An. Şt. Univ. Ovidius Constanţa Vol. 14(1), 2006, 45–66

Sur la tour des clôtures modulaires

Mustapha CHELLALI and El Hassane FLIOUET

Abstract

Soit K/k une extension purement inséparable. Soit K_1 la cloture modulaire de K/k. Soit k_1 un corps intermédiaire de K/k tel que K/k_1 est modulaire. Calculons de même K_2/k_2 à partir de K_1/k_1 et ainsi de suite. On montre que si K/k est finie (et plus généralement si K/k_r est finie et k_r/k modulaire avec k_r la cloture relativement parfaite de k dans K) alors la suite K_i est stationnaire. En particulier si on prend toujours $k_1 = K$ ou toujours k_1 le plus petit corps intermédiaire de K/k tel que K/k_1 est modulaire, alors la suite K_i/k_i est stationnaire

Let K/k be a purely inseparable field extension. Let K_1 be the modular closure of K/k. Let k_1 be an intermediary field of K/k such that K/k_1 is modular. We do the same with K_1/k_1 and so on. We show that if K/k is finite (and more generaly, if K/k_r is finite and k_r/k modular, where k_r is the perfecte relative closure of k in K), then the sequense K_i is finite. In particular if always $k_1 = K$ or always k_1 is the least intermediary field of K/k such that K/k_1 is modular, than the sequence of extension K_i/k_i is finite.

Subject Classification: 12F15.

1 Introduction

Soit K/k une extension purement inséparable. Soit K_1 la cloture modulaire de K/k. Soit k_1 un corps intermédiaire de K/k tel que K/k_1 est modulaire. Calculons de même K_2/k_2 à partir de K_1/k_1 et ainsi de suite. On montre que si K/k est finie (et plus généralement si K/k_r est finie et k_r/k modulaire avec k_r la cloture relativement parfaite de k dans K) alors la suite K_i est

Key Words: Pure inseparable extensions; Modular extensions; Galois theory.
Received: April, 2006

stationnaire. En particulier si on prend toujours $k_1 = K$ ou toujours k_1 le plus petit corps intermédiaire de K/k tel que K/k_1 est modulaire, alors la suite K_i/k_i est stationnaire. La preuve fait l'objet du §5.

Si on prend pour k_1 n'importe quel corps intermédiaire de K/k tel que K/k_1 est modulaire, l'extension limite K_i est telle que K_i/L est modulaire pour tout corps intermédiaire L de K_i/k_i. Le théorème 7.5 décrit explicitement de telle extensions.

Dans les §2,3 on reprend les notations et résultats de [5], puisque ils sont utilisés avec toute leur force ici. Le §4 présentent les propriété de modularité dont nous aurons besoin au §5.

2 Degré d'irrationalité d'une extension

Dans cette section, K/k designe une extension de corps commutatifs de caractéristique $p > 0$.

Définition 1.2 *Une partie G de K est dite r-générateur de K/k si $K = k(G)$; si de plus $|G|$ est minimum, G est dite r-base de K/k. Une partie A de K est dite r-libre sur k, si c'est une r-base de $k(A)/k$; dans le cas contraire A est dite r-lié sur k.*

On note, $di(K/k) = |G|$, (G une r-base de K/k) et $di(K/k)$ sera appellé le degré d'irrationalité de K/k.

D'àprès [14] on a :

Proposition 1.2 *Soit K/k une extension purement inséparable finie. Une partie G de K est une r-base de K/k si et seulement si G est une r-base de $K/k(K^p)$.*

Preuve : On a que K/k est purement inséparable finie; donc il existe $m_1 \in \mathbf{N}$ tel que $K^{p^{m_1}} \subseteq k$. Si G est une r-base de K/k, alors G est un r-générateur de $K/k(K^p)$; s'il existe $x \in G$ tel que $K = k(K^p)(G\backslash\{x\})$, alors $K = k(K^{p^2})(G\backslash\{x\}) = \cdots = k(K^{p^{m_1}})(G\backslash\{x\}) = k(G\backslash\{x\})$. C'est absurde car G est une r-base de K/k. Inversement, si G est une r-base de $K/k(K^p)$, alors $K = k(K^p)(G) = \cdots = k(K^{p^{m_1}})(G) = k(G)$; d'où $di(K/k) = di(K/k(K^p))$ ■

Remarque: Cette proposition permet de ramener l'étude des propriétés de r-indépendance$''$ sur k à des propriétés de p-indépendance sur $k(K^p)$ lesquelles sont plus riches (théorème de la base incomplète ...), $K/k(K^p)$ étant de hauteur 1.

Corollaire 1.2 *Si K/k est une extension purement inséparable finie, alors*

$$[K : k(K^p)] = p^{di(K/k)}.$$

Proposition 2.2 *Soit L/k une sous-extension d'une extension finie K/k. On a:*

$$di(K/k) \leq di(K/L) + di(L/k),$$

avec l'égalité si et seulement si une r-base de L/k se prolonge en une r-base de K/k.

Preuve: Soit A une r-base de L/k, B une r-base de K/L; on a $K = L(B) = k(A)(B) = k(A \cup B)$; donc $di(K/k) \leq |A \cup B| = |A| + |B|$ (car $A \cap B = \emptyset$). S' il y a égalité $|A \cup B| = |A| + |B| = di(K/k)$, alors $A \cup B$ est une r-base de K/k. Inversement, si une r-base A de L/k se prolonge en une r-base $A \cup B$ (avec $A \cap B = \emptyset$) de K/k; il est immédiat que B est une r-base de $K/k(A)$; donc $di(K/k) = |A| + |B| = di(L/k) + di(K/L)$. ■

Une application type de cette proposition est: Soit B une r-base de K/k, $A \subset B$; alors A et $B \setminus A$ sont respectivement des r-bases de $k(A)/k$ et $K/k(A)$.

Proposition 3.2 *Soit K/k une sous-extension finie d'une extension Ω/k, L un sous-corps de Ω. On a*

$$di(L(K)/L(k)) \leq di(K/k).$$

Preuve : Il est immédiat qu'une r-base de K/k est r-générateur de $L(K)/L(k)$. ■

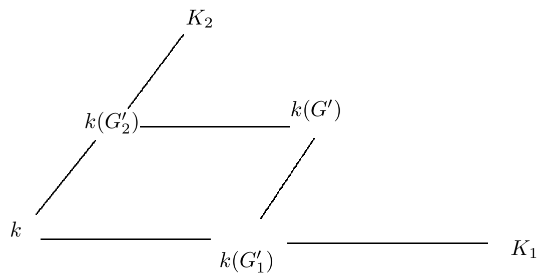
Soit S/k une sous-extension séparable de k dans K. Par le Théorème de l'élément primitif, il existe $\alpha_1 \in S$ tel que : $S = k(\alpha_1)$. Soient G une r-base de K/S et $\beta \in G$. Il est connu que $di(S(\beta)/k) = 1$. On en déduit : $di(K/k) = di(K/S)$, ce qui permet de ramener l'étude de di à une extension purement inséparable.

