De noveaux invariants numériques pour les extensions totalement ramifiées de corps locaux

Volker Heiermann

Institut für Reine Mathematik
Humboldt-Universität

D-10099 Berlin

Germany

Max-Planck-Institut für Mathematik
Gottfried-Claren-Straße 26
D-53225 Bonn

Germany

MPI / 94-122

De nouveaux invariants numériques pour les extensions totalement ramifiées de corps locaux

par *Volker Heiermann* de Berlin

Introduction

Une étude des extensions totalement ramifiées d'un corps local K à partir d'équations définissantes a été débutée simultanément par Arf [A] et Krasner [Kr1] dans les années 30. Ils en tirent notamment le théorème de Hasse-Arf dans le cas général [A] et le nombre d'extensions de degré donné d'un corps $\wp$-adique dans une clôture algébrique [Kr2].

Alors que Krasner adoptait le point de vue des polynômes d'Eisenstein avec comme outil technique le polygone de Newton, Arf a considéré un autre type d'équations qui est défini à partir de séries formelles:

En fixant une uniformisante t de l'anneau des entiers A de K, on fait correspondre à tout couple $(\mathcal{F}, n)$ formé d'une série formelle inversible $\mathcal{F}$ à coefficients dans A et d'un entier $n \geq 1$, une - à K-isomorphisme près - unique extension totalement ramifiée L de K dont une uniformisante u vérifie l'équation

$$(*) \qquad t = u^n \mathcal{F}(u).$$

Nous allons approfondir ici l'étude d'Arf et de Krasner. Notre résultat principal sont de nouveaux invariants numériques qui améliorent l'information donnée par la fonction de Herbrand.

Nous adopterons le point de vue d'Arf qui présente les avantages suivants:

- Il est mieux adapté à l'étude des substitutions de la forme $u \mapsto v^m \mathcal{X}(v)$ dans (*) (avec $\mathcal{X}$ série formelle inversible à coefficients dans A) qui décrivent complètement la catégorie des extensions totalement ramifiées de K.

- Il est mieux adapté au passage au quotient. Ceci est particulièrement intéressant dans le contexte de la théorie d'approximation de corps locaux de Krasner et Deligne [De1] dont le résultat principal est le suivant:
Soit K' un corps local dont l'anneau des entiers A' vérifie

$$A'/m_{A'}^{l+1} \simeq A/m_A^{l+1}$$

pour un entier $l \geq 1$. Alors, il existe un isomorphisme de groupe

$$\mathrm{Gal}(K'^{sep}/K')/\mathrm{Gal}(K'^{sep}/K')^l \longrightarrow \mathrm{Gal}(K^{sep}/K)/\mathrm{Gal}(K^{sep}/K)^l$$

entre les groupes de Galois d'extensions separables maximales données de K et K', quotientés par leur $l^{\text{ème}}$ groupe de ramification en notation supérieure.

Après avoir donné quelques préliminaires et fixé les notations au premier paragraphe, nous reformulons l'approche d'Arf au deuxième paragraphe dans un langage moderne et rigoureux, celui des catégories: Nous définissons une catégorie dont les objets sont les couples $(\mathcal{F}, n)$, formé d'une série formelle inversible $\mathcal{F}$ à coefficients dans un système de représentants multiplicatifs de A et d'un entier $n \geq 1$, et dont les morphismes sont définis par les substitutions de la forme $\mathcal{F} \to \mathcal{F}(U^m\,\mathcal{X})\,\mathcal{X}^n$ (où U est l'indéterminée et $(\mathcal{X}, m)$ vérifie les mêmes propriétés que $(\mathcal{F}, n)$). Nous montrons que cette catégorie est équivalente à celle des extensions totalement ramifiées de K (cf. théorème 2.18).

Au troisième paragraphe, nous définissons nos invariants à l'aide d'une certaine notion d'inséparabilité d'extensions d'anneaux de valuation discrète complets tronqués. Un tel anneau tronqué sera appelé un anneau *discret-complet.* La catégorie des anneaux discrets-complets est la plus grande catégorie d'anneaux à laquelle se généralisent les résultats de ce travail (cf. [T]). Une telle généralisation ne présente pas seulement de l'intérêt en elle-même (en particulier tout anneau commutatif fini est construit à partir d'anneaux discrets-complets finis), mais aussi pour la théorie des corps locaux en raison de la théorie d'approximation de Krasner-Deligne. En effet, le résultat rappelé ci-dessus s'obtient comme corollaire d'une équivalence entre une certaine catégorie d'extensions d'anneaux discrets-complets et une certaine catégorie de corps locaux. En particulier, la propriété d'inséparabilité de nos indices devrait se relever grâce à cette théorie dans le groupe de Galois absolu, ce qui donnerait une autre définition de ces indices.

Au quatrième paragraphe, nous énonçons le résultat principal concernant les substitutions $\mathcal{F} \mapsto \mathcal{F}(U^m\,\mathcal{X})\,\mathcal{X}^n$ (cf. théorème 4.6) avec ses corollaires, y compris le théorème d'Arf (cf. corollaire 4.13). Il est prouvé au paragraphe 5. Dans le paragraphe 6, ces résultats sont traduits dans la catégorie des extensions totalement ramifiées de K. Au septième paragraphe, nous prouvons finalement l'invariance des indices d'inséparabilité (cf. théorème 7.1 et proposition 7.4).

Les résultats de ce travail qui ont été annoncés en partie dans [H] font partie de ma thèse de Doctorat [T], soutenue en janvier 1994 à Marseille à l'Université de Provence sous la direction de J.-P. Soublin. Je l'en suis très reconnaissant. Mes remerciements vont également à P. Deligne pour quelques "petites suggestions" et à E.-W. Zink pour m'avoir conseillé de mieux mettre en valeur la multiplication $*$.

1. Notations et Préliminaires: - Nous nous fixons un anneau de valuation discrète complet A de caractéristique résiduelle p et une uniformisante t de A. Nous noterons v_A la valuation discrète normalisée de A, K le corps des fractions de A, $e(= v_A(p1_A))$ l'indice de ramification absolu de K, k le corps résiduel de A, et $a \mapsto \overline{a}$ l'application résiduelle qui associe à un élément a de A son image $\overline{a}$ dans k.

Nous supposerons l'indice de ramification absolu fini et le corps résiduel k parfait, bien que ces hypothèses ne soient pas absolument nécessaires. (Dans le cas d'égale caractéristique, la situation est même plus simple en raison de l'existence d'un corps de représentants).

Nous noterons S l'unique système de représentants du corps résiduel k dans A qui est multiplicatif (cf. [B]). Si k est fini de cardinal q, S est l'ensemble des racines $(q-1)^{\text{ème}}$ de l'unité. Nous désignerons par κ le plus petit sous-anneau de A contenant S. C'est un anneau de valuation discrète complet dont une uniformisante est donnée par $p1_A$. L'extension A/κ est non-ramifiée dans le sens défini ci-dessous.

Nous dirons qu'un anneau B est une *extension* de A, si B est un anneau de valuation discrète complet qui domine A en tant qu'anneau local. Une extension B/A est dite *finie,* si l'extension résiduelle l'est.

On définit une correspondance biunivoque entre les extensions finies L du corps local K et les extensions finies B de A, en associant à L la clôture intégrale B de A dans L. Le groupe des automorphismes de l'extension L/K s'identifiant à celui de l'extension B/A, la catégorie des extensions finies de K est ainsi isomorphe à celle des extensions finies de A.

Nous dirons qu'une extension finie B de A vérifie une propriété $(\mathcal{P})$, si l'extension des corps des fractions vérifie $(\mathcal{P})$. Par exemple, une extension B/A sera dite totalement ramifiée de degré n, si l'extension des corps des fractions est de degré n et si l'extension résiduelle est de degré 1.

Nous noterons $\mathrm{Ext}_{tot}(A,t)$ la catégorie dont les objets sont les couples (B,u) formés d'une extension totalement ramifiée B de A et d'une uniformisante u de B, et dont un morphisme de source (B,u) et de but (C,v) est un A-morphisme de B dans C (on ne suppose pas que u est envoyé sur v), la composition des morphismes étant la composition usuelle.

En associant à un objet (B,u) de la catégorie $\mathrm{Ext}_{tot}(A,t)$ l'anneau B, on définit un foncteur quasi-inversible de la catégorie $\mathrm{Ext}_{tot}(A,t)$ dans la catégorie $\mathrm{Ext}_{tot}(A)$ des extensions totalement ramifiées de A.

Par ailleurs, nous utiliserons dans la suite les notations suivantes:

$]z[$: plus petit entier $\geq z$, z nombre réel;

$\mathrm{coeff}(\mathcal{F},\alpha)$: coefficient du terme de degré α d'une série formelle $\mathcal{F}$ de $A[[U]]$;

$\overline{\mathrm{coeff}}(\mathcal{F},\alpha)$: l'image de $\mathrm{coeff}(\mathcal{F},\alpha)$ dans k.

2. Extensions totalement ramifiées et séries formelles

(2.1) Posons $E_A = A[[U]]^* \times \mathbf{N}^*$. Nous appelerons *degré* (resp. *série sous-jacente*) d'un élément de E_A l'entier (resp. la série formelle) correspondant à cet élément.

Tout élément de E_A définit une extension totalement ramifiée de A, comme le font les polynômes d'Eisenstein:

(2.2) Théorème: *Soit $(\mathcal{F}, n)$ un élément de E_A. Alors, l'anneau*

$$A_{\mathcal{F}} = A[[U]]/(t - U^n\,\mathcal{F})A[[U]]$$

est une extension totalement ramifiée de degré n de A dont une uniformisante est donnée par la classe $\widetilde{U}$ de U.

Si B est une extension totalement ramifiée de A, et si u est une uniformisante de B, telle que $t = u^n\,\mathcal{F}(u)$, il existe un unique A-isomorphisme de $A_{\mathcal{F}}$ sur B qui envoie $\widetilde{U}$ sur u.

Preuve: Existence: Il faut montrer que $A_{\mathcal{F}}$ est un anneau de valuation discrète complet d'uniformisante $\widetilde{U}$, que l'application canonique $A \to A_{\mathcal{F}}$ est injective et que le corps résiduel de $A_{\mathcal{F}}$ s'identifie à celui de A par cette injection.

Rappelons qu'un anneau de valuation discrète est un anneau intègre, local et noethérien dont l'idéal maximal est principal et non nul.

L'anneau $A_{\mathcal{F}}$ est noethérien comme quotient d'un anneau de séries formelles à coefficients dans un anneau noethérien. Comme l'anneau $A[[U]]$ est local d'idéal maximal $M = tA[[U]] + UA[[U]]$, l'anneau $A_{\mathcal{F}}$ est lui aussi local, et son idéal maximal est l'image de M qui est $\widetilde{U}A_{\mathcal{F}}$. Il est facile de voir que tout élément de $A_{\mathcal{F}}$ peut s'écrire sous la forme $\sum_{\alpha=0}^{\infty} s_\alpha \widetilde{U}^\alpha$ avec s_α dans le système de représentants multiplicatifs S. Montrer que $A_{\mathcal{F}}$ est intègre et que $\widetilde{U}A_{\mathcal{F}} \neq 0$ revient donc à prouver que $\widetilde{U}$ n'est pas nilpotent. Supposons $\widetilde{U}$ nilpotent. Il existe alors un entier $l > 0$ et une série $\mathcal{H}$ de $A[[U]]$, telle que $U^l = (t - U^n\,\mathcal{F})\,\mathcal{H}$. L'anneau A étant intègre, U engendre un idéal premier de $A[[U]]$. Par suite, il existe $\mathcal{H}^*$ dans $A[[U]]$, telle que $\mathcal{H} = U^l\,\mathcal{H}^*$. On a donc $1 = (t - U^n\,\mathcal{F})\,\mathcal{H}^*$, ce qui est absurde, la série $t - U^n\,\mathcal{F}$ n'étant pas inversible dans $A[[U]]$.

L'anneau $A_{\mathcal{F}}$ est donc bien de valuation discrète, et il est clair qu'il est complet. Si l'application canonique $A \to A_{\mathcal{F}}$ n'était pas injective, t serait nilpotent dans $A_{\mathcal{F}}$, et $\widetilde{U}$ serait alors nilpotent dans $A_{\mathcal{F}}$, ce qui est faux comme on vient de le voir.

Il est clair que l'application composée $A \to A_{\mathcal{F}} \to A_{\mathcal{F}}/\widetilde{U}A_{\mathcal{F}}$ est surjective et qu'elle se factorise par l'idéal maximal de A. L'injection $A \to A_{\mathcal{F}}$ induit donc bien un isomorphisme entre les corps résiduels de A et $A_{\mathcal{F}}$.

Unicité: Soit B un autre anneau de valuation discrète complet et u une uniformisante de B, tels que les hypothèses du théorème soient vérifiées. La surjection $A[[U]] \to B$ qui

associe à une série $\mathcal{H}(U)$ l'élément $\mathcal{H}(u)$ de B induit un homomorphisme surjectif entre $A_{\mathcal{F}}$ et B qui est injectif, l'image de $\widetilde{U}$ par cet homomorphisme ne pouvant être nilpotent. □

(2.3) Définition: Soit $(\mathcal{F}, n)$ un élément de E_A. Un objet (B, u) de la catégorie $\mathrm{Ext}_{tot}(A, t)$ qui vérifie $t = u^n\,\mathcal{F}(u)$ sera dit *défini par* $(\mathcal{F}, n)$. On dira aussi que (B, u) *est défini par* $(\mathcal{F}, n)$ *relativement à* (A, t).

(2.4) Proposition: *Soit (B, u) une extension de (A, t) définie par un élément $(\mathcal{F}, n)$ de E_A. Soit F le polynôme minimal de u sur A.*

La série $t - U^n\,\mathcal{F}$ est le produit de F par un inversible de $A[[U]]$. Si $\mathcal{F}$ n'est pas un polynôme, les éléments de B qui annulent la série $t - U^n\,\mathcal{F}$ sont exactement les racines de F dans B. Si $\mathcal{F}$ est un polynôme, $t - U^n\,\mathcal{F}$ est le produit de F par un polynôme H dont les racines, dans toute extension finie de A, sont des unités (de cet anneau).

Preuve: Ceci résulte du théorème de préparation de Weierstrass (cf. [L]). □

(2.5) Remarque: La proposition montre que, si $\mathcal{F}$ est un polynôme, les anneaux $A[[U]]/(t - U^n\,\mathcal{F})A[[U]]$ et $A[U]/(t - U^n\,\mathcal{F})A[U]$ ne sont en général pas isomorphes. Pour qu'ils soient isomorphes, il faut (et il suffit) que $\mathcal{F}$ soit constant.

(2.6) Corollaire: (avec les hypothèses et notations de la proposition 2.4) *La différente de l'extension B/A est l'idéal principal de B, engendré par la dérivée de $U^n\,\mathcal{F}(U)$ en u.*

Preuve: Ecrivons $F = (t - U^n\,\mathcal{F})\,\mathcal{H}$. La différente de B/A est l'idéal principal engendré par la dérivée de F en u (cf. [Se] ch. III §6). Compte tenu de la proposition 2.4, la dérivée de F en u est égal au produit de la dérivée de $U^n\,\mathcal{F}(U)$ en u par un inversible de B, d'où le corollaire. □

(2.7) Il existe évidemment une infinité de couples de E_A définissant un objet (B, u) donné de la catégorie $\mathrm{Ext}_{tot}(A, t)$. Pour avoir une unicité, posons $E_k = S[[U]]^* \times \mathbb{N}^*$, $S[[U]]^*$ désignant le sous-ensemble de $A[[U]]^*$, formé des séries formelles à coefficients dans S.

(2.8) Proposition: *Soient $(\mathcal{F}, n)$ dans E_A, et (B, u) un objet de $\mathrm{Ext}_{tot}(A, t)$ défini par $(\mathcal{F}, n)$. Il existe un unique élément $(\mathcal{F}_S, n)$ dans E_k définissant (B, u) relativement à*

(A,t). *On a*

$$\mathcal{F}_S = (1+U^n\,\mathcal{R})\,\mathcal{F} - t\,\mathcal{R},$$

où $\mathcal{R}$ *est déterminée de façon unique comme élément de* $A[[U]]$.

Preuve: Comme $n \geq 1$, les coefficients r_α de $\mathcal{R}$ sont déterminés de manière unique par la relation de récurrence

$$-r_\alpha t + \mathrm{coeff}((1+U^n\,\mathcal{R})\,\mathcal{F}, \alpha) \quad \text{est dans } S.$$

Par ailleurs, on a

$$\begin{aligned} u^n\,\mathcal{F}_S(u) &= u^n\{(1+u^n\,\mathcal{R}(u))\,\mathcal{F}(u) - t\,\mathcal{R}(u)\} \\ &= u^n\,\mathcal{F}(u) + u^n\,\mathcal{R}(u)\{u^n\,\mathcal{F}(u) - t\} \\ &= t. \end{aligned}$$

L'unicité de $\mathcal{F}_S$ est évidente, tout élément de B s'écrivant de façon unique comme série en u à coefficients dans S. □

(2.9) Définition: (avec les hypothèses et notations de la proposition 2.8) Le couple $(\mathcal{F}_S, n)$ sera appelé la *classe* modulo t de $(\mathcal{F}, n)$ et la série formelle $\mathcal{R}$ le *reste* modulo t de $(\mathcal{F}, n)$.

On va munir l'ensemble E_k d'une multiplication, ce qui nous permettra d'énoncer une équivalence entre la catégorie des extensions totalement ramifiées de (A,t) et une certaine catégorie $E_k(\Delta)$ définie à partir de E_k et d'une multiplication $*_\Delta$.

