phi_{d_i,n})$ be a sequence of key polynomials of degree d_i such that the sequence $(\nu(\Phi_{d_i,n}))$ is increasing and cofinal in $\nu(\chi^{d_i}-K_{d_i-1}[\chi])$. Then we can let $\mathcal{F}$ be the family of the $\nu_{\Phi_{d_1,n_1},\ldots,\Phi_{d_k,n_k}}$'s, where k and the n_i's run over $\mathbb{N}$. If the degree of f is less than d_{k+1}, then $\nu(f)$ is the maximum of the family $\nu_{\Phi_{d_1,n_1},\ldots,\Phi_{d_k,n_k}}$, and infinitely many $\nu_{\Phi_{d_1,n_1},\ldots,\Phi_{d_k,n_k}}$'s are equal to $\nu(f)$ (Theorem 4.11).

Since the key polynomials of each degree are defined independently, the proof of this approximation theorem is short and it relies on a decreasing induction on the degrees of key polynomials. Furthermore, the rank of the valuation does not appear in the proof, it works whenever the rank is 1 or not. Note that in the case of an infinite rank, the only difference would be that the cardinal of the family is not necessarily countable, since in the $\nu_{\Phi_{d_1,n_1},\ldots,\Phi_{d_k,n_k}}$'s it may occur that the n_i's run over an uncountable ordered set.

If there is at most one immediate strict key degree, then we get an algorithm to calculate $\nu(f)$ for every polynomial f. Let d_k be the greatest key degree which is a most equal to the degree of f. Then $\nu_{\Phi_{d_1,n},\ldots,\Phi_{d_k,n}}(f)=\nu(f)\Leftrightarrow\nu_{\Phi_{d_1,n},\ldots,\Phi_{d_k,n}}(f)=\nu_{\Phi_{d_1,n+1},\ldots,\Phi_{d_k,n+1}}(f)$. Hence we compute $\nu_{\Phi_{d_1,n},\ldots,\Phi_{d_k,n}}(f)$, and we stop when this condition holds.

If we have $\nu(r)\leq\nu(q\Phi)$ instead of $\nu(r)<\nu(q\Phi)$ in the definition of strict key polynomials, then we say that Φ is a *key polynomial*. Key polynomials can also be characterized in the following way. Let Φ be a monic irreducible polynomial and d be the degree of Φ. Assume that $d\leq[K[\chi]:K]/2$. Since the K-modules $K_{d-1}[\chi]$, $K_{d-1}[X]$ and $K[X]/(\Phi)$ are isomorphic (where $K[X]$ denotes the ring of formal polynomials), ν induces a K-module valuation $\bar{\nu}$ on $K[X]/(\Phi)$ by setting, for $f\in K_{d-1}[X]$, $\bar{\nu}(f(X)+(\Phi))=\nu(f(\chi))$. Note that $\bar{\nu}(K[X]/(\Phi))=\nu(K_{d-1}[\chi])$. Now, Φ is a key polynomial if, and only if, $(K[X]/(\Phi),\bar{\nu})$ is a valued field (i.e. $\bar{\nu}$ is multiplicative). If Φ is a strict key polynomial, then in addition the residue field $(K[X]/(\Phi))_{\bar{\nu}}$ is canonically isomorphic to $(K_{d-1}[\chi])_\nu$ (so, it embeds in $(K[\chi])_\nu$).

Some model theory.

In above study, we see that the simpler case is the separate one. In the model theorical study of extensions of valued fields, separate extensions also give interesting results. 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 agebraic extension of K. A famous theorem of J. Ax, S. Kochen and Y. Ershov ([AK 65]) 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 [D 91] 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 indecidable and admits $2^{\aleph_0}$ completions. The failure comes from the sets $\nu(l-K)$, where $l\in L$. Now, if K, L are henselian, $\mathrm{char}K_\nu=0$, and $(L|K,\nu)$ is separate, 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 [B 81], [B 82], [L 89], [L 03]). 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 separate and $(L|H,\nu)$ is immediate (see [D 88]). This shows that it can be interesting to focus on separate and immediate extensions.

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. Then we focus on the case of simple extensions. We prove Proposition 1.7, and we generalize a result of F. Delon which shows that if the residue characteristic is 0 and ν is archimedean, then any simple immediate algebraic extension of valued field is dense (Theorem 1.10). We also recall definitions and properties of pseudo-Cauchy sequences which will be used later. Section 2 is devoted to separate extensions. In the same way as in Section 1, we focus on the case of simple extensions, and we prove Proposition 2.19. Then we recall definitions and properties of the graded algebras associated to valuations, since they are useful in the study of separate extensions. In Section 3, we characterize key polynomials and key degrees. We compare this definition with the definition of S. MacLane and M. Vaquié (Proposition 3.23). We study the K-module valuations defined by key polynomials, and the associated bases generated by these key polynomials. Next we set properties of key degrees. We prove, for example, that if d is an immediate key degree and d' is the next strict key degree, then the extension $(K_{d'-1}[\chi]|K_{d-1}[\chi],\nu)$ is immediate (Theorem 3.36). We also give characterizations of the successor of a given strict key degree (Theorems 3.36 and 3.37). In particular, we look at conditions for being the greatest strict key degree. For example, we show that this holds if $\nu(\chi^d - K_{d-1}[\chi]) = \nu K_{d-1}[\chi] = \nu K(\chi)$ (Proposition 3.41). Next, we look at the links between the separate strict key polynomials and the graded algebra of a valuation. Then, in Section 4, we use key polynomials to define the K-module valuations which approximate a given valuation of $K(\chi)|K$. We focus on the particular cases of immediate and separate extensions. We also show some links with the definitions of the families of key polynomials by M. Vaquié and by F. J. Herrera Govantes, W. Mahloud, M. A. Olalla Acosta and M. Spivakovsky (without going into the details). In Section 5 we come back to the definitions of decomposition, inertia and ramification fields, which are defined by means of subgroup of the Galois group of a normal extension. In this study also appear an immediate step and separate steps. However, this approach differs from the approach by means of key polynomials. We show this in some examples.

In the present paper we study only the properties which follow in a natural way from our definition of key polynomials, and we do not look at all properties studied in previous papers. In particular, we do not investigate the number of immediate strict key degrees or the links with the defect of an extension.

1. Immediate extensions

In this section, $L|K$ is an extension of fields and ν is a K-module valuation on L. 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 $\nu(xy) = \nu(x) + \nu(y) > \nu(y)$.

1.1. **Basic properties.** We generalize the definitions of immediate and dense extensions to extensions of K-modules.

Notations 1.1. Let $l \in L$ and M be a K-submodule of L. We denote by $\nu(l-M)$ the subset $\{\nu(l-x) \mid x \in M\backslash\{l\}\}$ of νM. For any polynomial f, we denote by $\nu(f(M))$, or $\nu f(M)$, the subset $\{\nu(f(x)) \mid x \in M\}\backslash\{\infty\}$.

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

Definitions 1.2. 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.

Remark 1.3. It follows that if $(N|M,\nu)$ is dense, then it is immediate.

Lemma 1.4. *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 $\nu(l-y) > \nu(l-x)$.*

Proof. If l is pseudo-limit, then $\nu(l-M)$ has no maximal element. Hence, for every $x \in M$ there exists $y \in M$ such that $\nu(l-y) > \nu(l-x)$. Conversely, if for every $x \in M$ there exists $y \in M$ such that $\nu(l-y) > \nu(l-x)$, then $\nu(l-M)$ has no maximal element. Now, let x, y in M such that $\nu(l-y) > \nu(l-x)$. Then, since $\nu(l-x) = \nu(l-y+y-x) < \nu(l-y)$, it follows that $\nu(l-y) = \nu(y-x) \in \nu M$. Hence $\nu(l-M) \subseteq \nu M$. Consequently, l is pseudo-limit over M. □

Notations 1.5. 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 od $M_{0,\nu}$.

For $f \in K[l]$ with $\nu(f) \geq \gamma$, we denote by $f_{\gamma,\nu}$ the class of f modulo the ideal $\{g \in K[l] \mid \nu(g) > \gamma\}$ of the ring $K[l]$.

Remark 1.6. .
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. .
1) We assume that $(N|M,\nu)$ is immediate. Let $l \in N$. Since l is pseudo-limit over M, there is $x \in M$ such that $\nu(l-0) < \nu(l-x)$. Hence $\nu(l) = \nu(x) \in \nu M$. Let $\gamma \in \nu M$ and $l \in N$ such that $\nu(l) = \gamma$. There exists $x \in M$ such that $\gamma = \nu(l-0) < \nu(l-x)$. Hence $l_{\gamma,\nu} = x_{\gamma,\nu} \in M_{\gamma,\nu}$.

Assume that $\nu N = \nu M$ and, for every $\gamma \in \nu M$, $N_{\gamma,\nu} = M_{\gamma,\nu}$. Let $l \in N$ and $x \in M$. Let y_1 in M such that $\nu(y_1) = \nu(l-x)$ and $(y_1)_{\nu(y_1),\nu} = l_{\nu(y_1),\nu}$. Therefore, $\nu(l-x-y_1) > \nu(y_1) = \nu(l-x)$. We let $y := x + y_1$. By Lemma 1.4, $(N|M,\nu)$ is immediate.
2) It remains to prove that if $\nu N = \nu K$ and $N_\nu = K_\nu$, then for every $\gamma \in \nu M$, $N_{\gamma,\nu} = M_{\gamma,\nu}$. Let $\gamma \in \nu K$ and $l \in N$ such that $\nu(l) = \gamma$. We take $x_1 \in K\backslash\{0\}$ such that $\nu(x_1) = \nu(l)$. Hence $\nu(l/x_1) = 0$. Since N is a K-module, l/x_1 belongs to N. Now, let $x_2 \in K$ such that $(l/x_1)_\nu = (x_2)_\nu$. Therefore, $\nu(l/x_1 - x_2) > 0$. Set $x := x_1x_2$. Then, $\nu(l-x) = \nu(x_1(l/x_1 - x_2)) = \nu(x_1) + \nu(l/x_1 - x_2) > \nu(x_1) = \nu(l)$. It follows that $l_{\gamma,\nu} = x_{\gamma,\nu}$. □

1.2. **Extensions generated by one element.** In this subsection, $K(\chi)|K$ is a simple extension of valued fields, where χ is algebraic or transcendental over K.

By definition, if $(K(\chi)|K,\nu)$ is immediate, then χ is pseudo-limit over K. We show that, with some additional conditions, a limit (resp. pseudo-limit) element can generate a dense (resp. immediate) extension. First, we characterize the immediate and dense extensions by means of the sets $\nu(\chi^n - K_{n-1}[\chi])$.

Proposition 1.7. *Let d, d' in $\mathbb{N} \cup \{\infty\}$ such that $0 \leq d < d' \leq [K[\chi]:K] - 1$, (that is, if χ is algebraic over K, then $d' < [K[\chi]:K]$). Recall that we defined $K_0[\chi] = K$ and $K_\infty[\chi] = K[\chi]$.*
a) $(K_{d'}[\chi]|K_d[\chi],\nu)$ is immediate if, and only if, for every $n \in \{d+1,\dots,d'\}$, $\nu(\chi^n - K_{n-1}[\chi])$ has no maximal element.
b) Assume that ν is a p-m valuation on $K(\chi)$ 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 $n \in \{d+1,\dots,d'\}$, $\nu(\chi^n - K_{n-1}[\chi]) = \nu K_d[\chi]$.

Proof. a) $\Rightarrow$. Assume that, for some $n \in \{d+1,\dots,d'\}$, $\nu(\chi^n - K_{n-1}[\chi])$ 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 1.6 1), the extension is not immediate. If $\nu(f) \in \nu K_d[\chi]$, 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 $\nu(f(\chi)) \notin \nu K_d[\chi]$, 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 $\nu(g-f) = \gamma$. By minimality of n, 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 $\nu(\chi^n - K_{n-1}[\chi])$.

b) If $(K_{d'}[\chi]|K_d[\chi],\nu)$ is dense, then it is immediate. Hence for every $n \in \{d+1,\dots,d'\}$ 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 $n \in \{d+2,\dots,d'\}$ 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 $n \in \{d+1,\dots,d'\}$ 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 $n \in \{d+1,\dots,d'\}$. We show that for every $\gamma \in K_d[\chi]$ there is $g \in K_d[\chi]$ such that $\nu(f-g) > \gamma$. Since $\nu(\chi^n - K_{n-1}[\chi]) = \nu K_d[\chi]$ which is a group, there is $g_{n-1} \in K_{n-1}[\chi]$ 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 $\nu(f-g_d) = \nu(f-g_{n-1}+\cdots+g_{d+1}-g_d) \geq \min(\nu(f-g_{n-1}),\dots,\nu(g_{d+1}-g_d)) > \gamma$. 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. □

Proposition 1.8. *Assume that ν is a p-m valuation on $K(\chi)$. Let A be the valuation ring of (K,ν) and $n \geq 2$, $n < [K(\chi):K]$. If $\nu(\chi^n - (K_{n-1}[\chi] \cap A[\chi])) = \nu(K_{n-1}[\chi] \cap A[\chi])$ and $\nu K[\chi] = \nu K_{n-1}[\chi]$, then $(K[\chi]|K_{n-1}[\chi],\nu)$ is dense. In particular, if $\nu(\chi - A) = \nu(A)$ and $\nu K[\chi] = \nu K$, then $(K[\chi]:K,\nu)$ is dense.*

Proof. Let (f_i) be a sequence of polynomials of $K_{n-1}[X]\cap A[X]$ such that the sequence $(\nu(\chi^n-f_i(\chi)))$ is increasing and cofinal in $\nu K_{n-1}[\chi]$. Let $f\in K[X]$. By multiplying all the coefficients of f by an element of K, we can assume that $f\in A[X]$. If $f\in K_{n-1}[X]$, then $f(\chi)$ it is limit over $K_{n-1}[\chi]$. Assume that $\deg(f)\geq n$, and for every i let $f(\chi)=g_i(\chi)\cdot(\chi^n-f_i(\chi))+h_i(\chi)$ be the euclidean division. Since $\chi^n-f_i(\chi)$ is a monic polynomial, when we do the euclidean division we see that the valuations of all the coefficients of g_i and of h_i belong to A. In particular, $\nu(g_i(\chi))\geq\min(n\nu(\chi),0)$ and $\nu(h_i(\chi))\geq\min(n\nu(\chi),0)$. Now, for i large enought we have $\nu(\chi^n-f_i(\chi))>-\min(n\nu(\chi),0)+\nu(f(\chi))$, hence $\nu(f(\chi))=\nu(h_i(\chi))<\nu(g_i(\chi)(\chi^n-f_i(\chi)))$. It follows that $\nu(f(\chi)-h_i(\chi))=\nu(g_i(\chi)(\chi^n-f_i(\chi)))\geq\nu(\chi^n-f_i(\chi))+\min(n\nu(\chi),0)$ is cofinal in $\nu K_{n-1}[\chi]$, and that $\nu(f(\chi)-K_{n-1}[\chi])=\nu K[\chi]$. So $f(\chi)$ is limit over (K,ν). Consequently, $(K[\chi]|K_{n-1}[\chi],\nu)$ is dense. □

Definition 1.9. A finite immediate extension $(L|K,\nu)$ of valued fields is *defectless* if the restriction of ν to K admits $[L:K]$ distinct extensions to L. In general, this number of extensions divides $[L:K]$.

Theorem 1.10. *Assume that ν is multiplicative on L and that $(L|K,\nu)$ is a finite algebraic immediate defectless and Galois extension of valued fields, such that ν is an archimedean valuation (i.e. νL embeds in $\mathbb{R}$). Then $(L|K,\nu)$ is dense.*

To prove this theorem, we need to sate more properties. 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 px 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 $f_{(p)}(X)=(1/p!)\cdot p!=1$.

Proposition 1.11. *Assume that χ is limit over (K,ν), and that ν is a p-m valuation on $K(\chi)$. Then $(K(\chi)|K,\nu)$ is dense.*

Proof. Let $f\in K[X]$. If $f(\chi)\in K$, then it is limit over (K,ν). Otherwise, for every $x\in K$, $f(\chi)\neq f(x)$. Let n be the degree of f. For $x\in K$, we let $f(x)=(x-\chi)^n f_{(n)}(\chi)+\cdots+(x-\chi)f_{(1)}(\chi)+f(\chi)$ be the Taylor expansion of $f(x)$. Since $f(\chi)\neq f(x)$, one of the $f_{(j)}$, $1\leq j\leq n$, is different from 0. Then $\nu(f(x)-f(\chi))\geq\min\limits_{1\leq j\leq n}\nu((x-\chi)^j f_{(j)}(\chi))=\min\limits_{1\leq j\leq n}j\nu(x-\chi)+\nu(f_{(j)}(\chi))$. Since the set of $\nu(x-\chi)$'s is cofinal in νK and $f_{(1)}(\chi),\ldots,f_{(n)}(\chi)$ are fixed elements, this proves that the set of $\nu(f(x)-f(\chi))$'s is cofinal in νK. Hence $f(\chi)$ is limit over (K,ν). Consequently $(K[\chi]|K,\nu)$ is dense. Now, assume that χ is transcendental over K. Let f, g in $K[X]$ and x, y in K such that $\nu(f(\chi)-f(x))>\nu(f(\chi))=\nu(f(x))$ and $\nu(g(\chi)-g(y))>\nu(g(\chi))=\nu(g(y))$. Then

$$\nu\left(\frac{f(\chi)}{g(\chi)}-\frac{f(x)}{g(y)}\right)=\nu(f(\chi)g(y)-g(\chi)f(x)-\nu(g(\chi))-\nu(g(y))=$$
$$=\nu(f(\chi)(g(y)-g(\chi))+g(\chi)(f(\chi)-f(x)))-2\nu(g(\chi)).$$

Now, the sets of $\nu(g(y)-g(\chi))$'s and $\nu(f(\chi)-f(x))$'s are cofinal in νK. Hence the set of $\nu\left(\dfrac{f(\chi)}{g(\chi)}\right)$'s is cofinal in νK. It follows that $(K(\chi)|K,\nu)$ is dense. □

The following proposition generalizes a result of [D 82] (p. 103) to the case when the residue field need not have characteristic 0. The proof is based on the same idea. We give it for completeness. We get a sufficient condition for being dense, by proving that some initial segment is closed under addition.

Proposition 1.12. *(Delon) Let A be the valuation ring of K. Assume that χ is separable algebraic and pseudo-limit over K, and let f be the irreducible polynomial of χ over K. Assume in addition that ν is a p-m valuation on $K(\chi)$, that $f(X)\in A[X]$ and $\nu(f'(\chi))=0$. We have the following.*
1) The initial segment of νK generated by $\nu f(K)$ is closed under addition.
2) If (K,ν) is archimedean, then $(K(\chi)|K,\nu)$ is dense.

Proof. We keep the notations of the proof of Proposition 1.11.

1) Since $f(X)$ is a monic polynomial of $A[X]$, by properties of extensions of valued fields we have $\nu(x)\geq 0$. We show that for every $x\in K$, such that $\nu(x-\chi)>0$, we have $\nu(f'(x))=0$ (note that $f'=f_{(1)}$). Since $f(X)\in A[X]$, for every $i\geq 0$ we have $f_{(i)}(X)\in A[X]$. Hence $\nu(f_{(i)}(\chi))\geq 0$. Set $h(X)=f'(X)$, and let $h(x)-h(\chi)=(x-\chi)h_{(1)}(\chi)+\cdots+(x-\chi)^d h_{(d)}(\chi)$ be the Taylor expansion. Then

$$\nu(f(x)-f(\chi))\geq\min_{1\leq i\leq d}(i\nu(x-\chi)+\nu(h_{(i)}(\chi)))\geq\nu(x-\chi)>0.$$

Hence $\nu(h(x))=\nu(h(\chi))=0$. Now, let $x_0\in A$, such that $\nu(\chi-x_0)>0$. First we show that $\nu(f(x_0))=\nu(\chi-x_0)$. Indeed, we can write $f(x_0)$ as $f(x_0)=(x_0-\chi)f_{(1)}(x_0)+(x_0-\chi)^2 g(x_0,\chi)$, where the coefficients of g belong to A (since the coefficients of f belong to A). Now, $\nu(\chi)\geq 0$ and $\nu(\chi-x_0)>0$. Hence $\nu(x_0)\geq 0$. Therefore, $\nu(g(x_0,\chi))\geq 0$. Consequently, $\nu((x_0-\chi)f_{(1)}(x_0))=\nu(x_0-\chi)<2\nu(x_0-\chi)\leq$

$\nu((x_0-\chi)^2 g(x_0,\chi))$. So $\nu(f(x_0)) = \nu(x_0-\chi)$.

Let $x_1 \in K$ be such that

$$\nu\left(x_1 - x_0 + \frac{f(x_0)}{f_{(1)}(x_0)}\right) > 2\nu(x_0-\chi). \text{ Since } \nu\left(\frac{f(x_0)}{f_{(1)}(x_0)}\right) = \nu(f(x_0)) = \nu(x_0-\chi),$$

this implies that $\nu(x_1-x_0) = \nu(x_0-\chi)$. Using Taylor expansion, $f(x_1)$ can be written as $f(x_1) = f(x_0)+(x_1-x_0)f_{(1)}(x_0)+(x_1-x_0)^2\lambda$, with $\nu(\lambda) \geq 0$. Hence $\nu(f(x_1)) \geq \min(\nu(f(x_0)+(x_1-x_0)f_{(1)}(x_0)), \nu((x_1-x_0)^2\lambda)) \geq 2\nu(x_0-l)$. Since the set $\nu(f(K))$ is an initial segment of νK, it follows that $\nu(f(K))$ is closed under addition.

2) Let x_1 be as in 1). Since $\nu(x_1-x_0) = \nu(x_0-\chi)$, we have $\nu(x_1-\chi) \geq \nu(x_0-\chi)$. Hence $\nu(x_1-\chi) = \nu(f(x_1))$. It follows that $\nu(\chi - K)$ contains a nontrivial initial segment which is closed under addition. Assume that νK is archimedean. Then $\nu(\chi-K) = \nu K$, hence χ is limit over K. Now, it follows from Proposition 1.11 that $(K(\chi)|K,\nu)$ is dense. □

Now, we give sufficient conditions for hypothesis of Proposition 1.12 being satisfied.