Proposition 4.2 *Soient K_1/k et K_2/k des sous-extensions finies d'une extension K/k. On a:*

1. *$di(K_1(K_2)/K_2) \leq di(K_1/k)$ avec l'égalité si K_1 et K_2 sont k-linéairement disjoints.*

2. *$di(K_1(K_2)/k) \leq di(K_1/k) + di(K_2/k)$ avec l'égalité si K_1 et K_2 sont k-linéairement disjoints et K_1/k, K_2/k purement inséparables.*

Preuve : Soit S la clôture séparable de k dans K_1. D'après la remarque ci-dessus, on a : $di(K_1/k) = di(K_1/S)$ et $di(K_1(K_2(S))/S(K_2)) = di(K_1(K_2)/K_2)$,. Donc on peut supposer que K_1/k est purement inséparable. Soit G est une r-base de K_1/k; alors $K_1(K_2) = K_2(G)$. Soit $G' \subset G$ vérifiant $K_1(K_2) = K_2(G')$; comme K_1/k et K_2/k sont k-linéairement disjointes, alors $K_1/k(G')$ et $K_2(G')/k(G')$ sont $k(G')$-linéairement disjointes. Il en résulte que $K_1 = K_1 \cap (K_1(K_2)) = K_1 \cap (K_2(G')) = k(G')$. Donc $G = G'$, car G est minimal. Soient G_1 et G_2 des r-bases respectives de K_1/k et K_2/k; on a $K_1(K_2) = k(G_1 \cup G_2)$; donc $di(K_1(K_2)/k) \leq |G_1 \cup G_2| \leq |G_1| + |G_2|$. Soit $G' \subset G_1 \cup G_2$ tel que $K_1(K_2) = k(G')$; on peut écrire $G' = G'_1 \cup G'_2$ avec $G'_1 \subset G_1$ et $G'_2 \subset G_2$; comme K_1/k et K_2/k sont k-linéairement disjointes, par la transitivité de cette propriété (cf. figure), K_1 et $k(G')$ sont $k(G'_1)$-linéairement disjoints; en particulier $K_1 \cap k(G') = k(G'_1)$. Soit $K_1 = k(G'_1)$; donc $G'_1 = G_1$; de même $G'_2 = G_2$. ■



Ce qui suit est le résultat de [1] énoncé d'une façon légèrement améliorée :

Théorème 1.2 *Soit L/L' une sous-extension de K/k. Alors $di(L/L') \leq di(K/k)$.*

Preuve : On se ramène imédiatement au cas $L' = k$.
Cas où K/k est purement inséparable : Par le corollaire 1, on a

$$p^{di(K/k)} = [K : k(K^p)] = \frac{[K : L][L : k(L^p)]}{[k(K^p) : k(L^p)]}.$$

Or, $[k(K^p) : k(L^p)] \leq [K^p : L^p] = [K : L]$; donc $p^{di(L/k)} = [L : k(L^p)] \leq p^{di(K/k)}$.
Cas Général : Soit S la clôture séparable de K/k. On a : $L/L \cap S$ est purement inséparable et $S/L \cap S$ est séparable; donc $S/L \cap S$ et $L/L \cap S$ sont $L \cap S$-linéairement disjointes; donc $di(L/k) = di(L/L \cap S) = di(S(L)/S) \leq di(K/S) = di(K/k)$. ■

Rappelons qu'on appel le degré d'imperfection d'un corps commutatif k le cardinal d'une p-base de k (une r-base de k/k^p); on le notera $di(k)$.

Exemple : Si P est parfait $di(P(X_1, X_2, \ldots, X_n)) = n$.

Le théorème suivant est la généralisation naturelle du théorème de l'élément primitif.

Théorème 2.2 *Supposons $di(k)$ fini et k non parfait. Alors pour toute extension finie K de k, on a*

$$di(K/k) \leq di(k).$$

Preuve: En utilisant l'extension normale engendrée et la proposition 4.2, on se ramène à K/k purement inséparable. Soit m tel que $K^{p^m} \subset k$, B une p-base de k; soit dans une clôture purement inséparable de K, A tel que $A^{p^m} = B$. On a $K^{p^m} \subset k = k^p(B) = k^{p^m}(B) = k^{p^m}(A^{p^m})$; d'où $K \subset k(A)$; donc $di(K/k) \leq |A| = di(k)$ ■.

Ceci amène à regarder de près l'entier $di(k)$. On a (cf [15]) :

Théorème 3.2 *Supposons $di(k)$ fini. On a :*
1) Si K/k est fini $di(K) = di(k)$.
2) Si K/k est algébrique séparable, $di(K) = di(k)$.
3) Si K/k est purement inséparable infini, $di(K) < di(k)$.

Preuve : 1) Si K/k est fini on a :

$$[K, K^p] = \frac{[K, k][k, k^p]}{[K^p, k^p]} = \frac{[K, k][k, k^p]}{[K, k]} = [k, k^p].$$

2) Si K/k est séparable, $K^p \cap k = k^p$ et $K^p(k) = K$; de plus K^p/k^p est séparable et k/k^p purement inséparable; donc k et K^p sont k^p-linérement disjoint; l'égalité resulte de la proposition 4.2.

3) Soit K/k purement inséparable; soit B une p-base de K, $B_1 \subset B$ finie, $k_1 = k(B_1)$; B_1 est p-libre sur K, donc sur k_1; donc $|B_1| \leq di(k_1) = di(k)$ car k_1/k finie. Par suite $K/K^p(k)$ est fini. Soit B' une r-base de $K/K^p(k)$, $L = k(B')$. On a:

$$[K, K^p] = [K^p(k)(B'), K^p] = [L(K^p), L^p(K^p)].$$

Donc

$$[K, K^p] \leq [L, L^p],$$

avec l'égalité si et seulement si K^p et L sont L^p-linéairement disjoints, c'est-à-dire si et seulement si K/L est séparable, c'est-à-dire si et seulement si $K = L$ (puisque K/L est purement inséparable). ■

Corollaire 2.2 *Si K/k est algébrique, on a $di(K) \leq di(k)$.*

Dans la même suite d'idée, on dit que K/k est relativement parfaite si $k(K^p) = K$. On a :

- Si K/L et L/k sont relativement parfaites, alors K/k est relativement parfaite.
- Si K/k est relativement parfaite, alors LK/Lk est relativement parfaite.
- Si K_i/k $(i \in I)$ sont relativement parfaites, alors $\prod_i K_i/k$ est relativement parfaite.

Par suite, il existe une plus grande sous-extension k_r/k de K/k relativement parfaite. On la notera $k_r = rp(K/k)$. On a ces relations d'associativité-transitivité :

Proposition 5.2 *Soit L un corps intermédiaire de K/k ($L \in [k, K]$). On a*

$$rp(rp(K/L)/k) = rp(K/k)$$

$$rp(K/rp(L/k)) = rp(K/k)$$

Preuve : Pour la première relation, posons $Y = rp(K/L)$ et $k_r = rp(K/k)$, on a Lk_r/L est relativement parfaite, donc $Lk_r \subset Y$, donc $k_r \subset Y$, donc $k_r \subset rp(Y/k)$. Pour la même raison comme $rp(Y/k)$ est relativement parfaite sur k, on a $rp(Y/k) \subset k_r$

Pour la deuxième relation on a par la transitivté $rp(K/rp(L/k))$ relativement parfaite sur k, donc $rp(K/rp(L/k)) \subset rp(K/k)$. Comme $rp(K/k)$ est relativement parfaite sur $rp(L/k)$ (car $k \subset rp(L/k) \subset rp(K/k)$), $rp(K/k) \subset rp(K/rp(L/k))$ ■

Dans la suite il est commode de noter $[k, K]$ l'ensemble des corps intermédiaires d'une extension K/k.

Corollaire 3.2 *Posons $k_r = rp(K/k)$. Soit $L \in [k, K]$, alors*

$$K/L \textit{ finie} \Longrightarrow k_r \subset L.$$

En particulier si K/k est relativement parfaite, on a

$$K/L \ finie \ \Longrightarrow L = K.$$

Schématiquement on a un *trou*

$$\begin{array}{ccc} k \longrightarrow & & K\ ; \\ & \uparrow & \\ & \textit{trou} & \end{array}$$

Ce *trou* caractérise K/k relativement parfaite ; en effet si K/k vérifie le *trou*, soit B une p-base de K/k. Si $B \neq \emptyset$ soit $x \in B$ et $L = k(K^p)(B \setminus \{x\})$; on a K/L finie donc $K = L$ ce qui est absurde.