(2.10) On notera $\Delta = (\mathcal{F}_0, e)$ l'élément de E_k qui définit (A,t) relativement à $(\kappa, p1_\kappa)$, κ étant l'anneau de coefficients de A (cf. [B] et paragraphe 1).

(2.11) Définition - Proposition: *En associant à deux éléments* $(\mathcal{X}, m)$ *et* $(\mathcal{F}, n)$ *de* E_k *le couple* $(\mathcal{G}, mn)$ *qui est la classe modulo* t *de* $(\mathcal{F}(U^m\,\mathcal{X})\,\mathcal{X}^n, mn)$, *on munit l'ensemble* E_k *d'une loi de composition.*

On écrira

$$(\mathcal{G}, mn) = (\mathcal{X}, m) *_\Delta (\mathcal{F}, n).$$

Preuve: La multiplication $*_\Delta$ ne dépend pas du choix de l'extension (A,t) de $(\kappa, p1_\kappa)$ définie par Δ, car deux extensions définies par Δ sont isomorphes par un isomorphisme qui envoie l'uniformisante de l'une sur l'uniformisante de l'autre et qui laisse invariant l'anneau κ et le système de représentants S (cf. théorème 2.2). □

(2.12) Proposition: *Soient $(\mathcal{X},m)$, $(\mathcal{F},n)$ dans E_k, (B,u) une extension de (A,t) définie par $(\mathcal{F},n)$, et (C,v) une extension de (B,u) définie par $(\mathcal{X},m)$.*

Pour qu'un élément $(\mathcal{G},mn)$ de E_k vérifie

$$(\mathcal{G},mn) = (\mathcal{X},m) *_\Delta (\mathcal{F},n),$$

il faut et il suffit que

$$t = v^{mn}\,\mathcal{G}(v).$$

Preuve: Comme

$$v^{mn}(\mathcal{X}(v))^n\,\mathcal{F}(v^m\,\mathcal{X}(v)) = (v^m\,\mathcal{X}(v))^n\,\mathcal{F}(v^m\,\mathcal{X}(v)) = u^n\,\mathcal{F}(u) = t,$$

l'extension (C,v) est définie par $\mathcal{X}^n\,\mathcal{F}(U^m\,\mathcal{X})$ relativement à (A,t). Compte tenu de la proposition 2.8, l'égalité

$$t = v^{mn}\,\mathcal{G}(v)$$

revient à dire que $(\mathcal{G},mn)$ est la classe modulo t de $(\mathcal{X}^n\,\mathcal{F}(U^m\,\mathcal{X}),mn)$ dans E_k, ce qui équivaut par définition à

$$(\mathcal{G},mn) = (\mathcal{X},m) *_\Delta (\mathcal{F},n).$$ □

(2.13) Proposition: *Soient (B,u) et (C,v) des extensions de (A,t) définies respectivement par des éléments $(\mathcal{F},n)$ et $(\mathcal{G},mn)$ de E_k.*

On définit une bijection entre l'ensemble des éléments $(\mathcal{X},m)$ de E_k, tels que

$$(\mathcal{G},mn) = (\mathcal{X},m) *_\Delta (\mathcal{F},n)$$

et l'ensemble des A-morphismes de B dans C, en associant à $(\mathcal{X},m)$ le A-morphisme qui envoie u sur $v^m\,\mathcal{X}(v)$.

Preuve: Soit σ un A-morphisme de B dans C. Il est évidemment injectif, et le couple $(\sigma(B),\sigma(u))$ est également défini par $(\mathcal{F},n)$ relativement à (A,t). Soit $(\mathcal{X},m)$ l'élément de E_k qui définit (C,v) relativement à $(\sigma(B),\sigma(u))$. On a donc $\sigma(u) = v^m\,\mathcal{X}(v)$, ce qui implique

$$(\mathcal{G},mn) = (\mathcal{X},m) *_\Delta (\mathcal{F},n),$$

en raison de 2.12.

Inversement, soit $(\mathcal{X},m)$ un élément de E_k qui vérifie

$$(\mathcal{G},mn) = (\mathcal{X},m) *_\Delta (\mathcal{F},n).$$

Soit (C',v') une extension de (B,u) définie par $(\mathcal{X},m)$. Le théorème 2.2 montre qu'il existe un A-isomorphisme σ de C' sur C qui envoie v' sur v. Sa restriction à gauche à B est un A-morphisme de B dans C qui envoie u sur

$$\sigma(u) = \sigma(v'^m\,\mathcal{X}(v')) = v^m\,\mathcal{X}(v).$$

Ayant deux applications, l'une l'inverse de l'autre, ceci prouve la proposition. □

(2.14) Lemme: *Soit B un anneau de valuation discrète complet, et soit $\mathcal{X}$ une série formelle inversible de $A[[U]]$. L'application $u \mapsto u\,\mathcal{X}(u)$ permute les uniformisantes de B.*

Preuve: Voir par exemple [Kr1], page 142. □

Notons quelques propriétés formelles de la multiplication $*_\Delta$:

(2.15) Proposition: *La multiplication $*_\Delta$ vérifie les propriétés suivantes:*
1) *Son élément neutre est $(1,1)$.*
2) *Pour qu'un élément $(\mathcal{X},m)$ de E_k soit inversible, il faut et il suffit que $m=1$.*
3) *On a*

$$(\mathcal{Y},l) *_\Delta [(\mathcal{X},m) *_\Delta (\mathcal{F},n)] = [(\mathcal{Y},l) *_\Theta (\mathcal{X},m)] *_\Delta (\mathcal{F},n)$$

pour tous $(\mathcal{Y},l)$, $(\mathcal{X},m)$ de E_k avec $\Theta = (\mathcal{F},n) *_{(1,1)} \Delta$.

Preuve: Il est clair que $(1,1)$ est un élément neutre, et on sait qu'une loi de composition admet au plus un élément neutre.

La condition $m=1$ est alors nécessaire, pour que $(\mathcal{X},m)$ soit inversible. Elle est suffisante en raison du lemme 2.14 et de la proposition 2.12.

La propriété 3) découle immédiatement de 2.12. □

(2.16) Définition: Soit $E_k(\Delta)$ la collection dont les objets sont les éléments de E_k.

1) Pour deux objets $(\mathcal{F},n)$ et $(\mathcal{G},l)$ donnés de $E_k(\Delta)$, on appellera *morphisme* de source $(\mathcal{F},n)$ et de but $(\mathcal{G},l)$ un élément $(\mathcal{X},m)$ de E_k qui vérifie

$$(\mathcal{G},l) = (\mathcal{X},m) *_\Delta (\mathcal{F},n).$$

2) Pour trois objets $(\mathcal{F},n)$, $(\mathcal{G},m)$ et $(\mathcal{H},l)$ donnés de $E_k(\Delta)$, la *loi de composition*

$$\mathrm{Mor}((\mathcal{G},m),(\mathcal{H},l)) \times \mathrm{Mor}((\mathcal{F},n),(\mathcal{G},m)) \to \mathrm{Mor}((\mathcal{F},n),(H,l))$$

sera définie par la multiplication $*_\Theta$ avec $\Theta = (\mathcal{F},n) *_{(1,1)} \Delta$.

(2.17) Proposition: *La collection $E_k(\Delta)$ munie des données de la définition* 2.16 *est une catégorie dont les isomorphismes sont les éléments de la forme $(\mathcal{X},1)$ de E_k.*

Preuve: Ceci résulte de la proposition 2.15: En effet, l'associativité de la composition des morphismes découle de la propriété 3), alors que la propriété 1) montre que, pour tout objet $(\mathcal{F},n)$ de $E_k(\Delta)$, $(1,1)$ est un morphisme de source $(\mathcal{F},n)$ et de but $(\mathcal{F},n)$ qui est

l'élément neutre pour la composition des morphismes. La propriété 2) montre finalement que les isomorphismes sont les éléments de la forme $(\mathcal{X}, 1)$ de E_k. □

(2.18) Théorème: *En associant à tout objet (B,u) de la catégorie $\mathrm{Ext}_{tot}(A,t)$ l'objet $\mathcal{T}(B,u) = (\mathcal{F},n)$ de la catégorie $E_k(\Delta)$ qui définit (B,u) relativement à (A,t), et en associant à un morphisme σ de source (B,u) et de but (C,v), le morphisme $\mathcal{T}(\sigma) = (\mathcal{X},m)$ de source $\mathcal{T}(B,u)$ et de but $\mathcal{T}(C,v)$, tel que $\sigma(u) = v^m\,\mathcal{X}(v)$, on définit un foncteur quasi-inversible de la catégorie $\mathrm{Ext}_{tot}(A,t)$ dans la catégorie $E_k(\Delta)$.*

En particulier, les catégories $\mathrm{Ext}_{tot}(A,t)$ et $E_k(\Delta)$ sont équivalentes.

Preuve: Le théorème 2.2 montre que, pour tout objet (B,u) de $\mathrm{Ext}_{tot}(A,t)$, $\mathcal{T}(B,u)$ ainsi défini est un objet de la catégorie $E_k(\Delta)$. La proposition 2.12 montre que, pour tout morphisme σ de la catégorie $\mathrm{Ext}_{tot}(A,t)$, $\mathcal{T}(\sigma)$ est un morphisme de la catégorie $E_k(\Delta)$.

Si $\sigma = \mathrm{id}_{(B,u)}$, on a $\mathcal{T}(\sigma) = (1,1)$. Le fait que $\mathcal{T}$ est compatible avec la composition des morphismes résulte également de la proposition 2.12.

Le foncteur $\mathcal{T}$ est pleinement fidèle en raison de la proposition 2.13.

Finalement, si $(\mathcal{F},n)$ est un objet de $E_k(\Delta)$, et si (B,u) est une extension de (A,t) définie par $(\mathcal{F},n)$, alors (B,u) est un objet de $\mathrm{Ext}_{tot}(A,t)$ qui vérifie $\mathcal{T}(B,u) = (\mathcal{F},n)$, ce qui montre que $\mathcal{T}$ est quasi-inversible. □

3. Inséparabilité formelle

(3.1) Définition: Un *anneau discret-complet* sera un anneau commutatif qui n'est pas un corps et qui est l'image d'un anneau de valuation discrète complet par un homomorphisme.

(3.2) Fixons pour la suite un anneau discret-complet $\widehat{A}$ qui est l'image de A par un homomorphisme noté $a \mapsto \widehat{a}$ dans ce paragraphe. Cet anneau est local et son unique idéal maximal $m_{\widehat{A}}$ est principal, engendré par $\widehat{t}$. Sa caractéristique résiduelle est p, et $\widehat{S}$ est l'unique système de représentants de k dans $\widehat{A}$ qui est multiplicatif.

On dira que $\widehat{t}$ est une *uniformisante* de $\widehat{A}$. L'application $v_{\widehat{A}} : \widehat{A} \to \mathbf{Z} \cup \{+\infty\}$ qui associe à un élément non nul $\widehat{a}$ de $\widehat{A}$ le plus grand entier v, tel que $\widehat{a} \in m_{\widehat{A}}^v$, et qui vérifie $v_{\widehat{A}}(0) = +\infty$ sera appelée la *pseudo-valuation* de $\widehat{A}$. La borne supérieure dans $\overline{\mathbf{R}}$ de l'ensemble des entiers $l > 0$, tels que $\widehat{t}^{l-1} \neq 0$, sera appelée la *longueur de* $\widehat{A}$, notée $l(\widehat{A})$. Remarquons que l'anneau $\widehat{A}$ est un anneau de valuation discrète complet, si et seulement si sa longueur est $+\infty$.

Une *extension* de $\widehat{A}$ sera un anneau discret-complet $\widehat{B}$ qui domine $\widehat{A}$ en tant qu'anneau local. Lorsque $\widehat{B}$ est une extension de $\widehat{A}$, l'entier $e = v_{\widehat{B}}(\widehat{t})$ sera appelé l'*indice de ramifica-*

tion et l'entier $f = [\widehat{B}/m_{\widehat{B}} : \widehat{A}/m_{\widehat{A}}]$ le *degré résiduel* de l'extension. On dira que l'extension $\widehat{B}/\widehat{A}$ est *totalement ramifiée* si son degré résiduel est 1 et qu'elle est *non-ramifiée* si son indice de ramification est 1. Le *degré* de l'extension $\widehat{B}/\widehat{A}$, noté $[\widehat{B} : \widehat{A}]$, sera le produit ef de son indice de ramification e avec son degré résiduel f. Remarquons que, comme l'extension résiduelle est séparable, l'extension $\widehat{B}/\widehat{A}$ se décompose par le lemme de Hensel en une extension non-ramifiée suivie d'une extension totalement ramifiée.

(3.3) Définition: Un élément $\widehat{u}$ d'un sur-anneau de $\widehat{A}$ sera dit de *degré fini* sur $\widehat{A}$, si $\widehat{A}[\widehat{u}]$ est une extension finie de $\widehat{A}$. L'entier $[\widehat{A}[u] : \widehat{A}]$ sera appelé le *degré* de u sur $\widehat{A}$.

Par exemple, toute uniformisante d'une extension totalement ramifiée de degré n de $\widehat{A}$ est de degré n sur $\widehat{A}$. Si $\widehat{B}/\widehat{A}$ est une extension non-ramifiée de degré n, tout élément de $\widehat{B}$ dont l'image engendre l'extension résiduelle est de degré n sur $\widehat{A}$.

(3.4) Définition: Soit $\widehat{u}$ un élément de degré n sur $\widehat{A}$. On dira que $\widehat{u}$ est *formellement inséparable* sur $\widehat{A}$, si $\widehat{u}^p$ est de degré $\frac{n}{p}$ sur $\widehat{A}$. La plus grande puissance p^j de p, telle que $\widehat{u}^{p^j}$ soit de degré $\frac{n}{p^j}$ sur $\widehat{A}$, sera appelée le *degré d'inséparabilité formelle* de $\widehat{u}$ sur $\widehat{A}$.

(3.5) Proposition: *Soient $\widehat{u}$ une uniformisante d'une extension totalement ramifiée de degré n de $\widehat{A}$. Pour que le degré d'inséparabilité formelle de $\widehat{u}$ sur $\widehat{A}$ soit $\geq p^j$, il faut et il suffit que p^j divise n et qu'il existe une série formelle $\widehat{\mathcal{F}}$ dans $\widehat{S}[[U^{p^j}]]$, telle que $\widehat{t} = \widehat{u}^n \widehat{\mathcal{F}}(\widehat{u})$.*

Preuve: Ecrivons $\widehat{t} = \widehat{u}^n \widehat{\mathcal{F}}(\widehat{u})$ avec $\widehat{\mathcal{F}}$ dans $\widehat{S}[[U]]^*$. Si $\widehat{\mathcal{F}}$ est dans $\widehat{S}[[U^{p^j}]]$, on peut écrire $\widehat{t} = (\widehat{u}_j)^{\frac{n}{p^j}} \widehat{\mathcal{F}}_j(\widehat{u}_j)$, où $\widehat{u}_j = \widehat{u}^{p^j}$ et $\widehat{\mathcal{F}}_j$ est l'élément de $\widehat{S}[[U]]^*$ qui vérifie $\widehat{\mathcal{F}}_j(U^{p^j}) = \widehat{\mathcal{F}}(U)$. En relevant $\widehat{\mathcal{F}}_j$ en un élément de $S[[U]]^*$, on conclut du théorème 2.2 que $\widehat{A}[\widehat{u}^{p^j}]$ est un anneau discret-complet.

Réciproquement, supposons $\widehat{u}$ de degré d'inseparabilité formelle $\geq p^j$ sur $\widehat{A}$. Alors, on vérifie facilement que $\widehat{u}^{p^j}$ est une uniformisante de $\widehat{A}[\widehat{u}^{p^j}]$ et que $\widehat{S}$ est un système de représentants du corps résiduel dans cet anneau. On peut donc choisir un élément $\widehat{\mathcal{F}}$ dans $\widehat{S}[[U]]$, tel que $\widehat{t} = \widehat{u}^n \widehat{\mathcal{F}}(\widehat{u}^{p^j})$, et la série $\widehat{\mathcal{F}}(U^{p^j})$ a toutes les propriétés demandées. □

(3.6) Définition: Soient u une uniformisante d'une extension totalement ramifiée B de degré n de A, et j un entier, $0 \leq j < v = v_p(n)$.

On appelera *indice d'inséparabilité d'ordre j* de u sur A, noté $\widetilde{\imath}_j(A, u)$, le plus grand entier i, tel que l'image $\widehat{u}$ de u dans B/m_B^{n+i} soit de degré d'inséparabilité formelle $\geq p^{j+1}$ sur $A/A \cap m_B^{n+i}$. Si un tel entier n'existe pas, on posera $\widetilde{\imath}_j(A, u) = +\infty$. On fait la convention que $\widetilde{\imath}_v(A, u) = 0$.

(3.7) Définition: Soit $(\mathcal{F}, n)$ un élément de E_k. Soit j un entier, $0 \leq j < v = v_p(n)$. On appellera *indice d'ordre j* de $(\mathcal{F}, n)$, noté $\widetilde{\imath}_j(\mathcal{F}, n)$, le plus petit entier i de valuation

p-adique $\leq j$, tel que le terme de degré i de la série $\mathcal{F}$ soit non nul. Si un tel entier n'existe pas, on posera $\widetilde{i}_j(\mathcal{F},n) = +\infty$. On fait la convention que $\widetilde{i}_v(\mathcal{F},n) = 0$.