Proposition 1.13. *Assume that ν is multiplicative on L and that $(L|K,\nu)$ is a finite immediate defectless Galois extension of valued fields. Then, there is $\chi \in L$ with irreducible polynomial f in $A[X]$ such that $\nu(f'(\chi)) = 0$ and $L = K[\chi]$ (where A is the valuation ring of (K,ν)).*

Before proving this proposition, we recall some definitions of [R 68] and [E 72]. Let L be a field together with valuations $\nu_1,\dots,\nu_n$, and for $i \in \{1,\dots,n\}$ let A_i be the valuation rings of (L,ν_i) and $U_i = \nu_i^{-1}(\{0\})$ be the group of units of A_i. For $i \neq j$ in $\{1,\dots,n\}$, the valuations ν_i and ν_j are said to be *incomparable* if nor $A_i \subseteq A_j$ nor $A_j \subseteq A_i$. They are *independent* if $A_i \cdot A_j = L$. Note that if these valuations are archimedean, then they are independent if, and if, they are incomparable, which in turn is equivalent to: $\nu_i \neq \nu_j$ (see [E 72, p. 82]). Now, we assume that $\nu_1,\dots,\nu_n$ are pairwise incomparable. Then one can prove that, for $i \neq j$ in $\{1,\dots,n\}$, $\nu_j(U_i)$ is a nontrivial convex subgroup of $\nu_j L$. A n-tuple $(\gamma_1,\dots,\gamma_n) \in \nu_1 L \times \cdots \times \nu_n L$ is *compatible* if there exists $l \in L$ such that $\nu_1(l) = \gamma_1, \dots, \nu_n(l) = \gamma_n$ (Théorème 1 p. 135 in [R 68]). One can prove that if, for every $i \in \{1,\dots,n\}$, $\gamma_i \in \bigcap_{j\neq i} \nu_i(U_j)$, then $(\gamma_1,\dots,\gamma_n)$ is compatible. Since $\bigcap_{j\neq i} \nu_i(U_j)$ is an intersection of finitely many non trivial convex subgroups, it is non trivial. Now, if the $\nu_i L$ are embedded in the same ordered group, then there exists a compatible n-tuple $(\gamma_1,\dots,\gamma_n)$ such that $0 < \gamma_1 < \cdots < \gamma_n$. By the approximation Theorem (Théorème 3, p. 136, in [R 68]), if $(\gamma_1,\gamma_2,\dots,\gamma_n)$ is compatible and $l_1, l_2, \dots, l_n$ are elements of L, such that $\forall i,\ 1 \leq i \leq n,\ \nu_i(l_i) < \gamma_i \Rightarrow \gamma_i - \nu_i(l_i) \in \bigcap_{j\neq i} \nu_i(U_j)$, then there exists $l \in L$ such that $\forall i,\ 1 \leq i \leq n,\ \nu_i(l-l_i) = \gamma_i$.

Proof of Proposition 1.13. Let $\nu_1 = \nu, \dots, \nu_n$ be the extensions to L of the restriction of ν to K, and $(\gamma_1,\dots,\gamma_n) \in \nu_1 L \times \cdots \times \nu_n L$ be a compatible n-tuple such that $0 < \gamma_1 < \cdots < \gamma_n$. Let $x_1,\dots,x_n$ in K such that $x_i \neq 0 \Rightarrow \nu(x_i) = 0$, $(x_i)_\nu \neq (x_1)_\nu$ (for $i > 1$). If K_ν is infinite, then we can assume that the $(x_i)_\nu$'s are pairwise distinct. Otherwise, if $(x_i)_\nu = (x_j)_\nu$, then we assume $x_i = x_j$. By the approximation Theorem, there exists $l \in L$ such that, for every $i \in \{1,\dots,n\}$, $\nu_i(l-x_i) = \gamma_i$. Denote by f its irreducible polynomial over K. Let $\sigma_1,\dots,\sigma_n$ be the elements of the Galois group of $L|K$, and $l_i = \sigma_i(l)$. We know that we can assume that for $i \in \{1,\dots,n\}$ we have: $\nu_i = \nu_1 \circ \sigma_i$ ([R 68, p. 166]). By hypothesis, $\nu_1(l-x_1) > 0$ and, for $i \in \{2,\dots,n\}$, $\nu_1(l_i - l) = \nu_1(l_i - x_i + x_i - l)$. Since $l_{\nu_1} = (x_1)_{\nu_1} \neq (x_i)_{\nu_1}$, it follows: $\nu_1(x_i - l) = 0$. Now, $\nu_1(l_i - x_i) = \nu_1(\sigma_i(l) - \sigma_i(x_i))$ (because $x_i \in K$, hence $x_i = \sigma_i(x_i)$) and $\nu_1(l_i - x_i) = \nu_i(l-x_i) > 0$. Therefore $\nu_1(l_i - l) = 0$ and $(l_i)_{\nu_1} \neq l_{\nu_1}$.

Since the roots of f belong to the set $\{l_1,\dots,l_n\} \subseteq A_1$ (indeed, $\nu_1(l_i - x_j) = 0$ and $\nu_1(x_j) \geq 0 \Rightarrow \nu_1(l_i) \geq 0$), it follows that $f \in A_1[X]$. Consequently, $f \in A[X]$ (because $f \in K[X]$).

Let $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$ and $f_\nu(X) = X^n + (a_{n-1})_\nu X^{n-1} + \cdots + (a_1)_\nu X + (a_0)_\nu$. The element l_{ν_1} is a root of f_ν and $f'_\nu = (f_\nu)'$. Now, $f(X) = \prod_{i=1}^n (X-l_i)$ hence $f'(X) = \sum_{i_0=1}^n \prod_{i\neq i_0}(X-l_i)$.
We have $f'(X) = (X-l_2)(X-l_3)\cdots(X-l_n) + \sum_{i_0=2}^n \prod_{i\neq i_0}(X-l_i)$,
$(f'_\nu)(X) = (X-(l_2)_\nu)(X-(l_3)_\nu)\cdots(X-(l_n)_\nu) + \sum_{i_0=2}^n \prod_{i\neq i_0}(X-(l_i)_\nu)$
$(f'_\nu)((l_1)_\nu) = ((l_1)_\nu - (l_2)_\nu)((l_1)_\nu - (l_3)_\nu)\cdots((l_1)_\nu - (l_n)_\nu) + 0$.
Hence $(f'_\nu)((l_1)_\nu) \neq 0$ because we proved: $\forall i, 2 \leq i \leq n, (l_i)_\nu \neq (l_1)_\nu$. So, $(l_1)_\nu$ is a simple root of f_ν and $\nu(f'(l_1)) = 0$.

We show that $\nu_1, \nu_2, \dots, \nu_n$ are pairwise distinct on $K(l)$. Let $1 \leq i < j \leq n$.

If $x_i \neq x_j$, then by hypothesis $(x_i)_\nu \neq (x_j)_\nu$, and $l_{\nu_i} = (x_i)_\nu \neq (x_j)_\nu = l_{\nu_j}$. Consequently $\nu_i \neq \nu_j$ on $K(l)$.

If $x_i = x_j$, $\nu_i(l-x_i) = \gamma_i \neq \gamma_j = \nu_j(l-x_j)$. Therefore $\nu_i \neq \nu_j$ on $K(l)$.

This proves that ν admits n distinct extensions to $K(l)$, hence $[K(l):K] \geq n$. Since $K(l) \subseteq L$, it follows that $[K(l):K] = n = [L|K]$. Therefore: $K(l) = L$. We let $\chi = l$. □

Proof of Theorem 1.10. Follows from Propositions 1.12 and 1.13. □

Remark 1.14. If $L|K$ is not algebraic, then the extension $(L|K,\nu)$ need not be dense, even if it is archimedean and separable. For example, let k be the field $\mathbb{Q}$ or $\mathbb{F}_p$ with p prime. Let K be the field of generalized polynomials $k(\mathbb{Q}) := \{f = \sum_{i=1}^{n} x_i X^{\gamma_i} \mid n \in \mathbb{N}^*,\ x_1,\dots,x_n \text{ in } k,\ \gamma_1,\dots,\gamma_n \text{ in } \mathbb{Q}\}$, and for $f \in K$ let $\nu(f)$ be the minimum of the set of γ_i's such that $x_i \neq 0$. Denote by

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

the field of generalized formal power series with coefficients in k and exponents in $\mathbb{Q}$. If $\gamma \notin \Lambda$, then we set $x_i = 0$. For $f \in k((\mathbb{Q}))$, the set $\{\gamma \in \Gamma \mid x_\gamma \neq 0\}$ is called the *support* of f. It follows that the support of f is well-ordered. We let $\nu(f)$ be the minimum of the support of f if $f \neq 0$, and $\nu(0) = \infty$. By properties of valued fields, $k((\mathbb{Q}))$ is a valued field such that the extension $(k((\mathbb{Q}))|K,\nu)$ is immediate. Now, let $l = \sum_{i=1}^{\infty} X^{1-\frac{1}{i}} \in k((\mathbb{Q}))$. Then for every positive integer n, $\nu(l - \sum_{i=1}^{n} X^{1-\frac{1}{i}}) = 1 - \frac{1}{n+1}$, and this sequence is cofinal in $\nu(l-K)$, but not in $\mathbb{Q}$. Therefore, $\nu(l-K) = \{\gamma \in \mathbb{Q} \mid \gamma < 1\}$ is bounded. So $(K(l)|K,\nu)$ is not dense.

We saw in Proposition 1.11 that if χ is limit over (K,ν) and ν is a p-m valuation on $K(\chi)$, then the extension $(K(\chi)|K,\nu)$ is dense. We will show in the following subsection that if χ is pseudo-limit on (K,ν), then the extension $(K(\chi)|K,\nu)$ is not necessarily immediate. Now, with additional conditions, if l is pseudo-limit over (K,ν), then the extension $(K(l)|K,\nu)$ is immediate.

1.3. **Pseudo-Cauchy sequences.** We assume that χ is pseudo-limit over (K,ν), and we let (x_i) be a sequence of elements of K such that the sequence $(\nu(\chi - x_i))$ is increasing and cofinal in $\nu(\chi - K)$. We say that (x_i) is a *pseudo-Cauchy sequence* which *pseudo-converges* to χ, and that χ is a *pseudo-limit* of (x_i). Pseudo-Cauchy sequences were introduced by Kaplansky in [K 42]. The reader can find definitions and properties online in the Book of F-V Kuhlmann [FVK]. We recall below some properties of pseudo-Cauchy sequences, that we will also need in Subsection 4.2.

Definitions 1.15. A *pseudo-Cauchy sequence* of the valued field (K,ν) is a sequence (x_i) of elements of K (where i runs over a well-ordered set) such that for every $i < j < k$, $\nu(x_i - x_j) < \nu(x_j - x_k)$.
An element x of K is a *pseudo-limit* of (x_i) if for every i we have: $\nu(x - x_i) = \nu(x_i - x_{i+1})$.

Remark 1.16. Let x be a pseudo-limit of a pseudo-Cauchy sequence (x_i), and x' be another element. Then x' is a pseudo-limit of (x_i) if, and only if, for every i, $\nu(x - x') > \nu(x - x_i)$. Now, if the sequence $(\nu(x - x_i))$ is cofinal in νK, then there is no other pseudo-limit. So, we can say that x is the limit of the pseudo-Cauchy sequence (x_i).

Proposition 1.17. *Let $(L|K,\nu)$ be an extension of valued fields.*
1) The extension $(L|K,\nu)$ is immediate if, and only if, every element of L is pseudo-limit of a pseudo-Cauchy sequence of K which has no pseudo-limit in K.
2) The extension $(L|K,\nu)$ is dense if, and only if, it is immediate and every element of $L\backslash K$ is limit of a pseudo-Cauchy sequence of K without pseudo-limit in K.

Proposition 1.18. *Let (x_i) be a pseudo-Cauchy sequence of a valued field (K,ν). For every polynomial $f(X) \in K[X]$ (the ring of formal polynomials), the sequence $(\nu(f(x_i)))$ is either increasing or increasing then constant. In this last case, if x is a pseudo-limit of (x_i), then $(\nu(f(x_i)))$ is eventually equal to $\nu(f(x))$. Furthermore, there is a unique monic polynomial f of minimal degree such that the sequence $(\nu(f(x_i)))$ is not eventually constant, and f is irreducible.*

Definitions 1.19. Let (x_i) be a pseudo-Cauchy sequence of the valued field (K,ν).
1) If for every $f \in K[X]$ the sequence $(\nu(f(x_i)))$ is eventually constant, then (x_i) is said to be of *transcendental type*.
2) Otherwise, (x_i) is said to be of *algebraic type*. The monic polynomial f of degree minimal such that the sequence $(\nu(f(x_i)))$ is not eventually constant is called the *irreducible polynomial* of the sequence (x_i) over (K,ν).

Remark 1.20. Assume that χ is algebraic over K and is pseudo-limit of a pseudo-Cauchy sequence of (K,ν) without pseudo-limit in K. Then (x_i) is of algebraic type, and its irreducible polynomial has degree at most equal to the degree of the irreducible polynomial of χ.

One can define the extension of a valuation, to an immediate extension, by means of pseudo-Cauchy sequences.

Proposition 1.21. *Let (x_i) be a pseudo-Cauchy sequence of a valued field (K,ν), without pseudo-limit in K.*
1) Assume that (x_i) is of transcendental type and that χ is transcendental over K. There is a unique

extension of ν to $K(\chi)$ such that $(K(\chi)|K,\nu)$ is immediate and χ is a pseudo-limit of (x_i). We know that for every $f(X)\in K[X]$, the sequence $(\nu(f(x_i)))$ is eventually equal to some γ. We set $\nu(f(\chi))=\gamma$.
2) Assume that (x_i) is of algebraic type and that χ is a root of the irreducible polynomial of (x_i). Let d be the degree of this irreducible polynomial. Then $K(\chi)=K_{d-1}[\chi]$ and we can define $\nu(f(\chi))$, for every $f(X)\in K_{d-1}[X]$, in the same way as in 1).

Lemma 1.22. *Let ν be a p-m valuation of $K(\chi)|K$. Assume that χ is pseudo-limit of a pseudo-Cauchy sequence (x_i) of K (without pseudo-limit in K). Let $f(X)\in K[X]$, and assume that the sequence $(\nu(f(x_i)))$ is eventually equal to some γ. Then $\gamma=\nu(f(\chi))$, and $f(\chi)_{\gamma,\nu}\in K_{\gamma,\nu}$.*

Proof. Let $f(X)-f(\chi)=(X-\chi)^n f_{(n)}(\chi)+\cdots+(X-\chi)f_{(1)}(\chi)$ be the Taylor expansion of $f(X)$, as in Proposition 1.11. For every x_i we have $\nu(f(x_i)-f(\chi))=\nu((x_i-\chi)^n f_{(n)}(\chi)+\cdots+(x_i-\chi)f_{(1)}(\chi))\geq \min_{1\leq j\leq n}\nu((x_i-\chi)^j f_{(j)}(\chi))=\min_{1\leq j\leq n}(j\nu(x_i-\chi)+\nu(f_{(j)}(\chi))$. Now, since the sequence $(\nu(x_i-\chi))$ is increasing, the $j\nu(x_i-\chi)+\nu(f_{(j)}(\chi)$'s are eventually pairwise distinct. Hence the minimum is carried by only one index, say j_0. Consequently, $\nu(f(x_i)-f(\chi))=\nu((x_i-\chi)^n f_{(n)}(\chi)+\cdots+(x_i-\chi)f_{(1)}(\chi))=j_0\nu(x_i-\chi)+\nu(f_{(j_0)}(\chi))$ is increasing. Since $\nu(f(x_i))=\gamma$ and $\nu(f(\chi))$ are constant, it follows that $\nu(f(\chi))=\nu(f(x_i))<\nu(f(\chi)-f(x_i))$. Therefore, $f(\chi)_{\nu(f(\chi)),\nu}=f(x_i)_{\nu(f(\chi)),\nu}\in K_{\nu(f(\chi)),\nu}$. □

Definitions 1.23. A valued field (K,ν) is said to be *maximal* if (K,ν) admits no immediate extension. It is said to be *algebraically maximal* if (K,ν) admits no immediate algebraic extension.

Proposition 1.24. *Let (K,ν) be a valued field.*
The field (K,ν) is maximal if, and only if, every pseudo-Cauchy sequence of (K,ν) has a pseudo-limit in (K,ν).
The field (K,ν) is algebraically maximal if, and only if, every pseudo-Cauchy sequence of (K,ν) of algebraic type has a pseudo-limit in (K,ν).

Proposition 1.25. *Let ν be a p-m valuation of valued field on $K(\chi)$. Assume that χ is pseudo-limit of a pseudo-Cauchy sequence (x_i) of K (without pseudo-limit in K) and that (x_i) is of transcendental type over (K,ν). Then the extension $(K(\chi)|K,\nu)$ is immediate.*

Proof. By Lemma 1.22, for every $f(X)\in K[X]$ we have $f(\chi)\in\nu K$ and $f(\chi)_{\nu(f(\chi)),\nu}\in K_{\nu(f(\chi)),\nu}$. By Remark 1.6, the extension $(K(\chi)|K,\nu)$ is immediate. □

Corollary 1.26. *Let ν be p-m valuation of valued fields on $K(\chi)$. Assume that (K,ν) is algebraically maximal and that χ is pseudo-limit over (K,ν). Then $(K[\chi]|K,\nu)$ is immediate.*

The following example shows that we cannot delete the condition (x_i) of transcendental type in Proposition 1.25.

Example 1.27. Assume hat $(L|K,\nu)$ is an extension of valued fields such that $\nu L>\nu K$, and that L contains an element l' which is pseudo-limit and algebraic over (K,ν). We let $f(X)$ be its irreducible polynomial, d be the degree of $f(X)$, (x_i) be a pseudo-Cauchy sequence of (K,ν) without pseudo-limit in K and which pseudo-converges to l'. We assume that f is also the irreducible polynomial of the sequence (x_i). For every monic polynomial $g(X)$ of degree $n<d$, we know that the sequence $(\nu(g(x_i)))$ is eventually constant. Now, let $g(x_i)-g(l')=(x_i-l')^{n-1}g_{(1)}(l')+\cdots+(x_i-l)g_{(n)}(l')$ be its Taylor expansion. Since l' is pseudo-limit, the set of $\nu(x_i-l')$'s is infinite. Hence for $\nu(x_i-l)$ large enought, the minimum of the $\nu((x_i-l')^j g_{(j)}(l')=j\nu(x_i-l')+\nu(g_{(j)}(l'))$ is carried by only one j, and this index is fixed, say j_0. Then, $\nu(g(x_i)-g(l'))=j_0\nu(x_i-l')+\nu(g_{(j_0)}(l'))$ is increasing. By hypothesis, the sequence $(\nu(g(x_i)))$ is eventually constant. Hence $(\nu(g(x_i)))$ is eventually equal to $\nu(g(l'))$, and $\nu(g(l'))<\nu(g(l')-g(x_i))$, with $g(x_i)\in K$. Hence $g(l')$ is not the maximum of $\nu((l')^n-K_{n-1}[l'])$. By Proposition 1.7 the extension $(K_{d-1}[l']|K,\nu)$ is immediate. Now, let l'' in L such that $\nu(l'')>\nu K$, and $l=l'+l''$. Let g be a monic polynomial of degree $n<d$, and $g(l)-g(l')=(l-l')^{n-1}g_{(1)}(l')+\cdots+(l-l')g_{(n)}(l')$ be its Taylor expansion. Then, $g(l)-g(l')=(l'')^{n-1}g_{(1)}(l')+\cdots+(l'')g_{(n)}(l')$ has valuation greater than νK. Consequently, $\nu(g(l))=\nu(g(l'))$. This proves that the extension $(K_{d-1}[l]|K,\nu)$ is immediate. Now, $f(l)=f(l)-f(l')=(l'')^{d-1}f_{(1)}(l')+\cdots+(l'')f_{(d)}(l')$ is greater than νK. It follows that $f(l)$ is the maximum of $\nu(l^d-K_{d-1}[l])$, and that the extension $(K_d[l]|K_{d-1}[l],\nu)$ is not immediate.

2. Separate extensions

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

2.1. **Basic properties.**

Definitions 2.1. (Baur, [B 82]) Let M be a K-submodule of L.
1) A sequence $(l_1,\ldots,l_n)$ of L is said to be *separate over M* (or ν-separate if necessary) if for every $x_1,\ldots,x_n$ in M, we have: $\nu(x_1l_1+\cdots+x_nl_n)=\min_{1\leq i\leq n}\nu(x_il_i)$. If $M=K$, then we say separate instead of separate over K.

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

Definition 2.2. Let M be a finitely generated K-submodule of L. If M admits a basis which is separate over K, then we say that M is *separate*.

Remark 2.3. ([B 81]) If the sequence $(l_1,\dots,l_n)$ of L is separate over K, then $l_1,\dots,l_n$ are linearly independent over K.

In the remainder of this subsection we will prove the following two theorems.

Theorem 2.4. *(Delon) Let N be a K-submodule of L. Then, $(N|K,\nu)$ is a separate extension if, and only if, for every finitely generated K-submodule M of N and $l\in N\backslash M$, the set $\nu(l-M)$ has a maximal element.*

This theorem has been stated in [D 88, p. 421], assuming that (K,ν) is henselian and $\mathrm{char}(K_\nu)=0$. So we give the proof for completeness.

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 1.6, $(L|K,\nu)$ is immediate if, and only if, $1=[L_\nu:K_\nu](\nu L:\nu K)$. The following theorem proves that $(L|K,\nu)$ being separate can be seen as the opposite case.

Theorem 2.5. *Assume that $L|K$ is a finite algebraic extension of fields and that ν is multiplicative on L. Then $(L|K,\nu)$ is separate if, and only if, $[L:K]=[L_\nu:K_\nu](\nu L:\nu K)$.*

Definition 2.6. Let $(L|K,\nu)$ be a finite extension of valued fields (where ν is multiplicative). Then $(L|K,\nu)$ is *defectless* if $\dfrac{[L:K]}{[L_\nu:K_\nu](\nu L:\nu K)}$ is equal to the number of extensions of $\nu_{|K}$ to L.

We recall that (K,ν) is *henselian* if ν admits a unique extension to every algebraic extension of K.

Corollary 2.7. *If (K,ν) is henselian, then every defectless finite algebraic extension of (K,ν) is separate.*

We start with properties a separate sequences.

Lemma 2.8. *(*[B 82] *p. 676) Let $(l_1,\dots,l_n)$ be a separate sequence of elements of L, y in L and $k_1,\dots,k_n$ in K. The following holds.*
Every subsequence of $(l_1,\dots,l_n)$ is separate.
The sequence $(k_1l_1,\dots,k_nl_n)$ is separate.
If ν is multiplicative on L then the sequence $(yl_1,\dots,yl_n)$ is separate.

Lemma 2.9. *(*[B 81], [B 82] *(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 separate 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 $\nu(l_1)=\cdots=\nu(l_n)=g$, then $(l_1,\dots,l_n)$ is separate if, and only if, for every $x_1,\dots,x_n$ in $\{x\in K\mid\nu(x)=0\}\cup\{0\}$, either $\nu(x_1l_1+\cdots+x_nl_n)=g$ or $x_1=\cdots=x_n=0$.*

Proposition 2.10. *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 separate.
For every i in $\{1,\dots,p\}$, $l_{i1},l_{i2},\dots,l_{in_i}$ is separate.
If ν is mutiplicative 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 separate. Then by Lemma 2.8, for $1\leq i\leq p$, the sequence $l_{i1},l_{i2},\dots,l_{in_i}$ is separate.

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 $y_i=x_{i1}l_{i1}+\cdots+x_{in_i}l_{in_i}$. Since $l_{i1},\dots,l_{in_i}$ is separate, 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 $\nu(y_1+\cdots+y_p)=\min\{\nu(y_i)\mid 1\leq i\leq p\}$. 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 separate.