Lemme 1.2 *Soit K/k une extension purement inséparable avec $K/rp(K/k)$ finie. La suite décroissante $(K^{p^n}(k))_{n\in \mathbf{N}}$ est stationnaire sur $K^{p^{n_0}}(k) = rp(K/k)$.*

Preuve: Posons $k_r = rp(K/k)$. Comme K/k_r est finie, il existe n tel que $k(K^{p^n}) \subset k_r$. Or $k_r = k(k_r^{p^n}) \subset k(K^{p^n})$ ■

On aura besoin aussi de :

Proposition 6.2 *Soit K/k une extension purement inséparable avec $K/rp(K/k)$ finie. Soit $L \in [k, K]$, on a*

$$rp(L/k) = Lrp(K/k).$$

Preuve : Posons $k_r = rp(K/k)$, on a Lk_r/L relativement parfaite. Donc $Lk_r \subset rp(K/L)$. On alors $rp(K/L)/Lk_r$ finie, purement inséparable et relativement parfaite. Donc $rp(K/L) = Lk_r$ ■

Proposition 7.2 *Soit K/k une extension purement inséparable avec $di(K)$ fini, alors $K/rp(K/k)$ est finie.*

Preuve : On a $K = K^p(B)$ avec B fini. Il existe e tel que $B^{p^e} \subset k$. Donc $K^{p^e} = K^{p^{e+1}}(B^{p^e}) \subset k(K^{p^{e+1}})$. Donc $k(K^{p^e}) = k(K^{p^{e+1}})$. Posons $L = k(K^{p^e})$. On a $k(L^p) = L$. Donc $L \subset rp(K/k)$. Et on a $[K, L] \leq [K, K^{p^e}]$ fini. ■

3 Exposants des extensions purement inséparable

Définition 2.3 *Soit K/k une extension purement inséparable finie de caractéristique $p \neq 0$, $x \in K$. Posons : $o(x/k) = inf\{m \in \mathbf{N} : x^{p^m} \in k\}$, $o_1(K/k) = inf\{m \in \mathbf{N} : K^{p^m} \subset k\}$. Une r-base $B = \{a_1, a_2, \ldots a_n\}$ de K/k est dite canoniquement ordonnée si pour $j = 1, 2, \ldots, n$*

$$o(a_j/k(a_1, a_2, \ldots a_{j-1})) = o_1(K/(a_1, a_2, \ldots a_{j-1})).$$

Remarque 1.3 *Toute r-base peut être canoniquement ordonnée.*

Lemme 2.3 *Si $G = \{a_1, \ldots, a_n\}$ une r-base canoniquement ordonnée de K/k, alors*

$$o(a_s/k(a_1, \ldots, a_{s-1})) = \inf\{m \in \mathbf{N} : di(k(K^{p^m})/k) \leq s - 1\}.$$

Preuve : Posons $o(a_s/k(a_1,\ldots,a_{s-1})) = m_s$ et $m'_s = \inf\{m \in \mathbf{N} : di(k(K^{p^m})/k) \leq s-1\}$. Par définition de la r-base canoniquement ordonnée de K/k on a: pour tout $i \in \{1,\ldots,n\}$, $a_i^{p^{m_s}} \in k(a_1,\ldots,a_{s-1})$, donc $k(K^{p^{m_s}}) \subseteq k(a_1,\ldots,a_{s-1})$. Par le théorème 1.2, on a $di(k(K^{p^{m_s}})/k) \leq s-1$, donc $m'_s \leq m_s$. Supposons $m'_s < m_s$; on a $di(k(K^{p^{m'_s}}) \leq s-1$ donc $di(k(a_1^{p^{m'_s}},\ldots,a_s^{p^{m'_s}})) \leq s-1$ (th 1.2); donc $(a_1^{p^{m'_s}},\ldots,a_s^{p^{m'_s}})$ est r-lié sur k, donc sur $L = k(k(a_1^{p^{m'_s}},\ldots,a_s^{p^{m'_s}}))^p$ (prop 1.2, §2); donc il existe $j \leq s$ tel que

$$a_j^{p^{m'_s}} \in L(a_1^{p^{m'_s}},\ldots,a_{j-1}^{p^{m'_s}}) = k(a_1^{p^{m'_s}},\ldots,a_{j-1}^{p^{m'_s}},a_j^{p^{m'_s+1}},\ldots a_s^{p^{m'_s+1}}).$$

Comme $m'_s < m_s \leq m_j$ on en déduit que

$$(a_j^{p^{m'_s}})^{p^{m_j-m'_s-1}} \in k(a_1^{p^{m_j-1}},\ldots,a_{j-1}^{p^{m_j-1}},a_j^{p^{m_j}},\ldots a_s^{p^{m_j}}) \subset k(a_1,\ldots,a_{j-1}),$$

ce qui est absurde car $m_j = o(a_j/k(a_1,\ldots,a_{j-1}))$. ∎

Il en résulte immédiatement ([15])

Théorème 4.3 *Les entiers $o(a_i/k(a_1,\ldots,a_{i-1}))$, $(1 \leq i \leq n)$ sont indépendants du choix de la r-bases canoniquement ordonnée $\{a_1,\ldots,a_n\}$ de K/k.*

On appellera $o(a_i/k(a_1,\ldots,a_{i-1}))$ le i-ème exposant de K/k et on le notera $o_i(K/k)$. On a

$$o_1(K/k) \geq o_2(K/k) \geq \cdots \geq o_n(K/k).$$

On pose $o_i(K/k) = 0$, si $i > n$.

Proposition 8.3 *Soit K et L des corps intérmédiaires d'une extension Ω/k avec K/k purement inséparable fini. Alors pour tout entier j, on a $o_j(K(L)/k(L)) \leq o_j(K/k)$.*

Preuve : Posons $m_j = o_j(K/k)$; on a $di((K(L)^{p^{m_j}}k(L)/k(L) = = di(K^{p^{m_j}}(k)(L)/k(L)) \leq di(k(K^{p^{m_j}})/k) \leq j-1$; donc $o_j(K(L)/k(L) \leq m_j$. ∎

Proposition 9.3 *Si K_1/k et K_2/k sont deux sous-extensions de K/k, alors K_1/k et K_2/k sont k-linéairement disjointes si et seulement si $o_j(K_1(K_2)/K_2) = o_j(K_1/k)$, $(\forall j \in \mathbf{N})$.*

Preuve : Soit $\{a_1, \dots, a_n\}$ une r-base canoniquement ordonnée de K_1/k; on a pour tout $i \in \mathbf{N}$, $o_i(K_1/k) \geq o_i(K_1(K_2)/K_2)$. Or

$$[K_1(K_2) : K_2] = p^{o_1(K_1(K_2)/K_2)} \dots p^{o_n(K_1(K_2)/K_2)} = [K_1 : k] = p^{o_1(K_1/k)} \dots p^{o_n(K_1/k)}.$$

Il en résulte que pour tout $i \in \mathbf{N}$, $o_i(K_1/k) = o_i(K_1(K_2)/k)$. Réciproquement, on a $[K_1(K_2) : K_2] = \prod_{i\in\mathbf{N}} p^{o_i(K_1(K_2)/K_2)} = \prod_{i\in\mathbf{N}} p^{o_i(K_1/k)} = [K_1 : k]$. Donc K_1/k et K_2/k sont k-linéairement disjointes. ■

Proposition 10.3 *Soit K/k une extension purement inséparable finie. Pour toute sous-extension L/L' de K/k. Pour tout $j \in \mathbf{N}$, on a $o_j(L/L') \leq o_j(K/k)$.*

Preuve : On a $di(L'(L^{p^{o_j(K/k)}})/L') \leq di(L'(K^{p^{o_j(K/k)}})/L') \leq di(k(K^{p^{o_j(K/k)}})/k) \leq j-1$. Donc $o_j(L/L') \leq o_j(K/k)$. ■

Proposition 11.3 *(Algorithme de complétion des r-bases) Soient K/k une extension purement inséparable finie et G un r-générateur de K/k. Si $\{\alpha_1, \dots, \alpha_s\}$ est un système de K tel que $o(\alpha_j/k(\alpha_1, \dots, \alpha_{j-1})) = o_j(K/k)$, $1 \leq j \leq s$, alors, pour toute suite $\alpha_{s+1}, \alpha_{s+2}, \dots$ d'éléments de G vérifiant $o(\alpha_j/k(\alpha_1, \dots, \alpha_{j-1})) = \max_{a\in G}(o(a/k(\alpha_1, \dots, \alpha_{j-1})))$, $j \geq 1$, la suite s'arrête sur un plus grand entier n tel que $o(\alpha_n/k(\alpha_1, \dots, \alpha_{n-1})) > 0$ et on a $\{\alpha_1, \dots, \alpha_n\}$ est une r-base de K/k.*

