ANNALES MATHÉMATIQUES

BLAISE PASCAL

M'hammed Boulagouaz

Une caractérisation de l'existence de l'élément primitif pour une extension gr-séparable des gradués associés à une extension de corps valués

Volume 16, n° 1 (2009), p. 101-111.

<http://ambp.cedram.org/item?id=AMBP_2009__16_1_101_0>

Publication éditée par le laboratoire de mathématiques de l'université Blaise-Pascal, UMR 6620 du CNRS Clermont-Ferrand — France

cedram

Article mis en ligne dans le cadre du Centre de diffusion des revues académiques de mathématiques
http://www.cedram.org/

Annales mathématiques Blaise Pascal **16**, 101-111 (2009)

Une caractérisation de l'existence de l'élément primitif pour une extension gr-séparable des gradués associés à une extension de corps valués

M'hammed Boulagouaz

Résumé

Un anneau gradué unitaire où tout élément homogène non nul est inversible est appelé un anneau à division gradué. Cet article est une contribution à l'étude de la correspondance existante entre les anneaux à division valués et les anneaux à division gradués , voir [1], [2], [3], [4], [6] et [7].

Il a été prouvé dans [5, Remarque de la page 26], que toute extension gr-séparable finie de corps gradués n'est pas simple. Dans ce travail on donne un critère pour l'existence d'élément primitif dans une extension finie gr-séparable de gradués associée à une extension de corps valués, voir le Théorème1.

A criterion for the existence of a primitif element in a simple gr-separable graded fields extension associated with a valued fields extension

Abstract

A unit graded ring where each homogeneous element non equal to zero is invertible is called a graded division ring. This article is a contribution to the stady of the correspondance between the valued division rings and the graded division rings, see [1], [2], [3], [4], [6] and [7].

It's proved in [5, Remark of page 26], that a finite gr-separable graded field extension is not always a simple extension. In this work we give a criterion for the existence of a primitif element in a finite gr-separable extension of graded fields associated with a valued fields extension, see Theorem1.

Mots-clés : Corps valué, extension valuée modérée, corps gradué, extension gr-algébrique, extension gr-séparable.
Classification math. : 11R27, 11R29, 11R37.

1. **Préliminaires**

Soit Γ un groupe noté additivement et $(A, +, .)$ un anneau unitaire.

Définition 1.1. A est dit un anneau gradué par Γ s'il existe une famille $(A_\delta\ )$ indexée par Γ, de sous-groupes du groupe additif $(A, +)$, telle que :
i) $A = \bigoplus_{\delta\in\Gamma} A_\delta$,
ii) $A_\delta A_\gamma \subset A_{\delta+\gamma}$.

Exemples :
1- Pour $\Gamma = \mathbf{Z}$, le groupe des entiers relatifs et $A = K[X]$, l'anneau des polynômes en X à coefficients dans le corps K, la famille des $A_i = KX^i$ si $i \geq 0$ et $A_i = \{0\}$ si $i < 0$ définit sur $K[X]$ une structure d' anneau gradué par $\mathbf{Z}$.
2- Pour tout groupe Γ et pour tout anneau R, la famille des sous-groupes $A_\delta = R\delta$ du groupe additif de l'anneau de groupe $R[\Gamma]$ définit sur l'anneau $A = R[\Gamma]$ une structure d'anneau gradué par Γ.