If ν is multiplicative on L, then

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

By Lemma 2.9, 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. □

Lemma 2.11. *(*[D 88] *Lemme 5) Let $M\subseteq N$ be two K-submodules of L such that M is finitely generated and N admits a separate basis. Then M admits a separate basis (in other words, it is separate).*

The following theorem is an immediate consequence of Lemma 2.11.

Theorem 2.12. *Assume that L is a finite algebraic extension of K. Then $(L|K,\nu)$ is separate if, and only if, the K-module L admits a separate basis.*

Remark. Theorem 2.12 is not true if $(L|K)$ is not a finite algebraic extension, (see [D 88] p. 426). However, we will see later that it remains true if L is generated by one transcendental element and ν is multiplicative.

Proof of Theorem 2.5. Set $r := [L_\nu : K_\nu]$ et $q := (\nu L : \nu K)$. By properties of valuations, we have that $rq \leq [L:K]$.

Assume that $[L:K] = rq$. Let $x_1, \dots, x_r, y_1, \dots, y_q$ be elements of L such that $\nu(x_1) = \cdots = \nu(x_r) = 0$, $(x_1)_\nu, \dots, (x_p)_\nu$ are linearly independent over K_ν, and $\nu(y_1), \dots, \nu(y_q)$ are pairwise non-congruent modulo νK. By Proposition 2.10, the sequence $\{x_i y_j \mid 1 \leq i \leq r,\ 1 \leq j \leq q\}$ is separate. It follows that they are linearly independent over K. Since its cardinal is rq, it is a basis of L over K. Now, by Theorem 2.12, $(L|K,\nu)$ is separate.

Assume that $(L|K,\nu)$ is separate, so L admits a separate basis $\mathcal{B}$. We define an equivalence relation over $\mathcal{B}$ by setting $y_1 \sim y_2 \Leftrightarrow \nu(y_1) \equiv \nu(y_2)$ modulo νK. By Lemma 2.8, we can assume that all the elements of every class of $\mathcal{B}$ modulo $\sim$ have the same valuation. Let $\mathcal{C} = \{l_1, \dots, l_p\}$ be a class of $\mathcal{B}$ modulo $\sim$. By Lemma 2.8 $1, (l_2/l_1), \dots, (l_p/l_1)$ is a separate sequence of elements of L with valuation 0. We deduce from Lemma 2.9 that $p \leq r$. Now, if $p < r$, then there exists l'_{p+1} in L such that $1_\nu, (l_2/l_1^{-1})_\nu, \dots, (l_p/l_1^{-1})_\nu, (l'_{p+1})_\nu$ are linearly independent over K_ν. Then $1, (l_2/l_1^{-1}), \dots, (l_p/l_1^{-1}), l'_{p+1}$ is a separate sequence, hence so is $l_1, l_2, \dots, l_p, l_{p+1}$, where $l_{p+1} = l'_{p+1} l_1$. By Proposition 2.10, $\mathcal{B} \cup \{l_{p+1}\}$ is a separate sequence, hence $\mathcal{B}$ is not a maximal subset of linearly independent elements, so it is not a basis: a contradiction. It follows that $p = r$. Now, there are at most $(\nu L : \nu K) = q$ classes modulo $\sim$. Since $\mathcal{B}$ is a separate basis, for every $l \in L$ there exists $x \in K$ and $b \in \mathcal{B}$ such that $\nu(l) = \nu(xb)$. It follows that there are exactly q classes modulo $\sim$. Hence $\mathcal{B}$ is the disjoint union of q classes, which one contains r elements. It follows: $[L:K] = \mathrm{card}(\mathcal{B}) = rq$. □

Lemma 2.13. *Assume that $(L|K,\nu)$ is separate. Let M be a finite K-submodule of L and $l \in L \backslash M$. Then every separate basis of M extends to a separate basis of the K-submodule generated by M and l.*

Proof. Consider a separate basis $\mathcal{B}$ of M and a separate basis $\mathcal{B}'$ of $N := M \oplus K{\cdot}l$. Since $\nu(M) \subseteq \nu(N)$, the number of classes of $\mathcal{B}'$ modulo the relation $\sim$ defined in the proof of Theorem 2.5 is greater or equal to the number of classes of $\mathcal{B}$ modulo $\sim$. If it is greater, then we add to $\mathcal{B}$ and element of the additional class, and we get the separate basis of N. Otherwise, one of the classes of $\mathcal{B}'$ has more elements than the corresponding class of $\mathcal{B}$. Say $l'_1, \dots, l'_{k+1}$ and $l_1, \dots, l_k$. By Lemma 2.8, we can assume that all the element of these classes have the same valuation γ. Assume that there exists a family $(x_{ij})_{1 \leq i \leq k+1,\ 1 \leq j \leq k}$ in $\{x \in K \mid \nu(x) = 0\} \cup \{0\}$ such that for $i \in \{1, \dots, k+1\}$: $(*i)$ $\nu(l'_i - (x_{i1}l_1 + \cdots + x_{ik}l_k)) > \gamma$. We show that we get a contradiction. Without loss of generality we can assume that $x_{11} \neq 0$. Then: $\nu(l_1 + x_{12}x_{11}^{-1}l_2 + \cdots + x_{1k}x_{11}^{-1}l_k - x_{11}^{-1}l'_1) > \gamma$. For $i \geq 2$ we put $x_{11}^{-1}l'_1 - (x_{12}x_{11}^{-1}l_2 + \cdots + x_{1k}x_{11}^{-1}l_k)$ in place of l_1. So we get an inequality $\nu(l'_i + x_{11}^{-1}l'_1 - (x_{12}x_{11}^{-1} + x_{i2})l_2 - \cdots - (x_{1k}x_{11}^{-1} + x_{ik})l_k) > \gamma$. We can eliminate $(x_{1j}x_{11}^{-1} + x_{ij})l_j$ if $\nu(x_{1j}x_{11}^{-1} + x_{ij}) > 0$, so we can assume that all the coefficients belong to $\{x \in K \mid \nu(x) = 0\} \cup \{0\}$. We proceed in the same way with $l_2, \dots, l_k$. Since there are $k+1$ inequalities $(*i)$, finally we get some $\nu(y_1 l'_1 + \cdots + y_{k+1}l'_{k+1}) > \gamma = \min \nu(y_i l'_i)$: a contradiction. Hence there is some l'_i, say l'_{k+1} such that for every x_j in $\{x \in K \mid \nu(x) = 0\} \cup \{0\}$ $(1 \leq j \leq k)$: $\nu(l'_{k+1} + x_1 l_1 + \cdots + k l_k) = \gamma$. It follow that the sequence $l_1, \dots, l_k, l'_{k+1}$ is separate. By Proposition 2.10, the sequence $\mathcal{B} \cup \{l'_{k+1}\}$ is separate. □

Proof of Theorem 2.4. Assume that $(N|K,\nu)$ is separate. Let M be a finitely generated K-submodule of N, and $l \in N \backslash M$. By Lemma 2.13, there exist a basis $l_1, \dots, l_k$ of $M \oplus K{\cdot}l$ such that $l_1, \dots, l_{k-1}$ belong to M. Now, l can be written as $l = x_1 l_1 + \cdots + x_k l_k$, with $x_1, \dots, x_k$ in K. Since $l \notin M$, we have $x_k \neq 0$. Hence for every y in M there exist $y_1, \dots, y_{k-1}$ in K such that $l - y = y_1 l_1 + \cdots + y_{-1} l_{k-1} + x_k l_k$, hence $\nu(l-y) \leq \nu(x_k l_k)$. So $\nu(x_k l_k) = \max \nu(l - M)$. Conversely, we prove by induction on the dimension of the submodule M that it contains a separate basis. If $\dim(M) = 1$, then the result is trivial. Assume that M admits a separate basis $l_1, \dots, l_k$ and let $l \notin M$. Let $y \in M$ such that $\nu(l-y) = \max \nu(l - M)$, and set $l_{k+1} = l - y$. We show that the family $l_1, \dots, l_k, l_{k+1}$ is separate. Let $x_1, \dots, x_k, x_{k+1}$ in K, with $x_{k+1} \neq 0$, and $\gamma = \min(\nu(x_1 l_1), \dots, \nu(x_k l_k))$. If $\gamma < \nu(x_{k+1} l_{k+1})$, then $\nu(x_1 l_1 + \cdots + x_k l_k + x_{k+1} l_{k+1}) = \gamma = \min(\nu(x_1 l_1), \dots, \nu(x_k l_k), \nu(x_{k+1} l_{k+1}))$. If $\gamma > \nu(x_{k+1} l_{k+1})$, then $\nu(x_1 l_1 + \cdots + x_k l_k + x_{k+1} l_{k+1}) = \nu(x_{k+1} l_{k+1}) = \min(\nu(x_1 l_1), \dots, \nu(x_k l_k), \nu(x_{k+1} l_{k+1}))$. Assume that $\gamma = \nu(x_{k+1} l_{k+1})$. Since $\nu(l_{k+1})$ is the maximum of $\nu(l - M)$, $\gamma \leq \nu(x_1 l_1 + \cdots + x_k l_k + x_{k+1} l_{k+1}) = \nu(x_{k+1}) + \nu(x_1 x_{k+1}^{-1} l_1 + \cdots + x_k x_{k+1}^{-1} l_k + l_{k+1}) \leq \nu(x_{k+1}) + \nu(l_{k+1}) = \gamma$. So, $\nu(x_1 l_1 + \cdots + x_k l_k + x_{k+1} l_{k+1}) = \min(\nu(x_1 l_1), \dots, \nu(x_k l_k), \nu(x_{k+1} l_{k+1}))$. □

The following properties show more links between separate and immediate extensions.

Proposition 2.14. *([B 81]) If (K,ν) is a maximal valued field, then every multiplicative extension of (K,ν) is separate.*

Theorem 2.15. *([D 88, Corollaire 7]) Assume that ν is multiplicative on L and that (K,ν) is henselian of residue characteristic 0. Then any algebraic extension of (K,ν) is separate.*

Theorem 2.16. *([D 88, p. 421]) Assume that ν is multiplicative on L and that (K,ν) is henselian of residue characteristic 0. Then $(L|K,\nu)$ is separate if, and only if, L is linearly disjoint over K from every immediate extension of (K,ν).*

2.2. **Extensions generated by one element.** In this subsection, $K(\chi)|K$ is a simple extension of fields, where χ is algebraic or transcendental over K.

Proposition 2.17. *Let $d \in \mathbb{N}\cup\{\infty\}$ such that $0 < d \leq [K[\chi]:K]-1$. Then $(K_d[\chi]|K,\nu)$ is separate if, and only if, the K-module $K_d[\chi]$ admits a separate basis. Furthermore, we can assume that the degree mapping is one-to-one, and that every polynomial of this basis is monic.*
Assume that χ is transcendental over K, and that ν is multiplicative on $K(\chi)$. Then $(K(\chi)|K,\nu)$ is separate if, and only if, the K-module $K[\chi]$ admits a separate basis. ($\Rightarrow$ holds even if ν is not multiplicative).

Proof. Assume that $(K_d[\chi]|K,\nu)$ is separate. By Lemma 2.13, the separate basis 1 of K can be completed in a separate 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 separate basis of $(n+1)$ elements of respective degrees 0, 1, ..., n. By Lemma 2.13, this separate basis can be completed in a separate basis of $K_{n+1}[\chi]$, and the degree of the new element is $n+1$. So we get the required separate basis by induction. By Lemma 2.8 we can assume that every polynomial of this basis is monic.

Conversely, assume that $K_d[\chi]$ contains a separate basis, and let M be a finitely generated K-submodule. By Lemma 2.11, M has a separate basis.
Assume that χ is transcendental over K, and that ν is multiplicative on $K(\chi)$ and let M be a finitely generated submodule of $K(\chi)$. Then there is a polynomial $f(\chi)\neq 0$ such that $f(\chi)\cdot M \subseteq K[\chi]$. We take a separate basis of $f(\chi)\cdot M$, and we divide all its elements by $f(\chi)$ so that, since ν is multiplicative, by Lemma 2.8, we get a separate basis of M. □

Example 2.18. Let (K,ν) be a valued field. Pick some x in K, some γ in an extension of νK, and, for every $x_0, x_1, \ldots, x_n$ in K, set $\nu'(x_n(\chi-x)^n+\cdots+x_1(\chi-x)+x_0) = \min(\nu(x_n)+n\gamma, \ldots, \nu(x_1)+\gamma, \nu(x_0))$. Then one can check that ν' defines a p-m valuation on the ring $K[\chi]$. We say that ν' is a *Gauss valuation*. Then ν' is a separate valuation and $1, (\chi-x), \ldots, (\chi-x)^n, \ldots$ is a separate 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 $K[\chi]$, $\nu'(f)\leq\nu''(f)$.

We state a refinement of Theorem 2.4, which characterizes separate extensions by means of initial segments. This proposition completes Proposition 1.7.

Proposition 2.19. *Let $d \in \mathbb{N}\cup\{\infty\}$ such that $0 < d \leq [K[\chi]:K]-1$. The extension $(K_d[\chi]|K,\nu)$ is separate 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 separate if, and only if, for every $n\in\mathbb{N}^*$, $\nu(\chi^n - K_{n-1}[\chi])$ has a maximal element.

Proof. In both equivalences, $\Rightarrow$ follows from Theorem 2.4. In order to prove the converse, we construct by induction a separate basis such that the degree mapping is one-to-one. Then, by Proposition 2.17, $(K_d[\chi]|K,\nu)$ is separate. The case where χ is transcendental also follows from Proposition 2.17. Trivially, 1 is a separate basis of $K_0[\chi]=K$. Assume that we have a separate basis $(f_0,\ldots,f_{n-1})$ 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, $(f_0,\ldots,f_{n-1},f_n)$ is a basis of $K_n[\chi]$. Let $f=x_nf_n+\cdots+x_0$ in $K_n[\chi]$. If $x_n=0$, then by induction hypothesis $\nu(f)=\min\limits_{0\leq i\leq n-1}\nu(x_if_i)=\min\limits_{0\leq i\leq n}\nu(x_if_i)$. Now we assume: $x_n\neq 0$. Since $\nu(f_n)$ is maximal, we have $\nu\left(\dfrac{f}{x_n}\right)\leq\nu(f_n)$. If $\nu\left(\frac{f}{x_n}-f_n\right)<\nu(f_n)$, then $\nu\left(\dfrac{f}{x_n}-f_n\right)=\nu\left(\dfrac{f}{x_n}\right)$. So:

$$\nu(f)=\nu(x_n)+\nu\left(\frac{f}{x_n}\right)=\nu(x_n)+\nu\left(\frac{f}{x_n}-f_n\right)=$$

$$=\nu(x_n)+\min_{0\leq i\leq n-1}\nu\left(\frac{x_if_i}{x_n}\right)=\min_{0\leq i\leq n-1}\nu(x_if_i)=\min_{0\leq i\leq n}\nu(x_if_i).$$

If $\nu\left(\dfrac{f}{x_n}-f_n\right)\geq\nu(f_n)$, then $\min\limits_{0\leq i\leq n-1}\nu(x_if_i)\geq\nu(x_nf_n)$. Furthermore, since $\nu(f_n)$ is maximal we have $\nu\left(\dfrac{f}{x_n}\right)=\nu(f)$. Therefore: $\nu(f)=\min\limits_{0\leq i\leq n}\nu(x_if_i)$. □

2.3. **Graded algebra associated to a valuation.** In the proofs of Remark 3.35 and Theorem 3.37 we will introduce the graded algebra associated to a valuation. We will also show more properties in Subsection 3.6 because they are used in the definition of key polynomials by F. J. Herrera Govantes, W. Mahloud, M. A. Olalla Acosta and M. Spivakovsky. Now, we review some basic facts. 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 (see Remark 1.14), then $G_\nu(K)$ is isomorphic to the ring of generalized polynomials $k[\Gamma]$. More generally, the K-module $G_\nu(K)$ is isomorphic to the K-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 [K 75]). 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 $\mathrm{char}(K_\nu) = 0$, 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 $in_\nu\left(\sum_{\gamma\in\Lambda} x_\gamma \chi^\gamma\right) = x_{\gamma_0}\chi^{\gamma_0}$, where γ_0 is the smallest element of the support of the serie (i.e. the well ordered subset Λ of νK such that $x_{\gamma_0} \neq 0$, see Remark 1.14). 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 $in_\nu(x+y) = 0$. 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 inversible 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 $\bigoplus_{\gamma\in\nu M} M_{\gamma,\nu}$.

Let $(L|K,\nu)$ be an extension of valued fields, and $l_1,\dots,l_n$ in L. Recall that the family $(l_1,\dots,l_n)$ is a separate over (K,ν) if, and only if, for every $x_1,\dots,x_n$ in K, $\nu(x_1l_1,\dots,x_nl_n) = \min(\nu(x_1l_1),\dots,\nu(x_nl_n))$. Now, this equivalent to saying that for every $x_1,\dots,x_n$ in K with $\nu(x_1l_1) = \cdots = \nu(x_nl_n)$, we have $\nu(x_1l_1,\dots,x_nl_n) = \nu(x_1l_1)$. This last equality is equivalent to $in_\nu(x_1)in_\nu(l_1) + \cdots + in_\nu(x_n)in_\nu(l_n) \neq 0$. 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 separate. Now, assume that for every $x_1,\dots,x_n$ in K with $\nu(x_1l_1) = \cdots = \nu(x_nl_n)$, we have $\nu(x_1l_1,\dots,x_nl_n) = \nu(x_1l_1)$. Let $y_1,\dots,y_n$ in $G_\nu(K)$. Every y_j can be written as a finite sum of homogeneous elements: $y_j = in_\nu(x_{j,1}) + \cdots + in_\nu(x_{j,i_j})$. It follows that $y_1in_\nu(l_1) + \cdots + y_nin_\nu(l_n)$ can be written as a sum of $in_\nu(x_{1,k_1})in_\nu(l_1) + \cdots + in_\nu(x_{n,k_n})in_\nu(l_n)$, where the non-zero $in_\nu(x_{j,k_j})in_\nu(l_j)$ have the same valuation. Therefore, $y_1in_\nu(l_1) + \cdots + y_nin_\nu(l_n) \neq 0$. Consequently, the family $(l_1,\dots,l_n)$ is separate 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 separate 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 $[L_\nu : K_\nu]\cdot(\nu L : \nu K)$. Hence, by Theorem 2.5, $(L|K,\nu)$ is separate if, and only if, $G_\nu(L)$ is a $G_\nu(K)$-module of dimension $[L:K]$.

Turning to immediate extensions, by Remark 1.6, $(L|K,\nu)$ is immediate if, and only if, $G_\nu(L) = G_\nu(K)$.

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

Proof. See for example [HOS 07]. □

We sometimes call *homogeneous* a polynomial $in_\nu(\chi)^n + in_\nu(x_{n-1})in_\nu(\chi)^{n-1} + \cdots + in_\nu(x_0)$, where $x_0,\dots,x_{n-1}$ belong to K , such that $\nu(x_0) = \cdots = \nu(x_{n-1}\chi^{n-1}) = \nu(\chi^n)$.

3. Key polynomials.

In this section, $K(\chi)|K$ is an extension of fields, where χ is algebraic or transcendental over K.

3.1. **Definitions.** We generalize the definition of key polynomials of S. MacLane ([ML 36a] and [ML 36b]). In next subsection we will compare S. MacLane's definition and the following one.

Notation 3.1. 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 3.2. Let ν be a K-module valuation on $K(\chi)$ and Φ be a monic polynomial of degree $d \geq 1$.
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 $\nu(fg) = \nu(r(f,g))$.
We say that Φ is a *strict 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.
We say that d is a *strict key degree* of $(K(\chi)|K,\nu)$ if there exists a strict 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 a *separate* 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.

Remarks 3.3. 1) The integer 1 is a strict key degree. Furthermore, every monic polynomial of degree 1 is a strict key polynomial.
2) Every key polynomial is irreducible.
3) If ν is partially multiplicative and Φ is a key polynomial (resp. a strict key polynomial) for ν of degree d, then, for every p-m 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 key polynomial (resp. a strict key polynomial) for ν'.
4) Assume that ν is partially multiplicative. If Φ is a key polynomial, then $\nu(\Phi) \geq \{\nu(r(f,g)) - \nu(q(f,g)) \mid f \in K_{d-1}[\chi],\ g \in K_{d-1}[\chi],\ \deg(f)+\deg(g) < [K[\chi]:K]\}$. If Φ is a monic polynomial, then Φ is a strict 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 key polynomial for ν.
4) Clearly, if Φ is a key polynomial (resp. a strict 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 $\nu(r(f,g)) - \nu(fg)$. □

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

Lemma 3.4. *Let d be a positive integer. Assume that $\nu(\chi^d - K_{d-1}[\chi])$ has a maximum $\nu(\Phi)$. Then 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 $\nu(\Phi) \in \nu K_{d-1}[\chi]$. Since $\nu(\Phi)$ is maximal in $\nu(\chi^d - K_{d-1}[\chi])$, 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 $\Phi_{\nu(\Phi),\nu} \notin (K_{d-1}[\chi])_{\nu(\Phi),\nu}$. □

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 $\rho : K[X] \to K[X]/(\Phi)$ 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 $d \leq [K(\chi):K]/2$.

Notation 3.5. Let Φ be a monic irreducible polynomial of $K[\chi]$ of degree d, $1 \leq d \leq [K(\chi):K]/2$. The field $(K_{d-1}[\chi], +, *)$ defined above will be denoted by K_Φ.

Note that if ν is a p-m 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 3.6. *Let Φ be an irreducible monic polynomial of degree d, $1 \leq d \leq [K(\chi):K]/2$, and ν be a p-m valuation on $K(\chi)$. Then Φ is a 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 key polynomial. □

Corollary 3.7. *Let Φ be a key polynomial of degree d, $1\leq d\leq [K(\chi):K]/2$, and ν be a p-m valuation on $K(\chi)$. Then $\nu K_{d-1}[\chi]$ is a subgroup of $\nu K(\chi)$.*

Proof. Indeed, if Φ is a key polynomial, then for every $f,\ g$ in $K_{d-1}[\chi]$ we have $\nu(f*g)=\nu(r_\Phi(f,g))=\nu(fg)=\nu(f)+\nu(g)$. Hence $\nu K_\Phi=\nu K_{d-1}[\chi]$. □

Remark 3.8. Let Φ be a monic polynomial of degree d, $1\leq d\leq [K(\chi):K]/2$, and ν be a p-m valuation on $K(\chi)$.

(1) The polynomial Φ is a strict 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 $\nu(fg-r_\Phi(f,g))>0$ is equivalent to $(fg)_{\nu(fg),\nu}=(r_\Phi(f,g))_{\nu(fg),\nu}$.

(2) If Φ is a strict key polynomial, then the group $G_\nu(K_{d-1}[\chi])$ is a subalgebra of $G_\nu(K(\chi))$. Indeed, since $(fg)_{\nu(fg),\nu}=f_{\nu(f),\nu}g_{\nu(g),\nu}$, Φ is a strict 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 $G_\nu(K_{d-1}[\chi])$ is a subalgebra of $G_\nu(K(\chi))$, and it is isomorphic to $G_\nu(K_\Phi)$. Hence $G_\nu(K)$ embeds in $G_\nu(K_\Phi)$ and $G_\nu(K_\Phi)$ embeds in $G_\nu(K(\chi))$.