Preuve : Soit $m_j = o_j(K/k)$, $m'_j = o(\alpha_j/k(\alpha_1, \dots, \alpha_{j-1}))$. Comme G est un r-générateur de K/k et que pour tout $a \in G$, $a^{p^{m'_j}} \in k(\alpha_1, \dots, \alpha_{j-1})$, on a $di(k(K^{p^{m'_j}})) \leq j-1$; donc $m'_j \geq m_j$. D'autre part,

$$p^{\sum_{j=1}^{t} m'_j} = [k(\alpha_1, \dots, \alpha_t), k] \leq [K, k] = p^{\sum_j m_j}.$$

donc $\sum_{j=1}^{t} m'_j \leq \sum_j m_j$ $\forall t \in \mathbf{N}$; donc $m'_j = m_j$ et on a $k(\alpha_1, \dots, \alpha_n) = K$. D'où $\{\alpha_1, \dots, \alpha_n\}$ est une r-base de K/k ■

Soit m_j le j-ème exposant de K/k , $\{\alpha_1, \dots, \alpha_n\}$ une r-base canoniquement ordonnée de K/k. Appliquons l'algorithme ci-dessus à $k(K^{p^{m_j}}) = k(\alpha_1^{p^{m_j}}, \dots, \alpha_n^{p^{m_j}})$. Par récurrence sur j on obtient la proposition suivante.

Proposition 12.3 *Soit $1 \leq j \leq n$. On a*
1) $\alpha_j^{p^{m_j}} \in k(\alpha_1^{p^{m_j}}, \dots, \alpha_{j-1}^{p^{m_j}})$

2) $k(K^{p^{m_j}}) = k(\alpha_1^{p^{m_j}}, \dots, \alpha_{j-1}^{p^{m_j}})$
3) Soit $\Lambda_j = \{(i_1, \dots i_{j-1}) \mid 0 \leq i_1 < p^{m_1 - m_j}, \dots, 0 \leq i_{j-1} < p^{m_{j-1}-m_j}\}$*; alors*
$\{(\alpha_1, \dots \alpha_{j-1})^{p^{m_j}\xi} | \xi \in \Lambda_j\}$ *est une base de* $k(K^{p^{m_j}})$ *sur* k
4) Soit $n \in N$ *,* j *le plus grand entier tel que* $m_j > n$*; alors* $\{\alpha_1^{p^n}, \dots, \alpha_j^{p^n}\}$ *est une r-base canoniquemnt ordonnée de* $k(K^{p^n})/k$ *et sa liste des exposants est* $(m_1 - n, m_2 - n, \dots, m_j - n)$.

4 Extensions modulaires

On rappelle qu'une extension quelconque K/k est dite modulaire si pour tout $n \in \mathbf{N}$, K^{p^n} et k sont $K^{p^n} \cap k$-linéairement disjointes. Cette notion caractérise les extensions purement inséparables finies qui sont produit tensoriel d'extensions simples (cf. [16]). Le théorème de [16] a été légerement amélioré dans [11]. On a

Théorème 5.4 *Soit* K/k *une extension purement inséparable. Soit* k_r *la cloture relativement parfaite de* k *dans* K*. Supposons* K/k_r *finie et* k_r/k *modulaire. Il est équivalent de dire :*

1. K/k *est modulaire.*
2. *Il existe une r-base canoniquement ordonnée* $(\theta_1, \theta_2, \dots, \theta_m)$*de* K/k_r *telle que*

$$K = k_r \otimes_k k(\theta_1) \otimes_k k(\theta_2) \otimes_k \cdots \otimes_k k(\theta_m)$$

Dans notre résultat principal (Théorème 6.5), on se place sous les hypothèses générales du théorème ci-dessus. Aussi le théorème ci-dessus joue un rôle important dans la suite. En voici la preuve :

1. $\Longrightarrow$ 2. : Si K/k est modulaire, soit $(\theta_1, \theta_2, \dots, \theta_m)$ une r-base canoniquement ordonnée de K/k_r. Posons $e_i = o_i(K/k_r)$. On a (proposition 12.3)

$$\theta_i^{p^{e_i}} \in k_r(\theta_1^{p^{e_i}}, \theta_2^{p^{e_i}}, \dots, \theta_{i-1}^{p^{e_i}})$$

On a k_r/k relativement parfaite. Donc $k_r = k(k_r^{p^{e_i}})$. Donc il existe $B \subset k_r$ tel que $B^{p^{e_i}}$ soit une base linéaire de k_r/k. Donc

$$\theta_i^{p^{e_i}} \in k(B^{p^{e_i}}, \theta_1^{p^{e_i}}, \theta_2^{p^{e_i}}, \dots, \theta_{i-1}^{p^{e_i}})$$

Ce qui s'écrit linéairment

$$\theta_i^{p^{e_i}} = \sum_\alpha c_\alpha d_\alpha^{p^{e_i}},$$

$(d_\alpha^{p^{e_i}})$ base linéaire de $k(B^{p^{e_i}}, \theta_1^{p^{e_i}}, \theta_2^{p^{e_i}}, \ldots, \theta_{i-1}^{p^{e_i}})/k$. On a $(d_\alpha^{p^{e_i}})$ système de $K^{p^{e_i}}$ libre sur k, donc sur $k \cap K^{p^{e_i}}$, donc peut étre prolongé à une base de $K^{p^{e_i}}/k \cap K^{p^{e_i}}$. Comme K/k est modulaire, $K^{p^{e_i}}$ et k sont inéairment disjoints. Donc c'est aussi une base de $k(K^{p^{e_i}})/k$. Comme $\theta_i^{p^{e_i}} \in K^{p^{e_i}}$, par identification les $c_\alpha \in k \cap K^{p^{e_i}}$. Notons $a_\alpha = c_\alpha^{p^{-e_i}}$. On a $a_\alpha \in K$ et $a_\alpha^{p^{e_i}} \in k$ et

$$\theta_i = \sum_\alpha a_\alpha d_\alpha$$

On a $d_\alpha \in k_r(\theta_1, \ldots, \theta_{i-1})$ et

$$o(a_\alpha/k_r(\theta_1, \ldots, \theta_{i-1})) \leq o(a_\alpha/k) \leq e_i$$

Si chaque a_α vérifie $o(a_\alpha/k_r(\theta_1, \ldots, \theta_{i-1})) < e_i$ alors $o(\theta_i/k_r(\theta_1, \ldots, \theta_{i-1}))) < e_i$, contradiction. Donc il existe α tel que $o(a_\alpha/k_r(\theta_1, \ldots, \theta_{i-1})) = e_i$. Par la proposition 11.3, on voit qu'on peut substituer a_α à θ_i et donc se ramener à θ_i tel que

$$o(\theta_i/k_r(\theta_1, \ldots, \theta_{i-1})) = o(\theta_i/k(\theta_1, \ldots, \theta_{i-1})) = o(\theta_i/k)$$

Ceci succesivement pour $i = 1, 2, \ldots, m$. La r-base finale obtenue, vérifie

$$[k_r(\theta_1, \ldots, \theta_m), k_r] = [k(\theta_1, \ldots, \theta_m), k] = \prod_i [k(\theta_i), k]$$

Ce qui équivaut à

$$K = k_r \otimes_k k(\theta_1) \otimes_k k(\theta_2) \otimes_k \cdots \otimes_k k(\theta_m)$$

2. $\Longrightarrow$ 1. car si 2., K est produit tensoriel d'extensions modulaires et on a

Lemme 3.4 *Soit K/k une extension purement inséparable. Si $K = K_1 \otimes_k K_2$, avec K_i/k modulaires, alors K/k est modulaire.*

Preuve : K_1 est réunion inductive d'extensions finies F_i/k. Soit M_i/k la cloture modulaire de F_i/k. On a $M_i \subset K_1$. On sait que M_i/k est finie (voir aussi la proposition 15.4). Par suite K_1 est réunion inductive d'extensions modulaires finies M_i/k. De même pour K_2. Donc K est réunion inductive d'extensions $M_i \otimes_k M_j$ qui sont modulaires par [16]. Donc K/k est modulaire. ■

Comme conséquence immédiate de la définition de modularité; on a

Proposition 13.4 *Soient $m, n \in \mathbb{Z}$ avec $n \geq m$, si K/k est modulaire, alors K^{p^m}/k^{p^n} est modulaire.*

La condition $n \geq m$ assure $k^{p^n} \subset K^{p^m}$.