Vocabulaire et notations :

Si $A = \bigoplus_{\delta\in\Gamma} A_\delta$, est un anneau gradué par Γ alors :
i)$H(A) = (\cup_{\delta\in\Delta} A_\delta) - \{0\}$ est dit l'ensemble des éléments homogènes de A.
ii) Un élément $x \in A_\delta - \{0\}$ est dit homogène de grade δ.
iii) On note $gr(x) = \delta$ pour dire que x est homogène de grade δ, ou encore que $x \in A_\delta - \{0\}$.
iv) Si $a = \Sigma_{\text{finie}} a_\delta$ où les $a_\delta \in A_\delta - \{0\}$ alors a_δ est appelé la composante homogène de grade δ de a. On dit aussi que A_δ est la composante homogène de grade δ de l'anneau gradué A.
v) L'ensemble $\Gamma_A = \{\lambda \in \Gamma \mid A_\lambda \neq \{0\}\}$ est appelé le support de l'anneau gradué A. Γ_A n'est pas en général un sous-groupe de Γ. On dit que A est un anneau gardué de type Γ si A est un anneau gradué par Γ et $\Gamma_A = \Gamma$. Donc un anneau gradué A est un anneau gradué de type Γ_A.

Définition 1.2. On appelle *corps gradué* un anneau gradué commutatif A tel que $A \neq \{0\}$ et où tout élément homogène non nul est inversible dans A.

L'anneau des polynômes de Laurent à coefficients dans $\mathbf{Q}$,

$$R = \mathbf{Q}[X^{-1}, X] = \bigoplus_{n\in\mathbf{Z}} \mathbf{Q}X^n,$$

a une structure de corps gradué par $\mathbf{Z}$.

Si $R = \bigoplus_{\gamma \in \Gamma_R} R_\gamma$ est un corps gradué alors :

a) Γ_R, le support de la graduation de R est un sous-groupe de Γ, appelé le groupe des grades de R. Pour $R = \bigoplus_{n \in \mathbf{Z}} \mathbf{Q}X^n$ le support Γ_R de la graduation de R est $\mathbf{Z}$.

b) Un corps gradué n'est pas intègre en général mais si Γ_R est un groupe totalement ordonné(condition équivalente à Γ_R est sans torsion) alors un corps gradué R est intègre et Γ_R a une clôture rationnelle unique.

c) Le groupe clôture rationnelle $\Gamma_R \otimes_{\mathbf{Z}} \mathbf{Q}$ du groupe Γ_R sera désigné par Δ_R. Pour $R = \bigoplus_{n \in \mathbf{Z}} \mathbf{Q}X^n$ le groupe $\Gamma_R \otimes_{\mathbf{Z}} \mathbf{Q} = \mathbf{Q}$.

d) $(H(R), .)$ est un groupe appelé le groupe des éléments homogènes de R. Pour $R = \bigoplus_{n \in \mathbf{Z}} \mathbf{Q}X^n$ on a $(H(R), .) = \{aX^n / a \in (\mathbf{Q} - \{0\}), n \in \mathbf{Z}\}$.

e) $(\forall e_\gamma \in R_\gamma^*)(\forall \gamma \in \Gamma_R)\ : R_\gamma = R_0 e_\gamma$.

Remarque : dans toute la suite les corps gradués considérés seront supposés de groupe de grade sans torsion.

2. Graduations de $R[X]$

Soient $R = \oplus_{\Gamma_R} R_\delta$ un corps gradué, X une d'indeterminée sur R et G un groupe dont Γ_R est un de ses sous-groupes. Pour chaque $\omega \in G$, désignons par $\Gamma_R[\omega]$ le semi-groupe de G engendré par Γ_R et ω. La donnée de ω définit une graduation sur l'anneau $R[X]$, de support $\Gamma_R[\omega]$, de la manière suivante : La composante homogène de grade un $\alpha \in \Gamma_R[\omega]$ est l'ensemble des polynômes de la forme $\Sigma_{j=1}^s a_j X^j$ tels que $a_j \in H(R) \cup \{0\}$ et $gr(a_j) + j\omega = \alpha$, dès que $a_j \neq 0$. L'anneau $R[X]$ ainsi gradué sera noté $R[X]^{(\omega)}$. Dans $R[X]^{(\omega)}$, les monômes X^i sont homogènes de grade $i\omega$.