(3.8) Exemple: Supposons $p > 3$, $n = p^2$ et

$$\mathcal{F} = 1 + U^{p^2+p} + U^{3p^2+p} + U^{4p^2+p-3} + U^{4p^2+5p+1}.$$

Alors, on trouve

$$\widetilde{i}_2 = 0, \qquad \widetilde{i}_1 = p^2 + p, \qquad \widetilde{i}_0 = 4p^2 + p - 3.$$

(3.9) Proposition: *Soit (B,u) un objet de $\mathrm{Ext}_{tot}(A,t)$, défini par un élément $(\mathcal{F},n)$ de E_k. Alors, les indices d'inséparabilité de u sont donnés par les indices de $(\mathcal{F},n)$.*

Preuve: Soit j un entier, $0 \leq j \leq v_p(n)$. Le cas $j = v_p(n)$ étant trivial, supposons $j < v_p(n)$. Notons i l'indice d'ordre j de $\mathcal{F}$. La série formelle $\mathcal{F}_i$, formé des termes de degré $< i$ de $\mathcal{F}$, est un élément de $A[[U^{p^{j+1}}]]$ qui vérifie la congruence

$$t \equiv u^n\, \mathcal{F}_i(u) \qquad \mod\ m_B^{n+i},$$

ce qui prouve que le degré d'inséparabilité formelle de l'image de u dans $B/m_B^{n+i}B$ sur $A/A \cap m_B^{n+i}B$ est $\geq p^{j+1}$ (cf. proposition 3.5).

Par contre, si $\mathcal{G}$ est une série formelle à coefficients dans S qui vérifie

$$t \equiv u^n\, \mathcal{G}(u) \qquad \mod\ m_B^{i'}$$

pour un entier $i' > i$, alors son terme de degré i est nécessairement non nul, tout élément de B s'écrivant de manière unique comme série en u à coefficients dans le système de représentants S. Elle ne peut donc être un élément de $S[[U^{p^{j+1}}]]^*$, ce qui prouve que l'image de u dans $B/m_B^{n+i'}B$ ne peut être de degré d'inséparabilité formelle $\geq p^{j+1}$ sur $A/A \cap m_B^{n+i'}$. □

(3.10) Corollaire: *Soit t' une autre uniformisante de A. Alors, l'élément $(\mathcal{F}\,',n)$ de E_k qui définit (B,u) relativement à (A,t') a les mêmes indices que $(\mathcal{F},n)$.*

(3.11) Proposition: *Soient B une extension totalement ramifiée de A, u une uniformisante de B, et $F = \sum_{\alpha=0}^{n} a_\alpha X^\alpha$ le polynôme minimal de u sur A. Ecrivons $a_\alpha = \sum_{\beta=1}^{\infty} a_{\alpha,\beta} t^\beta$ avec $a_{\alpha,\beta}$ dans S, et posons $\mathcal{F} = \sum_{\alpha=0}^{n-1} \sum_{\beta=0}^{\infty} a_{\alpha,\beta+1} U^{n\beta+\alpha}$.*

Alors, les indices d'inséparabilités de u sur A sont donnés par les indices de $(\mathcal{F}, n)$.

Preuve: En utilisant une version adaptée de la proposition 3.5, on peut faire un raisonnement analogue à celui qui prouve la proposition 3.9. □

Remarquons qu'il n'y a aucune raison que (B, u) soit défini par le couple $(\mathcal{F}, n)$ de la proposition 3.11. Il a été introduit uniquement pour faire comprendre, comment on trouve les indices d'inséparabilité sur un polynôme d'Eisenstein.

(3.12) Les indices d'inséparabilité d'une uniformisante u d'une extension totalement ramifiée B de A dépendent en général du choix de u, comme le montre l'exemple suivant. Ce ne sont donc pas des invariants de l'extension B/A. Traduit en terme de la catégorie $E_k(\Delta)$, ceci signifie que les indices d'un objet $(\mathcal{F}, n)$ de la catégorie $E_k(\Delta)$ ne constituent pas des invariants de la classe d'isomorphie de $(\mathcal{F}, n)$.

Supposons $e = 1$, $n = p$, $\mathcal{F} = 1$ et $\mathcal{X} = 1 + U$. On a

$$\mathcal{F}(U\,\mathcal{X})\,\mathcal{X}^p = \mathcal{X}^p = \sum_{\alpha=0}^{p} \binom{p}{\alpha} U^\alpha = 1 + U^p + p \sum_{\alpha=1}^{p-1} \frac{1}{p} \binom{p}{\alpha} U^\alpha.$$

Les nombres $\frac{1}{p}\binom{p}{\alpha}$ avec $1 \leq \alpha \leq p-1$ étant des entiers rationnels, le reste $\mathcal{R}$ modulo t par rapport à E_k de $(\mathcal{F}, n)$ est congru à $\sum_{\alpha=1}^{p-1} \frac{1}{p}\binom{p}{\alpha} U^\alpha$ modulo U^{p+1}, d'où

$$\begin{aligned} &\overline{\text{coeff}}((1 + U^p\,\mathcal{R})\,\mathcal{F}(U\,\mathcal{X})\,\mathcal{X}^p, p+1) \\ =&\overline{\text{coeff}}(\mathcal{F}(U\,\mathcal{X})\,\mathcal{X}^p, p+1) + \overline{\text{coeff}}(\mathcal{R}\,\mathcal{F}(U\,\mathcal{X})\,\mathcal{X}^p, 1) \\ =&1. \end{aligned}$$

On voit que l'indice d'ordre 0 de $(\mathcal{F}, p)$ est $+\infty$, alors que l'indice d'ordre 0 de $(\mathcal{G}, p) = (1 + U, 1) *_\Delta (\mathcal{F}, p)$ est $p + 1$.

Pour obtenir des invariants de l'extension B/A (ou de la classe d'isomorphie de $(\mathcal{F}, n)$), il faut régulariser les indices définis au-dessus de la manière suivante (cf. théorème 7.1):

(3.13) Définition: Soient $\widetilde{i}_v$, ...,$\widetilde{i}_0$ les indices d'un objet $(\mathcal{F}, n)$ de $E_k(\Delta)$, où $v = v_p(n)$.

Les entiers i_v,...,i_0, définis de façon récursive par $i_v = 0$ et

$$i_j = \begin{cases} \widetilde{i}_j, & \text{si } \widetilde{i}_j < i_{j+1} + ne; \\ i_{j+1} + ne, & \text{sinon;} \end{cases}$$

lorsque $0 \leq j < v$, seront appelés les *indices régularisés de* $(\mathcal{F}, n)$, l'entier i_j étant *l'indice régularisé d'ordre* j, noté $i_j(\mathcal{F}, n)$.

L'indice régularisé d'ordre j de $(\mathcal{F},n)$ sera dit *régulier,* si $j = v$ ou si sa valuation p-adique est $\leq j$, auquel cas on a $i_j = \widetilde{i}_j$.

(3.14) Remarque: Les indices de $(\mathcal{F},n)$ sont définis pour $(\mathcal{F},n)$ en tant qu'élément de l'ensemble E_k, alors que les indices régularisés de $(\mathcal{F},n)$ sont définis pour $(\mathcal{F},n)$ en tant qu'objet de la catégorie $E_k(\Delta)$, puisqu'ils dépendent du degré e de Δ.

(3.15) Exemple: Dans les notations et hypothèses de l'exemple 3.8, on trouve

$$\begin{array}{llll} i_2 = 0, & i_1 = p^2, & i_0 = 2p^2, & \text{si } e = 1, \\ i_2 = 0, & i_1 = p^2 + p, & i_0 = 3p^2 + p, & \text{si } e = 2, \\ i_2 = 0, & i_1 = p^2 + p, & i_0 = 4p^2 + p - 3, & \text{si } e \geq 3. \end{array}$$

(3.16) Lemme: *Soit $(\mathcal{F},n)$ un objet de la catégorie $E_k(\Delta)$. Soit j un entier, $0 \leq j \leq v_p(n)$. L'indice régularisé d'ordre j de $(\mathcal{F},n)$ est le plus petit entier s'écrivant*

$$\widetilde{i}_{j'} + (j' - j)ne$$

avec $j \leq j' \leq v_p(n)$, $\widetilde{i}_{j'}$ désignant l'indice d'ordre j' de $(\mathcal{F},n)$.
Si $i_j = \widetilde{i}_{j'} + (j' - j)ne$ avec $j' > j$ et $\widetilde{i}_{j'} \neq 0$, on a $j' = v_p(i_j)$.

Preuve: Pour prouver la première partie du lemme, il suffit de faire une récurrence descendante sur j, en commençant par $j = v_p(n)$.
Quant à la deuxième partie, on a $v_p(i_j) = v_p(\widetilde{i}_{j'}) \leq j'$. Si $v_p(\widetilde{i}_{j'}) < j'$, alors $\widetilde{i}_{j'-1} + (j' - 1 - j)ne < \widetilde{i}_{j'} + (j' - j)ne$, ce qui est absurde. □

L'indice régularisé d'ordre 0 de $(\mathcal{F},n)$ n'est rien d'autre que le nombre supplémentaire de Hilbert de la différente de l'extension B/A:

(3.17) Proposition: *La différente $D_{B/A}$ d'une extension totalement ramifiée B/A, définie par $(\mathcal{F},n)$, vérifie*

$$v_B(D_{B/A}) = i_0 + n - 1,$$

v_B et i_0 désignant respectivement la valuation discrète normalisée de B et l'indice régularisé d'ordre 0 de $(\mathcal{F},n)$.

Preuve: Par 2.6, $D_{B/A}$ est égal à l'idéal principal de B, engendré par $\sum_{\alpha=0}^{\infty}(n+\alpha)\, f_\alpha\, u^{n+\alpha-1}t$, f_α désignant le coefficient du terme de degré α de $\mathcal{F}$.
Il suffit par suite de montrer que l'infimum des $v_p(n+\alpha)ne + n + \alpha - 1$ avec $\alpha \geq 0$ tel que $f_\alpha \neq 0$ n'est atteint qu'une seule fois et qu'il est égal à $i_0 + n - 1$.

Or, pour que $v_p(n+\widetilde{\imath})ne+n+\widetilde{\imath}-1$ soit minimal dans l'ensemble des $v_p(n+\alpha)ne+n+\alpha-1$, tels que $\alpha \geq 0$ et $f_\alpha \neq 0$, il faut que $\widetilde{\imath}$ soit un indice de $(\mathcal{F},n)$. Une comparaison des valuations p-adiques montre que les entiers de la forme $v_p(n+\widetilde{\imath})ne+\widetilde{\imath}$, avec $\widetilde{\imath}$ indice de $(\mathcal{F},n)$, $\widetilde{\imath}<+\infty$, sont tous distincts. D'autre part, comme $\widetilde{\imath}=\widetilde{\imath}_{v_p(\widetilde{\imath})}$ pour tout indice $\widetilde{\imath}$ de $(\mathcal{F},n)$, tel que $0\neq\widetilde{\imath}<+\infty$, le lemme 3.16 montre que leur infimum est égal à l'indice d'ordre 0 de $(\mathcal{F},n)$. □

4. Description partielle de la multiplication $*$

On se fixe dans ce paragraphe un objet $(\mathcal{F},n)$ de la catégorie $E_k(\Delta)$. On notera v la valuation p-adique de n, $\widetilde{\imath}_v,\ldots,\widetilde{\imath}_0$ les indices de $(\mathcal{F},n)$, et $i_v,\ldots,i_0$ les indices régularisés de $(\mathcal{F},n)$.

(4.1) Définition: Un morphisme de la catégorie $E_k(\Delta)$ sera dit *constant* (resp. *unitaire*), si la série sous-jacente est constante (resp. de terme constant 1).

La proposition suivante montre que tout morphisme de $E_k(\Delta)$ peut se décomposer en un morphisme constant suivi d'un morphisme unitaire.

(4.2) Proposition: *Soit $(\mathcal{X},m)$ un élément de E_S. Notons x le terme constant de la série sous-jacente. On a*

$$(\mathcal{X},m)*_\Delta(\mathcal{F},n)=(x^{-1}\,\mathcal{X},m)*_\Delta(\mathcal{F}(xU)x^n,n).$$

Preuve: Posons $(\mathcal{G},mn)=(\mathcal{X},m)*_\Delta(\mathcal{F},n)$. Le couple $(\mathcal{G},mn)$ est la classe modulo t de $(\mathcal{F}(U^m\,\mathcal{X})\,\mathcal{X}^n,mn)$. En posant $\mathcal{F}_x=\mathcal{F}(xU)x^n$ et $\mathcal{X}_u=x^{-1}\,\mathcal{X}$, on a

$$\mathcal{F}_x(U^m\,\mathcal{X}_u)\,\mathcal{X}_u^n=\mathcal{F}(U^m x\,\mathcal{X}_u)x^n\,\mathcal{X}_u^n=\mathcal{F}(U^m\,\mathcal{X})\,\mathcal{X}^n,$$

ce qui montre que $(\mathcal{G},mn)$ est également la classe modulo t de $\mathcal{F}_x(U^m\,\mathcal{X}_u)\,\mathcal{X}_u^n$, d'où la proposition. □

(4.3) Pour simplifier les énoncés qui suivent, on va introduire une fonction $w_{p,n}$ qui est une tronquée de la valuation p-adique: Elle associe à un entier z sa valuation p-adique, si celle-ci est $\leq v=v_p(n)$, et elle vaut v sinon. Notons les trois propriétés suivantes:

a) $w_{p,n}(0)=v$;

b) $w_{p,n}(n+\alpha) = w_{p,n}(\alpha)$ pour tout entier α;
c) $w_{p,n}(\alpha) < w_{p,n}(\beta)$ implique $v_p(\alpha) < v_p(\beta)$ pour tous entiers α et β.

(4.4) On va définir des fonctions $\widetilde{\varphi}_j^m$, φ_j^m et P_j^m, à l'aide desquelles nous décrirons la multiplication $*$.

Fixons des entiers m et j, $m \geq 0$ et $0 \leq j \leq v$.

L'application affine qui associe à un nombre réel $l \geq 0$ la valeur $mi_j + lp^j$, sera notée $\widetilde{\varphi}_j^m$.

On notera φ_j^m l'infimum des fonctions $\widetilde{\varphi}_{j'}^m$, $0 \leq j' \leq j$.

Lorsque l est un entier ≥ 0, tel que $\varphi_j^m(l)$ vérifie $w_{p,n}(\varphi_j^m(l)) \leq j$, on désignera par $P_j^m(l)$ le polynôme de $k[X]$ qui est égal à la classe de

$$\sum_{j'} h_{i_{w_{p,n}(i_{j'})}} (\xi f_0^e)^{(w_{p,n}(i_{j'})-j')} f_{i_{w_{p,n}(i_{j'})}} X^{p^{j'}} \qquad \text{mod } tA[X],$$

où

$$h_{i_{w_{p,n}(i_{j'})}} = \frac{n + i_{w_{p,n}(i_{j'})}}{p^{w_{p,n}(i_{j'})}}$$

et ξ est donné par $p1_A = \xi t^e$, la somme portant sur les j' tels que $\widetilde{\varphi}_{j'}^m(l) = \varphi_j^m(l)$. (On remarque que l'indice d'ordre $w_{p,n}(i_{j'})$ de $(\mathcal{F}, n)$ est régulier, si l'égalité $\widetilde{\varphi}_{j'}^m(l) = \varphi_j^m(l)$ vaut.)

Si $w_{p,n}(\varphi_j^m(l))$ est $> j$, on posera $P_j^m(l) = 0$.

On omettra l'exposant m, si $m = 1$.

Remarquons que, pour tous entiers $l \geq 0$, $m \geq 1$, on a $\varphi_j^m(l) = m\varphi_j(l/m)$, $0 \leq j \leq v$, et $P_v^m(l) = P_v(l/m)$ si l est divisible par m. Cette dernière égalité permet de définir P_v pour tout nombre rationnel, en posant $P_v(l/m) = P_v^m(l)$. (On vérifie facilement que cette définition est bonne.)

(4.5) Remarque: Pour tout j, $0 \leq j \leq v$, et tout entier $m \geq 1$, le graphe de $\widetilde{\varphi}_j^m(l)$ est une demi-droite coupant l'axe des ordonnées en l'indice régularisé d'ordre j de $(\mathcal{F}, n)$ multiplié par m, et le polynôme $P_j^m(l)$ est un polynôme additif de $k[X]$, c'est-à-dire l'application polynomiale de k dans k associée est un homomorphisme de $\mathbf{F}_p$-modules.

Par ailleurs, on verra (cf. 6.10) que l'égalité $\varphi_v(l) = \varphi_{B/A}(l)$ vaut pour tout $l \geq 0$, $\varphi_{B/A}$ désignant la fonction de Herbrand d'une extension B/A définie par $(\mathcal{F}, n)$ (celle-ci pouvant se définir aussi pour des extensions non-galoisiennes grâce â l'existence d'une théorie de ramification non-galoisienne (cf. [He])).

Enonçons notre résultat principal.

(4.6) Théorème: *Soient l un entier ≥ 1, $\mathcal{X}$ un polynôme de degré $\leq l-1$ à coefficients dans S de terme constant 1, et x un élément de S.*

Les éléments $(\mathcal{G}_{l-1}, mn)$ *et* $(\mathcal{G}_l, mn)$ *de* E_k, *tels que*

$$(\mathcal{G}_{l-1}, mn) = (\mathcal{X}, m) *_\Delta (\mathcal{F}, n)$$

et

$$(\mathcal{G}_l, mn) = (\mathcal{X}+xU^l, m) *_\Delta (\mathcal{F}, n),$$

vérifient les deux propriétés suivantes:

a) Les coefficients de degré d *de* $\mathcal{G}_{l-1}$ *et de* $\mathcal{G}_l$ *sont égaux, lorsque* d *est un entier qui vérifie* $d < \varphi^m_{w_{p,n}(d)}(l)$.

b) Si j *est un entier,* $0 \leq j \leq v$, *tel que* $\varphi^m_j(l)$ *vérifie* $w_{p,n}(\varphi^m_j(l)) \leq j$, *l'égalité*

$$\overline{\text{coeff}}(\mathcal{G}_l, \varphi^m_j(l)) = \overline{\text{coeff}}(\mathcal{G}_{l-1}, \varphi^m_j(l)) + (P^m_j(l))(\overline{x}).$$

vaut.