On a vu au §3 que toute r-base peut être canoniquement ordonnée. Dans certain cas cet ordre, peut être compatible même avec un corps intermédiaire. On a

Proposition 14.4 *Soit K/k une extension purement inséparable. Soit k_r la clôture relativement parfaite de k dans K. Supposons K/k_r fini. Soit k_1/k une sous-extension de K/k. Supposons K/k modulaire, alors il existe une r-base canoniquement ordonnée $(\theta_1, \theta_2, \ldots, \theta_m)$ de K/k_r verifiant*

1. *$K = k_r \otimes_k k(\theta_1) \otimes_k \cdots \otimes_k k(\theta_m)$*
2. *$(\theta_1, \theta_2, \ldots, \theta_m)$ est canoniquement ordonnée sur $k_r k_1$. C'est à dire*

$$\forall i \qquad o(\theta_i/k_1k_r(\theta_1, \theta_2, \ldots, \theta_{i-1})) = o(K/k_1k_r(\theta_1, \theta_2, \ldots, \theta_{i-1})) \quad (= o_i(K/k_1k_r))$$

Preuve : Supposons l'existance d'une r-base canoniquement ordonnée $(\theta_1, \theta_2, \ldots, \theta_m)$ vérifiant 1. et vérifiant 2. jusqu'à $i = s-1$. Il existe $j \geq s$ tel que

$$o(\theta_j/k_1k_r(\theta_1, \theta_2, \ldots, \theta_{s-1})) = o(K/k_1k_r(\theta_1, \theta_2, \ldots, \theta_{s-1}))$$

Si on ne peut prendre $j = s$, c'est à dire si

$$o(\theta_j/k_1k_r(\theta_1, \theta_2, \ldots, \theta_{s-1})) > o(\theta_s/k_1k_r(\theta_1, \theta_2, \ldots, \theta_{s-1})),$$

posons $\theta'_s = \theta_s + \theta_j$. Alors

$$o(\theta'_s/k_1k_r(\theta_1, \theta_2, \ldots, \theta_{s-1})) = o(K/k_1k_r(\theta_1, \theta_2, \ldots, \theta_{s-1}))$$

$$o(\theta'_s/k_r(\theta_1, \theta_2, \ldots, \theta_{s-1})) = o(K/k_r(\theta_1, \theta_2, \ldots, \theta_{s-1}))$$

$$o(\theta'_s/k(\theta_1, \theta_2, \ldots, \theta_{s-1})) = o(K/k(\theta_1, \theta_2, \ldots, \theta_{s-1}))$$

et en comparant les degrés

$$k(\theta'_s, \theta_j) = k(\theta'_s) \otimes_k k(\theta_j).$$

Donc $(\theta_1, \theta_2, \ldots, \theta'_s, \theta_{s+1}, \ldots \theta_{m-1})$ vérifie 1. et 2. jusqu'à $i = s$ ■

Proposition 15.4 *Soit K/k une extension purement inséparable. Soit k_r la cloture relativement parfaite de k dans K. Soit K_1/k la cloture modulaire de K/k. Supposons K/k_r finie. Alors sont équivalents :*

1. *K_1/K finie.*
2. *k_r/k modulaire.*

Et dans ce cas on a : $o(K_1/k_r) = o(K/k_r)$

Preuve : Si K_1/K finie, alors k_r est aussi la cloture relativement parfaite de k dans K_1 (proposition 5.2). Donc $k_r = \bigcap_n k(K_1^{p^n})$ modulaire sur k.

Si k_r/k modulaire. Posons $e = o(K/k_r)$. On a $K^{p^e} \subset k_r$, donc $K \subset k_r^{p^{-e}}$. D'autre part k_r/k est relativement parfaite. Donc $k_r = k_r^p(k)$. Donc il existe $B \subset k$ p-base de k_r. On a alors $k_r = k_r^{p^e}(B)$, soit $k_r^{p^{-e}} = k_r(B^{p^{-e}})$. Comme K/k_r finie et $K \subset k_r^{p^{-e}}$, il existe $B_1 \subset B$, B_1 finie, telle que $K \subset k_r(B_1^{p^{-e}})$. Comme B_1 est aussi p-libre sur k, on a $[k_r(B_1^{p^{-e}}), k_r] = [k(B_1^{p^{-e}}), k](= p^{e|B_1|})$. Donc $k(B_1^{p^{-e}})$ et k_r sont k-linéairement disjoints. Donc

$$k_r(B_1^{p^{-e}}) = k_r \otimes \bigotimes_{x \in B_1} k(x)$$

Soit $k_r(B_1^{p^{-e}})$ modulaire sur k. Donc $K_1 \subset k_r(B_1^{p^{-e}})$. Donc K_1/K finie.

On a $e = o(K/k_r) \leq o(K_1/k_r) \leq o(k_r(B_1^{p^{-e}})/k_r) = e$ ■

Dans les questions de linéarité disjointe, on rencontre souvent la propriété suivante :

Lemme 4.4 *Soit $K_1, K_2, \ldots, K_m$ des sous-corps d'un même corps Ω. Soient L_i un sous corps de K_i $(i = 1, 2, \ldots, m)$, $\widetilde{L}_i = \prod_{j \neq i} L_j$, et $L = \prod L_i$. Si $K_1, K_2, \ldots, K_m$ sont k-linéairement disjoints, alors $\widetilde{L}_1 K_1, \widetilde{L}_2 K_2, \ldots, \widetilde{L}_m K_m$ sont kL-linéairement disjoints.*

La propriété est bien connue si $m = 2$, et se généralisent aisement par recurrence. ■

5 Finitude de la tour des clôtures modulaires

Soit K/k une extension purement inséparable. Soit K_1 la cloture modulaire de K/k. Soit k_1 un corps intermédiaire de K/k tel que K/k_1 est modulaire. Calculons de même K_2/k_2 à partir de K_1/k_1 et ainsi de suite. On a :

Théorème 6.5 *Soit k_r la cloture relativement parfaite de k dans K. Si $di(k)$ est fini ou si K/k_r finie et k_r/k modulaire, alors la suite K_i stationne sur K_{i_0} tel que K_{i_0}/k_{i_0} est modulaire.*

Remarque 1 La condition K/k_r finie et k_r/k modulaire est vérifiée si K/k est finie.

Remarque 2 Si $di(k)$ est fini, K/k_r est finie (Proposition 7.2). De plus les $di(K_i)$ sont finis. Comme K_i croit, par le théorème 3.2 $di(K_i)$ décroit, donc pour i assez grand $di(K_i) = di(K_{i+1})$, soit toujours d'après le théorème 3.2 K_{i+1}/K_i est finie, on est donc ramené à K_1/K finie, par la proposition 15.4 k_r/k est modulaire. Donc pour i assez grand on se ramène à K/k_r finie et k_r/k modulaire.

Remarque 3 Si K/k_r est finie et k_r/k modulaire. On a $rp(K/k_1) = k_1k_r$ (proposition 6.2). Comme K/k_1 est modulaire, k_1k_r/k_1 est modulaire (proposition 15.4). Et comme K_1/K est finie , $rp(K_1/k_1) = k_1k_r$ (proposition 5.2). On a donc aussi K_1/k_1k_r est finie et k_1k_r/k_1 modulaire. La propriété s'étent donc par recurrence à toute K_i/k_i. De plus $rp(K_i/k_i) = k_rk_i$.