Nous dirons qu'un polynôme $P(X) = \Sigma_{j=1}^s a_j X^j$ de $R[X]$, non réduit à un monôme, est *homogèneisable* s'il existe un $\omega \in \Delta_{\Gamma_R}$ tel que $P(X)$ est homogène comme élément de l'anneau gradué $R[X]^{(\omega)}$. Donc $P(X) = \Sigma_{j=1}^s a_j X^j$ de $R[X]$ est homogènéisable s'il existe un ω dans Δ_{Γ_R} tel que :

i) $a_j \neq 0 \Rightarrow a_j \in H(R)$.

ii) $gr(a_j) - gr(a_i) = (i - j)\omega$ si a_j et a_i sont non nuls.

A remarquer aussi que si $P(X) = \Sigma_{j=1}^s a_j X^j \in R[X]$ n'est pas réduit à un monôme et homogénéisable pour un certain ω alors ω est rationnelle sur Γ_R, c'est à dire il existe $n \in \mathbf{N}^*$ tel que $n\omega \in \Gamma_R$.

Exemple :
Soit K un corps quelconque et $R = K[T, T^{-1}] = \bigoplus_{\mathbf{Z}} KT^n$ l'anneau des polynômes de laurent à coefficients dans K, alors :
1) $F(X) = 2T^4 + 4TX^3 + X^4$ est homogène dans $R[X]^{(1)}$.
2) $G(X) = T^3 + X^6 + TX^4 + 2T^2X^2$ est homogène dans $R[X]^{(\frac{1}{2})}$.

3. Extension gr-algébrique

Soit R un corps gradué et S un anneau commutatif contenant R comme sous-anneau. Un élément de S est dit gr-algébrique sur R s'il annule un polynôme homogénéisable de $R[X]$. A remarquer que si $a \in S$ est gr-algébrique sur R alors il existe un polynôme de degré minimal homogénéisable de $R[X]$ annulé par a, qu'on note $f_{a/R}(X)$, de plus $R(a) := R[X]/f_{a/R}(X)$ est un sous-corps gradué de S et $gr(a)$ est rationnelle sur Γ_R.
Pour une extension de corps gradués S/R on pose les définitions suivantes :
1) S/R est gr-algébrique sur R si tout élément homogène de S l'est.
2) Un élément a de S non gr-algébrique sur R est dit *gr-transcendant* sur R. On montre que toute extension de degré fini de corps gradués est gr-algébrique.
3) S/R est gr-séparable si tout élément homogène de S annule un polynôme homogénéisable n'ayant que des racines simples.
4) S/R est une extension simple de corps gradués s'il existe un élément homogène x de S tel que, le corps gradué engendré par R et x dans S noté $R(x)$ soit exactement S, ou encore si $S = R(x)$. Voir [5] ou [6] pour plus de détails sur la notion de gr-algébricité et gr-séparabilité.

4. Corps gradué associé à un corps valué

Soit F un corps muni d'une valuation v, alors pour chaque $\gamma \in \Gamma_F := \Gamma_v$ (le groupe de la valuation v) on définit :
1)$F_\gamma = \{x \in F / v(x) \geq \gamma\}$ est un sous-groupe additif de $(F, +)$,
2)$F_{\gamma^+} = \{x \in F / v(x) > \gamma\}$ est un sous-groupe de F_γ,
3) $gr(F)_\gamma$ comme étant le groupe quotient de F_γ par F_{γ^+} i.e :

$$gr(F)_\gamma := F_\gamma / F_{\gamma^+}.$$

A remarquer que pour $\gamma = 0$ on obtient :
$1^{'})F_0 = \{d \in F/v(d) \geq 0\}$ est l'anneau de valuation de (F, v).
$2^{'})F_{0^+} = \{d \in F/v(d) > 0\}$ est l'idéal de la valuation de (F, v).
$3^{'})gr(F)_0$ est le corps résiduel de (F, v), qui est souvent noté $\bar{F}$.