Avant de donner la preuve de ce théorème, ce qui se fera au prochain paragraphe, énonçons quelques corollaires concernant la multiplication $*_\Delta$.

(4.7) Corollaire: *Soit* $(\mathcal{X}, 1)$ *un élément de* E_k. *Pour tout entier* $l \geq 0$, *notons* $\mathcal{X}_l$ *le polynôme formé des termes de degré* $\leq l$ *de* $\mathcal{X}$.

Alors, la suite $(\mathcal{G}_l)_{l\geq 0}$ *définie par*

$$(\mathcal{G}_l, n) = (\mathcal{X}_l, 1) *_\Delta (\mathcal{F}, n)$$

converge pour la topologie U*-adique vers une série* $\mathcal{G}$, *telle que*

$$(\mathcal{G}, n) = (\mathcal{X}, 1) *_\Delta (\mathcal{F}, n).$$

Preuve: A l'aide de la proposition 4.2, on se ramène au cas où la série $\mathcal{X}$ a terme constant 1. Par le théorème 4.6, on a

$$\mathcal{G}_l \equiv \mathcal{G}_{l-1} \qquad \text{mod } U^{\varphi_v(l)} A[[U]],$$

lorsque l est un entier ≥ 1.

La fonction $l \mapsto \varphi_v(l)$ divergeant vers $+\infty$, la suite $(\mathcal{G}_l)_{l\geq 1}$ est de Cauchy. Elle admet donc une limite $\mathcal{G}$ qui est un élément de $S[[U]]^*$.

Soit (B, u) défini par $(\mathcal{F}, n)$ relativement à (A, t). Pour tout entier $l \geq 0$, notons u_l l'uniformisante de B qui vérifie $u = u_l\, \mathcal{X}_l(u_l)$, et x_l le terme de degré l de $\mathcal{X}$.

Comme

$$\begin{aligned} 0 &= u_l\, \mathcal{X}_l(u_l) - u_{l-1}\, \mathcal{X}_{l-1}(u_{l-1}) \\ &= (u_l - u_{l-1})\, \mathcal{Y}(u_l, u_{l-1}) + x_l u_l^{l+1} \end{aligned}$$

avec $\mathcal{Y}(u_l, u_{l-1}) = \sum_{\alpha=0}^{l-1} x_\alpha \dfrac{u_l^{\alpha+1} - u_{l-1}^{\alpha+1}}{u_l - u_{l-1}}$, et que $\mathcal{Y}(u_l, u_{l-1})$ est une unité dans B, on a $u_l \equiv u_{l-1} \bmod m_B^{l+1}$, m_B désignant l'idéal maximal de B. La suite $(u_l)_{l\geq 0}$ est donc de Cauchy dans B, et sa limite u' est une uniformisante de B. Les suites $(u_l\,\mathcal{X}_l(u_l))_{l\geq 0}$ et $(u_l^n\,\mathcal{G}_l(u_l))_{l\geq 0}$ convergeant respectivement vers $u'\,\mathcal{X}(u')$ et $u'^n\,\mathcal{G}(u')$ dans B, on a $u = u'\,\mathcal{X}(u')$ et $t = u'^n\,\mathcal{G}(u')$, et il résulte de la proposition 2.12 que

$$(\mathcal{G}, n) = (\mathcal{X}, 1) *_\Delta (\mathcal{F}, n). \qquad \square$$

(4.8) Corollaire: *Soit $(\mathcal{X}, 1)$ un élément de E_k dont la série sous-jacente a terme constant 1. Notons x_l le coefficient du terme de degré l de $\mathcal{X}$, $\mathcal{X}_l$ le polynôme formé des termes de degré $\leq l$ de $\mathcal{X}$, et $(\mathcal{G}_l, n)$ l'élément de E_k tel que*

$$(\mathcal{G}_l, n) = (\mathcal{X}_l, 1) *_\Delta (\mathcal{F}, n).$$

(On a donc $\mathcal{G}_0 = \mathcal{F}$.)

Alors, pour qu'un élément $(\mathcal{G}, n)$ de E_k vérifie

$$(\mathcal{G}, n) = (\mathcal{X}, 1) *_\Delta (\mathcal{F}, n),$$

il faut et il suffit que les deux propriétés suivantes soient vérifiées:

a) Les termes de degré d de $\mathcal{F}$ et de $\mathcal{G}$ sont égaux, si d vérifie $d < \varphi_{w_{p,n}(d)}(1)$.

b) L'égalité

$$\overline{\mathrm{coeff}}(\mathcal{G}, \varphi_j(l)) = \overline{\mathrm{coeff}}(\mathcal{G}_{l-1}, \varphi_j(l)) + (P_j(l))(\overline{x}_l)$$

vaut, si j, l sont des entiers, $0 \leq j \leq v$ et $l \geq 1$, tels que $w_{p,n}(\varphi_j(l)) \leq j$.

Preuve: Soit $(\mathcal{G}, n)$ tel que $(\mathcal{G}, n) = (\mathcal{X}, 1) *_\Delta (\mathcal{F}, n)$. Par le théorème 4.6, les termes de degré d de $\mathcal{G}_l$ et de $\mathcal{G}_{l-1}$ sont égaux, lorsque d vérifie $d < \varphi_{w_{p,n}(d)}(1)$, d'où a) compte tenu du corollaire précédent.

Soient j, l des entiers, $0 \leq j \leq v$ et $l \geq 1$, tels que $w_{p,n}(\varphi_j(l)) \leq j$. Le théorème 4.6 montre que $\mathcal{G}_{l'}$ et $\mathcal{G}_l$ ont même terme de degré $\varphi_j(l)$ si $l' > l$, d'où l'on déduit à l'aide du corollaire précédent que $\mathcal{G}$ et $\mathcal{G}_l$ ont même coefficient de degré $\varphi_j(l)$. La propriété b) résulte alors de la partie b) de 4.6.

Réciproquement, soit $\mathcal{G}$ un élément de $S[[U]]^*$, satisfaisant aux conditions a) et b) de l'énoncé. Posons

$$(\mathcal{G}', n) = (\mathcal{X}, 1) *_\Delta (\mathcal{F}, n).$$

Il faut montrer que $\mathcal{G} = \mathcal{G}'$.

Par ce qui précède, la série $\mathcal{G}'$ possède également les propriétés a) et b). Soit d un entier ≥ 0, et posons $j = w_{p,n}(d)$. On va montrer que $\mathcal{G}$ et $\mathcal{G}'$ ont même terme de degré d.

Si $d < \varphi_j(1)$, les termes de degré d de $\mathcal{G}$ et $\mathcal{G}'$ sont égaux grâce à la propriété a).

Si $d \geq \varphi_j(1)$, il existe un entier $l \geq 1$, tel que $d = \varphi_j(l)$, puisque φ_j est une fonction strictement croissante, affine par morceaux de pente ≥ 1 et que les pentes des morceaux

divisent $d - \varphi_j(0)$. La propriété b) montre alors que les termes de degré d de $\mathcal{G}$ et de $\mathcal{G}'$ sont égaux. □

(4.9) On désignera par $s_0(\mathcal{F}, n)$ le plus petit nombre réel $l \geq 0$, tel que $\varphi_v(l) = \varphi_0(l)$.

(4.10) Corollaire: *Soit $(\mathcal{G}, n)$ un élément de E_k qui vérifie*

$$\mathcal{G} \equiv \mathcal{F} \qquad U^l A[[U]]$$

pour un entier $l > i_0(\mathcal{F}, n) + s_0(\mathcal{F}, n)$.

Alors, $(\mathcal{G}, n)$ et $(\mathcal{F}, n)$ sont isomorphes dans la catégorie $E_k(\Delta)$. L'isomorphisme peut être obtenu par un morphisme dont la série sous-jacente est congrue à 1 modulo $U^{l-i_0(\mathcal{F},n)}A[[U]]$.

Preuve: Comme $\varphi_v(s_0(\mathcal{F}, n)) = i_0(\mathcal{F}, n) + s_0(\mathcal{F}, n)$, et que $\varphi_v(l - i_0(\mathcal{F}, n)) = l$, ceci est une conséquence du corollaire précédent, le polynôme $P_j(l)$ étant un monôme de degré 1 lorsque $l > s_0$. □

(4.11) Corollaire: *Dans la catégorie $E_k(\Delta)$, $(\mathcal{F}, n)$ est isomorphe à un objet $(\mathcal{G}, n)$ dont la série sous-jacente est un polynôme de degré $\leq \varphi_v(s_0(\mathcal{F}, n))$ dont tous les termes de degré non divisible par p - à l'exception de celui de degré i_0 peut-être - sont nuls.*

Preuve: Ceci est une conséquence immédiate des corollaires précédents, le polynôme $P_0(l)$ étant un monôme de degré 1, lorsque $\varphi_0(l)$ est premier à p. □

(4.12) Corollaire: *Soit $(\mathcal{X}, m)$ un élément de E_k. Notons pour tout entier $l \geq 0$ par $\mathcal{X}_l$ le polynôme formé des termes de degré $\leq l$ de $\mathcal{X}$.*

Alors, la suite $(\mathcal{G}_l)_{l \geq 0}$ définie par

$$(\mathcal{G}_l, mn) = (\mathcal{X}_l, m) *_\Delta (\mathcal{F}, n)$$

converge pour la topologie U-adique vers une limite $\mathcal{G}$, telle que

$$(\mathcal{G}, mn) = (\mathcal{X}, m) *_\Delta (\mathcal{F}, n).$$

Preuve: Remarquons d'abord que l'on ne peut pas se contenter de généraliser la preuve du corollaire 4.7.

Par la proposition 4.2, on peut supposer que $\mathcal{X}$ a terme constant 1.

Fixons un objet (B, u) défini par $(\mathcal{F}, n)$ relativement à (A, t), et un objet (C, v) défini par $(\mathcal{X}, m)$ relativement à (B, u). Par le corollaire 4.10, $(\mathcal{X}_l, m)$ et $(\mathcal{X}, m)$ sont isomorphes dans la catégorie $E_k(\Theta)$ avec $\Theta = (\mathcal{F}, n) *_{(1,1)} \Delta$, si $l > i_0(\mathcal{X}, m) + s_0(\mathcal{X}, m)$. Par

ailleurs, on peut choisir un isomorphisme dont la série sous-jacente est congrue à 1 modulo $U^{l-i_0(\mathcal{X},m)}A[[U]]$.

Pour tout entier $l > i_0(\mathcal{X},m)+s_0(\mathcal{X},m)$, il existe donc une uniformisante v_l de C, telle que (C,v_l) soit défini par $(\mathcal{X}_l,m)$ relativement à (B,u). On a $v_C(v-v_l) \geq l-i_0(\mathcal{X},m)+1$, et (C,v_l) est défini par $(\mathcal{G}_l,mn)$ relativement à (A,t).

Par 4.6, la suite $(\mathcal{G}_l)_l$ est de Cauchy. Notons $\mathcal{G}$ sa limite qui est un élément de $S[[U]]^*$. La suite $(v_l)_l$ convergeant vers v, $v_l^{mn}\,\mathcal{G}_l(v_l)$ converge vers $v^{mn}\,\mathcal{G}(v)$. On a donc $t = v^{mn}\,\mathcal{G}(v)$, ce qui prouve que $(\mathcal{G},mn)$ définit (C,v) relativement à (A,t). On déduit alors de 2.12 que

$$(\mathcal{G},mn) = (\mathcal{X},m) *_\Delta (\mathcal{F},n).$$ □

(4.13) Corollaire: *Soient l un entier ≥ 1, $(\mathcal{X},m)$ et $(\mathcal{X}\,',m)$ des éléments de E_k dont les séries sous-jacentes sont congrues modulo $U^l A[[U]]$. Posons*

$$(\mathcal{G},mn) = (\mathcal{X},m) *_\Delta (\mathcal{F},n) \qquad et \qquad (\mathcal{G}',mn) = (\mathcal{X}\,',m)_\Delta(\mathcal{F},n)$$

Alors, on a

$$\mathcal{G}' \equiv \mathcal{G} \qquad \mathrm{mod}\, U^d A[[U]]$$

et

$$\overline{\mathrm{coeff}}(\mathcal{G}',d) - \overline{\mathrm{coeff}}(\mathcal{G},d) = P_v(l/m)(\overline{x}),$$

avec $d = m\varphi_v(l/m)$ et $\overline{x} = \overline{\mathrm{coeff}}(\mathcal{X}\,' - \mathcal{X},l)$.

Preuve: Pour tout entier $l' \geq 0$, notons $\mathcal{X}_{l'}$ (resp. $\mathcal{X}\,'_{l'}$) le polynôme formé des termes de degré $\leq l'$ de la série $\mathcal{X}$ (resp. $\mathcal{X}\,'$). Posons

$$(\mathcal{G}_{l'},mn) = (\mathcal{X}_{l'},m) *_\Delta (\mathcal{F},n) \qquad \text{et} \qquad (\mathcal{G}'_{l'},mn) = (\mathcal{X}_{l'}\,',m) *_\Delta (\mathcal{F},n).$$

Le corollaire précédent et le théorème 4.6 prouvent qu'avec les notations de l'énoncé les congruences

$$\mathcal{G}_l \equiv \mathcal{G} \qquad \mathrm{mod}\, U^{d+1}A[[U]] \qquad \text{et} \qquad \mathcal{G}'_l \equiv \mathcal{G}' \qquad \mathrm{mod}\, U^{d+1}A[[U]]$$

valent, alors que

$$\mathcal{G}'_l \equiv \mathcal{G}_l \qquad \mathrm{mod}\, U^d A[[U]]$$

et

$$\overline{\mathrm{coeff}}(\mathcal{G}'-\mathcal{G},d) = P_v(l/m)(\overline{x})$$

par 4.6, compte tenu des formules pour φ^m et P^m. □

(4.14) Remarque: Le résultat du corollaire 4.13 a déjà été énoncé à langage près par Arf [A]. Krasner [Kr1] avait obtenu auparavant un résultat semblable pour les polynômes

d'Eisenstein, en se restreignant au cas $m = 1$. Son outil technique était le polygone de Newton. Ils ont aussi déjà remarqué que l'égalité $\varphi_v(l) = \varphi_{B/A}(l)$ vaut dans le cas galoisien (Arf) aussi bien que dans le cas d'un corps résiduel fini (Krasner) pour tout $l \geq 0$, $\varphi_{B/A}$ désignant la fonction de Herbrand d'une extension B de A définie par $(\mathcal{F}, n)$.

(4.15) Remarque: Le lecteur aura probablement remarqué que les corollaires de 4.6 qui améliorent le résultat d'Arf n'utilise que la partie $m = 1$ du théorème 4.6. En effet, si m est divisible par p, le passage à la limite dans la preuve du corollaire 4.8 ne s'effectue plus aussi aisément. En particulier, on n'obtient plus un aussi joli résultat que le corollaire 4.8. Avec un petit astuce, il est cependant possible de donner une description partielle du passage à la limite quand p divise m (cf. [T]), mais, comme nous n'en donnerons pas d'application ici, nous n'avons pas voulu y insister.

5. Preuve du théorème principal

On va prouver d'abord le cas $m = 1$, en utilisant un raisonnement qui se généralise facilement. Remarquons que, si on veut établir le théorème 4.6 uniquement pour $m = 1$, on peut simplifier la démonstration considérablement, car, en utilisant des arguments de limite, on peut se restreindre à $\mathcal{X} = 1$. Ces arguments de limite ne se généralisent malheureusement pas.

(5.1) Posons $\mathcal{Y} = \mathcal{X} + xU^l$ et fixons un entier j, $0 \leq j \leq v$. Soit $\mathcal{R}$ (resp. $\mathcal{S}$) le reste modulo t de $(\mathcal{F}(U\,\mathcal{X})\,\mathcal{X}^n, n)$ (resp. de $(\mathcal{F}(U\,\mathcal{Y})\,\mathcal{Y}^n, n)$). On a

$$\begin{aligned} \mathcal{G}_{l-1} &= (1 + U^n\,\mathcal{R})\,\mathcal{F}(U\,\mathcal{X})\,\mathcal{X}^n - t\,\mathcal{R} \\ &\equiv \mathcal{F}(U\,\mathcal{X})\,\mathcal{X}^n + U^n\,\mathcal{R}\,\mathcal{F}(U\,\mathcal{X})\,\mathcal{X}^n \mod tA[[U]] \\ \text{et} \qquad \mathcal{G}_l &\equiv \mathcal{F}(U\,\mathcal{Y})\,\mathcal{Y}^n + U^n\,\mathcal{S}\,\mathcal{F}(U\,\mathcal{Y})\,\mathcal{Y}^n \mod tA[[U]]. \end{aligned}$$

On va comparer d'abord les termes $\mathcal{F}(U\,\mathcal{X})\,\mathcal{X}^n$ et $\mathcal{F}(U\,\mathcal{Y})\,\mathcal{Y}^n$, et ensuite les termes $U^n\,\mathcal{R}\,\mathcal{F}(U\,\mathcal{X})\,\mathcal{X}^n$ et $U^n\,\mathcal{S}\,\mathcal{F}(U\,\mathcal{Y})\,\mathcal{Y}^n$.

(5.2) Lemme: *Soit α un entier ≥ 0. On a*

$$\operatorname{coeff}((\mathcal{X} + xU^l)^{n+\alpha} - \mathcal{X}^{n+\alpha}, d) \equiv \begin{cases} 0, & \text{si } v_p(d) < v'; \\ 0, & \text{si } 0 \leq d < lp^{v'}; \\ h_\alpha x^{p^{v'}}, & \text{si } d = lp^{v'}; \end{cases} \mod tA$$

avec $v' = v_p(n + \alpha)$ et $h_\alpha = \frac{n+\alpha}{p^{v'}}$.