Corollaire 4.5 *Si on prend toujours $k_1 = K$ ou toujours k_1 le plus petit corps intermédiaire de K/k tel que K/k_1 est modulaire, alors la suite K_i/k_i est stationnaire*

En effet, dans ce cas si $K_{i+1} = K_i$, alors K_i/k_i est modulaire, donc $k_{i+1} = k_i$ ■

Corollaire 5.5 *Si on prend pour k_1 n'importe quel corps intermédiaire de K/k tel que K/k_1 est modulaire, l'extension limite K_i est telle que K_i/L est modulaire pour tout corps intermédiaire L de K_i/k_i.*

Les extensions K/k telle que K/L est modulaire pour tout corps intermédiaire L de K/k ont été décrit explicitement dans le cas où K/k admet une r-base modulaire (cf. [12]). Le théorème 7.5 décrit explicitement de telle extensions sous les hypothèses plus générale ci dessus . Une déscription tout à fait générale se trouve dans [3].

Pour prouver le théorème 6.5, nous allons définir une mesure de modularité sur les extensions K_j/k_j. On pose

$$d(j) = inf\,\{s \in \mathbb{N} | o_s(K_j/k_r k_{j-1}) > o_s(K_j/k_r k_j)\}$$

Proposition 16.5 *Posons s=d(j). Alors $K_j/k_r k_j$ admet une r-base canoniquement ordonnée $(\theta_1, \theta_2, \dots, \theta_m)$ tel que*

$$k_r k_j(\theta_1, \dots, \theta_{s-1}) = k_r k_j \otimes_{k_j} k_j(\theta_1) \otimes_{k_j} \cdots \otimes_{k_j} k_j(\theta_{s-1})$$

En particulier $k_r k_j(\theta_1, \theta_2, \dots, \theta_{s-1})/k_j$ est modulaire.

Preuve : Par construction K_j/k_{j-1} est modulaire. Et on a k_j corps intérmèdiaire de K_j/k_{j-1} ($k_{j-1} \subset k_j \subset K_{j-1} \subset K_j$). Par la proposition 14.4, il existe une r-base canoniquement ordonnée $(\theta_1, \theta_2, \dots, \theta_m)$ de K_j/k_{j-1} vérifiant

$$(*) \qquad \begin{cases} K_j = k_r k_{j-1} \otimes_k k(\theta_1) \otimes_k \cdots \otimes_k k(\theta_m) \\ \forall i \qquad o(\theta_i/k_j k_r(\theta_1, \dots, \theta_{i-1})) = o(K_j/k_j k_r(\theta_1, \dots, \theta_{i-1})) \end{cases}$$

Par définition de $s = d(j)$ on a pour $i = 1, 2, \dots, s-1$

$$o(\theta_i/k_r k_{j-1}(\theta_1, \dots, \theta_{i-1})) = o(\theta_i/k_r k_j(\theta_1, \dots, \theta_{i-1}))$$

Or par $(*)$ et le lemme 4.4

$$o(\theta_i/k_r k_{j-1}(\theta_1, \dots, \theta_{i-1})) = o(\theta_i/k_{j-1}(\theta_1, \dots, \theta_{i-1}))$$

et

$$o(\theta_i/k_r k_j(\theta_1, \dots, \theta_{i-1})) \leq o(\theta_i/k_j(\theta_1, \dots, \theta_{i-1})).$$

Donc

$$o(\theta_i/k_{j-1}(\theta_1, \dots, \theta_{i-1})) \leq o(\theta_i/k_j(\theta_1, \dots, \theta_{i-1})).$$

Donc

$$o(\theta_i/k_{j-1}(\theta_1, \dots, \theta_{i-1})) = o(\theta_i/k_j(\theta_1, \dots, \theta_{i-1})).$$

Par suite

$$[k_r k_j(\theta_1, \dots, \theta_{s-1}), k_r k_j] = [k_j(\theta_1, \dots, \theta_{s-1}), k_j]$$

Soit

$$k_r k_j(\theta_1, \dots, \theta_{s-1}) = k_r k_j \otimes_{k_j} k_j(\theta_1, \dots, \theta_{s-1})$$

De même, par $(*)$ on a

$$o(\theta_i / k_r k_{j-1}(\theta_1, \dots, \theta_{i-1})) = o(\theta_i / k_{j-1}),$$

et

$$o(\theta_i / k_r k_j(\theta_1, \dots, \theta_{i-1})) \leq o(\theta_i / k_j).$$

Donc

$$o(\theta_i / k_{j-1}) = o(\theta_i / k_j).$$

Donc

$$o(\theta_i / k_j(\theta_1, \dots, \theta_{i-1})) = o(\theta_i / k_j).$$

Donc

$$k_j(\theta_1, \dots, \theta_{s-1}) = k_j(\theta_1) \otimes_{k_j} \cdots \otimes_{k_j} k_j(\theta_{s-1}).$$

Donc

$$k_r k_j(\theta_1, \dots, \theta_{s-1}) = k_r k_j \otimes_{k_j} k_j(\theta_1) \otimes_{k_j} \cdots \otimes_{k_j} k_j(\theta_{s-1}).$$

Par la remarque 3, $k_r k_j / k_j$ est modulaire. La proposition en resulte par le lemme 3.4. ■

Proposition 17.5 *Supposons $d(j) = \infty$, alors K_j / k_j est modulaire (et donc $K_j = K_{j+1} = \dots$).*

Preuve : On a $k_{j-1} k_r \subset k_j k_r \subset K_j$ et $K_j / k_{j-1} k_r$ finie. Donc si $d(j) = \infty$ cela signifie :

$$\forall i \qquad o_i(K_j / k_{j-1} k_r) = o_i(K_j / k_j k_r)$$

Par suite $k_{j-1} k_r = k_j k_r$. En particulier $k_j \subset k_{j-1} k_r$. Et on a K_j / k_{j-1} modulaire, donc par la Proposition 5.4, il existe une r-base canoniquement ordonnée $(\theta_1, \theta_2, \dots, \theta_m)$ de K_j / k_{j-1} vérifiant

$$K_j = k_r k_{j-1} \otimes_k k(\theta_1) \otimes_k \cdots \otimes_k k(\theta_m)$$

Comme $k_j \subset k_{j-1} k_r$, par le lemme 4.4

$$K_j = k_r k_{j-1} \otimes_{k_j} k_j(\theta_1) \otimes_{k_j} \cdots \otimes_{k_j} k_j(\theta_m)$$

Par la Remarque 3 et le lemme 3.4, K_j/k_j est modulaire. ■

Lemme 5.5 *Supposons que pour tout $n \geq j$, $d(n) \geq d$. Alors pour tout $n \geq j+1$, on a*

$$(o_d(K_n/k_r k_n) \leq)\ o_d(K_n/k_r k_{n-1}) \leq o_d(K_j/k_r k_j)\ (\leq o_d(K_j/k_r k_{j-1}))$$

Preuve : Comme $d(j) \geq d$, par la proposition 16.5, $K_j/k_r k_{j-1}$ admet une r-base canoniquement ordonnée $(\theta_1, \theta_2, \ldots, \theta_m)$ tel que

$$k_r k_j(\theta_1, \ldots, \theta_{d-1}) = k_r k_j \otimes_{k_j} k_j(\theta_1) \otimes_{k_j} \cdots \otimes_{k_j} k_j(\theta_{d-1})$$

Posons $e = o_d(K_j/k_r k_j)$. On a

$$K_j^{p^e} \subset k_r k_j(\theta_1^{p^e}, \ldots, \theta_{d-1}^{p^e}).$$

Donc

$$K_j \subset (k_r k_j(\theta_1^{p^e}, \ldots, \theta_{d-1}^{p^e}))^{p^{-e}} \qquad \text{qui est modulaire sur } k_j.$$

Par suite

$$K_{j+1} \subset (k_r k_j(\theta_1^{p^e}, \ldots, \theta_{d-1}^{p^e}))^{p^{-e}}.$$