(3) It follows from Proposition 3.6 that if Φ is a strict key polynomial, then $K_{d-1}[\chi]_\nu$ is a subfield of $K(\chi)_\nu$.

3.2. **MacLane's key polynomials.** In [ML 36a] and [ML 36b] S. MacLane defined key polynomials in the case of discrete valuations. M. Vaquié ([V 07]) generalized this definition to arbitrary valuations. In [V 07] the key polynomials are defined on the ring of formal polynomials. The case of algebraic extensions is obtained by means of a pseudo-valuation, by quotienting $K[\chi]$ by the socle of ν. A *pseudo-valuation* ν of K is a mapping from K onto a linearly ordered group νK together with an element ∞ which shares the properties of multiplicative valuations except $\nu(x)=\infty\Rightarrow x=0$. In this case the set $I=\{x\in K\mid \nu(x)=\infty\}$ is a prime ideal which is called the *socle* of ν. Then ν induces a p-m valuation on the integral domain K/I. So, in [V 07] χ is transcendental over K and ν is a valuation or a pseudo-valuation. Now, in Definition 3.2, we can assume that ν is a pseudo-valuation and that χ is transcendental. Here we extend the definition of [V 07] to the case of an algebraic extension, and we do not require χ being transcendental.

In this subsection, ν is a K-module valuation on $K(\chi)$ or a pseudo-valuation.

Definition 3.9. Let Φ be a monic polynomial of degree d and $d'=[K[\chi]:K]-d$. 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 *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: $\forall h\in K_{d'-1}[\chi]\ \nu(fg-h\Phi)=\min(\nu(fg),\nu(h\Phi))$.

Remark 3.10. By setting $h=1$ in above definition, we see that every monic polynomial, which is ν-minimal and ν-irreducible, is irreducible.

Proposition 3.11. *Assume that ν is a p-m valuation or a pseudo-valuation. Let $d<[K[\chi]:K]$ in $\mathbb{N}^*$, $d'=[K[\chi]:K]-d$, 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 key polynomial such that the sequence (Φ^m) $(md<[K(\chi):K])$ is separate over $K_{d-1}[\chi]$.

Before proving Proposition 3.11 we state a lemma.

Lemma 3.12. *(*[ML 36a] *Lemma 4.3) Assume that ν is a p-m valuation or a pseudo-valuation. Let $d<[K[\chi]:K]$ in $\mathbb{N}^*$, $d'=[K[\chi]:K]-d$, Φ be a ν-minimal non constant monic polynomial in $K[\chi]$ of degree d. Let $f\in K[\chi]$ and $f=q\Phi+r$ be the euclidean division of f by Φ. The following assertions are equivalent.*
a) $\nu(r)>\nu(f)$
b) $\nu(r)>\min(\nu(f),\nu(q\Phi))$
c) $\exists h\in K_{d'-1}[\chi]\ \nu(f-h\Phi)>\min(\nu(f),\nu(h\Phi))$.

Proof. Trivially we have: a) ⇒ b) and b) ⇒ c). We prove c) ⇒ a). Let $h\in K_{d'-1}[\chi]$. By hypothesis, $\deg(r)<d$ and $\deg(q)<d'$. Hence $\nu(f-h\Phi)=\nu((q-h)\Phi+r)=\min(\nu((q-h)\Phi),\nu(r))\leq\nu(r)$. Therefore $\nu(f-h\Phi)>\min(\nu(f),\nu(h\Phi))\Rightarrow\nu(r)>\min(\nu(f),\nu(h\Phi))$. Now, $\nu(f-h\Phi)>\min(\nu(f),\nu(h\Phi))\Rightarrow\nu(f)=\nu(h\Phi)$, hence $\nu(r)>\nu(f)$. □

Proof of Proposition 3.11.

2) $\Rightarrow$ 1). Assume that Φ satisfies the hypothesis of 2). By setting $g = 1$ if 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 et g can be written as $f = q\Phi + r$ and $g = q'\Phi + r'$. By Lemma 3.12, we have $\nu(f) = \nu(r)$ and $\nu(g) = \nu(r')$. Let $h \in K_{d'-1}[\chi]$. Then $\nu(fg - h\Phi) = \nu((qq'\Phi + qr' + q'r - h)\Phi + rr') = \min(\nu((qq'\Phi + qr' + q'r - h)\Phi), \nu(rr'))$, because both of r and r' belong to $K_{d-1}[\chi]$. Hence $\nu(fg - h\Phi) \leq \nu(rr') = \nu(fg)$. Now, we have $\min(\nu(fg), \nu(h\Phi)) \leq \nu(fg - h\Phi) \leq \nu(fg)$. So, $\nu(fg - h\Phi) = \min(\nu(fg), \nu(h\Phi))$. Hence Φ is ν-irreducible.

1) $\Rightarrow$ 2). We assume that Φ be a monic, ν-minimal and ν-irreducible polynomial. 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 $K[\chi]$ 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). Assume that Φ satisfies the hypothesis of 1) and 2). Let f, g in $K_{d-1}[\chi]$ with $\deg(f) + \deg(g) < [K[\chi] : K]$. By letting $h = -q_\Phi(f, g)$, 2) implies $\nu(r_\Phi(f, g)) = \min(\nu(fg), \nu(q_\Phi(f, g)\Phi))$. Since Φ is ν-minimal, by Lemma 3.12 we have $\nu(r_\Phi(f, g)) = \nu(fg)$. Hence Φ is a key polynomial. Now, let $m \in \mathbb{N}^*$ with $dm < [K[\chi] : K]$, $f_0, \ldots, f_m$ in $K_{d-1}[\chi]$. We have: $\nu(f_m\Phi^m + \cdots + f_0) = \min(\nu((f_m\Phi^{n-1} + \cdots + f_1)\Phi), \nu(f_0))$, $\nu(f_m\Phi^{n-1} + \cdots + f_1) = \min(\nu((f_m\Phi^{n-2} + \cdots + f_2)\Phi), \nu(f_1))$, and so on. So by induction we have $\nu(f_m\Phi^m + \cdots + f_0) = \min(\nu(f_m\Phi^{n-1}), \ldots, \nu(f_0))$. Hence the family $(\Phi^m)_{m\in\mathbb{N}}$ is separate over $K_{d-1}[\chi]$.

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 $h = h_m\Phi^m + \cdots + h_\Phi + h_0$, where $h_m, \ldots, h_1, h_0$ 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: $\nu(fg + h\Phi) = \nu(h_m\Phi^{m+1} + \cdots + h_1\Phi^2 + (q + h_0)\Phi + r) = \min(\nu(h_n\Phi^{m+1}), \ldots, \nu(h_1\Phi^2), \nu((q + h_0)\Phi), \nu(r))$. Since Φ is a 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: $\nu(fg + h\Phi) = \min(\nu(h_m\Phi^{m+1}), \ldots, \nu(h_1\Phi^2), \nu(h_0\Phi)\nu(fg)) = \min(\nu(h\Phi), \nu(fg))$. □

Remark 3.13. We use the hypothesis "ν is a p-m 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.

In MacLane's definition, the key polynomials are the ν-minimal and ν-irreducible polynomials. Proposition 3.11 shows that this definition is stronger than Definition 3.2. The difference will appear more clearly in Subsection 3.3 (for example Remark 3.18). Now, we extend the definition of S. MacLane to K-module valuations.

Definition 3.14. Let Φ be a polynomial of degree d. We say that Φ is a *ML key polynomial for* ν if Φ is a key polynomial such that the sequence (Φ^m) $(md < [K(\chi) : K])$ is separate over $K_{d-1}[\chi]$.

3.3. **Separate valuations defined by key polynomials.** We generalize the definition of augmented valuations of S. MacLane ([ML 36a] and [ML 36b]).

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

Assume that ν is a p-m valuation on $K(\chi)$ and that Φ is a key polynomial for ν of degree d. We saw in Remarks 3.3 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. We also define an element $-\infty < \nu K(\chi)$, and we let $\delta + \infty = \infty$, $\delta - \infty = -\infty$, for every δ in the Dedekind completion of $\nu K(\chi)$.

Proposition 3.15. *Let Φ be a monic irreducible polynomial of degree d, γ be an element of an extension of $\nu K(\chi)$, ν be a K-module valuation defined on $K_{d-1}[\chi]$, 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 separate over $K_{d-1}[\chi]$.
2) Assume that ν is a p-m valuation and that Φ is a key polynomial for ν. Denote by β the upper-bound of the set $\{\nu(r(f, g)) - \nu(q(f, g)) \mid f \in K_{d-1}[\chi],\ g \in K_{d-1}[\chi],\ \deg(f) + \deg(g) < [K[\chi] : K]\}$, and assume that $\gamma \geq \beta$.
a) For every $f = f_m\Phi^m + \cdots + f_1\Phi + f_0$, $g = g_m\Phi^m + \cdots + g_1\Phi + g_0$, with $f_0, \ldots, f_m, g_0, \ldots, g_m$ 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 p-m valuation.*
b) The polynomial Φ *is a ML key polynomial for* ν'*. Furthermore it is a strict key polynomial if, and only if,* $\gamma>\beta$ *or* β *is not a maximum.*

Proof. 1) Clearly, if ν' is a K-module valuation, then the family (Φ^m) is separate over $K_{d-1}[\chi]$. Let $f_0,\dots,f_m,g_0,\dots,g_m$ in $K_{d-1}[\chi]$ and let $f=f_m\Phi^m+\cdots+f_1\Phi+f_0$, $g=g_m\Phi^m+\cdots+g_1\Phi+g_0$. We have trivially

$$\nu'(f+g)=\min_{0\leq j\leq m}(\nu(f_j+g_j)+j\gamma)\geq\min_{0\leq j\leq m}(\min(\nu(f_j)+j\gamma,\nu(g_j))+j\gamma)$$
$$\geq\min(\nu'(f),\nu'(g)).$$

We have that $\nu'(f)=\infty\Leftrightarrow f=0$. Now, for $x\in K$, $\nu'(xf)=\nu'(x)+\nu'(f)$, since ν is a K-module valuation.

2) a) Since $\deg(f)+\deg(g)<[K[\chi]:K]$, for every i, j we have $\deg(f_i)+\deg(g_j)<[K(\chi):K]$. Hence $\nu(f_ig_j)=\nu(f_i)+\nu(g_j)$. Denote by i_0 (resp. j_0) the smallest index such that $\nu'(f)=\nu(f_{i_0}+i_0\gamma)$ (resp. $\nu'(g)=\nu(g_{j_0}+j_0\gamma)$), and for $i>m$ set $f_i=g_i=0$. We have

$$\nu'(fg)=\nu'\left(\sum_{j=0}^{2m}\left(\sum_{i=0}^{j}f_ig_{j-i}\right)\Phi^j\right)\geq\min_{0\leq i\leq j\leq 2m}(\nu'(f_ig_{j-i})+j\gamma)$$
$$\geq\min_{0\leq i\leq j\leq 2m}(\nu(f_i)+i\gamma+\nu(g_{j-i})+(j-i)\gamma)\geq\nu'(f)+\nu'(g).$$

For every i, j, let $q_{i,j-i}=q(f_i,g_{j-i})$ and $r_{i,j-i}=r(f_i,g_{j-i})$.

$$fg=\sum_{j=0}^{2m}\left(\sum_{i=0}^{j}q_{i,j-i}\Phi+r_{i,j-i}\right)\Phi^j=$$
$$=\sum_{j=1}^{2m+1}\left(\sum_{i=0}^{j-1}q_{i,j-i-1}\right)\Phi^j+\sum_{j=0}^{2m}\left(\sum_{i=0}^{j}r_{i,j-i}\right)\Phi^j.$$

Since $\max(\deg(f_i),\deg(g_{j-i}))<d$, ν is a p-m valuation and Φ is a key polynomial, we have:
$\nu'(f_i)+\nu'(g_{j-i})=\nu(f_i)+\nu(g_{j-i})=\nu(r_{i,j-i})=\nu'(r_{i,j-i})=\nu'(f_ig_{j-i})$, and
$\nu(r_{i,j-i})\leq\nu(q_{i,j-i})+\beta\leq\nu'(q_{i,j-i})+\gamma$.
Furthermore, $\nu'(f)+\nu'(g)=\nu(f_{i_0})+i_0\gamma+\nu(g_{j_0})+j_0\gamma\leq$
$\leq\nu(f_i)+i\gamma+\nu(g_{i,j-i-1})+(j-i-1)\gamma=\nu(f_ig_{i,j-i-1})+(j-1)\gamma=$
$=\nu(r_{i,j-i-1})+(j-1)\gamma\leq\nu(q_{i,j-i-1})+\beta+(j-1)\gamma=\nu(q_{i,j-i-1})+j\gamma-(\gamma-\beta)$.

$$\text{Consequently: }\nu'\left(fg-\sum_{j=0}^{2m}\left(\sum_{i=0}^{j}r(f_i,g_{j-i})\right)\right)\geq\nu'(f)+\nu'(g)+(\gamma-\beta).$$

Now, let $h_{i_0+j_0}$ be the coefficient of $\Phi^{i_0+j_0}$ in the decomposition of fg by Φ. We have

$$h_{i_0+j_0}=r_{0,i_0+j_0}+r_{1,i_0+j_0-1}+\cdots+r_{i_0,j_0}+\cdots+r_{i_0+j_0,0}+q_{0,i_0+j_0-1}+\cdots+q_{i_0+j_0-1,0}.$$

By hypotheses, for $0\leq i\leq i_0+j_0-1$ we have:
$\nu(q_{i,i_0+j_0-1-i})+(i_0+j_0)\gamma\geq\nu(q_{i,i_0+j_0-1-i})+\beta+(i_0+j_0-1)\gamma\geq\nu(f_ig_{i_0+j_0-1-i})+(i_0+j_0-1)\gamma=$
$=\nu(f_i)+i\gamma+\nu(g_{i_0+j_0-1-i})+(i_0+j_0-1-i)\gamma$.
If $i\leq i_0-1$, then $\nu(f_i)+i\gamma>\nu'(f)$. Otherwise, $i_0+j_0-1-i\leq j_0-1$, and $\nu(g_{i_0+j_0-1-i})+(i_0+j_0-1-i)>\nu'(g)$. In any case, $\nu(q_{i,i_0+j_0-1-i})+(i_0+j_0)\gamma>\nu'(f)+\nu'(g)$. In the same way, for $0\leq i\leq i_0+j_0$:
$\nu(r_{i,i_0+j_0-i})+(i_0+j_0)\gamma=\nu(f_i)+i\gamma+\nu(g_{i_0+j_0-i})+(i_0+j_0-i)\gamma\geq\nu'(f)+\nu'(g)$,
and equality holds if, and only if, $i=i_0$ and $j=j_0$. Hence the minimum is carried by a unique term, so $\nu(h_{i_0+j_0})=\nu(f_{i_0}g_{j_0})=\nu(f_{i_0})+\nu(g_{j_0})$. Consequently: $\nu'(fg)=\nu'(f)+\nu'(g)$.

Assume that χ is transcendental over K. For all nonzero f, g in $K[\chi]$, set $\nu'(f/g)=\nu'(f)-\nu'(g)$. Then, for every f, f', g, g' in $K[\chi]$, with $g\neq0\neq g'$, we have:

$$\nu\left(\frac{f}{g}\cdot\frac{f'}{g'}\right)=\nu\left(\frac{ff'}{gg'}\right)=\nu(f)+\nu(f')-\nu(g)-\nu(g')=\nu\left(\frac{f}{g}\right)+\nu\left(\frac{f'}{g'}\right),\text{ and}$$
$$\nu\left(\frac{f}{g}+\frac{f'}{g'}\right)=\nu\left(\frac{fg'+f'g}{gg'}\right)=\nu(fg'+f'g)-\nu(g)-\nu(g')\geq$$

$$\geq \min(\nu(fg'),\nu(f'g)) - \nu(g) - \nu(g') = \min\left(\nu\left(\frac{f}{g}\right), \nu\left(\frac{f'}{g'}\right)\right).$$

Hence ν' is a multiplicative valuation.

2) b) If f, g belong to $K_{d-1}[\chi]$, then $f = f_0$, $g = g_0$ and $\nu'(fg) = \nu'(r(f,g)) \leq \nu'(fg - r(f,g)) - (\gamma - \beta) = \nu'(q(f,g)) - (\gamma - \beta)$. Hence Φ is a key polynomial for ν'. If $\gamma > \beta$ or β is not a maximum, then the inequality is strict. If β is a maximum, say $\beta = \nu(r_\Phi(f,g)) - \nu(q_\Phi(f,g))$, then $\nu(q_\Phi(f,g)\Phi) = \nu(q_\Phi(f,g)) + \beta = \nu(r_\Phi(f,g))$. Hence Φ is not a strict key polynomial. Since the family (Φ^m) $(dm < [K[\chi]:K])$ is separate over $K_{d-1}[\chi]$, by 3) of Proposition 3.11, Φ is a ML key polynomial for ν'. □

Notations 3.16. The K-module valuation ν' defined in Proposition 3.15 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 $\deg(\Phi_1) < \deg(\Phi_2)$, 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 $\Phi_1, \ldots, \Phi_n$, with $\deg(\Phi_1) < \cdots < \deg(\Phi_n)$, we define the K-module valuation $\nu_{\Phi_1,\ldots,\Phi_n}$.

Remark 3.17. 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 3.15 shows that the Gauss valuations defined in Example 2.18 are p-m valuations. So, for every monic $\Phi \in K[\chi]$, the p-m valuation ν_Φ can be called a *generalized Gauss valuation.*

Remark 3.18. If ν is a p-m valuation, then it follows from Proposition 3.15 that Φ is a ML key polynomial for ν if, and only if, Φ is a key polynomial for ν and $\nu = \nu_\Phi$.

Proposition 3.19. *Let Φ be a monic polynomial of degree d and ν be a p-m valuation on $K[\chi]$. Then Φ is a key polynomial for ν if, and only if, there exists a p-m 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 p-m 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 ML key polynomial for $\nu_{\Phi,\gamma}$.

Proof. Assume that ν' is a p-m 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 $\nu(q\Phi) < \nu'(q\Phi)$. It follows that $\nu(q\Phi) \neq \nu(r)$ or $\nu'(q\Phi) \neq \nu(r)$, hence $\nu(q\Phi + r) = \min(\nu(q\Phi), \nu(r))$ or $\nu'(q\Phi + r) = \min(\nu'(q\Phi), \nu(r))$. In any case, since $\nu(q\Phi) = \nu(q) + \nu(\Phi) < \nu'(q) + \nu'(\Phi) = \nu'(q\Phi)$ we see that this minimum is $\nu(r)$ and that $\nu(r) \leq \nu(q\Phi) - (\nu'(\Phi) - \nu(\Phi))$. Now, if Φ is a key polynomial for ν, then the hypotheses of Proposition 3.15 2) are satisfied. Hence, the proof of the converse follows the proof of Proposition 3.15.

The remainder also follows from Proposition 3.15. □

Notation 3.20. 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 3.21. 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 3.15.

Remark 3.22. In valuation theory, we say that ν' is *finer* than ν if $\forall x\ \nu'(x) \geq 0 \Rightarrow \nu(x) \geq 0$ (see [R 68, 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 Corollaire 5, p. 158 in [R 68]). 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 3.23. *Let ν be a p-m valuation on $K[\chi]$, and Φ be a non constant monic polynomial in $K[\chi]$ of degree d. Then Φ is a key polynomial for ν if, and only if, there exists a p-m valuation $\nu' \leq \nu$ such that the restrictions of ν and ν' to $K_{d-1}[\chi]$ are equal, and Φ is a ML key polynomial for ν'. Furthermore, we can take $\nu' = \nu_\Phi$.*

Proof. $\Leftarrow$. If Φ is a ML key polynomial for ν', then it is a key polynomial for ν'. Now, by 3) of Remark 3.3, it is a key polynomial for ν.

$\Rightarrow$. By Proposition 3.19, ν_Φ is a p-m valuation such that Φ is a ML key polynomial for ν_Φ. By construction, the restrictions of ν and ν_Φ to $K_{d-1}[\chi]$ are equal. By Remark 3.21 1) we have $\nu_\Phi \leq \nu$. □

3.4. **Bases generated by polynomials.** Let $\Phi_1, \ldots, \Phi_n, \ldots$ be monic irreducible polynomials of $K[\chi]$ of degrees $d_1 = 1, d_2, \ldots, d_n,$ respectively, where d_{n-1} divides d_n (if the family has a maximal element d_n, we set $d_{n+1} = [K(\chi):K]$). We let $\mathcal{B}$ be the family of the $\Phi_1^{e_1} \cdots \Phi_n^{e_n}$, where for $0 \leq i \leq n-1$ we have: $0 \leq e_i < \dfrac{d_{i+1}}{d_i}$. Since the degree mapping 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 $d_1 = 1 < d_2 < \cdots < d_n < \cdots$, we require: for every n, $e_1 + e_2 d_2 + \cdots + e_n d_n < d_{n+1}$.

Definition 3.24. Let $\mathcal{B}$ be a K-basis of $K[\chi]$. We say that $\mathcal{B}$ is *generated by polynomials* if it is constructed in the above way. If so, then $\Phi_1, \Phi_2, \ldots, \Phi_n, \ldots$, are called the *generating polynomials* for $\mathcal{B}$.

Remark 3.25. Let ν be a K-module valuation on $K(\chi)$, $\Phi_1, \ldots, \Phi_k, \ldots$ be generating polynomials for a basis $\mathcal{B}$. For $k \geq 1$, fix $\nu'(\Phi_k)$. For every $e_1, \ldots, e_k$ with $e_1 + e_2 d_2 + \cdots + e_k d_k < d_{k+1}$, let $\nu'(\Phi_1^{e_1} \cdots \Phi_k^{e_k}) = e_1\nu'(\Phi_1) + e_2\nu'(\Phi_2) + \cdots + e_k\nu'(\Phi_k)$ and for every pairwise distinct $y_1, \ldots, y_k$ in $\mathcal{B}$, $x_1, \ldots, x_k$ in K set $\nu'(x_1y_1 + \cdots + x_ky_k) = \min\limits_{1 \leq i \leq k} \nu(x_i)\nu'(y_i)$. Then ν' is a separate 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 $\nu_{\Phi_{d_1}, \ldots, \Phi_{d_k}}$ defined in Notations 3.16.

3.5. **Properties of key degrees.**

Proposition 3.26. *Let d be an integer and ν be a p-m valuation on $K[\chi]$.*
1) Assume that d is an immediate key degree and let Φ be a key polynomial of degree d. Then every monic polynomial Φ' of degree d, such that $\nu(\Phi') > \nu(\Phi)$, is a strict key polynomial (so d is a strict key degree).
2) Assume that d is a separate key degree and let Φ be a key polynomial of degree d.
a) If Φ is a strict key polynomial, then every monic polynomial Φ' of degree d, such that $\nu(\Phi') \geq \nu(\Phi)$, is a strict 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 strict key polynomial.
b) If d is not strict, then every key polynomial of degree d has valuation $\nu(\Phi)$, and $\nu(\Phi)$ is maximal in $\nu(\chi^d - K_{d-1}[\chi])$.