Preuve: Ceci est une conséquence immédiate de la congruence

$$(\mathcal{X}+xU^l)^{n+\alpha} \equiv (\mathcal{X}^{p^{v'}}+x^{p^{v'}}U^{lp^{v'}})^{h_\alpha} \qquad \mathrm{mod}\, tA. \qquad \square$$

(5.3) On notera s_j la fonction qui associe à un nombre réel $l \geq 0$ le plus petit nombre s'écrivant $\widetilde{\imath} + lp^{w_{p,n}(\widetilde{\imath})}$ avec $\widetilde{\imath}$ indice (non-régularisé) d'ordre $\leq j$ de $(\mathcal{F}, n)$. L'ensemble des indices $\widetilde{\imath}$ d'ordre $\leq j$ de $(\mathcal{F}, n)$, tels que $s_j(l) = \widetilde{\imath} + lp^{w_{p,n}(\widetilde{\imath})}$ sera noté $I_j(l)$.

(5.4) Lemme:

a) Les coefficients de degré d de $\mathcal{F}(U\,\mathcal{X})\,\mathcal{X}^n$ et de $\mathcal{F}(U\,\mathcal{Y})\,\mathcal{Y}^n$ sont congrus modulo tA, lorsque d est un entier $< s_j(l)$ qui vérifie $w_{p,n}(d) \leq j$.

b) Si $w_{p,n}(s_j(l)) \leq j$, l'égalité

$$\overline{\mathrm{coeff}}(\mathcal{F}(U\,\mathcal{Y})\,\mathcal{Y}^n, s_j(l)) = \overline{\mathrm{coeff}}(\mathcal{F}(U\,\mathcal{X})\,\mathcal{X}^n, s_j(l)) + \sum_i \overline{h}_i \overline{f}_i \overline{x}^{p^{w_{p,n}(i)}}$$

vaut avec $h_i = \frac{n+i}{p^{w_{p,n}(i)}}$, la somme portant sur les éléments de $I_j(l)$.

Preuve: Soit d un entier $\leq s_j(l)$ qui vérifie $w_{p,n}(d) \leq j$. Ecrivons

$$\overline{\mathrm{coeff}}(\mathcal{F}(U\,\mathcal{Y})\,\mathcal{Y}^n - \mathcal{F}(U\,\mathcal{X})\,\mathcal{X}^n, d) = \sum_{\alpha=0}^{d} \overline{f}_\alpha \overline{\mathrm{coeff}}((\mathcal{X}+xU^l)^{n+\alpha} - \mathcal{X}^{n+\alpha}, d-\alpha)$$

Posons $c_\alpha = \overline{\mathrm{coeff}}((\mathcal{X}+xU^l)^{n+\alpha} - \mathcal{X}^{n+\alpha}, d-\alpha)$.

Supposons d'abord que $d \neq s_j(l)$. Pour établir la partie a) du lemme, il suffit de montrer que $\overline{f}_\alpha c_\alpha = 0$ pour tout entier $\alpha \geq 0$. Si $\alpha = d$, ou si $w_{p,n}(d-\alpha) < w_{p,n}(n+\alpha)$, on a $c_\alpha = 0$ en raison du lemme 5.2 et de la propriété c) de $w_{p,n}$ (cf. 4.3) qui montre que $v_p(d-\alpha) < v_p(n+\alpha)$.

Si α est un entier $< d$ tel que $f_\alpha \neq 0$ et qui vérifie $w_{p,n}(d-\alpha) \geq w_{p,n}(n+\alpha)$, on a $w_{p,n}(\alpha) \leq j$ (en effet, $w_{p,n}(\alpha) > j$ impliquerait $w_{p,n}(d-\alpha) \leq j$, puisque $w_{p,n}(d) \leq j$, d'où $w_{p,n}(\alpha) = w_{p,n}(n+\alpha) \leq w_{p,n}(d-\alpha) \leq j$, ce qui est absurde), d'où

$$d - \alpha \leq d - \widetilde{\imath}_{w_{p,n}(\alpha)} < lp^{w_{p,n}(\alpha)},$$

puisque $d < s_j(l)$. On conclut du lemme 5.2 que $c_\alpha = 0$.

Supposons alors $w_{p,n}(s_j(l)) \leq j$, et posons $d = s_j(l)$. Si $\alpha = d$, si $w_{p,n}(d-\alpha) < w_{p,n}(n+\alpha)$, ou si α est un entier $< d$ de valuation $w_{p,n}(d-\alpha) \geq w_{p,n}(n+\alpha)$ qui n'est pas dans $I_j(l)$ et tel que $f_\alpha \neq 0$, le raisonnement précédent reste valable. Il montre que $c_\alpha = 0$. Si α est un élément de $I_j(l)$, on a $d - \alpha = lp^{w_{p,n}(\alpha)}$, et on conclut du lemme 5.2

et des propriétés de $w_{p,n}$ que $c_\alpha = h_\alpha \overline{x}^{p^{w_{p,n}(\alpha)}}$. En sommant sur les éléments de $I_j(l)$, on trouve b). □

Le traitement du deuxième terme sera nettement plus compliqué. On se servira d'un lemme de comparaison des restes modulo t de deux éléments de degré n de E_A. Les séries $\mathcal{R}$ et $\mathcal{S}$ et les entiers l et j de l'énoncé ci-dessous ne sont pas nécessairement ceux auxquels on vient de s'intéresser.

(5.5) Lemme: *Soient $(\mathcal{G}, n)$ et $(\mathcal{H}, n)$ deux éléments de E_A dont les séries sous-jacentes ont même terme constant f appartenant à S. Notons $\mathcal{R}$ et $\mathcal{S}$ les restes modulo t de $(\mathcal{G}, n)$ et de $(\mathcal{H}, n)$ respectivement. Soient r, l des entiers ≥ 1, et j un entier, $0 \leq j \leq v_p(n)$.*
Supposons que

a) $\mathrm{coeff}(\mathcal{H}, d) \equiv \mathrm{coeff}(\mathcal{G}, d) \mod t^{]\frac{n+r-d}{ne}[e} A$, *lorsque d est un entier, $0 \leq d < r$, qui vérifie $w_{p,n}(d) \leq j$ ou $d \leq lp^j$;*

et

b) $\mathrm{coeff}(\mathcal{G}, \alpha) \equiv 0 \mod t^{]\frac{n+r-d+1}{ne}[e} A$, *lorsque α est un entier qui vérifie $w_{p,n}(\alpha) \leq j$ et que d est un entier $\leq r$ tel que $0 < \alpha < d - lp^j$;*

Alors, les coefficients de degré d de $\mathcal{SH}$ et de $\mathcal{RG}$ sont congrus modulo tA pour tout entier d, $0 \leq d < r$, qui vérifie $w_{p,n}(d) \leq j$.
Si en outre $w_{p,n}(r) \leq j$, et si a) est vérifiée pour $d = r$, alors on a

$$\mathrm{coeff}(\mathcal{SH}, r) \equiv \mathrm{coeff}(\mathcal{RG}, r) + \sum_{\delta=0}^{[\frac{r}{n}]} f^{\delta+1} x_\delta \qquad \mod tA,$$

où la classe modulo tA de x_δ est donnée par

$$x_\delta t^{\delta+1} \equiv \mathrm{coeff}(\mathcal{H}, r - \delta n) - \mathrm{coeff}(\mathcal{G}, r - \delta n) \qquad \mod t^{\delta+2} A$$

si δ est congru à -1 modulo e, $x_\delta = 0$ sinon.

Preuve: Remarquons d'abord que l'inégalité

$$]\tfrac{n+d}{ne}[e \geq]\tfrac{d}{n}[+1 \tag{1}$$

vaut pour tout entier d. (En effet, on a $]\frac{n+d}{ne}[e = \frac{1}{n}\,]\frac{n+d}{ne}[ne \geq \frac{1}{n}(n+d) = \frac{d}{n} + 1$.)

Lorsque d et α sont des entiers, $0 \leq d \leq r$ et $lp^j < \alpha < d+n$, qui vérifient $w_{p,n}(d) \leq j$ et $w_{p,n}(d - \alpha) \leq j$, on a

$$\mathrm{coeff}(\mathcal{R}, d - \alpha) \equiv 0 \qquad \mod t^{]\frac{r-d+1}{n}[} A. \tag{2}$$

Fixons un entier d, $0 \leq d \leq r$, tel que $w_{p,n}(d) \leq j$. On va effectuer une récurrence sur $N_\alpha =]\frac{d-\alpha}{n}[$. La plus petite valeur que peut prendre N_α est 0. On a alors $d - \alpha \leq 0$. La congruence est triviale, si l'inégalité est stricte, alors que le terme constant de $\mathcal{R}$ est nul, puisque celui de $\mathcal{G}$ appartient à S.

Soit N un entier, $1 \leq N \leq]\frac{d-lp^j}{n}[$ et supposons l'assertion pour tout α, tel que $N_\alpha \leq N - 1$. Soit α un entier satisfaisant aux hypothèses de l'énoncé ci-dessus et tel que $N_\alpha = N$. Comme $\mathrm{coeff}(\mathcal{R}, d - \alpha)$ est le reste modulo t par rapport à S du coefficient du terme de degré $d - \alpha$ de $\mathcal{G} + U^n \mathcal{R}\mathcal{G}$, et que

$$\mathrm{coeff}(\mathcal{G}, d - \alpha) \equiv 0 \qquad \mathrm{mod}\, t^{\,]\frac{r-d+1}{n}[+1} A,$$

par l'hypothèse b) du lemme et l'inégalité (1), on est ramené à prouver que

$$\mathrm{coeff}(\mathcal{R}\mathcal{G}, d - \alpha - n) \equiv 0 \qquad \mathrm{mod}\, t^{\,]\frac{r-d+1}{n}[+1} A.$$

Pour cela, il suffit de montrer que

$$\mathrm{coeff}(\mathcal{G}, \beta)\ \mathrm{coeff}(\mathcal{R}, d - \alpha - n - \beta) \equiv 0 \qquad \mathrm{mod}\, t^{\,]\frac{r-d+1}{n}[+1} A,$$

pour $0 \leq \beta \leq d - \alpha - n$. Or, on a alors $\beta < d - n - lp^j$, et il résulte de l'hypothèse b) du lemme et de l'inégalité (1) que

$$\mathrm{coeff}(\mathcal{G}, \beta) \equiv 0 \qquad \mathrm{mod}\, t^{\,]\frac{r-d+1}{n}[+1} A,$$

si $w_{p,n}(\beta) \leq j$ et $\beta \neq 0$, et de l'hypothèse de récurrence que

$$\mathrm{coeff}(\mathcal{R}, d - \alpha - n - \beta) \equiv 0 \qquad \mathrm{mod}\, t^{]\frac{r-d+1}{n}[+1} A,$$

si $w_{p,n}(\beta) > j$ ou $\beta = 0$.

Lorsque d est un entier, $-n < d < r$, qui vérifie $w_{p,n}(d) \leq j$ ou $d \leq lp^j$, on a

$$\mathrm{coeff}(\mathcal{R}, d) \equiv \mathrm{coeff}(\mathcal{S}, d) \qquad \mathrm{mod}\, t^{]\frac{r-d}{n}[} A. \tag{3}$$

et

$$\mathrm{coeff}(\mathcal{G}, \alpha)\ \mathrm{coeff}(\mathcal{R}, d - \alpha) \equiv \mathrm{coeff}(\mathcal{H}, \alpha)\ \mathrm{coeff}(\mathcal{S}, d - \alpha) \qquad \mathrm{mod}\, t^{]\frac{r-d+1}{n}[} A, \tag{4}$$

pour $0 < \alpha \leq d$.

En particulier, la congruence

$$\mathrm{coeff}(\mathcal{R}\mathcal{G}, d) \equiv \mathrm{coeff}(\mathcal{S}\mathcal{H}, d) \qquad \mathrm{mod}\, t^{]\frac{r-d}{n}[} A \tag{5}$$

vaut.

Remarquons que la première conclusion du lemme est une conséquence immédiate de la congruence (5).

On va montrer les congruences (3), (4) et (5) simultanément par récurrence sur $N_d =]\frac{d}{n}[$. La plus petite valeur que peut prendre N_d est 0. On a alors $d \leq 0$. Les congruences sont triviales, si l'inégalité est stricte, alors que les termes constants de $\mathcal{R}$ et $\mathcal{S}$ sont nuls, puisque ceux de $\mathcal{G}$ et $\mathcal{H}$ appartiennent à S.

Soit N un entier, $1 \leq N \leq]\frac{r-1}{n}[$, et supposons les congruences vérifiées pour tout entier d satisfaisant aux hypothèses ci-dessus et tel que $N_d \leq N-1$. Soit d tel que $N_d = N$. L'ensemble des entiers α, $0 < \alpha \leq d$, est réunion (disjointe) des quatre sous-ensembles suivants:

$E_1(d)$: $0 < \alpha < d - lp^j$ et $w_{p,n}(\alpha) \leq j$;

$E_2(d)$: $d - lp^j \leq \alpha \leq d$ et $w_{p,n}(\alpha) \leq j$;

$E_3(d)$: $\alpha \leq lp^j$ et $w_{p,n}(\alpha) > j$;

$E_4(d)$: $lp^j < \alpha \leq d$ et $w_{p,n}(\alpha) > j$.

Si α est dans $E_1(d)$, la congruence (4) est une conséquence immédiate des hypothèses b) et a) du lemme et de l'inégalité (1). Si α est dans $E_2(d)$ ou $E_3(d)$, la congruence

$$\mathrm{coeff}(\mathcal{G}, \alpha) \equiv \mathrm{coeff}(\mathcal{H}, \alpha) \qquad \mathrm{mod}\, t^{]\frac{r-d+1}{n}[} A$$

vaut grâce à l'hypothèse a) du lemme et de l'inégalité (1). La congruence (2) donne

$$\mathrm{coeff}(\mathcal{R}, d-\alpha) \equiv 0 \qquad \mathrm{mod}\, t^{]\frac{r-d+1}{n}[} A$$

pour α dans $E_4(d)$. La congruence (4) pour α dans $E_2(d) \cup E_3(d) \cup E_4(d)$ est donc une conséquence de la relation

$$\mathrm{coeff}(\mathcal{R}, d-\alpha) \equiv \mathrm{coeff}(\mathcal{S}, d-\alpha) \qquad \mathrm{mod}\, t^{]\frac{r-d+1}{n}[} A,$$

qui résulte du (3) de l'hypothèse de récurrence.

Reste à établir la congruence (3). Les coefficients des termes de degré d de $\mathcal{R}$ et $\mathcal{S}$ sont respectivement les restes modulo t par rapport à S des coefficients des termes de degré d de $\mathcal{G} + U^n \mathcal{R}\mathcal{G}$ et de $\mathcal{H} + U^n \mathcal{S}\mathcal{H}$. Il résulte de l'hypothèse a) du lemme et de l'inégalité (1) que

$$\mathrm{coeff}(\mathcal{H}, d) \equiv \mathrm{coeff}(\mathcal{G}, d) \qquad \mathrm{mod}\, t^{]\frac{r-d}{n}[+1} A,$$

et du (5) de l'hypothèse de récurrence que

$$\mathrm{coeff}(\mathcal{R}\mathcal{G}, d-n) \equiv \mathrm{coeff}(\mathcal{S}\mathcal{H}, d-n) \qquad \mathrm{mod}\, t^{]\frac{r-d}{n}[+1} A,$$

d'où (3).

La congruence (5) se trouve, en sommant les congruences (4) sur α, $0 < \alpha \leq d$, et en y ajoutant la congruence (3) multipliée par f qui est le coefficient du terme constant de $\mathcal{G}$ et de $\mathcal{H}$.

Supposons $w_{p,n}(r) \leq j$ et l'hypothèse a) vérifiée pour $d = r$. On observe que les congruences (3), (4) et (5) valent alors aussi pour $d = r$, les démonstrations se généralisant. (Les congruences (3) et (5) sont d'ailleurs triviales pour $d = r$.)

Pour terminer la démonstration du lemme, on va prouver par récurrence descendante sur δ' que

$$(6) \qquad \operatorname{coeff}(\mathcal{SH}, r - \delta' n) \equiv \operatorname{coeff}(\mathcal{RG}, r - \delta' n) + t^{\delta'} \sum_{\delta=\delta'}^{[\frac{r}{n}]} f^{\delta-\delta'+1} x_\delta \qquad \bmod t^{\delta'+1} A,$$

lorsque $0 \leq \delta' \leq [\frac{r}{n}] + 1$.

En faisant $\delta' = 0$ dans (6), on trouve en effet la dernière assertion du lemme.

Si $\delta' = [\frac{r}{n}] + 1$, on a $r - \delta' n < 0$, et la congruence est triviale.