Par suite

$$di(k_r k_j K^{p^e}/k_r k_j) < d.$$

Donc par le lemme 2.3

$$o_d(K_{j+1}/k_r k_j) \leq e (= o_d(K_j/k_r k_j)) \qquad ■$$

Corollaire 6.5 $\lim\limits_{n \longrightarrow \infty} d(n) = \infty$

Preuve : Par la Proposition 15.4 on a $d(n) \geq 2$, pour tout entier $n \geq 1$. Supposons que pour tout $n \geq j$, $d(n) \geq d$. Par le Lemme 5.5, la suite d'entiers $o_d(K_n/k_r k_n)$ est décroissante pour $n \geq j+1$. Donc stationne pour n assez grand. Toujours par le lemme 5.5, on aura

$$o_d(K_n/k_r k_n) \leq o_d(K_n/k_r k_{n-1}) \leq o_d(K_{n-1}/k_r k_{n-1}) = o_d(K_n/k_r k_n).$$

Comme déjà $d(n) \geq d$, il en résulte que $d(n) \geq d+1$ ■

Preuve du théorème 6.5 : Si il existe un entier j tel que $d(j) = \infty$, le théorème s'ensuit par la Proposition 17.5. Sinonn, posons pour tout entier $n \geq 1$

$$\widetilde{d}(n) = inf\,\{d(j) | j \geq n\}\,.$$

La suite $(\widetilde{d}(n))$ est une suite d'entiers croissante et tendant vers ∞. Par suite elle admet une sous suite $((\widetilde{d}(i_k)))$ strictement croissante. On a

$$\widetilde{d}(i_k) = d(s) \qquad s \in [i_k, i_{k+1}[.$$

Posons pour simplifier $d_k = \widetilde{d}(i_k)$. Montrons que la suite d'entiers $(o_{d_k}(K_{i_k}/k_r k_{i_k-1}))$ est strictement décroissante, ce qui serait absurde. On a

$$\begin{array}{rcll}
o_{d_{k+1}}(K_{i_{k+1}}/k_r k_{i_{k+1}-1}) & \leq & o_{d_k}(K_{i_{k+1}}/k_r k_{i_{k+1}-1}) & \text{car } d_k < d_{k+1} \\
& \leq & o_{d_k}(K_s/k_r k_s) & \text{par le Lemme 5.5 car } i_{k+1} \geq s+1 \\
& < & o_{d_k}(K_s/k_r k_{s-1}) & \text{car } d_k = d(s) \\
& \leq & o_{d_k}(K_{i_k}/k_r k_{i_k-1}) & \text{par le Lemme 5.5.} \quad \blacksquare
\end{array}$$

Nous allons maintenant décrire les extensions K/k vérifiant K/L modulaire pour tout corps intermédiaire de K/k. Une telle déscription existe déjà, dans le cas où K/k admet une r-base modulaire.

Proposition 18.5 *Soit K/k une extension purement inséparable. Il est équivalent de dire:*

1. *L'ensemble des corps intermédiaires de K/k est totalement ordonné pour l'inclusion.*
2. *K est réunion croissante d'extensions simples.*
3. *Toute sous-extension propre de K/k est simple.*
4. *Toute sous-extension finie de K/k est simple.*

Preuve: Montrons (1) $\Longrightarrow$ (2). Soit (1) et $E = \{k(\theta) | \theta \in K\}$. Si E est fini, par (1), $K = \bigcup k(\theta) = k(\widehat{\theta})$ avec $k(\widehat{\theta})$ le plus grand élément de E. Si E est infini, on peut construire une suite strictement croissante $k(\theta_1) \subset k(\theta_2) \subset \dots$. Soit $x \in K$; il existe i tel que $[k(\theta_i), k] > [k(x), k]$; on ne peut donc avoir $k(\theta_i) \subset k(x)$; donc $k(x) \subset k(\theta_i)$; donc $K = \bigcup k(\theta_i)$.

(2) $\Longrightarrow$ (3) car, si (2) soit L un corps intermédiaire propre de K/k. Ecrivons que $K = \bigcup_n k(a_n)$. Si L/k est fini, il existe n tel $L \subset k(a_n)$. Posons $[L, k] =$

p^t et $[k(a_n),k] = p^m$. Donc $[k(a_n),L] = p^{m-t}$. Donc $k(a_n^{p^{m-t}}) \subset L$. Or $[k(a_n^{p^{m-t}}),k] = p^t = [L,k]$. Donc $L = k(a_n^{p^{m-t}})$ simple. Si L/k est infini, comme $L \neq K$, il existe n tel que $a_n \notin L$. Soit $x \in L$. Comme ci-dessus $k(x,a_n)$ est simple. Clairement $o(k(x,a_n)/k) = max(o(x/k), o(a_n/k))$. Donc il existe $a \in \{x, a_n\}$ tel que $k(x,a_n) = k(a)$. Comme $a_n \notin k(x)(\subset L)$, on a $a = a_n$. Donc $x \in k(a_n)$. Soit $L \subset k(a_n)$. Donc L/k est finie, contradiction.

(3) $\Longrightarrow$ (4) immédiat.

Montrons (4) $\Longrightarrow$ (1). Soit (4), soient L_1, L_2 des corps intermédiaires de K/k . Si $L_1 \not\subset L_2$, soit $x \in L_1 \setminus L_2$; soit $y \in L_2$, on a $k(x,y)/k$ est fini, donc simple; donc $k(x) \subset k(y)$ ou $k(y) \subset k(x)$; or $k(x) \not\subset k(y) \subset L_2$; donc $k(y) \subset k(x)$; par suite, $L_2 \subset k(x) \subset L_1$. ■

Définition 3.5 *Une extension K/k purement inséparable est dite q-simple (lire quasi simple) si elle vérifie les propriétés équivalentes de la proposition ci-dessus.*

Les extensions de la forme $k(x^{p^{-\infty}})$ sont q-simples. Ils existent des extensions q-simples qui ne sont pas de cette forme (cf. [5]).

Théorème 7.5 *Soit K/k une extension purement inséparable. Pour que K soit modulaire sur tout corps intermédiaire de K/k il faut et il suffit que $di(k) \leq 2$ ou K est parfait ou que $K = S \otimes_k P$ avec S q-simple et $P^p \subset k$.*

Nous donnons ici une preuve sous les hypothèses du Théorème 6.5. Une preuve dans le cas le plus général est en cours d'étude et apparaitra dans [3].

Preuve : La condition est suffisante car si $di(k) \leq 2$ toute extension purement inséparable de k est modulaire (cf [6] Corollaire 3 page 381). Si $K = S \otimes_k P$ avec S q-simple et $P^p \subset k.$, soit L un corps intermédiaire de K/k. on a $K = L(S)(P)$. Comme P est un r-générateur de $K/L(S)$ et $P^p \subset L(S)$, il existe $P_1 \subset P$ avec P_1 r-base de $K/L(S)$. Comme P_1 est r-libre sur k et $P_1^p \subset k$, P_1 est aussi une r-base de $k(P_1)/k$. Donc $L(S)$ et $k(P_1)$ sont k-linéairement disjoints. Donc $K = L(S) \otimes_k k(P_1)$. Donc par le lemme 4.4, $K = L(S) \otimes_L L(P_1)$ Comme $L(S)/L$ est q-simple, elle est modulaire. Et comme $L(P_1)/L$ est d'exposant 1, elle est modulaire. Par suite, en vue du Lemme 3.4, K/L est modulaire.

Inversement si K est modulaire sur tout corps intermédiaire de K/k. Supposons $di(k) > 2$.

1. Cas : K/k relativement parfaite

   Posons $k_n = k^{p^{-n}} \cap K$. Comme K/k est modulaire, k_n/k est modulaire et d'exposant fini. Donc k_n/k admet une r-base modulaire B. Montrons que au plus un élements de B a un exposant ≥ 2. Il suffit de le montrer pour $n = 2$. Car si c'est le cas, posons pour $x \in B$, $e_x = o(x/k) - 2$ si $o(x/k) \geq 2$, et $e_x = 0$ sinon. Comme $k(x^{p^{e_x}})_{x\in B} \subset k_2$, on a $k(x^{p^{e_x+1}})_{x\in B} \subset kk_2^p$ qui alors simple sur k, donc $k(x^{p^{e_x+1}})_{x\in B}/k$ est simple.