On note $gr(F)$ l'anneau gradué associé :

$$gr(F) \;=\; \oplus_{\delta\in\Delta} gr(F)_\delta \,.$$

où la multiplication sur $gr(F)$ est induite par la multiplication de F, de la manière suivante, pour $x \in F_\delta$ et $y \in F_\epsilon$:

$$(x \,+\, F_{\delta^+})\,(\,y \,+\, F_{\epsilon^+}) \;=\; xy \,+\, F_{(\delta+\epsilon)^+}\,.$$

$(1 + F_{0^+})$ est l'élément neutre de cette multiplication et il est clair que tout élément homogène de $gr(F)$ est inversible : si $0 \neq (x \,+\, F_{\delta^+}) \in F_\delta/F_{\delta^+}$, c'est à dire si $v(x) = \delta$, alors $(x^{-1} \,+\, F_{\delta^+}) \in F_{-\delta}/F_{(-\delta)^+}$ et

$$(x \,+\, F_{\delta^+})\,(x^{-1} \,+\, F_{(-\delta)^+}) \;=\; 1 \,+\, F_{0^+}.$$

L'anneau $gr(F)$ est donc un corps gradué de type Γ_F.

Définition 4.1. On appelle **corps gradué associé au corps valué** (F, v) **:** l'anneau $gr(F)$. Sa composante homogène de degré zéro est le corps résiduel :

$$gr(F)_0 \;=\; \bar{F}$$

et son support est Γ_F, le groupe de valeurs de v

$$\Gamma_{gr(F)} \;=\; \Gamma_F\,.$$

Pour chaque $x \in F^*$ tel que $v(x) \geq \gamma$ on pose $\pi_\gamma(x) := x + F_{\gamma^+}$ et $\tilde{x} := \pi_{v(x)}(x) = x + F_{v(x)^+} \in gr(F)_{v(x)}$.
Pour plus de détail sur le gradué associé à un corps valué voir [2].

Remarque : Pour $x \in F^*$ on a si $v(x) \geq 0$ alors $\pi_0(x) = \bar{x}$ est la classe résiduelle de x qui est nulle si $v(x) > 0$, mais $\pi_{v(x)}(x) = \tilde{x} = x+A_{v(x)^+} \neq 0$.

Il est clair que si E/F est une extension de corps valués alors le quotient $gr(E)/gr(F)$ est une extension de corps gradués appelée l'extension graduée associée à l'extension valuée E/F. Pour plus de détails sur cette extension graduée associée voir [1], [2], [6] ou [7].

5. Polynôme résiduel d'ordre α

Soit (F, v) un corps valué de groupe de valuation Γ_F et de corps résiduel $\bar{F}$. Dans tout ce qui suit posons : $R = gr(F)$, $\Delta = \mathbf{Q} \bigotimes_{\mathbf{Z}} \Gamma_F$, Ω la clôture algébrique de F, désignons par w un prolongement de v à Ω et notons S_w le gradué de (Ω, w), il est simple de vérifier que S_w est une extension graduée de R.

Soit $\alpha \in \Delta$ et $f(X) = \Sigma_{i=1}^{n} a_i X^i$ un polynôme unitaire de $F[X]$ tel que

$$v(a_i) \geq \alpha(n - i) \ , \tag{5.1}$$

On définit :

$$\tilde{f}^{(\alpha)}(X) = \Sigma_{i=1}^{n} \pi_{\alpha(n-i)}(a_i) X^i,$$

lequel polynôme est appelé *reste résiduel d'ordre* α de $f(X)$.

Par ailleurs, on note $\tilde{f}(X)$ le polynôme $\prod_{i=1}^{n}(X - \pi_{w(x_i)}(x_i)) \in S[X]$. Où $x_1, ..., x_n$ sont les racines de $f(X)$ dans Ω.
Remarquons que $\tilde{f}^{(\alpha)}(X)$ est homogène de grade $n\alpha$ dans $R[X]^{(\alpha)}$.