This proposition is a consequence of the following lemma.

Lemma 3.27. *Let d be a positive integer, ν be a p-m valuation on $K[\chi]$, Φ and Φ' be monic polynomials of degree d such that Φ is a key polynomial for ν.*
1) If $\nu(\Phi') > \nu(\Phi)$, then Φ' is a key polynomial for ν_Φ, a strict key polynomial for ν, and $\nu_\Phi \leq \nu_{\Phi'}$.
2) If $\nu(\Phi') = \nu(\Phi)$ and Φ is a strict key polynomial for ν, then Φ' is a strict key polynomial for both of ν and ν_Φ. Furthermore, $\nu_\Phi = \nu_{\Phi'}$.
3) If $\nu(\Phi') = \nu(\Phi)$ and Φ, Φ' are 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) We assume that $\nu(\Phi') > \nu(\Phi)$. Hence $\nu(f) = \nu(\Phi)$. If $\nu_\Phi(q'\Phi') < \nu_\Phi(r')$ $(= \nu(r'))$, 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 strict key polynomial for ν. Since $\nu_\Phi(fg) = \nu(fg) = \nu(r') = \nu_\Phi(r')$, Φ' is a 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 3.21, we have $\nu_\Phi \leq \nu_{\Phi'}$.

2) We assume that $\nu(\Phi') = \nu(\Phi)$ and Φ is a strict key polynomial for ν. Let $q_1 = q_\Phi(q', h)$ and $r_1 = r_\Phi(q', h)$. Since Φ is a strict 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 strict 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 strict key polynomial for ν_Φ. In the same way as in 1), we have: $\nu_\Phi \leq \nu_{\Phi'}$. Now, since Φ' is a strict 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 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 3.21 we have: $\nu_{\Phi'} \leq \nu_\Phi$. In the same way, $\nu_\Phi \leq \nu_{\Phi'}$, hence $\nu_{\Phi'} = \nu_\Phi$. □

Lemma 3.28. *Let ν be a p-m 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 $\nu_\Phi(f)=\nu(f)$. □

Remark 3.29. The valuation of a strict key polynomial is not necessarily maximal. Indeed, we saw in Remark 3.3 1) that every monic polynomial of degree 1 is a strict key polynomial. This holds whether 1 is a separate key degree or not.

Remark 3.30. Let d be a key degree. Then d is an immediate key degree if, and only if, the extension $(K_d[\chi]|K_{d-1}[\chi],\nu)$ is immediate.

Proof. Assume that d is an immediate key degree. Let $\Phi\in K_d[\chi]\backslash K_{d-1}[\chi]$. Without loss of generality we can assume that Φ is a monic polynomial. Then, since $\nu(\chi^d-K_{d-1}[\chi])$ has no maximum element and $\Phi\in\chi^d-K_{d-1}[\chi]$, there is $y\in\chi^d-K_{d-1}[\chi]$ such that $\nu(\Phi-y)>\nu(\Phi)$. Then $\nu(\Phi)=\nu(y)\in\nu K_{d-1}[\chi]$ and $\Phi_{\nu(\Phi),\nu}=f_{\nu(\Phi),\nu}$. The converse follows from Lemma 3.4. □

The following two lemmas give useful criteria for being a key polynomial or a strict key polynomial.

Lemma 3.31. *Let ν, ν' be p-m valuations on $K(\chi)$, and Φ be a monic polynomial of degree $d\geq 1$. 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 key polynomial for ν' and a strict 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 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 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 strict 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 key polynomial for ν', we have $\nu'(fg)=\nu'(r)$. Hence $\nu'(fg+h\Phi)\geq\nu'(r)$. Note that $fg+h\Phi=(q+h)\Phi+r$, hence by 1) it follows: $\nu'(fg+h\Phi)=\nu(fg+h\Phi)$. Now, $\nu(fg)=\nu'(fg)=\nu'(h\Phi)<\nu(h\Phi)$, hence $\nu(fg+h\Phi)=\nu(fg)=\nu'(fg)=\min(\nu'(fg),\nu'(h\Phi))$. By 2) ⇒ 3) of Proposition 3.11 and Remark 3.18, we have $\nu'=\nu'_\Phi$. Now, since ν' and ν coincide on $K_d[\chi]$ we have $\nu'_\Phi=\nu_{\Phi,\nu'(\Phi)}$. □

Remark 3.32. It follows from Lemma 3.31 that if ν is a valuation on $K(\chi)$, then every p-m 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 $\nu'(\Phi)<\nu(\Phi)$.

Lemma 3.33. *Let ν be a p-m valuation on $K(\chi)$, Φ be a key polynomial for ν and Φ' be a monic polynomial such that $d=\deg(\Phi)<\deg(\Phi')=d'$.*
1) If $\nu(\Phi')=\nu_\Phi(\Phi')$, then Φ' is not strict key polynomial for ν.
2) Assume that $\nu_\Phi=\nu$ on $K_{d'-1}[\chi]$. Then, Φ' is a strict key polynomial for ν if, and only if, $\nu(\Phi')>\nu_\Phi(\Phi')$.

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

2) ⇐ follows from Lemma 3.31, ⇒ follows from 1). □

Proposition 3.34. *Let d be a positive integer, ν be a p-m valuation on $K[\chi]$.*
1) If $\nu=\nu_\Phi$ for some monic polynomial Φ, then there is no strict key degree greater than d.
2) If d is a separate key degree such that there is no strict key degree greater than d, and Φ is a key polynomial of degree d, with $\nu(\Phi)=\max(\nu(\chi^d-K_{d-1}[\chi]))$, then $\nu=\nu_\Phi$.

Proof. 1) Follows from Lemma 3.33.

2) By Lemma 3.28, ν and ν_Φ coincide on $K_d[\chi]$. Now, by Lemma 3.33, $\nu = \nu_\Phi$ on $K[\chi]$. □

Remark 3.35. Let ν be a multiplicative valuation on $K(\chi)$. If the irrational 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 Abhyankar's inequality is an equality), then there is a finite number of strict key degrees, and $\nu = \nu_\Phi$ for some key polynomial Φ.

Proof. Note that in this case χ is transcendental. Abhyankar's inequality states that the transcendence degree of $K(\chi)|K$ is at least equal to the product of the transcendence degree of $(K(\chi))_\nu|K_\nu$ by the irrational rank of $\nu(K[\chi])|\nu K$. Assume that the irrational 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 strict 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 $K_{d-1}[\chi]$ with $\deg(f) + \deg(g) < [K[\chi] : K]$ 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 strict 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 2.10, this implies that the family (Φ^k) is separate over $K_{d-1}[\chi]$. Therefore, $\nu = \nu_\Phi$. Now, by 1) of Proposition 3.34, if $d' > d$, then d is not a strict 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 2.20 $in_\nu(\Phi)$ is algebraic over K_ν (the converse is trivial). Consequently, $in_\nu(\Phi)$ is transcendental over K_ν if, and only if, it transcendental over $G_\nu(K)$. In particular, if the transcendence degree of $K(\chi)$ over K is 1, then 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: $in_\nu(fg) = in_\nu(q\Phi) \Leftrightarrow 0 = in_\nu(fg) - in_\nu(q\Phi) \Leftrightarrow \nu(fg - q\Phi) > \min(\nu(fg), \nu(q\Phi)) \Leftrightarrow \nu(r) > \min(\nu(fg), \nu(q\Phi))$. 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 $\nu(r) \leq \min(\nu(fg), \nu(q\Phi))$. This proves that Φ is a key polynomial. Let $f_0, \ldots, f_n$ in $K_{d-1}[\chi]$. By hypothesis, $in_\nu(f_0), \ldots, in_\nu(f_n)$ are algebraic over $G_\nu(K)$. Hence $in_\nu(f_n)in_\nu(\Phi)^n + \cdots + in_\nu(f_0) \neq 0$. It follows that $\nu(f_0 + \cdots + f_n\Phi^n) = \min(\nu(f_0), \cdots, \nu(f_n\Phi^n))$. This proves that the sequence (Φ^n) is separate over $K_{d-1}[\chi]$. Therefore, $\nu = \nu_\Phi$. By 1) of Proposition 3.34, if $d' > d$, then d is not a strict key degree. □

The following two theorems characterize the successor of a strict key degree.

Theorem 3.36. *Let ν be a p-m valuation on $K(\chi)$, d be an immediate key degree, and let (Φ_i) be a sequence of strict 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 strict key polynomial and d' is the next strict 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 strict 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 Lemma 3.33 1), f is not a strict 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 1.7 that the extension $(K_{d'-1}[\chi]|K_{d-1}[\chi], \nu)$ is immediate. Let Φ_i be a key polynomial of degree d such that $\nu(f) = \nu_{\Phi_i}(f)$, and let f be written as $f = f_k\Phi_i^k + \cdots + f_1\Phi_i + f_0$, where $f_0, f_1, \ldots, f_k$ belong to $K_{d-1}[\chi]$, f_k is monic, and $\deg(f_k) + kd = n$. Then $\nu(f) = \min(\nu(f_k\Phi_i^k), \ldots, \nu(f_1\Phi_i), \nu(f_0))$. Assume that $\nu(f_0) > \nu(f)$. Then $\nu(f) = \min(\nu(f_k\Phi_i^k), \ldots, \nu(f_1\Phi_i))$. Let Φ_j be a key polynomial of degree d such that $\nu(\Phi_j) > \nu(\Phi_i)$, and set $g = f_k\Phi_j^k + \cdots + f_1\Phi_j$. Then g is a monic polynomial of degree n, and $\nu(g) \geq \nu_{\Phi_j}(g) = \min(\nu(f_k\Phi_j^k), \ldots, \nu(f_1\Phi_j)) > \nu(f)$. 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 key polynomial of degree d such that $\nu(\Phi_j)>\nu(\Phi_i)$, and $g=f_k\Phi_j^k+\cdots+f_1\Phi_j$. Then $\nu(g)\geq\nu_{\Phi_j}(g)=\min(\nu(f_k\Phi_j^k),\dots,\nu(f_1\Phi_j))>\min(\nu(f_k\Phi_i^k),\dots,\nu(f_1\Phi_i))=\nu(f)$. □

Theorem 3.37. *Let ν be a p-m valuation on $K(\chi)$, d be a strict separate 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 strict key degree if it exists or $d'=[K[\chi]:K]$ otherwise.*
1) Φ is a strict key polynomial, and if $d'<[K[\chi]:K]$, then d' is the smallest degree such that there exists a monic polynomial Φ' of degree d' with $\nu_\Phi(\Phi')<\nu(\Phi')$.
2) The restrictions of ν and ν_Φ to $K_{d'-1}[\chi]$ are equal.
3) The fraction d'/d is equal to $[(K_{d'-1}[\chi])_\nu:(K_{d-1}[\chi])_\nu]\cdot(\nu(K_{d'-1}[\chi]):\nu(K_{d-1}[\chi]))$ (in particular $d\leq[K[\chi]:K]/2$).
4) If $(K_{d-1}[\chi]|K,\nu)$ is separate, then $(K_{d'-1}[\chi]|K,\nu)$ is separate.

Proof. 1) Since $\nu(\Phi)$ is the maximum of $\nu(\chi^d-K_{d-1}[\chi])$, by (2) of Proposition 3.26, Φ is a strict key polynomial. By Lemma 3.33, if $d'<[K[\chi]:K]$, then d' is the smallest degree such that there exists a monic polynomial Φ' of degree d' with $\nu_\Phi(\Phi')<\nu(\Phi')$.

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 3.4 $in_\nu(\Phi)\notin G_\nu(K(\chi))$. If $in_\nu(\Phi)$ is transcendental over the graded algebra generated by $G_\nu(K_{d-1}[\chi])$, then χ is transcendental over K. It follows that $[K(\chi):K]$ is infinite, and in the same way as in the proof of Remark 3.35 the family (Φ^n) is separate over $K_{d-1}[\chi]$ and $\nu=\nu_\Phi$. So, $d'=\infty$. The dimension of the $G_\nu(K)$-module $G_\nu(K(\chi))$ is also infinite, so $[(K_{d'-1}[\chi])_\nu:(K_{d-1}[\chi])_\nu]\cdot(\nu(K_{d'-1}[\chi]):\nu(K_{d-1}[\chi]))$ is infinite. Assume that $in_\nu(\Phi)$ is algebraic over $G_\nu(K_{d-1}[\chi])$, and that $G_\nu(K_{d-1}[\chi])$ is a graded algebra (by Remark 3.8 this holds if $d\leq[K[\chi]:K]/2$). Let $X^n+in_\nu(f_{n-1})X^{n-1}+\cdots+in_\nu(f_0)$ be its irreducible polynomial, whith $f_0,\dots,f_{n-1}$ in $K_{d-1}[\chi]$ and $\nu(f_0)=\cdots=\nu(f_{n-1}\Phi^{n-1})=\nu(\Phi^n)$, as in Lemma 2.20. Note that $dn<[K[\chi]:K]$, since, in $K[\chi]$, Φ^n is a polynomial of degree less than $[K[\chi]:K]$. By minimality of n, this implies that $in_\nu(1),in_\nu(\Phi),\dots,in_\nu(\Phi^{n-1})$ are linearely independent over $G_\nu(K_{d-1}[\chi])$. We saw in Subsection 2.3 that this is equivalent to saying that the sequence $1,\Phi,\dots,\Phi^{n-1}$ is separate over $K_{d-1}[\chi]$. Since $\nu_\Phi(\Phi^n+f_{n-1}\Phi^{n-1}+\cdots+f_0)=\min(\nu(\Phi^n),\nu(f_{n-1}\Phi^{n-1}),\cdots,\nu(f_0))<\nu(\Phi^n+f_{n-1}\Phi^{n-1}+\cdots+f_0)$, we have $d'=dn$. 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 $G_\nu(K(\chi))$. In particular, $(K_{d-1}[\chi])_\nu$ is a subfield of $(K[\chi])_\nu$ and $\nu K_{d-1}[\chi]$ is a subgroup of $\nu(\chi)$. Now, this also proves that $(in_\nu(1),in_\nu(\Phi),\dots,in_\nu(\Phi)^{n-1})$ is a basis of the $G_\nu(K_{d-1}[\chi])$-module $G_\nu(K_{d'-1}[\chi])$. Hence its dimension is n. Since this dimension is also equal to $[(K_{d'-1}[\chi])_\nu:(K_{d-1}[\chi])_\nu]\cdot(\nu(K_{d'-1}[\chi]):\nu(K_{d-1}[\chi]))$, the result follows.

If $[K[\chi]:K]$ is infinite, then by Remark 3.8 for, every strict key degree d, $G_\nu(K_{d-1}[\chi])$ is a graded algebra. We assume that $[K[\chi]:K]$ is finite and we show by induction that, for every strict key degree d, $G_\nu(K_{d-1}[\chi])$ is a graded algebra. If $d=1$, then $G_\nu(K_{d-1}[\chi])=G_\nu(K)$ and the result is trivial. Now, assume that $d\geq1$, that $G_\nu(K_{d-1}[\chi])$ is a graded algebra and that d is not the greatest key degree. Let d' be the next strict key degree. If d is immediate, then, by Theorem 3.36 3), The extension $(K_{d'-1}[\chi]|K_{d-1}[\chi],\nu)$ is immediate. Hence $G_\nu(K_{d'-1}[\chi])=G_\nu(K_{d-1}[\chi])$ is an algebra. We assume that d is a separate key degree, and we let Φ be a monic polynomial of degree d such that $\nu(\Phi)$ is the maximum of $\nu(\chi^d-K_{d-1}[\chi])$. We already proved above that $G_\nu(K_{d'-1}[\chi])=G_\nu(K_{d-1}[\chi])(in_\nu(\Phi))$ is a subalgebra of $G_\nu(K(\chi))$.

4) By Proposition 2.19, it is sufficient to show that for every integer $n\leq d'-1$, $\nu(\chi^n-K_{n-1}[\chi])$ has a maximum. Let $f=f_k\Phi^k+\cdots+f_1\Phi+f_0\in\chi^n-K_{n-1}[\chi]$, 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 and $g\in\chi^j-K_{j-1}[\chi]$ be 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 $\nu(\chi^n-K_{n-1}[\chi])$. □

Remark 3.38. In the proof of 3) of Theorem 3.37 we showed that, for every strict key degree d, $G_\nu(K_{d-1}[\chi])$ is a graded algebra. So, Remark 3.8 2) remains true without the restriction $d\leq[K[\chi]:K]/2$. Furthermore, if d is a separate strict key degree, then $d\leq[K[\chi]:K]/2$. It follows that the field K_Φ of Notation 3.5 is defined (where Φ is a monic polynomial of degree d such that $\nu(\Phi)$ is the maximum of $\nu(\chi^d-K_{d-1}[\chi])$). Note that the graded algebra $G_\nu(K_{d'-1}[\chi])$ is greater than $G_\nu(K_{d-1}[\chi])$ if, and only if, d is a strict separate key degree.

We deduce a characterization of valuational key degrees.

Proposition 3.39. *Let ν be a p-m 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 d is a strict key degree, and 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 strict key polynomial.*

Proof. $\Rightarrow$ follows from the definition and Corollary 3.7. 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 d is a strict key polynomial. Since $\nu(\phi)$ is the maximum of $\nu(\chi^d - K_{d-1}[\chi])$, d is a separate key degree. □

Corollary 3.40. *Let ν be a p-m 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 strict key degree.*

Now we show that if d is a strict key degree such that χ^d is limit over $K_{d-1}[\chi]$, then d is the greatest strict key degree.

Proposition 3.41. *Let $d \geq 2$, $\nu' \leq \nu$ be p-m 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 key polynomial for ν and ν', and $\nu' = \nu'_\Phi$.
2) The Φ_i's are strict 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 strict key degree greater than d.

Proof. 1) By Lemma 3.31, Φ is a key polynomial for ν', $\nu' = \nu'_\Phi$, and Φ is a strict key polynomial for ν. Hence d is a strict 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 Lemma 3.31, Φ_i is a strict 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 $f = f_{i,k}\Phi_i^k + \cdots + f_{i,1}\Phi_i + f_{i,0}$, 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 $\nu(f_{i,j}\Phi^j) > \nu(f)$. It follows that $\nu(f) = \nu(f_{i,0}) = \nu_{\Phi_i}(f)$. Since the sequence (ν_{Φ_i}) is increasing, 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 Lemma 3.33 1), f is not a strict key polynomial for ν. Hence d' is not a strict key degree. □

Remark 3.42. Example 1.27 shows that in Proposition 3.41 we cannot take χ^d pseudo-limit over $(K_{d-1}[\chi], \nu)$ instead of χ^d limit over $(K_{d-1}[\chi], \nu)$. Furthermore, in Example 1.27, 1 is an immediate key degree, and the following key degree is d, which is a separate key degree. So, the immediate key degrees are not necessarily greater than the separate ones.

3.6. **Key polynomials and graded algebras of valuations.** Let Φ be a strict key polynomial, and d be its degree. We saw in Remark 3.8 (2) that $G_\nu(K_d - 1)[\chi])$ is a subalgebra of $G_\nu(K[\chi])$; trivially, $\nu(\Phi)$ is not the maximum of $\nu(\chi^d - K_{d-1}[\chi])$ if, and only if, there is $f \in K_{d-1}[\chi]$ such that $\nu(\Phi - f) > \nu(\Phi)$. Now, $\nu(\Phi - f) > \nu(\Phi)$ is equivalent to $\nu(\Phi) = \nu(f) = \nu_\Phi(\Phi - f) < \nu(\Phi - f)$. Therefore, the irreducible polynomial of $in_\nu(\Phi)$ over $G_\nu(K_{d-1}[\chi])$ has degree 1 if, and only if, $\nu(\Phi)$ is not the maximum of $\nu(\chi^d - K_{d-1}[\chi])$.

Assume that $\nu(\Phi)$ is the maximum of $\nu(\chi^d - K_{d-1}[\chi])$ (so d is a separate strict key degree). By Theorem 3.37, d divides the next strict key degree d', and in the proof of this theorem we saw that $\frac{d'}{d}$ is the degree of the irreducible polynomial of $in_\nu(\Phi)$ over $G_\nu(K_{d-1}[\chi])$.

Assume that $\nu(\Phi) < \max \nu(\chi^d - K_{d-1}[\chi])$, and let $X - in_\nu(f)$ be its irreducible polynomial of $in_\nu(\Phi)$ over $G_\nu(K_{d-1}[\chi])$, with $f \in K_{d-1}[\chi]$. So, $\nu(\Phi) < \nu(\Phi - f)$. We let $\Phi_2 = \Phi - f$. If d is an immediate

key degree, then in this way we can construct a sequence (Φ_i) of key polynomials such that the sequence $(\nu(\Phi_i))$ is increasing.

In any case, for $f = f_n\Phi^n + f_{n-1}\Phi^{n-1} + \cdots + f_1\Phi + f_0$, where $f_0, \dots, f_{n-1}$ belong to $K_{d-1}[\chi]$, set

$$S_\Phi(f) = \{i \in \{0, \dots, n\} \mid \nu(f_i) + i\nu(\Phi) = \nu_\Phi(f) = \min(\nu(f_n) + n\nu(\Phi), \cdots, \nu(f_1) + \nu(\Phi), \nu(f_0))\},$$

and $in_{\nu,\Phi}(f)(X) = \sum_{i \in S_\Phi(f)} in_\nu(f_i)X^i$. Then, $\nu_\Phi(f) < \nu(f) \Leftrightarrow in_{\nu,\Phi}(f)(in_\nu(\Phi)) = 0$. This in turn is equivalent to saying that the irreducible polynomial of $in_\nu(\Phi)$ over $G_\nu(K_{d-1}[\chi])$ divides $in_{\nu,\Phi}(f)(X)$.

With above notations, let $g = \sum_{i \in S_\Phi(f)} f_i\Phi^i$. Then, $\nu_\Phi(g) < \nu(g)$, and we can say that g is *homogeneous with respect to* Φ. We have $in_{\nu,\Phi}(g)(X) = in_{\nu,\Phi}(f)(X)$. Assume that $]\nu_{\Phi_{d_k}}(g), \nu(g)[$ is nonempty and let $\gamma \in]\nu_{\Phi_{d_k}}(g), \nu(g)[$, $h_i\Phi_{d_k}^i$ be a monomial of valuation γ, and $h = g + h_i\Phi^i$. Then, $in_{\nu,\Phi}(h)(in_\nu(\Phi)) = in_{\nu,\Phi}(f)(in_\nu(\Phi))$, $\nu_\Phi(h) = \nu(f)$, and $\nu(h) = \gamma$. If we let Φ' be a lifting of the irreducible polynomial of $in_\nu(\Phi)$ over $G_\nu(K_{d-1}[\chi])$, then Φ' is a strict key polynomial of degree d'. Now, as we showed above, a priori we can't assume that $\nu(\Phi')$ is maximal, as required in Theorem 3.37.