   Désormais on suppose $n = 2$. Supposons que deux élements θ_1 et θ_2 de B vérifient $o(\theta_i/k) \geq 2$. Posons $C = B \setminus \{\theta_1, \theta_2\}$. Si on avait $k(C^p) \subset (k(C)(\theta_1, \theta_2))^p$, alors $k \subset K^p$, donc $k(K^p) = K^p$. Or K/k est relativement parfaite, donc $k(K^p) = K$. Donc $K = K^p$ parfait. Donc si K est non parfait; il existe $x \in k(C^p) \setminus (k(C)(\theta_1, \theta_2))^p$. Il en résulte que $(\theta_1^{p^2}, \theta_2^{p^2}, x)$ est p-libre sur $k(C)$. Posons $\xi = \theta_2^p - x\theta_1^p$. On a $(\theta_1^{p^2}, \xi, x)$ p-libre sur $k(C)(\xi)$. Car si $\theta_1^{p^2} \in (k(C)(\xi))^p$, alors $\theta_1^{p^2} \in (k(C))^p(\theta_2^{p^2} - x^p\theta_1^{p^2}, x)$: donc $\theta_1^{p^2} \in (k(C))^p(\theta_2^{p^2}, x)$. Et $x \notin (k(C)(\xi))^p(\theta_1^{p^2})$ (car sinon $x \in k(C)^p(\theta_1^{p^2}, \theta_2^{p^2})$) et $\xi \notin (k(C)(\xi))^p(\theta_1^{p^2}, x)$ (car sinon $\xi \in (k(C))^p(\theta_1^{p^2}, x)$, donc $\theta_2^p \in k(C)^p(\theta_1^p, x)$), donc $\theta_2^{p^2} \in k(C)^p(\theta_1^{p^2}, x)$). Posons $L = k(\xi, x)$. D'une part on a k_2/L est modulaire, car $L \subset k_1 \subset k^{p^{-1}}$ et $(k^{p^{-1}})^p \subset L$ donc $k^{p^{-1}}/L$ est modulaire, donc $k^{p^{-2}}/L$ est modulaire, comme K/L est modulaire (toujours) $k_2 = k^{p^{-2}} \cap K$ est modulaire sur L. D'autre part $o(\theta_1/L) = 2$ car si $\theta_1^p \in L$ alors $\theta_1^{p^2} \in k^p(\xi, x) \subset k(C)^p(\xi, x)$. On a $\theta_2^p = \xi + x\theta_1^p$, par un argument classique de modularité, on en déduit que $\xi, x \in k_2^p$. (En effet $(1, \theta_1^p)$ est libre sur L, donc sur $L \cap k_2^p$, donc se prolonge en une base de $k_2^p/L \cap k_2^p$, qui est une base de k_2L/L, d'où par identification $\xi, x \in k_2^p \cap L$). On a alors $k(C)(\theta_1^p, x^{p^{-1}}, \xi^{p^{-1}}) \subset k_2 = k(C)(\theta_1, \theta_2)$. Par le théorème 1.2, cela conterdit $(\theta_1^{p^2}, \xi, x)$ p-libre sur $k(C)(\xi)$. Par suite pour tout n, l'extension kk_n^p/k est simple. Donc $K = k(K^p) = \bigcup kk_n^p$ est q-simple sur k.

2. Cas général

   Soit k_r la cloture relativement parfaite de k dans K. Par la proposition 15.4, k_r/L est modulaire pour tout corps intermédiaire de k_r/k. Donc k_r/k est simple (1$^{\text{er}}$ cas). Comme K/k_r est fini, par le Théorème 5.4

$$K = k_r \otimes_k k(\theta_1) \otimes_k \cdots \otimes_k k(\theta_m)$$

On veut montrer que $o(\theta_i/k) = 1$. La preuve est semblable à celle de [12]. On a seulement remplacé une extension simple par une extension q-simple. Supposons $e = o(\theta_1/k) \geq 2$. Notons $\alpha_2 = \theta_1^{p^{e-2}}$. Posons $k^{p^{-1}} \cap k_r = k(\alpha_1^p)$ et $C = \{\theta_j | j \neq 1\}$. Comme $di(k) = di(k(C)(\alpha_1, \alpha_2)) > 2$, on ne peut avoir $k(C) \subset (k(C)(\alpha_1, \alpha_2))^p \subset k(C)(\alpha_1, \alpha_2)$, donc il existe $x \in k(C) \backslash (k(C)(\alpha_1, \alpha_2))^p$, alors $(x, \alpha_1^{p^2}, \alpha_2^{p^2})$ est p-libre sur $k(C)$. Posons comme ci-dessus, $\xi = \alpha_2^p - x\alpha_1^p$. On a $(\alpha_1^{p^2}, \xi, x)$ p-libre sur $k(C)(\xi)$. Posons $L = k(\xi, x)$. Comme K/L est modulaire et $o(\alpha_1/L) = 2$, par un argument de modarité comme ci-dessus, on en déduit que $x^{p^{-1}}, \xi^{p^{-1}} \in K$. On a $k(C)(\alpha_1^p, x^{p^{-1}}, \xi^{p^{-1}}) \subset k_r k(C)(\theta_1) = \bigcup_n k(a_n)k(C)(\theta_1)$. Comme $k(C)(\alpha_1^p, x^{p^{-1}}, \xi^{p^{-1}})/k(C)$ finie, il exite a_i tel que $k(C)(\alpha_1^p, x^{p^{-1}}, \xi^{p^{-1}}) \subset k(C)(a_i, \theta_1)$. Par le Théorème 1.2, ceci conterdit $(\alpha_1^{p^2}, \xi, x)$ p-libre sur $k(C)(\xi)$. ■

References

[1] Beckert, M.T. and Maclane S., *The minimum number of generators for inseparable algebraic extensions,* Bull . Am. Math. Soc, 46(1940), 182-186.

[2] M. Chellali *Sur le degré d'imperfection d'un corps* A paraître.

[3] M. Chellali *Extension absolument modulaires* An. St. Univ. Ovidius Constanta, 13(1), (2005), 15-20.

[4] M. Chellali et E. Fliouet, *w_0-generated field extensions,* A paraître.

[5] M. Chellali et E. Fliouet, *Extensions purement inséparables d'exposant non borné,* Archivum Mathematicum, 40(2004), 129-159.

[6] M. Chellali et E. Fliouet, *Sur les extensions purement inséparables,* Arch.Math. 81 (2003), 369-382.

[7] J.K. Deveney, *An intermediate theory for a purely inseparable Galois theory,* Trans. Amer. Math. Soc. 198(1975), 287-295.

[8] J.K. Deveney, *w_0-generated field extensions,* Arch. Math., 47(1986), 410-412.

[9] J.K. Deveney et J.N Mordeson, *Higher derivation Galois theory of inseparable field extensions,* Handbook of Algebra, Vol 1(1996), 189-220.

[10] J.K Deveney et J.N. Mordeson, Invariance in inseparable Galois theory, Rocky Mountain J. Math., 83(1979), 655-662.

[11] L.A Kime, *Purely inseparable modular extensions of unbounded exponent,* Trans. Amer. Math. Soc, 176(1973), 335-349.

[12] J.N Mordeson, *On a Galois theory for inseparable field extensions.* Trans. Am. Math. Soc. 214 (1975), 337-347.

[13] J.N Mordeson et W.W. Shoultz, *p-bases of inseparable field extensions,* Arch. Math, 227(1973), 44-49.

[14] J.N Mordeson and B.Vinograde, *Structure of arbitrary purely inseparable extension fields*, SLNM 173 Springer, Berlin (1970).

[15] G.Pickert, *Inseparable Körperweiterungen,* Math. Z., 52 (1949), 81-135.

[16] M.E Sweedler, *Structure of inseparable extensions*, Ann. Math., 87(2) (1968), 401-410.

[17] W.C. Waterhause, *The structure of inseparable field extensions,* Trans. Am. Maths. Soc. 211(1975), 39-56.

Mustapha CHELLALI Département de mathématiques Faculté des sciences,
Université Mohammed 1, Oujda, Maroc
e-mail: chellali@sciences.univ-oujda.ac.ma

El Hassane FLIOUETDépartement de mathématiques Faculté des sciences,
Université Mohammed 1, Oujda, Maroc
e-mail: fliouet@yahoo.fr