Exemple :
Soit p un entier premier, $F = \mathbf{Q}_p$ et v la valuation p-adique sur $\mathbf{Q}_p$.
$R = gr(\mathbf{Q}_p) = \mathbf{Z}/p\mathbf{Z}[T, T^{-1}]$ et $f(X) = p^4 + p^5 X + p^7 X^2 - 2pX^3 + X^4$.
1) Ce polynôme vérifie la condition $v(a_i) \geq (n - i)$ et

$$\tilde{f}^{(1)}(X) = T^4 - 2TX^3 + X^4 \in R[X].$$

2) De même que ce polynôme vérifie aussi $v(a_i) \geq (n - i)\frac{1}{2}$ et $\tilde{f}^{(\frac{1}{2})}(X) = X^4$.

6. Cas d'une valuation hensélienne

Soit $f(X) = \Sigma_{i=0}^{n} a_i X^i$, un polynôme unitaire de $F[X]$, notons $x_1, ..., x_n$ les racines de $f(X)$ dans Ω, la clôture algébrique de F. Il est montré dans [4] que :
1) $f(X) = \Sigma_{i=0}^{n} a_i X^i$ est tel que

$$v(a_i) \geq v(a_0)(1 - \frac{i}{n}), \tag{6.1}$$

si et seulement si toutes les racines de $f(X)$ ont la même valuation.
2) Si $f(X) \in F[X]$ est unitaire et ne vérifie pas la condition (6.1) alors

$f(X)$ est réductible.
3) Si $f(X)$ est tel que

$$v(a_i) \geq v(a_0)(1 - \frac{i}{n}),$$

alors

$$\tilde{f}^{(\frac{v(a_0)}{n})}(X) = \tilde{f}(X) = \Pi_{i=1}^{n}(X - \pi_{v(x_i)}(x_i)).$$

Conséquence : Si (F, v) est un corps valué hensélien, alors v a un unique prolongement à Ω qu' on notera aussi v, et pour tout polynôme irréductible et unitaire $f(X) = \Sigma_{i=0}^{n} a_i X^i \in F[X]$ on a :

$$v(a_i) \geq v(a_0)(1 - \frac{i}{n}),$$

et

$$\tilde{f}^{(\frac{v(a_0)}{n})}(X) = \Sigma_{i=1}^{n} \pi_{\frac{v(a_0)}{n}(n-i)}(a_i) X^i = \tilde{f}(X) = \Pi_{i=1}^{n}(X - \pi_{v(x_i)}(x_i)).$$

7. Une caractérisation de l'existence de l'élément primitif pour une extension gr-séparable de l'extension des gradués associés à une extension de corps valués

Rappelons qu'une extension de corps valués de degré n, d'indice résiduelle f et d'indice de ramification e est dite modérément ramifiée (ou encore modérée), si elle est non défective (i.e. $n = fe$), d'extension résiduelle séparable et e est non divisible par sa caractéristique résiduelle.

Une extension modérément ramifiée de corps valués n'est pas nécessairement simple, de même qu'une extension de corps gradués gr-séparable de degré fini n'est pas nécessairement simple, car il est prouvé dans [5, Remarque p.26], que le théorème de l'élément primitif n'est pas vrai pour les extensions de corps gradués gr-séparables de degré fini. Nous proposons dans la suite d'étudier le lien entre la simplicité d'une extension modérément ramifiée de corps valués et celle de l'extension de leurs gradués associés. Il est connu que E/F est modérée finie si et seulement si $gr(E)/gr(F)$ est gr-séparable finie et $[E : F] = [gr(E)/gr(F)]$, voir [6, Th5.2] ou encore [1, Corollaire 4]. Rappelons qu'une extension E/F de corps valués modérément ramifiée de degré fini (resp. une extension S/R de corps gradués de degré fini) est dite non ramifiée si $[E : F] = [\bar{E} : \bar{F}]$