Soit δ' un entier, $0 \leq \delta' < [\frac{r}{n}] + 1$, et supposons la congruence ci-dessus vérifiée pour $\delta' + 1$. On a donc

$$\operatorname{coeff}(\mathcal{SH}, r - \delta' n - n) \equiv \operatorname{coeff}(\mathcal{RG}, r - \delta' n - n) + t^{\delta'+1} \sum_{\delta=\delta'+1}^{[\frac{r}{n}]} f^{\delta-\delta'} x_\delta \qquad \bmod t^{\delta'+2} A.$$

Par l'hypothèse a) du lemme et définition de $x_{\delta'}$, on trouve

$$\operatorname{coeff}(\mathcal{H}, r - \delta' n) \equiv \operatorname{coeff}(\mathcal{G}, r - \delta' n) + x_{\delta'} t^{\delta'+1} \qquad \bmod t^{\delta'+2} A,$$

ayant $]\frac{n+\delta' n}{ne}[e \geq \delta' + 2$ si δ' n'est pas congru à -1 modulo e. Les coefficients des termes de degré $r - \delta' n$ de $\mathcal{S}$ et de $\mathcal{R}$ étant respectivement les restes modulo t des coefficients des termes de degré $r - \delta' n$ de $\mathcal{G} + U^n \mathcal{RG}$ et de $\mathcal{H} + U^n \mathcal{SH}$ par rapport à S, on conclut que

$$\operatorname{coeff}(\mathcal{S}, r - \delta' n) \equiv \operatorname{coeff}(\mathcal{R}, r - \delta' n) + t^{\delta'} \sum_{\delta=\delta'}^{[\frac{r}{n}]} f^{\delta-\delta'} x_\delta \qquad \bmod t^{\delta'+1} A.$$

La congruence (6) se trouve, en multipliant cette dernière congruence par f qui est le coefficient du terme constant de $\mathcal{G}$ et de $\mathcal{H}$, et en y ajoutant la somme des congruences (4) pour α, $0 < \alpha \leq r - \delta' n$. □

Pour appliquer le lemme 5.5 à la situation présente, il faudra comparer les séries $\mathcal{X}^b$ et $\mathcal{Y}^b$ pour tout entier $b \geq 0$. On va d'abord s'intéresser à la valuation p-adique des coefficients du binôme:

(5.6) Lemme: *Soient a et b deux entiers positifs, $b \geq a$. La valuation p-adique de $\binom{b}{a}$ est égale au nombre des retenues lors de la soustraction p-adique de b et a. En particulier, on a $v_p(\binom{b}{a}) \geq v_p(b) - v_p(a)$. L'égalité vaut, si a est p-primaire d'exposant $\leq v_p(b)$, et alors $\binom{b}{a} \equiv \frac{b}{a} \mod p^{v_p(b)-v_p(a)+1}$, en remarquant que $\frac{b}{a}$ est bien un entier.*

Preuve: Soient

$$b = b_0 + b_1 p + ... + b_s p^s,$$

$$a = a_0 + a_1 p + ... + a_s p^s \text{ et } \quad b - a = c_0 + c_1 p + ... + c_s p^s$$

respectivement les développements p-adiques de b, a et $b-a$ à coefficients dans $\{0, ..., p-1\}$. La valuation p-adique de $b!$ est donnée par

$$v_p(b!) = (b - b_0 - ... - b_s)/(p-1) \qquad \text{(cf. [N] page 38).}$$

En calculant de même les valuations p-adiques de a et de $b-a$, on trouve que

$$v_p(\binom{b}{a}) = \{(a_0 + c_0 - b_0) + (a_1 + c_1 - b_1) + ... + (a_s + c_s - b_s)\}/(p-1).$$

Pour tout entier α, $0 \leq \alpha \leq s$, posons $d_\alpha = 1$ s'il y a, lors de la soustraction p-adique de b et a, une retenue lors de la $\alpha^{\text{ème}}$ opération, et $d_\alpha = 0$ sinon. Comme $b \geq a$, il ne peut y avoir une retenue lors de la $s^{\text{ème}}$ opération, d'où $d_s = 0$. En posant $d_{-1} = 0$, on a

$$a_\alpha + c_\alpha - b_\alpha = d_\alpha \, p - d_{\alpha-1},$$

pour tout entier α, $0 \leq \alpha \leq s$. Par suite, la valuation p-adique de $\binom{b}{a}$ est bien égale à $\sum_{\alpha=0}^{s} d_\alpha$. La deuxième assertion découle immédiatement de la première.

Supposons que a soit p-primaire d'exposant $\leq v_p(b)$. La congruence énoncée pour $\binom{b}{a}$ est équivalente à

$$\binom{b}{a} \equiv \frac{b}{a} \mod^{\times} p,$$

où $\mod^{\times}$ désigne la congruence multiplicative de Hasse (cf. [Ha] page 35). Or, pour tout entier α, $1 \leq \alpha \leq a-1$, on a $v_p(\alpha) < v_p(a) \leq v_p(b-a)$ en raison de la p-primalité de a, et donc $\frac{b-a+\alpha}{\alpha} \equiv 1 \mod^{\times} p$, d'où la congruence ci-dessus, puisque $\binom{b}{a} = \frac{b}{a} \prod_{\alpha=1}^{a-1} \frac{b-a+\alpha}{\alpha}$. □

(5.7) Lemme: *Soit b un entier ≥ 1, et soient $a_0, ..., a_s$ des entiers ≥ 0 de somme égale à b. Alors, pour tout entier α, $0 \leq \alpha \leq s$,*

$$\binom{b}{a_\alpha} \quad \textit{divise} \quad \frac{b!}{a_0! ... a_s!}.$$

Preuve: Sans perte de généralité, on peut supposer que $\alpha = 0$. Le lemme résulte alors de l'égalité

$$\frac{b!}{a_0!...a_s!} = \binom{b}{a_0} \frac{(b-a_0)!}{a_1!...a_s!}. \qquad \square$$

(5.8) Lemme: *Soient b, a des entiers ≥ 1. Alors, la valuation en t du coefficient de degré a de $\mathcal{X}^b$ est $\geq (v_p(b) - v_p(a))e$.*

Preuve: Ecrivons $\mathcal{X} = \sum_{\alpha=0}^{l-1} x_\alpha U^\alpha$. Le coefficient du terme de degré a de $\mathcal{X}^b$ est égal à

$$\sum_{a_0,...,a_{l-1}} \frac{m!}{a_0!...a_{l-1}!} x_0^{a_0}...x_{l-1}^{a_{l-1}},$$

la somme portant sur tous les entiers $a_0, ..., a_{l-1} \geq 0$ de somme b qui vérifient $a_1 + 2a_2 + ... + (l-1)a_{l-1} = a$.

Or, si $a_0, ..., a_{l-1}$ sont des entiers qui vérifient les conditions ci-dessus, alors, pour au moins un indice α, a_α a une valuation p-adique plus petite ou égale à celle de a, d'où l'on déduit à l'aide des deux lemmes précédents que la valuation en t de $\frac{m!}{a_0!...a_{l-1}!}$ est $\geq (v_p(b) - v_p(a))e$. $\square$

(5.9) Lemme: *Soient a et b des entiers, $0 \leq a \leq lb$. Notons ρ le plus petit entier qui vérifie $a < lp^{\rho+1}$. Alors, la valuation en t du coefficient de degré a de $\mathcal{Y}^b - \mathcal{X}^b$ est minorée par $(v_p(b) - v_p(a))e$ et par $(v_p(b) - \rho)e$.*

Si $a = lp^\rho$, et si b est de valuation p-adique $\geq \rho$, le coefficient est congru à $\frac{b}{p^\rho} x^{p^\rho}$ modulo $t^{(v_p(b)-\rho)e+1}A$.

Si $a < l$, le coefficient est nul.

Preuve: Ecrivons

$$\mathcal{Y}^b - \mathcal{X}^b = (\mathcal{X} + xU^l)^b - \mathcal{X}^b = \sum_{\alpha=1}^{b} \binom{b}{\alpha} x^\alpha \ \mathcal{X}^{b-\alpha} \ U^{l\alpha}.$$

Tous les termes non nuls sont de degré $\geq l$. Comme

$$\text{coeff}(\mathcal{Y}^b - \mathcal{X}^b, a) = \sum_{\alpha=1}^{b} \binom{b}{\alpha} x^\alpha \ \text{coeff}(\mathcal{X}^{b-\alpha}, a - l\alpha),$$

il résulte des lemmes 5.6 et 5.8 que la valuation en t de chaque terme de la somme est

$$\geq \sup\{v_p(b) - v_p(\alpha), 0\}e \ + \ \sup\{(v_p(b-\alpha) - v_p(a-l\alpha))e, 0\},$$

ce qui est bien $\geq (v_p(b) - v_p(a))e$ comme on le vérifie facilement.

L'inégalité $a < lp^{\rho+1}$ montre que $\alpha < p^{\rho+1}$, si $a - l\alpha \geq 0$. Par suite, pour $1 \leq \alpha \leq \frac{a}{l}$, on a $v_p(\alpha) \leq \rho$ et, en raison du lemme 5.6, $v_p(\binom{b}{\alpha}) \geq v_p(b) - \rho$, d'où la deuxième minoration.

Supposons finalement $a = lp^\rho$ et $v_p(b) \geq \rho$. Alors, $v_p(\binom{b}{\alpha}) \geq v_p(b) - \rho + 1$ pour tout entier α, $1 \leq \alpha < p^\rho$, et la congruence énoncée resulte de la deuxième partie du lemme 5.6. □

On est maintenant enfin en mesure de comparer les termes $U^n \mathcal{R}\mathcal{F}(U\mathcal{X})\mathcal{X}^n$ et $U^n \mathcal{S}\mathcal{F}(U\mathcal{Y})\mathcal{Y}^n$.

(5.10) On notera r_j la fonction qui associe à un nombre réel $l \geq 0$ le plus petit nombre s'écrivant $\widetilde{\imath} + (w_{p,n}(\widetilde{\imath}) - j')ne + lp^{j'}$ avec j' entier, $0 \leq j' \leq j$, et $\widetilde{\imath}$ indice (non-régularisé) de $(\mathcal{F}, n)$ tel que $w_{p,n}(\widetilde{\imath}) > j'$.

L'ensemble des couples $(\widetilde{\imath}, j')$ ci-dessus qui vérifient l'égalité $\widetilde{\imath} + (w_{p,n}(\widetilde{\imath}) - j')ne + lp^{j'} = r_j(l)$ sera noté $R_j(l)$.

(5.11) Lemme: *Notons r le plus petit des deux entiers $r_j(l) - n$ et $s_j(l)$.*

a) Les coefficients de degré d de $\mathcal{S}\mathcal{F}(U\mathcal{Y})\mathcal{Y}^n$ et de $\mathcal{R}\mathcal{F}(U\mathcal{X})\mathcal{X}^n$ sont congrus modulo tA, lorsque d est un entier, $0 \leq d < r$, de valuation $w_{p,n}(d) \leq j$.

b) Supposons $r < s_j(l)$ et $w_{p,n}(r) \leq j$. Alors, l'égalité

$$\overline{\text{coeff}}(\mathcal{S}\mathcal{F}(U\mathcal{Y})\mathcal{Y}^n, r) = \overline{\text{coeff}}(\mathcal{R}\mathcal{F}(U\mathcal{X})\mathcal{X}^n, r) + \sum_{(i,j')} \overline{h}_i (\overline{\xi} \overline{f}_0^e)^{w_{p,n}(i) - j'} \overline{f}_i \overline{x}^{p^{j'}}$$

vaut avec $h_i = \frac{n+i}{p^{w_{p,n}(i)}}$, la somme portant sur les éléments de $R_j(l)$.

[Rappelons que ξ vérifie $p1_A = \xi t^e$.]

Preuve: On va appliquer le lemme 5.5 à $\mathcal{F}(U\mathcal{Y})\mathcal{Y}^n$ et $\mathcal{F}(U\mathcal{X})\mathcal{X}^n$. Pour cela, on va vérifier dans l'ordre les hypothèses a) et b), et calculer explicitement les coefficients x_δ.

Pour tout entier d, $0 \leq d < r$ qui vérifie $w_{p,n}(d) \leq j$ ou $d \leq lp^j$, le coefficient de degré d de $\mathcal{F}(U\mathcal{Y})\mathcal{Y}^n$ est congru modulo $t^{\left]\frac{n+r-d}{ne}\right[e}A$ à celui du même degré de $\mathcal{F}(U\mathcal{X})\mathcal{X}^n$.

Soit d un entier vérifiant les hypothèses ci-dessus. Ecrivons

$$\text{coeff}(\mathcal{F}(U\mathcal{Y})\mathcal{Y}^n - \mathcal{F}(U\mathcal{X})\mathcal{X}^n, d) = \sum_{\alpha=0}^{d} f_\alpha \ \text{coeff}(\mathcal{Y}^{n+\alpha} - \mathcal{X}^{n+\alpha}, d - \alpha).$$

Nous allons montrer que le coefficient de degré $d - \alpha$ de $\mathcal{Y}^{n+\alpha} - \mathcal{X}^{n+\alpha}$ est de valuation $\geq \left]\frac{n+r-d}{ne}\right[e$ en t pour tout entier α, $0 \leq \alpha \leq d$, tel que $f_\alpha \neq 0$. Par le lemme 5.9, celle-ci est minorée par $(v_p(n+\alpha) - v_p(d-\alpha))e$, et par $(v_p(n+\alpha) - \rho)e$, où ρ vérifie $d - \alpha < lp^{\rho+1}$. Si $d - \alpha < l$, le coefficient est nul.

Par suite, il suffit de prouver que tout entier α, $0 \leq \alpha \leq d$, tel que $f_\alpha \neq 0$, vérifie l'une des trois conditions suivantes: $v_p(n+\alpha) - v_p(d-\alpha) \geq]\frac{n+r-d}{ne}[$, $d-\alpha < lp^{w_{p,n}(\alpha)-]\frac{n+r-d}{ne}[+1}$, ou $d-\alpha < l$.

Supposons d'abord $w_{p,n}(\alpha) \geq j+]\frac{n+r-d}{ne}[$. Alors, on a en particulier $j < v$. Comme $w_{p,n}(d-\alpha) \leq j$ ou $d-\alpha \leq lp^j$, au moins une des deux inégalités ci-dessus est vérifiée.

Supposons ensuite $w_{p,n}(\alpha) < j+]\frac{n+r-d}{ne}[$. Notons $\widetilde{\imath}$ l'indice d'ordre $w_{p,n}(\alpha)$ de $(\mathcal{F}, n)$. Il vérifie $w_{p,n}(\widetilde{\imath}) \leq w_{p,n}(\alpha)$. On va distinguer trois cas:

Si $w_{p,n}(\widetilde{\imath}) = 0$, alors $d-\alpha < s_j(l) - \widetilde{\imath} \leq l$.

Si $]\frac{n+r-d}{ne}[> 1$ et $w_{p,n}(\widetilde{\imath}) \neq 0$, alors $d-\alpha = r-(r-d)-\alpha < r-((]\frac{n+r-d}{ne}[-1)ne-n)-\widetilde{\imath}$, car $(]\frac{n+r-d}{ne}[-1)ne - n =]\frac{n+r-d}{ne}[ne - ne - n < r-d$. Par définition de r, ceci est majoré par $r_j(l) - (]\frac{n+r-d}{ne}[-1)ne - \widetilde{\imath}$. Comme $w_{p,n}(\widetilde{\imath}) > w_{p,n}(\widetilde{\imath})-]\frac{n+r-d}{ne}[+1 \leq j$, cette dernière expression est, par définition de $r_j(l)$, majorée par $lp^{w(\alpha)-]\frac{n+r-d}{ne}[+1}$ ou par l, suivant que $w_{p,n}(\widetilde{\imath})$ est $\geq]\frac{n+r-d}{ne}[-1$ ou pas.

Si finalement $]\frac{n+r-d}{ne}[= 1$, alors $d-\alpha < r-\widetilde{\imath} \leq s_j(l) - \widetilde{\imath} \leq lp^{w_{p,n}(\widetilde{\imath})} \leq lp^{w_{p,n}(\alpha)}$ par définition de $s_j(l)$.

Lorsque α est un entier tel que $w_{p,n}(\alpha) \leq j$, le coefficient de degré α de $\mathcal{F}(U\,\mathcal{X})\,\mathcal{X}^n$ est congru à 0 modulo $t^{]\frac{n+r-d+1}{ne}[e}A$ pour tout entier $d \leq r$ qui vérifie $0 < \alpha < d - lp^j$.

Soient α et d des entiers vérifiant les hypothèses ci-dessus. Notons $\widetilde{\imath}$ l'indice d'ordre $j+]\frac{n+r-d+1}{ne}[-1$ de $(\mathcal{F}, n)$ si $j+]\frac{n+r-d+1}{ne}[-1 \leq v$, et posons $\widetilde{\imath} = 0$ sinon. Comme

$$r \leq r_j(l) - n \leq \widetilde{\imath} + (]\frac{n+r-d+1}{ne}[-1)ne + lp^j - n < \widetilde{\imath} + r - d + 1 + lp^j$$

par définition de r et de $r_j(l)$, on a $\alpha < d - lp^j \leq \widetilde{\imath}$.

En paticulier, on peut supposer $\widetilde{\imath} > 0$.

Ecrivons

$$\mathrm{coeff}(\mathcal{F}(U\,\mathcal{X})\,\mathcal{X}^n, \alpha) = \sum_{\beta=0}^{\alpha} f_\beta \ \mathrm{coeff}(\mathcal{X}^{n+\beta}, \alpha - \beta).$$

L'inégalité $\alpha < \widetilde{\imath}$ montre que $f_\alpha = 0$ et que, pour que $f_\beta \neq 0$ avec $0 \leq \beta < \alpha$, il faut $w_{p,n}(\beta) \geq j+]\frac{n+r-d+1}{ne}[$. Ceci implique

$$v_p(n+\beta) - v_p(\alpha - \beta) \geq w_{p,n}(\beta) - j \geq]\frac{n+r-d+1}{ne}[,$$

et il résulte de 5.8 que l'on a alors

$$\mathrm{coeff}(\mathcal{X}^{n+\beta}, \alpha - \beta) \equiv 0 \qquad \mathrm{mod}\, t^{]\frac{n+r-d+1}{ne}[e}A,$$

ce qui prouve l'assertion ci-dessus.

Les hypothèses a) et b) de 5.5 étant vérifiées, la partie a) de la proposition 5.11 est prouvée.