If $(K(\chi)|K, \nu)$ is an immediate extension, then $G_\nu(K(\chi)) = G_\nu(K)$. So we see that if Φ is an immediate key polynomial, then its image $in_\nu(\Phi)$ in $G_\nu(K(\chi))$ is already in $G_\nu(K)$. More generally, if Φ is an immediate key polynomial of degree d, then $in_\nu(\Phi)$ belongs to $G_\nu(K_{d-1}[\chi])$.

Let $d_{k_1} < \cdots < d_{k_i} < \cdots$ be the separate strict key degrees, and for every k_i, $\Phi_{d_{k_i}}$ is a key polynomial of degree d_{k_i} such that $\nu(\Phi_{d_{k_i}})$ is the maximum of $\nu(\chi^{d_{k_i}} - K_{d_{k_i}-1}[\chi])$. We saw in the proof of Proposition 3.37 3) that the family $(in_\nu(\Phi_{d_{k_i}})^{e_j})$, where $0 \le e_j \le \frac{d_{k_i+1}}{d_{k_i}}$, is a basis of the $G_\nu(K_{d_{k_i}-1}[\chi])$-module $G_\nu(K_{d_{(k_i+1)}-1}[\chi])$. Now, if d_k is an immediate key degree, we also noticed in the proof of Proposition 3.37 3) that $G_\nu(K_{d_k-1}[\chi]) = G_\nu(K_{d_{(k+1)}-1}[\chi])$. Assume that $k_i + 1 \neq k_{(i+1)}$, i.e. $k_i + 1$ is an immediate key degree. Then, we get by induction: $G_\nu(K_{d_{(k_i+1)}-1}[\chi]) = G_\nu(K_{d_{(k_i+2)}-1}[\chi]) = \cdots = G_\nu(K_{d_{k_{(i+1)}}-1}[\chi])$. Hence the family $(in_\nu(\Phi_{d_{k_i}})^{e_j})$, where $0 \le e_j \le \frac{d_{k_i+1}}{d_{k_i}}$, is a basis of the $G_\nu(K_{d_{k_i}-1}[\chi])$-module $G_\nu(K_{d_{k_{(i+1)}}-1}[\chi])$. Therefore, the family $(in_\nu(\Phi_{d_{k_1}}^{e_1} \cdots \Phi_{d_{k_i}}^{e_i}))$, where $0 \le e_1 \le \frac{d_{k_1+1}}{d_{k_1}}, \dots, 0 \le e_i \le \frac{d_{k_i+1}}{d_{k_i}}$, is a basis of the $G_\nu(K)$-module $G_\nu(K_{d_{k_i}-1}(\chi))$. It follows that the family of all $in_\nu(\Phi_{d_{k_1}}^{e_1} \cdots \Phi_{d_{k_i}}^{e_i})$'s is a basis of the $G_\nu(K)$-module $G_\nu(K(\chi))$.

4. Approximations of valuations of $K(\chi)|K$.

In the same way as S. MacLane and M. Vaquié, we define families of polynomials and associated separate valuations in order to calculate the valuation of any element of $K[\chi]$. We start with the case of separate extensions. Next we will study immediate and dense extensions. Note that they require properties of pseudo-Cauchy sequences of Subsection 1.3. Finally, we will turn to the general case.

4.1. **Separate extensions.**

Theorem 4.1. *Let ν be a multiplicative valuation on $K(\chi)$, $d \ge 1$ such that $d < [K[\chi] : K]$, and $d_1 < \cdots < d_k$ be the sequence of strict key degrees which are at most equal to d. Then $(K_d[\chi]|K, \nu)$ is separate over K if, and only if, $d_1, \dots, d_k$ are separate key degrees. Assume that this holds, and let $\Phi_{d_1}, \dots, \Phi_{d_k}$ be key polynomials associated to the key degrees $d_1, \dots, d_k$, with $\nu(\Phi_i) = \max(\nu(\chi^{d_i} - K_{d_i-1}[\chi]))$ $(1 \le i \le k)$. Then the restrictions of ν and $\nu_{\Phi_{d_1},\dots,\Phi_{d_k}}$ to $K_d[\chi]$ are equal.*

Proof. By Proposition 2.19, if $(K_d[\chi], K, \nu)$ is separate, then $d_1, \dots, d_k$ are separate key degrees. Now, assume that $d_1, \dots, d_k$ are separate key degrees. By Theorem 3.37 2), the restrictions of ν and ν_{Φ_1} to $K_{d_2-1}[\chi]$ are equal. This is equivalent to saying that $(1, \Phi, \dots, \Phi^{d_2-1})$ is a separate K-basis of $K_{d_2-1}[\chi]$. It follows by induction and by Theorem 3.37 4) that $(K_d[\chi]|K, \nu)$ is separate. By Theorem 3.37 2), for every j, $1 \le j \le k$, the restrictions of ν and ν_{Φ_j} to $K_{d_{j+1}-1}[\chi]$ are equal. Hence by induction $\nu = \nu_{\Phi_1,\dots,\Phi_k}$. □

Remark 4.2. Let $(K(\chi)|K, \nu)$ be a separate algebraic extension of valued fields. Then the valuation ν is determined by its restriction to K and by the couples $(\Phi_1, \nu(\Phi_1)), \dots, (\Phi_k, \nu(\Phi_k), \dots)$.

Theorem 4.1 holds for example if (K, ν) is maximal (see Proposition 2.14). It also holds if χ is algebraic over K and (K, ν) is henselian with residue characteristic 0 (see Theorem 2.15).

4.2. **Immediate and dense extensions.** If χ is pseudo-limit over (K,ν), then defining a pseudo-Cauchy sequence (x_i) with pseudo-limit χ is equivalent to defining a sequence of key polynomials $\Phi_i = \chi - x_i$ such that the sequence $(\nu(\Phi_i))$ is increasing and cofinal in $\nu(\chi - K[\chi])$. So, the key polynomials can be seen as generalizations of the pseudo-Cauchy sequences, as noted M. Vaquié in [V 07]. In this subsection we deepen the links between these two notions.

Theorem 4.3. *Let $(K(\chi)|K,\nu)$ be an extension of valued fields and (x_i) be a pseudo-Cauchy sequence without pseudo-limit in K and which pseudo-converges to χ. For every i we set $\Phi_i = \chi - x_i$.*
1) If (x_i) is of transcendental type, then $(K(\chi)|K,\nu)$ is immediate, χ is transcendental over K and 1 is the unique key degree. For every i and $f \in K[\chi]$, we have: $\nu(f) = \nu_{\Phi_i}(f) \Leftrightarrow \nu_{\Phi_i}(f) = \nu_{\Phi_{i+1}}(f)$.
2) Assume that $(K(\chi)|K,\nu)$ is immediate, that (x_i) is of algebraic type, and let d be the degree of its irreducible polynomial.
a) If $d = [K[\chi]:K]$, then 1 is the unique key degree.
b) Otherwise, d is the second key degree.
c) In any case, for every $i \geq 1$ and $f \in K_{d-1}[\chi]$, we have: $\nu(f) = \nu_{\Phi_i}(f) \Leftrightarrow \nu_{\Phi_i}(f) = \nu_{\Phi_{i+1}}(f)$.

Proof. If (x_i) is of transcendental type, then, by Remark 1.20, χ is transcendental, and we deduce from Lemma 1.22 that $(K(\chi)|K,\nu)$ is immediate. We now assume that the extension $(K(\chi)|K,\nu)$ is immediate. Let $f(X) \in K[X]$ (the ring of formal polynomials). In the same way as in Proposition 1.12, we let $f(X) = (X-x_i)^n f_{(n)}(x_i) + \cdots + (X-x_i)f_{(1)}(x_i) + f(x_i)$ be the Taylor expansion of $f(X)$. Then $f(\chi) = (\chi-x_i)^n f_{(n)}(x_i) + \cdots + (\chi-x_i)f_{(1)}(x_i) + f(x_i)$. Hence $\nu_{\Phi_i}(f(\chi)) = \min((n-1)\nu(\chi-x_i) + \nu(f_{(n-1)}(x_i)), \ldots, \nu(\chi-x_i)+\nu(f_{(1)}(x_i)), \nu(f(x_i)))$. Since the sequences $(\nu(f_{(j)}(x_i)))$ are increasing or eventually constant, the sequences $(\nu((\chi-x_i)^n f_{(n)}(x_i))), \ldots, (\nu((\chi-x_i)f_{(1)}(x_i)))$ are increasing. Hence, if $(\nu(f(x_i))$ is eventually equal to $\nu(f(\chi))$, then $\nu_{\Phi_i}(f(\chi))$ is eventually equal to $\nu(f(x_i)) = \nu(f(\chi))$. Furthermore, if the minimum of $(n-1)\nu(\chi-x_i) + \nu(f_{(n-1)}(x_i)), \ldots, \nu(\chi-x_i)+\nu(f_{(1)}(x_i)), \nu(f(x_i))$ is not $\nu(f(x_i))$, then $\nu_{\Phi_{i+1}}(f) > \nu_{\Phi_i}(f)$. If the minimum is $\nu(f(x_i))$, then at the next step it will be $\nu(f(x_{i+1}))$. It follows: $\nu_{\Phi_i}(f) = \nu(f) \Leftrightarrow \nu_{\Phi_i}(f) = \nu_{\Phi_{i+1}}(f)$. This proves 1), 2) a) and 2) c).

2) b) In the same way as above, if $n < d$, then $\nu_{\Phi_i}(f(\chi))$ is eventually equal to $\nu(f(\chi))$. So, the second key degree is at least equal to d. Now, let $g(X)$ be the irreducible polynomial of the sequence (x_i). Since the sequence $(\nu(g(x_i)))$ is increasing, the sequence $(\nu_{\Phi_i}(g(\chi)))$ is increasing. It follows that, for every i, $\nu_{\Phi_i}(g(\chi)) < \nu(g(\chi))$. By Theorem 3.36 2), d is the second key degree. □

Corollary 4.4. *Assume that (K,ν) is algebraically maximal and that χ is pseudo-limit over (K,ν). Then 1 is the unique key degree.*

Proof. Let (x_i) be a pseudo-Cauchy sequence without pseudo-limit in K and which pseudo-converges to χ. By Proposition 1.24 (x_i) is of transcendental type. We conclude by Theorem 4.3 1). □

Now, we turn to dense extensions. Recall that by Proposition 1.11 saying that $(K(\chi)|K,\nu)$ is a dense extension is equivalent to saying that χ is limit over (K,ν).

Lemma 4.5. *Let $(K(\chi)|K,\nu)$ be a dense extension of valued fields and (x_i) be a pseudo-Cauchy sequence without pseudo-limit in K and which pseudo-converges to χ. Then (x_i) is of algebraic type over (K,ν) if, and only if, χ is algebraic over K. If this holds, then the irreducible polynomial of the sequence (x_i) over (K,ν) is equal to the irreducible polynomial of χ over K.*

Proof. Assume that χ is algebraic over K and let f be its irreducible polynomial. We let $f(x) = (x_i-\chi)^n f_{(n)}(\chi) + \cdots + (x_i-\chi)f_{(1)}(\chi)$ be the Taylor expansion of $f(x_i)$. Since $f(X)$ is not constant, one of the $f_{(j)}(\chi)$, $1 \leq j \leq n$, is different from 0. Then

$$\nu(f(x_i)) \geq \min_{1\leq j\leq n} \nu((x_i-\chi)^j f_{(j)}(\chi)) = \min_{1\leq j\leq n} j\nu(x_i-\chi) + \nu(f_{(j)}(\chi))$$

which is cofinal in νK. Hence (x_i) is of algebraic type over (K,ν).

Assume that (x_i) is of algebraic type over (K,ν), let g be the irreducible polynomial of the sequence (x_i) over (K,ν) and $g(\chi) = (\chi-x_i)^d g_{(d)}(x_i) + \cdots + (\chi-x_i)g_{(1)}(x_i) + g(x_i)$ be the Taylor expansion of $g(\chi)$. By hypothesis, the sequences $(g_{(d)}(x_i)), \ldots, (g_{(1)}(x_i))$ are eventually constant and $(\nu(\chi-x_i))$ is cofinal in νK. Hence $(\nu(g(\chi)-g(x_i)))$ is cofinal in νK. Since $(\nu(g(x_i)))$ is increasing, it follows that $g(\chi) = 0$. Indeed, otherwise $(\nu(g(\chi)-g(x_i)))$ is eventually equal to $\nu(g(\chi))$: a contradiction. Hence, χ is algebraic over K, and its irreducible polynomial divides g. Now, g is irreducible, hence g is the irreducible polynomial of χ. □

Theorem 4.6. *Let $(K(\chi)|K,\nu)$ be a dense extension of valued fields. Then 1 is the unique key degree.*

Proof. Let (x_i) be a pseudo-Cauchy sequence without pseudo-limit in K and which pseudo-converges to χ. If χ is transcendental over K, then by Lemma 4.5 (x_i) is of transcendental type. Now, by Theorem 4.3 1), 1 is the unique key degree. Assume that χ is algebraic over K. By Lemma 4.5, (x_i) is of algebraic type and the degree of the irreducible polynomial of the sequence (x_i) is $[K(\chi):K]$. Hence by Theorem 4.3 2) a), 1 is the unique key degree. □

Proposition 4.7. *Assume that χ is separable algebraic over K and let ν be an archimedean valuation on the Galois extension L generated by $K(\chi)$ such that $(L|K,\nu)$ is immediate and defectless. We let (x_i) be a pseudo-Cauchy sequence of K, without a pseudo-limit in (K,ν) and with pseudo-limit χ. For every i we set $\Phi_i = \chi - x_i$. Then ν is the limit of the sequence of separate p-m valuations ν_{Φ_i}. For $f \in K[\chi]$, the sequence $\nu_{\Phi_i}(f)$ is eventually equal to $\nu(f)$. Furthermore, $\nu_{\Phi_i}(f) = \nu(f)$ if, and only if, $\nu_{\Phi_i}(f) = \nu_{\Phi_{i+1}}(f)$.*

Proof. Since $(K(\chi)|K,\nu)$ is archimedean, immediate and defectless, it is dense (see Theorem 1.10). Now the result follows from Theorems 4.6 and 4.3. □

Theorem 4.8. *Assume that ν is an archimedean valuation on $K(\chi)$ and that every algebraic extension of (K,ν) is Galois and defectless. We assume that χ is pseudo-limit over (K,ν) and we let (x_i) be a pseudo-Cauchy sequence of (K,ν) without limit in (K,ν) and which pseudo-converges to χ. For every i we set $\Phi_i = \chi - x_i$. Let $f \in K[\chi]$. Then the sequence $(\nu(f(x_i)))$ is eventually equal to $\nu(f(\chi))$, and for every i we have: $\nu(f) = \nu_{\Phi_i}(f) \Leftrightarrow \nu_{\Phi_i}(f) = \nu_{\Phi_{i+1}}(f)$.*

Proof. If (x_i) is of transcendental type, then this follows from Theorem 4.3 1). Assume that (x_i) is of algebraic type and let $g(X)$ be its irreducible polynomial over (K,ν). Let y be a root of g in any algebraic extension of K. By Proposition 1.21, ν extends to $K(y)$ in such a way that $(K(y)|K,\nu)$ is immediate. By hypothesis, $(K(y)|K,\nu)$ is Galois and defectless. Hence by Theorem 1.10 $(K(y)|K,\nu)$ is dense, so the sequence $(\nu(y-x_i))$ is cofinal in νK. Now, for every i we have $\nu(y-x_i) = \nu(x_{i+1}-x_i) = \nu(\chi - x_i)$. It follows that χ is limit over (K,ν). Now, by Proposition 1.11, the extension $(K(\chi)|K,\nu)$ is dense. So, the result follows from Proposition 4.7. Note that by Lemma 4.5, χ is algebraic over K, and g, is its irreducible polynomial. □

The condition that every algebraic extension of (K,ν) is Galois and defectless holds if the residue characteristic is 0. Now, it can hold for other fields, for example the fields which are called tame. For more details see the online book [FVK].

4.3. **General case.**

Definition 4.9. Let ν be a p-m valuation on $K(\chi)$, $1 = d_1 < d_2 < \cdots < d_k < \cdots$ be the sequence of strict key degrees of ν. Let $\mathcal{F}$ be a family of strict key polynomials which satisfies the following properties for every $k \geq 1$.
If d_k is a separate key degree, then $\mathcal{F}$ contains exactly one strict 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 strict 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 $\nu(\chi^{d_k} - K_{d_k-1}[\chi])$.
Then we say that $\mathcal{F}$ is a *defining family of key polynomials for ν*.

Remark 4.10. For every p-m valuation on $K[\chi]$ there exists a defining family of key polynomials.

Theorem 4.11. *Let ν be a p-m valuation on $K(\chi)$, $1 = d_1 < d_2 < \cdots < d_k < \cdots$ be the sequence of strict key degres of ν and $\mathcal{F}$ be a defining family of key polynomials for ν. If d_k is a separate key degree, then we let Φ_{d_k} be the unique strict key polynomial of degree d_k in $\mathcal{F}$, and for every integer m we set $\Phi_{d_k,m} = \Phi_{d_k}$. If d_k is an immediate key degree, then we let $(\Phi_{d_k,m})$ be the sequence of strict key polynomial of degree d_k in $\mathcal{F}$ such that the sequence $(\nu(\Phi_{d_k,m}))$ is increasing and cofinal in $\nu(\chi^{d_k} - K_{d_k-1}[\chi])$.*
For every k, $m_1, \ldots, m_k$, we let $\nu_{(m_1,\ldots,m_k)} = \nu_{\Phi_{d_1,m_1},\ldots,\Phi_{d_k,m_k}}$ (see Notations 3.16 and Remark 3.25). Then ν is the supremum of the family $(\nu_{(m_1,\ldots,m_k)})$ of separate K-module valuations. For every f, $\nu(f)$ is the maximum of the family $(\nu_{(m_1,\ldots,m_k)}(f))$, and there are infinitely many $(m_1,\ldots,m_k)$'s such that $(\nu_{(m_1,\ldots,m_k)}(f)) = \nu(f)$.

Proof. Note that, for every k, $m_1, \ldots, m_k$, we have $\nu_{(m_1,\ldots,m_k)} \leq \nu$. 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 3.37 and 3.36, 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 $f = f_j\Phi^j_{d_k,m_k} + \cdots + f_1\Phi_{d_k,m_k} + f_0$, where f_0, $f_1, \ldots,$ f_j belong to $K_{d_k-1}[\chi]$. We know that there is some m_{k-1} such that $\nu(f_0) = \nu_{\Phi_{d_{k-1},m_{k-1}}}(f_0), \ldots,$ $\nu(f_j) = \nu_{\Phi_{d_{k-1},m_{k-1}}}(f_j)$. 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 $(m_1,\ldots,m_k)$ such that $\nu(f) = \nu_{(m_1,\ldots,m_k)}(f)$.

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

Remark 4.12. Let d be the degree of f and $d_1 < \cdots < d_k$ be the sequence of strict key degrees which are at most equal to d. If $d_1, \ldots, d_k$ are separate key degrees, then $\nu_{(m_1,\ldots,m_k)} = \nu_{(m'_1,\ldots,m'_k)}$ for every k-uples $(m_1,\ldots,m_k)$ and $(m'_1,\ldots,m'_k)$. Hence, in fact all the K-module valuations $\nu_{(m_1,\ldots,m_k)}$ are equal. Note that the restrictions of ν and $\nu_{(m_1,\ldots,m_k)}$ to $K_d[\chi]$ are equal. Now, if at least one of $d_1, \ldots, d_k$ is

an immediate key degree, then there are indeed infinitely many distinct K-module valuations $\nu_{(m_1,\dots,m_k)}$ such that $\nu_{(m_1,\dots,m_k)}(f) = \nu(f)$.

In order to get an algorithm for calculating $\nu(f)$, for any $f \in K[\chi]$, by means of the valuations $\nu_{(m_1,\dots,m_k)}$, we need a criterion to know whether some $\nu_{(m_1,\dots,m_k)}(f)$ is the maximum of the family $(\nu_{(m_1,\dots,m_k)}(f))$. If the extension is separate, or dense, we saw in Subsection 4.1 and 4.2 that this criterion exists. Now, the dense case can be generalized, as shows the following proposition.

Proposition 4.13. *With the same hypothesis as in Theorem 4.11, assume that there is one immediate key degree d_k. Then, there is an algorithm for calculating $\nu(f)$, for any $f \in K[\chi]$.*

Proof. By Theorem 4.1 the restrictions of ν and $\nu_{\Phi_{d_1},\dots,\Phi_{d_{k-1}}}$ to $K_{d_k-1}[\chi]$ are equal. By 2) of Theorem 3.36, for every $f \in K_{d_{k+1}-1}[\chi]$ there is an integer m such that $\nu(f) = \nu_{\Phi_{d_k},m}(f)$. Now, since the sequence $(\nu_{\Phi_{d_k},m})$ is increasing, the family $(\nu_{\Phi_{d_k},m}(f))$ is eventually equal to $\nu(f)$. Hence $\nu_{\Phi_{d_k},m}(f) = \nu(f)$ if, and only if, $\nu_{\Phi_{d_k},m}(f) = \nu_{\Phi_{d_k},m+1}(f)$. Now, since the restrictions of ν and $\nu_{\Phi_{d_1},\dots,\Phi_{d_{k-1}}}$ to $K_{d_k-1}[\chi]$ are equal, $\nu_{\Phi_{d_k},m} = \nu_{\Phi_{d_1},\dots,\Phi_{d_{k-1}},\Phi_{d_k},m}$. For $j > k$, there is only one strict key polynomial Φ_{d_j} of degree d_j in the family, and for every f of degree in $\{d_j,\dots,d_{j+1}-1\}$ we have $\nu_{\Phi_{d_j}}(f) = \nu(f)$. Hence we can follow in the same way as in the proof of Theorem 4.11. The algorithm is the following: we let d_n be the greatest key degree which is at most equal to the degree of f. We compute $\nu_{\Phi_{d_1},m,\dots,\Phi_{d_n},m}(f)$ until $\nu_{\Phi_{d_1},m,\dots,\Phi_{d_n},m}(f) = \nu_{\Phi_{d_1},m-1,\dots,\Phi_{d_n},m-1}(f)$ holds. □

Now, in general, a priori $m'_1 \geq m_1,\dots,m'_k \geq m_k$ and $\nu_{(m_1,\dots,m_k)}(f) = \nu(f)$ does not imply $\nu_{(m'_1,\dots,m'_k)}(f) = \nu(f)$. So we cannot get a similar criterion.

In the case of a discrete archimedean valuation (in other words, $\nu K \simeq \mathbb{Z}$), every increasing sequence of νK is cofinal. Hence, if $\nu(\chi^d - K_{d-1}[\chi])$ has no maximal element, then it is cofinal. Therefore, χ^d is limit over $K_{d-1}[\chi]$ and by Proposition 3.41 $(K[\chi]|K_{d-1}[\chi],\nu)$ is dense and d is the greatest key degree. Consequently, the first strict key degrees are separate and there is at most one immediate strict key degree. So, as we noted above, there exists an algorithm for calculating $\nu(f)$, for every $f \in K[\chi]$. This is the case studied by S. MacLane ([ML 36a] and [ML 36b]).