(resp. $[S:R]=[S_0:R_0]$, où $[S:R]$ désigne le rang de S sur R comme R-module.)
Remarque 1 : Si E/F est une extension valuée telle que (F,v) est hensélien, alors il est vrai que pour $z \in E$, $deg(f_{z/F}(X)) = deg(\tilde{f}_{z/F}(X))$ et $f_{\tilde{z}/gr(F)}(X)$ divise $\tilde{f}_{z/F}(X)$.

Proposition 7.1. *Soit E/F une extension de corps valués modérée finie avec F hensélien et $gr(E)/gr(F)$ l'extension des corps gradués associés alors : $gr(E)/gr(F)$ est simple entraîne que E/F est simple.*

Démonstration. En tenant compte de la remarque 1, si $gr(E) = gr(F)(\tilde{z})$ pour un $z \in E$ alors :
$[E:F] \geq [F(z):F] = deg(f_{z/F}(X)) \geq deg(f_{\tilde{z}/gr(F)}(X)) = [gr(F)(\tilde{z}):F]$
$= [gr(E):gr(F)] = [E:F]$ d'où $E = F(z)$ ou encore E/F est simple. □

Remarque 2 : La réciproque de la proposition ci-dessus est fausse en général. Pour se convaincre il suffit de voir l'exemple 1 de la remarque 3 citée ci-dessous.

Rappelons qu'une extension E/F de corps valués modérément ramifiée de degré finie (resp. une extension S/R de corps gradués de degré fini) est dite non ramifiée si $[E:F] = [\bar{E}:\bar{F}]$ (resp. $[S:R] = [E_0:F_0]$.)

Proposition 7.2. *Soit E/F une extension de corps valués modérée non ramifiée de degré finie avec F hensélien et $gr(E)/gr(F)$ l'extension des corps gradués associés alors $gr(E)/gr(F)$ est simple.*

Démonstration. Si E/F est une extension de corps valués modérée alors le quotient $gr(E)/gr(F)$ est gr-séparable non ramifiée. De plus, $gr(E) = gr(F)gr(E)_0$ lequel est une extension séparable de $gr(F)$ si et seulement si l'extension de corps $gr(E)_0/gr(F)_0$ est fini séparable donc $gr(E)_0/gr(F)_0$ est une extension simple. De plus si $gr(E)_0 = gr(F)_0(x)$ alors $gr(E) = gr(F).gr(E)_0 = gr(F)(x)$. □

Rappelons qu'une extension E/F de corps valués modérément ramifiée de degré finie (resp. une extension S/R de corps gradués de degré fini) est dite totalement ramifiée si $[E:F] = (\Gamma_E:\Gamma_F)$ (resp. $[S:R] = (\Gamma_S:\Gamma_R)$.)

Proposition 7.3. *Soit E/F une extension de corps valués modérée totalement ramifiée de degré finie avec F hensélien et $gr(E)/gr(F)$ l'extension des corps gradués associés alors :*

1) $gr(E)/gr(F)$ est simple si et seulement si Γ_E/Γ_F est cyclique.
2) E/F simple entraîne $gr(E)/gr(F)$ est simple