Supposons $r < s_j(l)$ et $w_{p,n}(r) \leq j$. Remarquons que, sous ces hypothèses, le raisonnement qui prouve l'hypothèse a) du lemme 5.5 reste valable pour $d = r$, si on remplace l'inégalité du dernier cas de sa vérification par

$$d - \alpha \leq r - \widetilde{\imath} < s_j(l) - \widetilde{\imath} \leq lp^{w_{p,n}(\widetilde{\imath})} \leq lp^{w_{p,n}(\alpha)}.$$

La partie b) de la proposition 5.11 est alors une conséquence de l'assertion suivante:

Soit δ un entier ≥ 0, congru à -1 modulo e. Le coefficient de degré $r - \delta n$ de $\mathcal{F}(U\,\mathcal{Y})\,\mathcal{Y}^n - \mathcal{F}(U\,\mathcal{X})\,\mathcal{X}^n$ est congru à

$$t^{\delta+1} \sum_{(i,j')} \xi^{w_{p,n}(i)-j'} h_i f_i x^{p^{j'}} \qquad \mod t^{\delta+2}A,$$

où $h_i = \frac{n+i}{p^{w_{p,n}(i)}}$, la somme portant sur les éléments de $R_j(l)$ qui vérifient $(w_{p,n}(i) - j')e - 1 = \delta$.

On va comparer les coefficients de degré $r - \delta n - \alpha$ de $\mathcal{Y}^{n+\alpha}$ et de $\mathcal{X}^{n+\alpha}$ pour tout entier α, $0 \leq \alpha \leq r - \delta n$. Le résultat se trouvera alors en sommant sur α, ayant

$$\mathrm{coeff}(\mathcal{F}(U\,\mathcal{Y})\,\mathcal{Y}^n - \mathcal{F}(U\,\mathcal{X})\,\mathcal{X}^n, r - \delta n) = \sum_{\alpha=0}^{r-\delta n} f_\alpha \ \mathrm{coeff}(\mathcal{Y}^{n+\alpha} - \mathcal{X}^{n+\alpha}, r - \delta n - \alpha).$$

Supposons d'abord que α soit un indice $\widetilde{\imath}$ de $(\mathcal{F}, n)$ et qu'il existe un entier j' qui vérifie $(w_{p,n}(\widetilde{\imath}) - j')e - 1 = \delta$, tel que le couple $(\widetilde{\imath}, j')$ appartienne à $R_j(l)$. Alors, $r - \delta n - \widetilde{\imath} = lp^{j'}$ et

$$\mathrm{coeff}(\mathcal{Y}^{n+\widetilde{\imath}} - \mathcal{X}^{n+\widetilde{\imath}}, r - \delta n - \widetilde{\imath}) \equiv h_{\widetilde{\imath}} \xi^{w_{p,n}(\widetilde{\imath})-j'}\ t^{\delta+1}\ x^{p^{j'}} \qquad \mod t^{\delta+2}A$$

par 5.9, en rappelant les égalités $p1_A = \xi t^e$ et $(w_{p,n}(\widetilde{\imath}) - j')e = \delta + 1$.

Il reste donc à prouver que la valuation en t du coefficient de degré $r - \delta n - \alpha$ de $\mathcal{Y}^{n+\alpha} - \mathcal{X}^{n+\alpha}$ est $\geq \delta + 2$, si $f_\alpha \neq 0$ et si α ne vérifie pas les conditions ci-dessus.

Si $w_{p,n}(\alpha) \geq j + \frac{\delta+1}{e} + 1$, on a $w_{p,n}(r - \delta n - \alpha) \leq j$, et on peut conclure par le lemme 5.9.

Supposons $w_{p,n}(\alpha) < j + \frac{\delta+1}{e} + 1$. Compte tenu du lemme 5.9, il suffit de montrer que $r - \delta n - \alpha < lp^{w_{p,n}(\alpha) - \frac{\delta+1}{e}}$ ou $r - \delta n - \alpha < l$. Notons $\widetilde{\imath}$ l'indice d'ordre $w_{p,n}(\alpha)$ de $(\mathcal{F}, n)$. On va distinguer trois cas:

Si $w_{p,n}(\widetilde{\imath}) = 0$, alors $r - \delta n - \alpha < s_j(l) - \widetilde{\imath} \leq l$.

Si $0 < w_{p,n}(\widetilde{\imath}) < \frac{\delta+1}{e}$, alors $r - \delta n - \alpha \leq r_j(l) - n - \delta n - \widetilde{\imath} \leq l + w_{p,n}(\widetilde{\imath})ne - n - \delta n < l$.

Si $\frac{\delta+1}{e} \leq w_{p,n}(\widetilde{\imath}) \leq j + \frac{\delta+1}{e}$, alors $r - \delta n - \alpha \leq r - \delta n - \widetilde{\imath} = r - (\frac{\delta+1}{e}ne - n) - \widetilde{\imath} = r_j(l) - \frac{\delta+1}{e}ne - \widetilde{\imath} \leq lp^{w_{p,n}(\widetilde{\imath}) - \frac{\delta+1}{e}} \leq lp^{w_{p,n}(\alpha) - \frac{\delta+1}{e}}$ par définition de r et de $r_j(l)$. La première inégalité est stricte si $\alpha \neq \widetilde{\imath}$, et l'avant-dernière inégalité est stricte si $(\widetilde{\imath}, w_{p,n}(\widetilde{\imath}) - \frac{\delta+1}{e})$ n'est pas dans $R_j(l)$. Comme au moins une des deux hypothèses est vérifiée, l'inégalité est stricte. □

(5.12) Supposons $w_{p,n}(\varphi_j(l)) \leq j$. Si $s_j(l) = \varphi_j(l)$ (resp. $r_j(l) = \varphi_j(l)$), on désignera par $P_{s_j}(l)$ (resp. $P_{r_j}(l)$) le polynôme qui apparaît dans la partie b) du lemme 5.4 (resp. du lemme 5.11). Dans le cas contraire, on posera $P_{s_j}(l) = 0$ (resp. $P_{r_j}(l) = 0$).

(5.13) Lemme: *Le plus petit des deux entiers $r_j(l)$ et $s_j(l)$ est égal à $\varphi_j(l)$. Par ailleurs, l'égalité*

$$P_j(l) = P_{s_j}(l) + P_{r_j}(l)$$

vaut.

Preuve: Le plus petit des deux entiers $r_j(l)$ et $s_j(l)$ est le plus petit entier s'écrivant

$$\widetilde{\imath}_{j''} + (j'' - j')ne + lp^{j'}$$

avec $0 \leq j' \leq j$ et $j' \leq j'' \leq v$, car $w_{p,n}(\widetilde{\imath}_{j''}) \neq j''$ implique $\widetilde{\imath}_{j''} = \widetilde{\imath}_{j''-1}$.

Compte tenu du lemme 3.16, ceci est bien égal à $\varphi_j(l)$.

Il montre aussi que l'on a $i_{j'} = \widetilde{\imath}_{j''} + (j'' - j')ne$ avec $j'' = w_{p,n}(i_{j'})$, si $i_{j'}$ n'est pas régulier. Si $i_{j'}$ est régulier, et si $\varphi_j(l) = \widetilde{\varphi}_{j'}(l)$, on vérifie facilement que $j' = w_{p,n}(i_{j'})$. En associant à j' le couple $(\widetilde{\imath}_{w_{p,n}(i_{j'})}, j')$, on définit donc une application de l'ensemble des entiers j', $0 \leq j' \leq j$, tels que $\varphi_j(l) = \widetilde{\varphi}_{j'}(l)$, dans l'ensemble des couples $(\widetilde{\imath}, j')$, formés d'un entier j', $0 \leq j' \leq j$, et d'un indice $\widetilde{\imath}$ de $(\mathcal{F}, n)$, tels que $w_{p,n}(\widetilde{\imath}) \geq j'$ et que $\widetilde{\imath} + (w_{p,n}(\widetilde{\imath}) - j')ne + lp^{j'}$ soit le plus petit des deux entiers $r_j(l)$ et $s_j(l)$. On vérifie facilement que cette application est bijective.

Le monôme qui correspond dans 4.4 à un entier j', $0 \leq j' \leq j$, tel que $\varphi_j(l) = \widetilde{\varphi}_{j'}(l)$ étant le même que celui qui correspond dans la partie b) du lemme 5.4 ou du lemme 5.11 au couple $(\widetilde{\imath}_{w_{p,n}(i_{j'})}, j')$ (ou à l'indice $\widetilde{\imath}_{j'}$ si $w_{p,n}(i_{j'}) = j'$), ceci prouve que

$$P_j(l) = P_{r_j}(l) + P_{s_j}(l). \qquad \square$$

Déduisons finalement le théorème 4.6:

(5.14) *Preuve:* (du théorème 4.6) Compte tenu du lemme 5.13, le théorème 4.6 pour $m = 1$ est une conséquence directe des lemmes 5.4 et 5.11.

Supposons $m > 1$ et écrivons

$$\operatorname{coeff}(\mathcal{F}(U^m\,\mathcal{Y})\,\mathcal{Y}^n - \mathcal{F}(U^m\,\mathcal{X})\,\mathcal{X}^n, d) = \sum_{\alpha=0}^{d} f_\alpha \operatorname{coeff}(\mathcal{Y}^{n+\alpha} - \mathcal{X}^{n+\alpha}, d - m\alpha).$$

Les énoncés des lemmes 5.4 et 5.11 se généralisent si on remplace s_j par $s_j^m : l \mapsto m\widetilde{\imath}_j + lp^j$ et r_j par $r_j^m : l \mapsto mr_j(l/m)$. Le plus petit des deux entiers $s_j^m(l)$ et $r_j^m(l)$ est égal à $\varphi_j^m(l)$

et l'égalité $P_j^m = P_{s_j}^m + P_{r_j}^m$ vaut pour les polynômes $P_{s_j}^m$ et $P_{r_j}^m$ correspondants, d'où l'on déduit le théorème pour $m > 1$. □

6. Applications aux extensions totalement ramifiées

Nous gardons les notations du paragraphe précédent, et nous nous fixons de plus un objet (B, u) de la catégorie $\mathrm{Ext}_{tot}(A, t)$ défini par $(\mathcal{F}, n)$. Le groupe de Galois de l'extension B/A sera noté G.

(6.1) On posera

$$G_l = \{\sigma \in G / v_B(\sigma(u) - u) \geq l + 1\},$$

lorsque $l \geq 0$, v_B désignant la valuation discrète normalisée de B.

Si l'extension B/A est galoisienne, G_l est le $l^{\text{ème}}$ groupe de ramification de l'extension dans les notations de [Se]. Remarquons que, si on veut généraliser la théorie de ramification aux extensions non-galoisiennes, il ne suffit plus de considérer les G_l (cf. [He] et 6.7).

On montre comme dans le cas galoisien que la définition des G_l ne dépend pas du choix de u, que la suite $(G_l)_{l \geq 0}$ est une filtration décroissante du groupe G par des sous-groupes distingués, et que l'on a $G_l = \{1\}$ pour l suffisamment grand.

(6.2) On posera

$$(P_j(0))(X) = X^{n+i_j}$$

pour $0 \leq j \leq v$, et

$$P(l) = (P_v(l), ..., P_0(l)),$$

lorsque l est un entier ≥ 0.

Les applications polynomiales associées à $P(l)$, $l \geq 0$, définissent des morphismes de groupe $k^+ \to (k^+)^{v+1}$ et $k^* \to (k^*)^{v+1}$ respectivement.

(6.3) Proposition:

a) En associant à un élément σ de G_l l'image de $\frac{\sigma(u)}{u}$ dans k, on définit un morphisme de groupe de G_0 dans le noyau de $P(0)$. Par passage au quotient, on obtient un morphisme injectif $G_0/G_1 \to \ker P(0)$.

b) Soit l un entier ≥ 1. En associant à un élément σ de G_l l'image de $\frac{\sigma(u)-u}{u^{l+1}}$ dans k, on définit un morphisme de groupe de G_l dans le noyau de $P(l)$. Par passage au quotient, on obtient un morphisme injectif $G_l/G_{l+1} \to \ker P(l)$.

c) Supposons que $s_0 = s_0(\mathcal{F}, n)$ (tel que défini dans 4.9) soit un entier. Alors, s_0 est le plus grand entier s, tel que $G_s \neq \{1\}$, et on a $|G_s| = |\ker P_v(s)|$.

Preuve: Ceci résulte de 4.8, en identifiant G au groupe des automorphismes de $(\mathcal{F}, n)$ dans la catégorie $E_k(\Delta)$ grâce au foncteur quasi-inversible de 2.18 . □

(6.4) Corollaire: *Pour que l'extension B/A soit galoisienne, il faut que les deux propriétés suivantes soient vérifiées:*

a) L'abscisse de tout sommet du graphe de φ_v est un entier.

b) Le polynôme $P_v(l)$ est scindé sur k, et les applications $P(l)$ et $P_v(l)$ ont même noyau, lorsque l est l'abscisse d'un sommet du graphe de φ_v.

En particulier, G_l/G_{l+1} est isomorphe au noyau de $P_v(l)$, si l'extension B/A est galoisienne.

Preuve: Lorsque l est un entier ≥ 0, notons $d_v(l)$ le degré séparable de $P_v(l)$. En écrivant $n = hp^v$, on voit que $d_v(0) = h$. En notant pour tout entier $l \geq 1$ par $j_+(l)$ (resp. $j_-(l)$) le plus grand (resp. plus petit) entier j, tel que $\varphi_v(l) = \varphi_j(l)$, on a $d_v(l) = p^{j_+(l)-j_-(l)}$, $P_v(l)$ s'écrivant sous la forme $(Q_v(l))(X^{p^{j_-(l)}})$ avec $Q_v(l)$ polynôme séparable de degré $p^{j_+(l)-j_-(l)}$ de $k[X]$.

Ayant $\prod_{l=0}^{\infty} d_v(l) \leq n$, on déduit de la proposition 6.3 les inégalités

$$|G| = \prod_{l=0}^{\infty} |G_l/G_{l+1}| \leq \prod_{l=0}^{\infty} |\ker(P(l))| \leq \prod_{l=0}^{\infty} |\ker(P_v(l)| \leq \prod_{l=0}^{\infty} d_v(l) \leq n.$$

Pour que l'extension B/A soit galoisienne, il faut qu'il y ait l'égalité partout. En particulier, les abscisses s des sommets du graphe de φ_v doivent être des entiers, tels que $P_v(s)$ soit scindés sur k, et, pour tout s, l'égalité $|\ker(P_v(s))| = |\ker(P(s))|$ doit valoir, d'où le corollaire. □

(6.5) Remarque: Le corollaire 6.4 montre que dans le cas galoisien, les abscisses des sommets du graphe de φ_v s'identifient aux sauts de ramification de l'extension B/A, i.e. aux entiers s, tels que $G_s \neq G_{s+1}$. Du fait que $P(s)$ et $P_v(s)$ ont même noyau, on déduit directement (le résultat connu) que les sauts de ramification > 0 sont congrus modulo p (à i_0 qui est la valeur supplémentaire de Hilbert de la différente), car si $s \not\equiv i_0 \bmod p$, l'application $P_0(s)$ est injective.

(6.6) Remarques: De la proposition 6.3, on peut déduire des bornes pour le cardinal du groupe d'automorphismes d'une extension donnée de A. Ces bornes peuvent être utilisées pour estimer le nombre d'extensions non-conjuguées de degré donné de A (cf. [T]). (Le nombre d'extensions de degré donné dans une clôture algébrique du corps des fractions de A a été déterminé par Krasner [Kr2].)

L'exemple suivant montre que la proposition 6.3 et le corollaire 6.4 améliorent effectivement les résultats d'Arf et de Krasner qui n'avaient à leur disposition que la fonction P_v:

Supposons $e = 1$, $n = 2p^3$ et $p \geq 5$. Soit k le corps de décomposition de $(X^p + X)(X^{p^2} + X)$ sur F_p.

Posons

$$\mathcal{F} = 1 + U^{p^3-p^2} - \frac{1}{2}U^{2p^3-2p} + U^{2p^3-p-1}$$

$$\mathcal{G} = 1 + U^{p^3-p^2} + \frac{1}{2}U^{2p^3-2p} + U^{2p^3-p-1}$$

$$\mathcal{H} = 1 + U^{p^3-p^2} \qquad\qquad + U^{2p^3-p-1}$$

On trouve

$$\varphi_3(l) = \begin{cases} lp^3, & \text{si } 0 \leq l \leq 1; \\ p^3 + (l-1)p^2, & \text{si } 1 \leq l \leq p+1; \\ 2p^3 + (l-p-1), & \text{si } l \geq p+1; \end{cases}$$

$$P_3(l) = \begin{cases} X^{p^3} - X^{p^2}, & \text{si } l = 1; \\ -X^{p^2}, & \text{si } l = 2, 3, ..., p; \\ -X^{p^2} - X, & \text{si } l = p+1; \\ -X, & \text{si } l = p+2, p+3, ...; \end{cases}$$

et

$$P_j(1) = 0 \qquad \text{si } j = 0 \text{ ou } j = 2.$$

pour les trois objets $(\mathcal{F}, n)$, $(\mathcal{G}, n)$ et $(\mathcal{H}, n)$. Mais,

$$P_1(1) = \begin{cases} X^p - X, & \text{pour } (\mathcal{F}, n); \\ -X^p - X, & \text{pour } (\mathcal{G}, n); \\ -X, & \text{pour } (\mathcal{H}, n); \end{cases}$$

et donc

$$|\ker P(1)| = \begin{cases} p, & \text{pour } (\mathcal{F}, n); \\ 1, & \text{pour } (\mathcal{G}, n) \text{ et } (\mathcal{H}, n). \end{cases}$$

Des extensions définies par (G, n) et $(\mathcal{H}, n)$ ne peuvent donc être galoisiennes, mais, du corollaire 6.4, on ne sait rien dire sur une extension définie par $(\mathcal{F}, n)$.