Now, Theorems 3.36 and 3.37 show that, given the key polynomials associated to a strict key degree, we can define the next key degree. So, we can construct key polynomials by induction on the degrees. We get a construction similar to the construction of M. Vaquié in [V 07]. Now, in Theorem 4.11 the definition of the key polynomials of a given key degree is independent from the key polynomials of preceding key degrees. We will not go into the details of the constructions of families of key polynomials of [HOS 07] and [V 07], because it is not the purpose of this paper and it would take up too much space. We will only note some aspects related to previous studies. However, we will use the construction of [HOS 07] in an example at the end of next section.

In the case of a strict separate key degree d, M. Vaquié takes a monic polynomial Φ such that $\nu(\Phi)$ is maximal in $\nu(\chi^d - K_{d-1}[\chi])$. In the immediate case, he takes a sequence of monic polynomials such that the sequence of their valuations is cofinal in $\nu(\chi^d - K_{d-1}[\chi])$. So, our construction of the strict key polynomials is the same as the construction of M. Vaquié.

The construction of [HOS 07] can be seen as a kind of algorithm for building the key polynomials by induction. The first key polynomial is 1, the second is χ. For a polynomial $h(X) = x_nX^n + \cdots + x_1X + x_0$ in $K[X]$ let

$$S = \{i \in \{0,\dots,n\} \mid \nu(x_i) + i\nu(\chi) = \nu_\chi(h(\chi)) = \min(\nu(x_n) + n\nu(\chi),\cdots,\nu(x_1) + \nu(\chi),\nu(x_0))\}$$

and $in_{\nu,\chi}(h)(X)$ be the polynomial $\sum_{i\in S} in_\nu(x_i)X^i$. So that $in_{\nu,\chi}(h)(in_\nu(\chi))$ is a homogeneous element of $G_\nu(K)$ (i.e. all its non zero monomials belong to the same $(K(\chi))_{\gamma,\nu}$). They take a monic polynomial $h(X)$ such that $\nu(h(\chi)) > \nu_\chi(h(\chi)) = \min(n\nu(\chi),\nu(x_{n-1}) + (n-1)\nu(\chi),\cdots,\nu(x_1) + \nu(\chi),\nu(x_0))$ (for example the irreducible polynomial of χ over K, if χ is algebraic over K). Then $in_{\nu,\chi}(h)(in_\nu(\chi)) = 0$ in $G_\nu(K)$. They decompose $in_{\nu,\chi}(h)(X)$ into irreducible factors and they take the irreducible polynomial of $in_\nu(\chi)$ over $G_\nu(K)$, which is one of the irreducible factors of $in_{\nu,\chi}(h)(X)$. They let $\Phi_2(\chi) \in K[\chi]$ be a homogeneous polynomial such that $in_{\nu,\chi}(\Phi_2)(X)$ is this irreducible polynomial. Note that they require that the separate key polynomials be homogeneous.

Let $f \in K[\chi]$, $d_1,\dots,d_n$ be the strict key degrees which are at most equal to $\deg(f)$, and for every d_j let Φ_{d_j} be a strict key polynomial of degree d_j. We saw that $\nu_{\Phi_{d_1},\dots,\Phi_{d_n}}(f)$ is obtained by writing f as a linear combination of the elements of the basis generated by $\Phi_{d_1},\dots,\Phi_{d_n}$. Such a linear combination is called a standard expansion in [HOS 07].

5. Decomposition, inertia and ramification fields.

Immediate, residual and valuational key degrees appear in the study of strict key degrees. Now, the decomposition field, the inertia field and the ramification field carry interesting informations on algebraic

extensions of valued fields. The decomposition field can be seen as an immediate step, the inertia field as a residual step and the ramification field as a valuational step. Now, we will see in some examples that, in general, the degrees of the polynomials generating those subfields and the key degrees are not related.

5.1. **Definitions.** First we recall the definitions and properties of the decomposition, inertia and ramification fields (see for example [E 72] Chapters 15, 19, 20, 21 or [Bo 59]). We let $(L|K,\nu)$ be a normal extension of valued fields, A be the valuation ring of (L,ν) and G be the group of K-automorphisms of L. If the characteristic of K_ν is 0, then we let $p=1$. Otherwise, p is the characteristic of K_ν. If the characteristic of K is 0, then we let $p'=1$. Otherwise, we let $p'=p$.

We denote by K_{ins} the fixed field of G. Then, νK_{ins} is a p' extension of νK, and $(K_{ins})_\nu|K_\nu$ is purely inseparable.

The *decomposition group* of $(L|K,\nu)$ is $G_Z=\{\sigma\in G \mid \nu\circ\sigma=\nu\}$. It is a closed subgroup of G. The fixed field K_Z of G_Z is called the *decomposition field* of $(L|K,\nu)$. The extension $L|K_Z$ is a Galois extension, $(K_Z|K_{ins},\nu)$ is immediate, and the number of extensions of $\nu_{|K}$ to K_Z is equal to the number of extensions of $\nu_{|K}$ to L.

The *inertia group* of $(L|K,\nu)$ is $G_T=\{\sigma\in G \mid \forall x\in A\ \nu(\sigma(x)-x)>0\}$. It is a closed subgroup of G and a normal closed subgroup of G_Z. The fixed field K_T of G_T is called the *inertia field* of $(L|K,\nu)$. The extensions $L|K_T$ and $K_T|K_Z$ are Galois extensions, $\nu K_T=\nu K_Z$, $(K_T)_\nu$ is the separable closure of $(K_Z)_\nu$, $(K_T)_\nu|(K_Z)_\nu$ is a Galois extension and its Galois group $\mathrm{Gal}((K_T)_\nu|(K_Z)_\nu)$ is isomorphic to $\mathrm{Gal}(K_T|K_Z)$.

The *ramification group* of $(L|K,\nu)$ is $G_V=\{\sigma\in G \mid \forall x\in A\backslash\{0\}\ \nu(\sigma(x)/x-1)>0\}$. It is a normal closed subgroup of G_T and of G_Z. The fixed field K_V of G_V is called the *ramification field* of $(L|K,\nu)$. The extensions $L|K_V$ and $K_V|K_T$ are Galois extensions, $\mathrm{Gal}(K_V|K_T)$ is abelian, νK_V is a p-free extension of νK_T, $(K_V)_\nu=(K_T)_\nu$ and $L_\nu|(K_V)_\nu$ is purely inseparable.

Now, we assume that $L|K$ is a finite Galois extension. Hence $K_{ins}=K$ and there is a primitive element χ such that $L=K(\chi)$. Denote by $f(X)$ the irreducible polynomial of χ over K. Since all the extensions are separable, there exist polynomials $g_1(X)$, $g_2(X)$ and $g_3(X)$ in $K[X]$ such that $K_Z=K(g_1(\chi))$, $K_T=K(g_2(\chi))$ and $K_V=K(g_3(\chi))$. For $i\in\{1,2,3\}$ let $h_i(X)$ be the irreducible polynomial of $g_i(\chi)$ over K. Then $h_i(g_i(\chi))=0$, hence $f(X)$ divides $h_i\circ g_i(X)$. Now, the degree of $h_i(X)$ is $[K(\chi):K(g_i(\chi))]$, and the degree of $f(X)$ is $[K(\chi):K]=[K(\chi):K(g_i(\chi))][K(g_i(\chi)):K]$. Hence the degree of $g_i(X)$ is at least equal to $[K(g_i(\chi)):K]$. Since every subspace of the vector space $K(\chi)$ contains a basis of polynomials whose degrees are pairwise distinct, $K(g_i(\chi))$ contains a polynomial $g(\chi)$ such that the degree of $g_i(X)$ is at most equal to $[K(\chi):K]-[K(g_i(\chi)):K]+1$. In particular, K_Z contains a monic polynomial $g(\chi)$ such that the degree d of $g(X)$ is at most equal to $|G|-(|G|/|G_Z|)+1$, where $|G|$ denotes the cardinality of G. Note that in some cases, every non constant polynomial in $K(g_i(\chi))$ has degree at least equal to $[K(\chi):K]-[K(g_i(\chi)):K]+1$, as shows the example below. Now, assume that νK is archimedean and $(K_Z|K,\nu)$ is defectless. Then, by Theorem 1.10, $\nu(g_1(\chi)-K)=\nu K$. It follows that $\nu K\subset\nu(\chi^{d_1}-K_{d_1-1}[\chi])$, where d_1 is the degree of g_1. Hence $\nu(\chi^{d_1}-K_{d_1-1}[\chi])$ is cofinal in $\nu K(\chi)$. This proves that $\nu(\chi^{d_1}-K_{d_1-1}[\chi])$ is eventually equal to $\nu K(\chi)$.

5.2. **Example.** We study the decomposition, inertia and ramification fields, and the strict key degrees in an example (the author thanks Bruno Deschamps for suggesting this Galois extension). Let $K=\mathbb{Q}$, the field of rational numbers, j be the complex number with positive imaginary part such that $j^3=1$, and $\chi=j+\sqrt[3]{2}$. Then, $\mathbb{Q}(\chi)=\mathbb{Q}(j,\sqrt[3]{2})$, $\mathbb{Q}(\chi)|\mathbb{Q}$ is a Galois extension, its Galois group G is isomorphic to the group S_3 of the permutations of a set of three elements. It is generated by the transposition τ which sends $j+\sqrt[3]{2}$ to $j^2+\sqrt[3]{2}$ and the cycle σ which sends $j+\sqrt[3]{2}$ to $j+j\sqrt[3]{2}$. Then, $\sigma\circ\sigma$, $\sigma\circ\tau$ and $\tau\circ\sigma$ send $j+\sqrt[3]{2}$ respectively to $j+j^2\sqrt[3]{2}$, $j^2+j\sqrt[3]{2}$ and $j^2+j^2\sqrt[3]{2}$. The subfield $\mathbb{Q}(j)$ of $\mathbb{Q}(\chi)$ is the fixed field of the normal subgroup generated by σ. Hence $\mathbb{Q}(j)|\mathbb{Q}$ is a Galois extensions and $[\mathbb{Q}(j):\mathbb{Q}]=2$. The fixed field of the subgroup generated by τ is $\mathbb{Q}(\sqrt[3]{2})$. Since this subgroup is not normal, $\mathbb{Q}(\sqrt[3]{2})|\mathbb{Q}$ is not a Galois extension. We have: $[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]=3$.

In order to show that every non constant polynomial in $\mathbb{Q}(j)$ has degree 5, we start with calculations. The family $(1,j,\sqrt[3]{2},j\sqrt[3]{2},\sqrt[3]{4},j\sqrt[3]{4})$ is a $\mathbb{Q}$ basis of $\mathbb{Q}(\chi)$. In this basis, we have

$$1=1,\ \chi=j+\sqrt[3]{2},\ \chi^2=-1-j+2j\sqrt[3]{2}+\sqrt[3]{4},\ \chi^3=3-3\sqrt[3]{2}-3j\sqrt[3]{2}+3j\sqrt[3]{4},$$

$\chi^4=9j+6\sqrt[3]{2}-6\sqrt[3]{4}-6j\sqrt[3]{4}$, $\chi^5=-21-21j+15j\sqrt[3]{2}+12\sqrt[3]{4}$ and $\chi^6=45-36\sqrt[3]{2}-36j\sqrt[3]{2}+27j\sqrt[3]{4}$. So, in the basis $(1,j,\sqrt[3]{2},j\sqrt[3]{2},\sqrt[3]{4},j\sqrt[3]{4})$ the polynomial $g(\chi)=a_0+a_1\chi+a_2\chi^2+a_3\chi^3+a_4\chi^4+a_5\chi^5+a_6\chi^6$ can be written as

$$g(\chi)=a_0-a_2+3a_3-21a_5+45a_6+j(a_1-a_2+9a_4-21a_5)+\sqrt[3]{2}(a_1-3a_3+6a_4-36a_6)$$
$$+j\sqrt[3]{2}(2a_2-3a_3+15a_5-36a_6)+\sqrt[3]{4}(a_2-6a_4+12a_5)+j\sqrt[3]{4}(3a_3-6a_4+27a_6).$$

By setting $a_6=0$, calculations show that there is no non constant polynomial $g(X)$ of degree less than 5 such that $g(\chi)\in\mathbb{Q}(j)$. In fact the $\mathbb{Q}$ vector space $\mathbb{Q}(j)$ is generated by 1 and $2\chi^5+3\chi^4+6\chi^3-6\chi^2$. In

a similar way, we show that $\mathbb{Q}(\sqrt[3]{2})$ is generated by 1, $\chi^4+2\chi^3+3\chi^2+12\chi$ and $2\chi^5-15\chi^2+27\chi$. The number $\sqrt[3]{2}$ is in the $\mathbb{Q}$-vector space generated by 1 and $2\chi^5+3\chi^4+6\chi^3+3\chi^2+63\chi$.

By setting $a_6=1$ and $g(\chi)=0$, we get the irreducible polynomial of χ over $\mathbb{Q}$: $f(X)=X^6+3X^5+6X^4+3X^3+9X+9$.

Now, we study three valuations on $\mathbb{Q}(\chi)$.

5.2.1. *The 2-adic valuation.* We assume that $\mathbb{Q}$ is equipped with the 2-adic valuation ν_2, which is defined in the following way. We write every positive integer n as $n=\epsilon_0+\epsilon_1\cdot 2+\epsilon_2\cdot 2^2+\cdots+\epsilon_k\cdot 2^k$, where $\epsilon_0,\epsilon_1,\ldots,\epsilon_k$ belong to $\{0,1\}$, and we let $\nu_2(n)$ be the least i such that $\epsilon_i=1$. We let $\nu_2(-n)=\nu_2(n)$, $\nu_2(0)=\infty$ and if $q\neq 0$, then $\nu_2(n/q)=\nu_2(n)-\nu_2(q)$. The valuation group is $\mathbb{Z}$, and the residue field is the field $\mathbb{F}_2$ with two elements.

• Since $\sqrt[3]{2}$ is a root of the polynomial X^3-2, we have $3\nu_2(\sqrt[3]{2})=\nu_2((\sqrt[3]{2})^3)=\nu_2(2)=1$, hence $\nu_2(\sqrt[3]{2})=\frac{1}{3}$. Therefore 3 divides $(\nu_2\mathbb{Q}(\chi):\nu_2\mathbb{Q})$.

• The element j is a root of X^2+X+1, hence $0=\nu_2(1)=\nu_2(j+j^2)=\nu_2(j)+\nu_2(1+j)$. One can see that this implies $\nu_2(j)=0$. It follows that j_{ν_2} is a root of $X^2+X+1_{\nu_2}$, which has no root in $\mathbb{F}_2$. Hence $j_{\nu_2}\notin\mathbb{Q}_{\nu_2}$. Therefore 2 divides $[\mathbb{Q}(\chi)_{\nu_2}:\mathbb{Q}_{\nu_2}]$.

• Since $(\nu_2\mathbb{Q}(\chi):\nu_2\mathbb{Q})\cdot[\mathbb{Q}(\chi)_{\nu_2}:\mathbb{Q}_{\nu_2}]$ divides $[\mathbb{Q}(\chi):\mathbb{Q}]=6$, we have $(\nu_2\mathbb{Q}(\chi):\nu_2\mathbb{Q})=3$, $[\mathbb{Q}(\chi)_{\nu_2}:\mathbb{Q}_{\nu_2}]=2$, $(\nu_2\mathbb{Q}(\chi):\nu_2\mathbb{Q})\cdot[\mathbb{Q}(\chi)_{\nu_2}:\mathbb{Q}_{\nu_2}]=[\mathbb{Q}(\chi):\mathbb{Q}]$. Hence the extension is separate. By Proposition 2.10, the basis $(1,j,\sqrt[3]{2},j\sqrt[3]{2},\sqrt[3]{4},j\sqrt[3]{4})$ is separate.

• Since the extension $(\mathbb{Q}(\chi)|\mathbb{Q},\nu_2)$ is separate, we have $\mathbb{Q}(\chi)_Z=\mathbb{Q}$.

• The extension $\mathbb{Q}(\chi)_{\nu_2}|\mathbb{Q}_{\nu_2}$ is separable since the polynomial X^2+X+1 is. It follows that $[(\mathbb{Q}(\chi)_T)_{\nu_2}:\mathbb{Q}_{\nu_2}]=2$. Since $[\mathbb{Q}(\chi)_T:\mathbb{Q}]=[(\mathbb{Q}(\chi)_T)_{\nu_2}:\mathbb{Q}_{\nu_2}]$, we have $K_T=\mathbb{Q}(j)$. Hence the inertia group G_T is generated by σ.

• Now, $(\nu_2(\mathbb{Q}(\chi)):\nu_2\mathbb{Q})=3\neq 2$, so the extension $\nu_2(\mathbb{Q}(\chi))|\nu_2\mathbb{Q}$ is 2-free. Hence $\mathbb{Q}(\chi)_V=\mathbb{Q}(\chi)$, and G_V is the identity group.

Key degrees. We show that 1 is a residual strict key degree, that 2 is a residual key degree, and that they are the only key degrees. We use the algorithm of [HOS 07]. The image in the graded algebra of the irreducible polynomial $f(X)=X^6+3X^5+6X^4+3X^3+9X+9$ of χ over $\mathbb{Q}$ is $1_{0,\nu_2}X^6+1_{0,\nu_2}X^5+1_{1,\nu_2}X^4+1_{0,\nu_2}X^3+1_{0,\nu_2}X+1_{0,\nu_2}$. Since we consider homogeneous polynomials and $\nu_2(\chi)=0$, we can consider the polynomial of $\mathbb{F}_2[X]$: $X^6+X^5+X^3+X+1_{\nu_2}=(X^2+X+1_{\nu_2})^3$, where $X^2+X+1_{\nu_2}$ is irreducible since it has no root in $\mathbb{F}_2$. In particular χ_{ν_2} is not in $\mathbb{F}_2$. By Proposition 2.10, the basis $1,\chi$ of $\mathbb{Q}_1[\chi]$ is separate. Hence the maximum of $\nu_2(\chi-\mathbb{Q})$ is $\nu_2(\chi)=0$. We let $\Phi_1=\chi$. Note that 1 is a residual strict key degree.

• The polynomial $\Phi_2(X)$ is a lifting of the polynomial $X^2+X+1_{\nu_2}$ of $\mathbb{F}_2[X]$. Now, by letting $g(X)=X^2+X+1\in\mathbb{Q}[X]$, we have $a_0=a_1=a_2=1$ in above notations. Hence $\nu_2\left(\chi^2+\chi+1\right)=\nu_2(\sqrt[3]{2}+2j\sqrt[3]{2}+\sqrt[3]{4})=\frac{1}{3}$, which does not belong to $\mathbb{Z}$. Hence $\frac{1}{3}$ is the maximum of $\nu_2(\chi^2-\mathbb{Q}_1[\chi])$. By Theorem 3.37, 2 is a strict key degree, and we see that it is a valuational key degree. We let $\Phi_2=\chi^2+\chi+1$; Φ_2 is a strict key polynomial of degree 2 with maximal valuation.

• Now, since $\nu_2(j)=0<\frac{1}{3}=\nu_2(\sqrt[3]{2})$, we have $\chi_{\nu_2}=j_{\nu_2}\notin\mathbb{F}_2=\mathbb{Q}_{\nu_2}$. Furthermore, $0=\nu_2(1)$, $\frac{1}{3}=\nu_2(\Phi_2)$ and $\frac{2}{3}=\nu_2(\Phi_2^2)$ are pairwise non-congruent modulo $\mathbb{Z}=\nu_2\mathbb{Q}$. Hence, by Proposition 2.10, the basis $(1,\Phi_1,\Phi_2,\Phi_1\Phi_2,\Phi_2^2,\Phi_1\Phi_2^2)$ is separate. We deduce that the maximum of $\chi^3-\mathbb{Q}_2[\chi]$ is $\frac{1}{3}=\nu_2(\Phi_1\Phi_2)$, the maximum of $\chi^4-\mathbb{Q}_3[\chi]$ is $\frac{2}{3}=\nu_2(\Phi_2^2)$, and the maximum of $\chi^5-\mathbb{Q}_4[\chi]$ is $\frac{2}{3}=\nu_2(\Phi_1\Phi_2^2)$. Hence, by Theorem 3.37, 3, 4, 5 are not strict key degrees.

5.2.2. *The 3-adic valuation.* The 3-adic valuation ν_3 is defined in the same way as ν_2. The residue field is $\mathbb{F}_3$, the valuation group is $\mathbb{Z}$.

• In $\mathbb{F}_3$ we have $X^2+X+1_{\nu_3}=(X-1_{\nu_3})^2$ and $X^3-2_{\nu_3}=X^3+1_{\nu_3}=(X+1_{\nu_3})^3$. Hence $j_{\nu_3}=1_{\nu_3}$ and $\sqrt[3]{2}_{\nu_3}=2_{\nu_3}=(-1)_{\nu_3}$. It follows that $\nu_3(j)=0$, $\nu_3(\sqrt[3]{2})=0$, $\nu_3(j-1)>0$ and $\nu_3(\sqrt[3]{2}+1)>0$.

• In order to calculate $\nu_3(j-1)$, we see that $X^2+X+1=0\Leftrightarrow(X-1)^2=-3X$. Hence $2\nu_3(j-1)=\nu_2((j-1)^2)=\nu(-3j)=1$. Therefore, $\nu_3(j-1)=\frac{1}{2}$.

• Turning to $\nu_3(\sqrt[3]{2}+1)$, we have $X^3-2=0\Leftrightarrow(X+1)^3=-3(X^2+X+1)$. Since $\nu_3(\sqrt[3]{2}+1)>0=\nu_3((\sqrt[3]{2})^2)$, we have $\nu_3((\sqrt[3]{2})^2+\sqrt[3]{2}+1)=0$. Hence $3\nu_3(\sqrt[3]{2}+1)=\nu_3((\sqrt[3]{2}+1)^3)=\nu_3(-3((\sqrt[3]{2})^2+\sqrt[3]{2}+1))=1$. Therefore, $\nu_3(\sqrt[3]{2}+1)=\frac{1}{3}$.

• Consequently, $\nu_3\mathbb{Q}(\chi)$ contains the subroup generated by $\frac{1}{2}$ and $\frac{1}{3}$, which is the subgroup generated by $\frac{1}{6}$. Hence $[\mathbb{Q}(\chi):\mathbb{Q}]=6$ divides $(\nu_3\mathbb{Q}(\chi):\nu_3\mathbb{Q})$, which in turn divides $[\mathbb{Q}(\chi):\mathbb{Q}]$. Therefore, $[\mathbb{Q}(\chi):\mathbb{Q}]=(\nu_3\mathbb{Q}(\chi):\nu_3\mathbb{Q})$, $\nu_3\mathbb{Q}(\chi)=\frac{1}{6}\mathbb{Z}$, and the extension $(\mathbb{Q}(\chi)|\mathbb{Q},\nu_3)$ is separate.

• It follows that $\mathbb{Q}(\chi)_Z=\mathbb{Q}$.