Démonstration. 1) Il est vrai que si E/F est une extension valuée telle que (F, v) est hensélien, alors il est vrai que tous les conjugués sur F d'un $z \in E$ (resp. d'un $\tilde{x}$ de $gr(E)$) ont la même valuation (resp. le même grade), alors :
$deg(f_{z/F}(X)) = deg(\tilde{f}_{z/F}(X))$ et $f_{\tilde{z}/gr(F)}(X)$ divise $\tilde{f}_{z/F}(X)$.
Sous les hypothèses énoncées si $\Gamma_E = \Gamma_F(\alpha) = \Gamma_{gr(E)}$ considérons alors $\tilde{z} \in gr(E)$ tel que $gr(\tilde{z}) = \alpha$ alors $\Gamma_{gr(F)(\tilde{z})} = \Gamma_F(\alpha)$ et $f_{\tilde{z}/gr(F)}(X)$ est de la forme $X^d + T$, où d est l'ordre de α par rapport à Γ_F. En effet, $d\ \mathrm{gr}(\tilde{z}) = d\alpha = gr(\tilde{a}) \in \Gamma_{gr(F)}$, pour un $\tilde{a} \in gr(F)$. Donc $gr(\frac{\tilde{z}^d}{\tilde{a}}) = 0$ et il existe donc $\tilde{\beta} \in \bar{E} = \bar{F}$ tel que $\frac{\tilde{z}^d}{\tilde{a}} = \tilde{\beta}$. Conséquence de quoi $\tilde{z}$ est racine de $X^d - \tilde{\beta}\tilde{a} \in gr(F)$ et donc $f_{\tilde{z}/gr(F)}(X)$ divise $X^d - \tilde{\beta}\tilde{a}$. Si $\deg(f_{\tilde{z}/gr(F)}(X)) = e < d$, le fait que F est hensélien entraîne que toutes les conjuqués de $\tilde{z}$ ont le même grade et ils sont en nombre de e et $e\alpha = gr(b_0)$ si $f_{\tilde{z}/gr(F)}(X) = X^e + .. + b_0$, chose absurde car l'ordre de α sur $\Gamma_{gr(F)}$ est d. Donc $[gr(F)(\tilde{z}) : gr(F)] = deg(f_{\tilde{z}/gr(F)}(X)) = d = [gr(E) : gr(F)] = [E : F]$, d'où $gr(E)/gr(F)$ est simple.
Pour la réciproque, il a été montré dans [5, Corollaire 2, p.26] : pour qu'une extension de corps gradués soit simple il faut que Γ_E/Γ_F soit cyclique.
2) Si $E = F(x)$ alors $\Gamma_E = \Gamma_F(v(x))$ est donc Γ_E/Γ_F est cyclique et alors $gr(E)/gr(F)$ est simple. □

Théorème 7.4. *Soit E/F une extension de corps valués modérée finie avec F hensélien et $gr(E)/gr(F)$ l'extension des corps gradués associés alors :*
E/F est une extension simple engendrée par z et $\tilde{f}_{z/F}(X)$ est gr-séparable si et seulement si l'extension $gr(E)/gr(F)$ est simple engendrée par $\tilde{z}$.

Démonstration. Soit E une extension valuée modérée de F et soit

$$f_{z/F}(X) = X^n + \Sigma_{i=0}^{n-1} a_i X^i$$

le polynôme minimal d'un $z \in E$ par rapport à F. En tenant compte de la Remarque 1, le fait que $f_{z/F}(X)$ est irréductible entraîne que $v(a_i) \geq v(a_0)(1 - \frac{i}{n})$ d'après la conséquence de la section précédente. De plus $\tilde{f}_{z/F}(X)$ est irréductible d'après [4, Th.2.5]. Donc $\tilde{f}_{z/F}(X) = f_{\tilde{z}/gr(F)}(X)$, car $\tilde{z}$ est une racine de $\tilde{f}_{z/F}(X)$. Or $deg(f_{\tilde{z}/gr(F)}(X)) = [gr(F)(\tilde{z}) : F] \leq$

$[gr(F(z)) : gr(F)] = [F(z) : F] = deg(f_{z/F}(X))$. Donc $gr(F(z)) = gr(F)(\tilde{z})$. Inversement si $gr(E) = gr(F)(\tilde{z})$ alors

$$\begin{aligned}[F(z)\colon F] = deg(f_{z/F}(X)) \leq [E\colon F] \\ &= [gr(E)\colon gr(F)] = [gr(F)(\tilde{z})\colon gr(F)] \\ &= deg(f_{\tilde{z}/gr(F)}(X)) \leq deg(\tilde{f}_{z/F}(X)) = deg(f_{z/F}(X)).\end{aligned}$$