Rappelons brièvement quelques notions de la théorie de ramification non-galoisiennes. Pour plus de détails, le lecteur pourra consulter [He].

(6.7) Notons Ω la fermeture intégrale de B dans une clôture algébrique de son corps des fractions.

Nous désignerons par $E = E(B/A)$ l'ensemble des A-isomorphismes de B dans Ω.

On posera

$$E_l = \{\sigma \in E / v_B(\sigma(u) - u) \geq l + 1\},$$

lorsque l est un réel ≥ -1, v_B désignant l'unique prolongement à Ω de la valuation discrète normalisée de B. Cette définition ne dépend pas du choix de u.

Deux plongements σ et σ' sont dits *équivalents* modulo E_l, si $v_B(\sigma(u) - \sigma(u')) \geq l+1$. On définit ainsi une relation d'équivalence sur E dont l'espace quotient sera noté E/E_l. Remarquons que deux classes modulo un même E_l ont même cardinal.

(6.8) Proposition: *Supposons qu'il existe une extension galoisienne totalement ramifiée C de A contenant B. Notons m le degré de C sur B, identifions E à l'ensemble des A-morphismes de B dans C, et fixons une uniformisante v de C.*

a) En associant à un élément σ de E l'image de $\frac{\sigma(u)}{u}$ dans k, on définit une bijection de $E_0/E_{\frac{1}{m}}$ sur le noyau de $P_v(0)$.

b) Soit l un entier ≥ 1. En associant à un élément σ de $E_{\frac{l}{m}}$ l'image dans k de l'élément x de C qui vérifie $\frac{\sigma(u)-u}{u} = xv^l$, on définit une bijection de $E_{\frac{l}{m}}/E_{\frac{l+1}{m}}$ sur le noyau de $P_v(\frac{l}{m})$.

En particulier, les polynômes $P_v(\frac{l}{m})$ sont scindés sur k, et les dénominateurs des abscisses des sommets du graphe de φ_v divisent m.

Preuve: Il est clair que les procédés décrits dans a) et b) définissent des applications $E_0/E_{\frac{1}{m}} \to k^*$ et $E_{\frac{l}{m}}/E_{\frac{l+1}{m}} \to k$ respectivement que l'on notera ρ_l.

Notons $(\mathcal{G}, mn)$ et $(\mathcal{X}, m)$ les éléments de E_k qui définissent (C, v) relativement à (A, t) et (B, u) respectivement. On a donc $(\mathcal{G}, mn) = (\mathcal{X}, m) *_\Delta (\mathcal{F}, n)$. Notons x_0 le terme constant de $\mathcal{X}$. Fixons un entier $l \geq 0$, et un élément σ de $E_{\frac{l}{m}}$. Notons $(\mathcal{X}_\sigma, m)$ l'élément de E_k, tel que $\sigma(u) = v^m\, \mathcal{X}_\sigma(v)$, x_σ le coefficient du terme de degré l de $\mathcal{X}_\sigma$, et x celui de $\mathcal{X}$.

Si $l = 0$, on a $\rho_l(\sigma) = \frac{\overline{x}_\sigma}{\overline{x}}$.

Si $l > 0$, on peut écrire $\sigma(u) - u = v^m(\mathcal{X}_\sigma(v) - \mathcal{X}(v)) = v^{m+l}y$ avec $\overline{y} = \overline{x}_\sigma - \overline{x}$, d'où $\frac{\sigma(u)-u}{u} = \frac{v^m}{u} y v^l$ et $\rho_l(\sigma) = \frac{\overline{x}_\sigma - \overline{x}}{\overline{x}_0}$.

Ayant $(\mathcal{G}, m) = (\mathcal{X}_\sigma, m) *_\Delta (\mathcal{F}, n)$, on déduit de 4.2 et de 4.13 que $(P_v(l/m))(\frac{\overline{x}_\sigma}{\overline{x}_0}) = (P_v(l/m))(\frac{\overline{x}}{\overline{x}_0})$ si $l > 0$, et que $(P_v(0))(\overline{x}_\sigma) = (P_v(0))(\overline{x})$, ce qui prouve que $\rho_l(\sigma)$ est bien un élément du noyau de $P_v(l/m)$.

Comme le cardinal de E est n, et que les classes modulo un même $E_{\frac{l}{m}}$ ont toutes le cardinal $|E_{\frac{l}{m}}|$, l'inégalité

$$n = |E| = \prod_{l=0}^{\infty} |E_{\frac{l}{m}}/E_{\frac{l+1}{m}}| \leq \prod_{l=0}^{\infty} |\ker(P_v(l/m))| \leq n$$

vaut, et elle est en fait une égalité, ce qui montre que l'application ρ_l est bijective, que les polynômes $P_v(\frac{l}{m})$ sont scindés sur k, et que les dénominateurs des abscisses des sommets du graphe de φ_v divisent m. □

(6.9) L'application

$$l \mapsto \frac{1}{n} \int_0^l |E_\zeta| d\zeta$$

sera appelée *la fonction de Herbrand* de l'extension B/A, notée $\varphi_{B/A}$.

Si l'extension B/A est galoisienne, elle coïncide avec la fonction de Herbrand telle que définie dans [Se].

(6.10) Corollaire: *L'égalité*

$$\varphi_v(l) = n\varphi_{B/A}(l)$$

vaut pour tout nombre réel $l \geq 0$.

Preuve: Fixons une extension galoisienne C de A contenant B.

Supposons d'abord que C/A est totalement ramifiée. Notons pour tout entier j, $0 \leq j \leq v$, s_j le plus petit nombre réel s, tel que $\varphi_v(s) = \varphi_j(s)$. Alors, la proposition 6.8 montre que $|E_l| = p^j$ pour $s_j < l \leq s_{j-1}$, les différentes classes modulo un même E_l dans E ayant même cardinal. On en déduit que $\varphi_v(l) = \int_0^l |E_\zeta| d\zeta$, d'où le corollaire dans ce cas particulier.

Considérons maintenant le cas général. Comme le corps résiduel k de A est parfait, il existe une existence non-ramifiée A_0 de A, telle que C/A_0 est totalement ramifiée. Comme l'unique système de représentants multiplicatifs S_0 de A_0 contient S (cf. [B]), le couple $(\mathcal{F}, n)$ définit un objet (B_0, u) de $\mathrm{Ext}_{tot}(A_0, t)$, tel que $B \subset B_0 \subset C$, et l'extension B_0/B est non-ramifiée (en fait l'extension B_0/A_0 est obtenue à partir de l'extension B/A par extension du corps résiduel). Par ce qui précède, l'égalité $\varphi_v(l) = n\varphi_{B_0/A_0}(l)$ vaut pour tout $l \geq 0$. Par ailleurs, comme les extensions A_0/A et B_0/B sont non-ramifiées, leur fonction de Herbrand est l'identité, et la formule de transitivité que vérifie la fonction de Herbrand (cf. [He]) montre que

$$\varphi_{B/A} = \varphi_{A_0/A} \circ \varphi_{B_0/A_0} \circ \varphi_{B_0/B}^{-1} = \varphi_{B_0/A_0},$$

d'où le corollaire. □

(6.11) Remarque: Remarquons que la théorie de ramification non-galoisienne ne se généralise pas aux extensions totalement ramifiées d'un anneau de valuation discrète complet dont le corps résiduel est imparfait, car de telles extensions ne se plongent pas nécessairement dans une extension galoisienne à extension résiduelle séparable (cf. [De2]).

7. Invariance des indices d'inséparabilité

Nous gardons les notations du paragraphe précédent.

(7.1) Théorème: *Les indices régularisés de $(\mathcal{F},n)$ et les fonctions φ_j constituent des invariants de l'extension B/A. Ils ne dépendent ni du choix de l'uniformisante t de A ni de la classe d'isomorphie de $(\mathcal{F},n)$ dans la catégorie $E_k(\Delta)$.*

Les termes de $\mathcal{F}$ correspondant aux indices régularisés de $(\mathcal{F},n)$ sont invariants par isomorphisme unitaire, et ainsi sont les polynômes $P_j(l)$, $l \geq 0$.

Preuve: On a déjà prouvé que les indices et donc aussi les indices régularisés de $(\mathcal{F},n)$ ne dépendent pas du choix de t (cf. 3.10). Par ailleurs, il est clair que les indices régularisés sont invariants par isomorphismes constants. Par la proposition 4.2, on est donc ramené aux isomorphismes unitaires.

Soit $(\mathcal{G},n)$ un objet de $E_k(\Delta)$ qui est isomorphe à $(\mathcal{F},n)$ par un isomorphisme unitaire, et supposons qu'il existe un entier j, $0 \leq j \leq v$, tel que les indices régularisés d'ordre j de $(\mathcal{F},n)$ et de $(\mathcal{G},n)$ diffèrent. Supposons de plus j maximal pour cette propriété. On a $j < v$, puisque les indices régularisés d'ordre v sont nuls.

Comme les indices régularisés d'ordre $j+1$ de $(\mathcal{F},n)$ et de $(\mathcal{G},n)$ coïncident, le plus petit des indices régularisés d'ordre j de $(\mathcal{F},n)$ et de $(\mathcal{G},n)$ que l'on notera i est régulier pour l'objet correspondant. Par suite, on a $w_{p,n}(i) \leq j$.

Pour arriver à une contradiction, il suffit de montrer que les termes de degré i de $\mathcal{F}$ et de $\mathcal{G}$ sont égaux. Or, ceci résulte de la propriété a) de 4.8 et de l'inégalité

$$i \leq i_j(\mathcal{F},n) < \varphi_j(1) \leq \varphi_{w_{p,n}(i)}(1).$$

Les autres assertions du théorème sont alors immédiates. □

(7.2) Remarque: En généralisant les définitions précédentes au cas d'un système de représentants quelconque (i.e. non nécessairement multiplicatif) contenant 0, on peut facilement montrer que les indices régularisés d'un couple $(\mathcal{F},n)$ qui définit (B,u) relativement à (A,t) ne dépendent pas non plus du choix du système de représentants S dont lequel les coefficients de $\mathcal{F}$ sont choisis. Ceci est surtout intéressant, si on veut généraliser le présent travail au cas d'un corps résiduel imparfait, car il existe alors plusieurs systèmes de représentants multiplicatifs (cf. [B] et [T]).

(7.3) Définition: Soit j un entier, $0 \leq j \leq v$. L'indice régularisé d'ordre j de $(\mathcal{F},n)$ sera appelé l'*indice d'inséparabilité d'ordre j* de l'extension B/A et noté $i_j(B/A)$.

(7.4) Proposition: *Soit j un entier, $0 \leq j \leq v$, notons i (resp. $\widetilde{i}$) l'indice régularisé (resp. l'indice) d'ordre j de $(\mathcal{F}, n)$, et supposons $\widetilde{i} - i \geq p^j$.*

a) Si la fonction $P_j(1)$ n'est pas constante nulle sur le corps résiduel k, $(\mathcal{F}, n)$ est isomorphe dans $E_k(\Delta)$ à un objet $(\mathcal{G}, n)$ dont l'indice d'ordre j est donné par $i + p^j$.

b) Si $\widetilde{i} = i + p^j$, et si le polynôme $(P_j(1))(X) - \overline{\text{coeff}}(\mathcal{F}, \varphi_j(1))$ s'annule sur k, $(\mathcal{F}, n)$ est isomorphe dans $E_k(\Delta)$ à un objet $(\mathcal{G}, n)$ dont l'indice d'ordre j est $\neq \widetilde{i}$.

Preuve: Remarquons tout d'abord que les hypothèses sur i et $\widetilde{i}$ impliquent que $\varphi_j(1) = i + p^j$.

Supposons l'hypothèse de a) vérifiée. Il existe alors un élément x de S dont l'image dans k n'est pas une racine de $P_j(1)$, et il résulte de 4.8 que l'indice d'ordre j de $(\mathcal{G}, n)$,

$$(\mathcal{G}, n) = (1 + xU, 1) *_\Delta (\mathcal{F}, n),$$

est égal à $i + p^j$.

On prouve de même la partie b) de la proposition, en prenant pour x un élément de S dont l'image dans k annule le polynôme $(P_j(1))(X) - \overline{\text{coeff}}(\mathcal{F}, \varphi_j(1))$. □

(7.5) Remarque: La proposition 7.4 montre que la régularisation des indices de $(\mathcal{F}, n)$ était optimale. En effet, l'hypothèse $\widetilde{i} - i \geq p^j$ n'est pas restrictive, car $0 < \widetilde{i} - i < p^j$ entraîne $w_{p,n}(\widetilde{i}) \leq j - 1$, et $\widetilde{i}$ est alors égal à l'indice d'ordre $j - 1$ de $(\mathcal{F}, n)$. Les autres hypothèses de la proposition sont toujours vérifiées, quitte à effectuer une extension du corps résiduel.

(7.6) Corollaire: *Soit j un entier $0 \leq j < v$. Notons i l'indice d'inséparabilité d'ordre j de B/A si celui-ci est régulier, sinon soit i le plus petit des deux entiers $i_j(B/A) + p^j$ et $i_{j-1}(B/A)$.*

L'entier i est caractérisé par la propriété suivante:

C'est le plus grand entier j, tel que, lorsque B_0/A_0 soit une extension obtenue à partir de B/A par extension du corps résiduel, l'image de toute uniformisante u_0 de B_0 dans $B_0/m_{B_0}^{n+j}$ soit de degré d'inséparabilité formelle $\geq p^{j+1}$ sur $A_0/A_0 \cap m_{B_0}^{n+j}$, m_{B_0} désignant l'idéal maximal de B_0.

Preuve: Ceci résulte de la proposition 7.4 et de la remarque après, compte tenu de la proposition 3.9. □

(7.7) Remarque: L'exemple suivant montre que les indices d'inséparabilité sont des invariants plus fins que la fonction de Herbrand:

Supposons $p > 3$, $n = p^2$ (en sorte que $v = 2$), $e = 3$, et que $X^{p^2} - 3X$ se décompose sur k. Posons

$$\mathcal{F} = 1 + U^{3p^2-2p} + U^{3p^2-3} \qquad \text{et} \qquad \mathcal{G} = 1 + U^{3p^2-p} + U^{3p^2-3}.$$

On trouve

$$\varphi_2(l) = \begin{cases} lp^2, & \text{si } l \leq 3; \\ 3p^2 + l - 3, & \text{si } l \geq 3, \end{cases} \qquad \text{et} \qquad P_2(l) = \begin{cases} X^{p^2}, & \text{si } l = 1, 2; \\ X^{p^2} - 3X, & \text{si } l = 3; \\ -3X & \text{si } l \geq 4. \end{cases}$$

dans les deux cas. Le graphe de φ_2 n'ayant qu'un seul sommet dont l'abscisse est 3 et le polynôme $P_2(3)$ étant scindé sur k, des extensions définies par $(\mathcal{F}, n)$ ou $(\mathcal{G}, n)$ sont galoisiennes par la partie c) de la proposition 6.3. Par contre, les indices régularisés d'ordre 1 de $(\mathcal{F}, n)$ et de $(\mathcal{G}, n)$ diffèrent. Les objets $(\mathcal{F}, n)$ et $(\mathcal{G}, n)$ ne peuvent donc être isomorphes dans $E_k(\Delta)$. On en déduit deux extensions galoisiennes qui ont la même fonction de Herbrand et dont les groupes de Galois sont isomorphes par un isomorphisme de filtration, mais dont les indices d'inséparabilité d'ordre 1 diffèrent et qui ne sont donc pas A-isomorphes.

(7.8) Remarque: Remarquons qu'il n'est malheureusement pas toujours possible de déduire des indices d'inséparabilités de deux extensions consécutives B/A et C/B les indices d'inséparabilités de l'extension C/A.

Références bibliographiques:

[A] *C. Arf,* Untersuchungen über reinverzweigte Erweiterungen diskret bewerteter Kõrper, J. Reine Angew. Math. **181** (1939), 1-44.

[B] *N. Bourbaki,* Algèbre Commutative Ch. 9., Hermann, Paris 1961.

[De1] *P. Deligne,* Les corps locaux de caractéristique p, limites de corps locaux de caractéristique 0. Dans: Représentation des Groupes Réductifs sur un Corps Local, Hermann, Paris 1984.

[De2] *P. Deligne,* Lettre à l'auteur du 31 mars 1994.

[H] *V. Heiermann,* De nouveaux invariants numériques pour les extensions totalement ramifiées de corps locaux, C.R.Acad.Sci.Paris **318** (1994), 989-993.

[Ha] *H. Hasse,* Number Theory, Grundlehren der mathematischen Wissenschaften **229**, Springer-Verlag, Berlin-Heidelberg-New York 1980.

[He] *C. Helou,* Non Galois Ramification Theory for Local Fields, R. Fischer, München 1990.

[JP] *P. Jaffard, G. Poitou,* Introduction aux catégories et aux problèmes universels, Ediscience, Paris 1971.

[Kr1] *M. Krasner,* Sur la primitivité des corps p-adiques, Mathematica Cluj **13** (1937), 72-191.

[Kr2] *M. Krasner,* Nombre des extensions d'un degré donné d'un corps p-adique. Dans: "Les Tendances Géométriques en Algèbres et Théorie des Nombres", Colloques Internationaux du C.N.R.S. **143**, Paris, 1966, 143-169.

[L] *S. Lang,* Algebra, Addison-Wesley, 1984.

[N] *J. Neukirch,* Class Field Theory, Grundlehren der mathematischen Wissenschaften **280**, Springer-Verlag, Berlin-Heidelberg-New York-Tokyo 1986.

[Se] *J.-P. Serre,* Corps locaux, Hermann, Paris 1968.

[T] *V. Heiermann,* De nouveaux invariants numériques pour les extensions totalement ramifiées de corps locaux, Thèse de Doctorat, Université de Provence, Marseille 1994.

Zeppelinstr. 42, 46236 Bottrop