• Since $(\mathbb{Q}(\chi))_{\nu_3}=\mathbb{Q}_{\nu_3}$, we have $\mathbb{Q}(\chi)_T=\mathbb{Q}$.

• Now, since $[\mathbb{Q}(\chi)_V:\mathbb{Q}(\chi)_T]$ is 3-free and $[\mathbb{Q}(\chi):\mathbb{Q}(\chi)_V]$ is a 3-extension, we have $\mathbb{Q}(\chi)_V=\mathbb{Q}(j)$.

Key degrees. We show that the strict key degrees are 1 and 3, and that they are valuational

ones. We have $\nu_3(j-1)=\frac{3}{6}$, $\nu_3(\sqrt[3]{2}+1)=\frac{2}{6}$, $\nu_3((\sqrt[3]{2}+1)(\sqrt[3]{2}+1))=\frac{4}{6}$, $\nu_3((j-1)(\sqrt[3]{2}+1))=\frac{5}{6}$, $\nu_3((j-1)(\sqrt[3]{2}+1)(\sqrt[3]{2}+1)=\frac{7}{6}$, hence, by Proposition 2.10, the basis $(1, j-1, \sqrt[3]{2}+1, (\sqrt[3]{2}+1)^2, (j-1)(\sqrt[3]{2}+1), (j-1)(\sqrt[3]{2}+1)^2)$ is separate. Now, $\nu_3(\chi)=\nu_3(j+\sqrt[3]{2})=\nu_3(j-1+\sqrt[3]{2}+1)=\frac{1}{3}\notin\mathbb{Z}$. Hence, $\nu(\chi)$ is the maximum of $\nu(\chi-\mathbb{Q})$. The strict key degree 1 is a valuational one. We set $\Phi_1=\chi$.

• Since the family $1, \Phi_1, \Phi_1^2$ is separate, we get that the maximum of $\nu_3(\chi^2-\mathbb{Q}_1[\chi])$ is $\frac{2}{3}=\nu_3(\Phi_1^2)$. So 2 is not a strict key degree.

• In order to find the next key degree, we can note that $0=f(\chi)=\chi^6+3\chi^5+6\chi^4+3\chi^3+9\chi+9$, with $\nu_2(\chi^6)=\frac{6}{3}$, $\nu_2(3\chi^5)=\frac{8}{3}$ $\nu_2(6\chi^4)=\frac{7}{3}$, $\nu_2(3\chi^3)=\frac{6}{3}$, $\nu_2(9\chi)\frac{7}{3}$, $\nu_2(9)=\frac{6}{3}$. Hence: $\nu_2\left(\chi^6+3\chi^3+9\right)>\frac{6}{3}$. We can factorize the image of the polynomial $X^6+3X^3+3^3$ in the graded algebra. Here, we prefer to deduce directly the polynomial of degree 3 the valuation of which is the maximum of $\nu_3(\chi^3-\mathbb{Q}_2[\chi])$. Note that, for a, b, c in $\mathbb{Q}$, $\nu_3(a\Phi_1^2+b\Phi_1+c)$ belongs to $\frac{1}{3}\mathbb{Z}$. An element of $\chi^3-\mathbb{Q}_2[\chi]$ can be written as $\Phi_1^3+a\Phi_1^2+b\Phi_1+c$, with a, b, c in $\mathbb{Q}$, and $\Phi_1=\chi=(j-1)+(\sqrt[3]{2}+1)$. Now,

$$\Phi_1^2=(j-1)^2+2(j-1)(\sqrt[3]{2}+1)+(\sqrt[3]{2}+1)^2=-3-3(j-1)+2(j-1)(\sqrt[3]{2}+1)+(\sqrt[3]{2}+1)^2, \text{ and}$$

$$\Phi_1^3=-3(j-1)-3(j-1)^2+2(j-1)^2(\sqrt[3]{2}+1)+(j-1)(\sqrt[3]{2}+1)^2-3(\sqrt[3]{2}+1)-3(j-1)(\sqrt[3]{2}+1)+2(j-1)(\sqrt[3]{2}+1)^2$$
$$+(\sqrt[3]{2}+1)^3=12+6(j-1)-12(\sqrt[3]{2}+1)-9(j-1)(\sqrt[3]{2}+1)+3(\sqrt[3]{2}+1)^2+3(j-1)(\sqrt[3]{2}+1)^2.$$

$$\text{Hence } \Phi_1^3+a\Phi_1^2+b\Phi_1+c=c-3a+12+(6-3a+b)(j-1)+(b-12)(\sqrt[3]{2}+1)$$
$$+(2a-9)(j-1)(\sqrt[3]{2}+1)+(a+3)(\sqrt[3]{2}+1)^2+3(j-1)(\sqrt[3]{2}+1)^2,$$

with $\nu_3(j-1)=\frac{1}{2}=\frac{3}{6}$, $\nu_3(\sqrt[3]{2}+1)=\frac{1}{3}=\frac{2}{6}$, $\nu_3((\sqrt[3]{2}+1)^2)=\frac{2}{3}=\frac{4}{6}$, $\nu_3((j-1)(\sqrt[3]{2}+1))=\frac{5}{6}$, $\nu_3((j-1)(\sqrt[3]{2}+1)^2)=\frac{7}{6}$. Since this basis is separate, the valuation of $\Phi^3+a\Phi^2+b\Phi+c$ is the minimum of the valuation of the components. Note that if the maximum does not belong to $\frac{1}{3}\mathbb{Z}$, then it is $\frac{5}{6}$, $\frac{11}{6}$ or $\frac{13}{6}$. By setting $a=6$, $b=12$, $c=6$, we get the minimum of ∞, ∞, ∞, $\frac{11}{6}$, $\frac{20}{6}$, $\frac{13}{6}$. So it is $\frac{11}{6}$, which does not belong to $\frac{1}{3}\mathbb{Z}$. Now, for any a, b, c in $\mathbb{Q}$, $\Phi_1^3+a\Phi_1^2+b\Phi_1+c=\Phi_1^3+6\Phi_1^2+12\Phi_1+6+(a-6)\Phi_1^2+(b-12)\Phi_1+c-6$, with $\nu_3((a-6)\Phi_1^2+(b-12)\Phi_1+c-6)\in\frac{1}{3}\mathbb{Z}$, and $\nu_3(\Phi_1^3+6\Phi_1^2+12\Phi_1+6)=\frac{11}{6}\notin\frac{1}{3}\mathbb{Z}$. Consequently, $\nu_3(\Phi_1^3+a\Phi_1^2+b\Phi_1+c)=\min(\nu_3(\Phi_1^3+6\Phi_1^2+12\Phi_1+6), \nu_3((a-6)\Phi_1^2+(b-12)\Phi_1+c-6))$. Therefore, $\frac{11}{6}$ is the maximum of $\nu_3(\chi^3-\mathbb{Q}_2[\chi])$. We let $\Phi_2=\Phi_1^3+6\Phi_1^2+12\Phi_1+6$. The next strict key degree is 3, and it is a valuational one.

• Now, by Proposition 2.10, the basis $(1, \Phi_1, \Phi_1^2, \Phi_2, \Phi_1\Phi_2, \Phi_1^2\Phi_2)$ is separate, hence there is no strict key degree greater than 3.

5.2.3. *The* 5*-adic valuation.* In order to study a p-adic valuation where p does not divide $[\mathbb{Q}(\chi):\mathbb{Q}]$, we look at ν_5.

• The polynomial $X^2+X+1_{\nu_5}$ has no root in $\mathbb{F}_5$, hence j_{ν_5} does not belong to $\mathbb{Q}_{\nu_5}$, and 2 divides $[\mathbb{Q}(\chi)_{\nu_5}:\mathbb{Q}_{\nu_5}]$.

• The class 3_{ν_5} is the unique root of the polynomial $X^3-2_{\nu_5}$ in $\mathbb{F}_5$. The derivate polynomial is $3_{\nu_5}X^2$, and, in $\mathbb{F}_5$, $3_{\nu_5}3_{\nu_5}^2=2_{\nu_5}\neq 0_{\nu_5}$.

• From general properties of valuations it follows that the extension $(\mathbb{Q}(\sqrt[3]{2})|\mathbb{Q}, \nu_5)$ is immediate, and that there are three extensions of $(\nu_5)_{|\mathbb{Q}}$ to $\mathbb{Q}(\sqrt[3]{2})$ (since the number of extensions of $(\nu_5)_{|\mathbb{Q}}$ to $\mathbb{Q}(\chi)$ divides $[\mathbb{Q}(\chi):\mathbb{Q}]/[(\mathbb{Q}(\chi))_{\nu_5}:\mathbb{Q}_{\nu_5}]\leq 3$, this number is 3, and $[(\mathbb{Q}(\chi))_{\nu_5}:\mathbb{Q}_{\nu_5}]=2$). Now, one can see this fact. In $\mathbb{F}_5$, j_{ν_5} is a root of the polynomial $X^2+X+1_{\nu_5}$, and it also satisfies $j_{\nu_5}^3=1_{\nu_5}$. In $\mathbb{F}_5(j_{\nu_5})$, $X^3-2_{\nu_5}=(X-3_{\nu_5})(X-(3j)_{\nu_5})(X-(3j^2)_{\nu_5})$, and, in $\mathbb{Q}$, $X^3-2=(X-\sqrt[3]{2})(X-j\sqrt[3]{2})(X-j^2\sqrt[3]{2})$. Now, we can let $\sqrt[3]{2}$ be a lifting of any of the residual roots 3, $(3j)_{\nu_5}$, $(3j^2)_{\nu_5}$. So we get three different extensions of ν_5.

• We let $\sqrt[3]{2}$ be a lifting of 3, and we calculate $\nu_5(\sqrt[3]{2}-3)$. Since j_{ν_5} and $j_{\nu_5}^2$ do not belong to $\mathbb{F}_5$, $(3j)_{\nu_5}$ and $(3j^2)_{\nu_5}$ are different from $3_{\nu_5}=(\sqrt[3]{2})_{\nu_5}$. It follows that $\nu_5(\sqrt[3]{2}-3j)=\nu_5(\sqrt[3]{2}-3j^2)=0$. Now, in $\mathbb{Q}$, $(X-3)(X-3j)(X-3j^2)=X^3-3(1+j+j^2)X^2-3(1+j+j^2)X-27=X^3-2-25$. Hence $\nu_5(\sqrt[3]{2}-3)=\nu_5((\sqrt[3]{2}-3)(\sqrt[3]{2}-3j)(\sqrt[3]{2}-3j^2))=\nu_5(-25)=2$.

• Since $[\mathbb{Q}(\chi)_{\nu_5}:\mathbb{Q}_{\nu_5}]=2$, we deduce that $[\mathbb{Q}(\chi)_Z:\mathbb{Q}]=3$, and $\mathbb{Q}(\chi)_Z=\mathbb{Q}(\sqrt[3]{2})$. Therefore the group G_Z is generated by the transposition τ.

• Now, it follows that $\mathbb{Q}(\chi)_T=\mathbb{Q}(\chi)$, so G_T and G_V are equal to the identity group.

Key degrees. We show that 1 is a residual strict key degree, that 2 is an immediate key degree, and that they are the only key degrees. We have $(\sqrt[3]{2})_{\nu_5}=3_{\nu_5}$, and $j_{\nu_5}\notin\mathbb{F}_5=\mathbb{Q}_{\nu_5}$. Hence for every $a\in\mathbb{Q}$ with $\nu_5(a)\geq 0$ we have $(a+\sqrt[3]{2})_{\nu_5}\neq j_{\nu_5}$. So $\nu_5(\chi+a)=\nu_5(j+\sqrt[3]{2}+a)=0$. Hence 0 is the maximum of $\nu(\chi-\mathbb{Q})$. We can let $\Phi_1=\chi$. Note that 1 is a residual strict key degree.

• Since $(\mathbb{Q}(\sqrt[3]{2})|\mathbb{Q}, \nu_5)$ is immediate, $\sqrt[3]{2}$ is pseudo-limit of a pseudo-Cauchy sequence (x_n) of $\mathbb{Q}$, and $\sqrt[3]{4}$ is pseudo-limit of a pseudo-Cauchy sequence (y_n) of $\mathbb{Q}$. Since $\nu_5\mathbb{Q}=\mathbb{Z}$ is archimedean and discrete,

the values $\nu_5(\sqrt[3]{2}-x_n)$ and $\nu_5(\sqrt[3]{4}-y_n)$ are cofinal in $\mathbb{Z}$. An element of $\chi^2-\mathbb{Q}_1[\chi]$ can be written as $\chi^2+a\chi+b$, with a, b in $\mathbb{Q}$. Calculations show that

$$\chi^2+a\chi+b=2j\left(\sqrt[3]{2}+\frac{a-1}{2}\right)+a\left(\sqrt[3]{2}+\frac{a-1}{2}\right)+\sqrt[3]{4}+b-a\left(\frac{a-1}{2}\right)-1.$$

By letting $a=1-2x_n$ and $b=x_n(2x_n-1)+1-y_n$, we have $\chi^2+a\chi+b=2j(\sqrt[3]{2}-x_n)+(1-2x_n)(\sqrt[3]{2}-x_n)+\sqrt[3]{4}-y_n$, and the valuations of this sequence are cofinal in $\mathbb{Z}$. Consequently, $\nu(\chi^2-\mathbb{Q}_1[\chi])=\mathbb{Z}$, 2 is a strict immediate key degree, and there is no strict key degree greater than 2. For every integer n we let $\Phi_{2,n}=\chi^2+(1-2x_n)\chi+x_n(2x_n-1)+1-y_n$.

• In order to find the sequence (x_n), in the same way as in [HOS 07] we proceed by induction and by lifting polynomials of the graded algebra. By properties of p-adic valuations (see for example [La 65, p. 306]), since $\nu_5(\sqrt[3]{2})\geq 0$, x_n can be written in a unique way as $x_n=a_0+a_1\cdot 5+a_2\cdot 5^2+\cdots+a_m\cdot 5^m$, where, $m\geq n$ and for $0\leq k\leq m$, $a_k\in\{0,1,2,3,4\}$. For notational convenience, we let $m=n$, that is, if $a_n=0$, then $x_n=x_{n-1}$. Since $\sqrt[3]{2}=\sum_{k=0}^{+\infty}a_k\cdot 5^k$, for every n we have $\sqrt[3]{2}-x_n=\sum_{k=n+1}^{+\infty}a_k\cdot 5^k$. So, for every n, $(\sqrt[3]{2}-x_n)_{n+1,\nu_5}=(a_{n+1}\cdot 5^{n+1})_{n+1,\nu_5}$. As $(\sqrt[3]{2})_{\nu_5}=3_{\nu_5}$, we have $x_0=a_0=3$. Since the irreducible polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$ is X^3-2, the irreducible polynomial of $\sqrt[3]{2}-x_n$ is $(X+x_n)^3-2=X^3+3x_nX^2+3x_n^2X+x_n^3-2$. Let $n\in\mathbb{N}$ and m be the smallest integer such that $m>n$ and $a_m\neq 0$. Then $\nu_5(\sqrt[3]{2}-x_n)=m$ and $\nu_5(x_n)=0$, it follows: $\nu_5((\sqrt[3]{2}-x_n)^3)=3m>\nu_5(3x_n(\sqrt[3]{2}-x_n)^2)=2m>\nu_5(3x_n^2(\sqrt[3]{2}-x_n))=m$. Hence $m=\nu_5(3x_n^2(\sqrt[3]{2}-x_n))=\nu_5(x_n^3-2)$, and $\nu_5(3x_n^2(\sqrt[3]{2}-x_n)+(x_n^3-2))>m$.

For every $n\geq 2$, x_n is congruent to 3 modulo 5. Hence $3x_n^2$ is congruent to 2. The inverse of 2 modulo 5 is 3. Hence $(a_{n+1}\cdot 5^{n+1})_{n+1,\nu_5}=3(-(x_n^3-2))_{n+1,\nu_5}=2(x_n^3-2)_{n+1,\nu_5}$. We deduce by induction all the a_n and x_n. We have $x_0=3$, $2(3^3-2)=50$. Since $\nu_5(50)=2$, we have $a_1=0$. So $x_1=x_0=3$, $x_2=3+a_2\cdot 5^2$. Now, $2(x_1^3-2)=2\cdot 5^2$, hence $a_2=2$, and $x_2=53$. We have $53^3-2=1191\cdot 5^3$. So $(x_2^3-2)_{3,\nu_5}=(1191\cdot 5^3)_{3,\nu_5}=(5^3)_{3,\nu_5}$. Therefore, $a_3=2$. Now, $x_3^3-2=(53+2\cdot 5^3)^3-2=53^3+6{\cdot}53^2{\cdot}5^3+12{\cdot}53{\cdot}5^6+8{\cdot}5^9-2=53^3-2+6{\cdot}53^2{\cdot}5^3+12{\cdot}53{\cdot}5^6+8{\cdot}5^9=1191{\cdot}5^3+16854{\cdot}5^3+12{\cdot}53{\cdot}5^6+8{\cdot}5^9=18045{\cdot}5^3+12{\cdot}53{\cdot}5^6+8{\cdot}5^9=3609{\cdot}5^4+12{\cdot}53{\cdot}5^6+8{\cdot}5^9$. So $(x_3^3-2)_{4,\nu_5}=(3609{\cdot}5^4)_{4,\nu_5}=(4{\cdot}5^4)_{4,\nu_5}$. Hence $(a_4{\cdot}5^4)_{4,\nu_5}=(3{\cdot}4{\cdot}5^4)_{4,\nu_5}=(2{\cdot}5^4)_{4,\nu_5}$. Hence $a_4=2$. In this way, by induction one can get any x_n.

5.2.4. *The 2-adic valuation with an other generator.* We come back to ν_2, by taking the generator $\mathcal{Y}=2\chi+1$ of $\mathbb{Q}(\chi)$ instead of χ. Its irreducible polynomial over $\mathbb{Q}$ is $h(X)=X^6+9X^4-32X^3+27X^2-293$. In the same way as above, we can consider its image in $\mathbb{F}_2[X]$: $X^6+X^4+X^2+1_{\nu_2}=(X^3+X^2+X+1_{\nu_2})^2=(X+1_{\nu_2})^6$. So, $\mathcal{Y}_{\nu_2}=1_{\nu_2}$ belongs to $\mathbb{F}_2$. We let $\Phi_{1,1}(\mathcal{Y})=\mathcal{Y}$. Since the irreducible poynomial of $\mathcal{Y}_{\nu_2}$ over $\mathbb{F}_2$ has degree 1, the second key polynomial has degree 1, and it is a lifting of $X+1_{\nu_2}$. We can take $\Phi_{1,2}(\mathcal{Y})=\mathcal{Y}-1$. Then $\Phi_{1,2}(\mathcal{Y})=2\chi$, and $\nu_2(\Phi_{1,2}(\mathcal{Y}))=1$ is the maximum of $\nu_2(\mathcal{Y}-\mathbb{Q})$. The irreducible polynomial of the image of $\Phi_{1,2}(\mathcal{Y})$ in the graded algebra is $X^2+1_{1,\nu_2}X+1_{2,\nu_2}$. Indeed, $\nu_2\left(\Phi_{1,2}^2+2\Phi_{1,2}+2^2\right)=\nu_2\left(2^2\chi^2+2^2\chi+2^2\right)=2+\nu_2\left(\chi^2+\chi+1\right)>2=\nu_2\left(\Phi_{1,2}^2\right)=\nu_2\left(2\Phi_{1,2}\right)=\nu_2\left(2^2\right)$. Hence $\Phi_{2,1}$ is a lifting of $X^2+1_{1,\nu_2}X+1_{2,\nu_2}$. We can take $\Phi_{2,1}=\Phi_{1,2}^2+2\Phi_{1,2}+2^2$. In the same way as above, the algorithm stops because $\nu_{2\,(\Phi_{1,2},\Phi_{2,1})}=\nu_2$.

References

[AK 65] J. Ax, S. Kochen, *Diophantine problems over local fields 1 & 2*, American Journal of Mathematics 87 (1965), pp. 605-630 & 631-648.

[B 81] W. Baur, *Die Theorie der Paare reell abgeschlossener Körper*, Logic and Algorithmic (in honour of E. Specker), Monographies de l'Enseignement Mathématique, n° 30, Université de Genève, Geneva, 1982, pp. 25-34.

[B 82] W. Baur, *On the theory of pairs of real closed fields*, The Journal of Symbolic Logic, vol 47 (1982), pp. 669-679.

[Bo 59] N. Bourbaki, Algèbre, Chapitre 5, Corps Commutatifs, Hermann, Paris, 1959.

[D 82] F. Delon, *Quelques propriétés des corps valués en théorie des modèles*, thèse d'état, Paris 7, 1982.

[D 88] F. Delon, *Extensions séparées et immédiates de corps valués*, The Journal of Symbolic Logic, vol 53 (1988), pp. 421-428.

[D 91] F. Delon, *Indécidabilité de la théorie des paires de corps valués henseliens*, The Journal of Symbolic Logic, vol 56 (1991), pp. 1236-1242.

[E 72] O. Endler, *Valuation Theory*, Springer, Berlin, 1972.

[HMOS 14] F. J. Herrera Govantes, W. Mahloud, M. A. Olalla Acosta, M. Spivakovsky, *Key polynomials for simple extensions of valued fields* arXiv:1406.0657v2 [math.AG] 12 Jun 2014.

[HOS 07] F. J. Herrera Govantes, M. A. Olalla Acosta, M. Spivakovsky, *Valuations in algebraic field extensions*, J. of Algebra, 312 (2007), pp. 1033-1074.

[K 42] I. Kaplansky, *Maximal fields with valuations*, Duke Math Journal 9 (1942), pp. 303-321.

[K 75] S. Kochen, *The model theory of local fields*, Logic Conference, Kiel 1974, Lecture Notes in Mathematics (499), Springer Verlag, Berlin 1975.

[La 65] S. Lang, Algebra, Addison-Wesley, Reading, Massachussets, 1965.

[L 89] G. Leloup, *Théories complètes de paires de corps valués henseliens*, The Journal of Symbolic Logic, vol 55, n° 1, March 1990, pp. 323-339.

[L 03] G. Leloup, *Properties of extensions of algebraically maximal fields*, Collectanea mathematica, Vol 54, n° 1, 2003, pp. 53-72.
[ML 36a] S. MacLane, *A construction for absolute values in polynomials rings*, Trans. Amer. Math. Soc 40 (1936), pp. 363-395.
[ML 36b] S. MacLane, *A construction for prime ideals as absolute values of an algebraic field*, Duke Math. j. 2 (1936), pp. 492-510.
[R 68] P. Ribenboim, *Théorie des valuations*, Les Presses de l'Université de Montréal, Montréal, 1968.
[V 07] M. Vaquié, *Extension d'une valuation*, Trans. Amer. Math. Soc. 359 (7) (2007) pp. 3439-3481.
[FVK] https://math.usask.ca/ fvk/bookch8.pdf

ADDRESS

Gérard LELOUP, Laboratoire Manceau de Mathématiques, Faculté des Sciences, avenue Olivier Messiaen, 72085 LE MANS CEDEX, FRANCE, gerard.leloup-At-univ-lemans.fr