Donc $[F(z)\colon F] = [E\colon F]$ ou encore $E = F(z)$. De plus

$$\begin{aligned}deg(\tilde{f}_{z/F}(X)) = deg(f_{z/F}(X)) = [F(z)\colon F] = [E\colon F] \\ &= [gr(E)\colon gr(F)] = deg(f_{\tilde{z}/gr(F)}(X)),\end{aligned}$$

donc $f_{\tilde{z}/gr(F)}(X) = \tilde{f}_{z/F}(X)$, or $f_{\tilde{z}/gr(F)}(X)$ est gr-séparable vu que $gr(E)/gr(F)$ l'est. $\square$

Remarque 3 : On peut avoir,
1) $F(z)/F$ modérée et $gr(E)/gr(F)$ séparable non simple.
Exemple : Si $F(z)/F$ est une extension modérément ramifiée telle que $\Gamma_{F(z)}/\Gamma_F$ est la somme directe de deux groupes cycliques d'ordre différents non premiers entre eux :
$F = K(X, Y)$ et $E = K(X^{\frac{1}{2}}, Y^{\frac{1}{4}})$ où K est un corps de caractéristique nulle. Alors E/F est algébrique simple de plus $gr(F) = K[U, V]$ et $gr(E) = K[U^{\frac{1}{2}}, V^{\frac{1}{4}}]$ et alors $gr(E)/gr(F)$ est gr-séparable car la caractéristique de K est différente de deux et $gr(E)/gr(F)$ est non simple car $\Gamma_{gr(E)}/\Gamma_{gr(F)}$ est non cyclique.
2) $F(z)/F$ modéré et $\tilde{f}_{z/F}^{(\frac{v(a_0)}{n})}(X)$ non gr-séparable, comme le montre l'exemple suivant :
$F = \mathbf{Q}_3$ et $E = \mathbf{Q}_3(3^{\frac{1}{2}}, 7^{\frac{1}{2}})$ alors :
- le polynôme minimal de $3^{\frac{1}{2}} + 7^{\frac{1}{2}}$ est
$f(X) = X^4 - 20X^2 + 16$.
- $\tilde{f}^{(\frac{v_3(16)}{4})}(X) = X^4 - 2X^2 + 1 = (X^2 - 1)^2$.

Références

[1] M. Boulagouaz – *The graded and tame extension*, vol. Lecture note in pures and applied mathematics $n^0$153, M. Dekker Inc., New York, 1993.

[2] ———, « Le gradué d'une algèbre à division valuée », *Communication in Algebra* **23** (1995), no. 11, p. 4275–4300.

[3] ———, « Algèbre à division graduée centrale », *Communication in Algebra* **26** (1998), no. 9, p. 2933–2947.

[4] ———, « Une généralisation du lemme de hensel », *Bulletin of the belgian Mathematical Society Simon Stevin* **4** (1998), p. 665–673.

[5] ———, « An introduction to the Galois theory for graded fields », Algebra and number theory (Fez), Lecture Notes in Pure and Appl. Math., vol. 208, Dekker, New York, 2000, p. 21–31.

[6] Y.-S. Hwang et A. R. Wadsworth – « Algebraic extensions of graded and valued fields », *Comm. Algebra* **27** (1999), no. 2, p. 821–840.

[7] ———, « Correspondences between valued division algebras and graded division algebras », *J. Algebra* **220** (1999), no. 1, p. 73–114.

M'hammed Boulagouaz
Département de Mathématiques
Faculté des Sciences et Techniques
UFR : Algèbre-théorie des nombres et
applications aux sciences de l'information
Fès
MAROC
boulag@rocketmail.com