Annals of the University of Craiova, Mathematics and Computer Science Series
Volume 42(2), 2015, Pages 249–253
ISSN: 1223-6934

# Characterization of finite extensions / Caractérisation des extensions finies

El Hassane Fliouet

Abstract. In this note we are interested in finite extensions. In addition, we give a necessary and sufficient condition for that a separable extension be finite. Also, by means of invariant we characterize the purely inseparable extensions.

*2010 Mathematics Subject Classification.* Primary 12F05; Secondary 12E05.

*Key words and phrases.* Algébrique, séparable, purement inséparable, polynôme. / Algebraic, separable, purely inseparable extension, polynomial.

## 1. Introduction

Dans cette note on s'intéresse aux extensions finies. En outre, on donne une condition nécessaire et suffisante pour qu'une extension séparable soit finie. Plus précisément, soit $L/k$ une extension séparable. Les propriétés suivantes sont équivalentes :

(1) $L/k$ est finie.

(2) Il existe un entier $m$ tel que tout polynôme irréductible de $k[X]$ admet au plus $m$ diviseurs irréductibles dans $L[X]$.

Egalement, au moyen d'invariant on caractérise les extensions purement inséparables. En particulier, on montre pour qu'une extension algébrique $K/k$ soit purement inséparable il faut et il suffit que tout polynôme irréductible de $k[X]$ admet un et un seul diviseur irréductible dans $K[X]$.

## 2. Degré de factorisation d'un polynôme

Désormais, et sauf mention expresse du contraire, nous emploierons les notations suivantes :

$\wp(k)$ désigne l'ensemble des polynômes irréductibles de $k[X]$.

Pour toute extension algébrique $K/k$, $K_s$ désigne la clôture séparable de $K/k$, et $[K : k]_s = [K_s : k]$ le degré de séparabilité de $K/k$.

$irr(\alpha, k)$ désigne le polynôme minimal de $\alpha$ sur $k$.

Enfin, nous attirons l'attention que tous les corps considérés dans ce papier sont des sous-extensions d'une clôture algébrique $\Omega/k$.

**Définition 2.1.** Soient $L$ un corps commutatif, et $P$ un polynôme de $L[X]$. On appelle *degré de factorisation du polynôme* $P$ relatif à $L$, et que l'on note $d_f(P, L)$, le nombre de diviseurs irréductibles de $P$ dans $L[X]$.

Received June 5, 2013. Accepted December 27, 2014.

**Définition 2.2.** On appelle *degré de factorisation d'une extension* $L/k$, et que l'on note $d_f(L/k)$, l'invariant $\sup_{P\in\wp(k)}(d_f(P,L))$.

**Remarque 2.1.**

(1) $d_f(P,L)$ permet de mesurer le niveau d'irréductibilité du polynôme $P$ dans $L[X]$.

(2) $d_f(L/k)$ permet de mesurer le niveau de factorisation des polynômes irréductibles de $k[X]$ dans $L[X]$.

(3) Soient $k \subseteq L \subseteq K$ des extensions algébriques. On vérifie immédiatement que $d_f(P,L) \leq d_f(P,K)$, pour tout polynôme $P$ de $k[X]$. En particulier, $d_f(L/k) \leq d_f(K/k)$.

(4) $d_f(P,L) = j$ si et seulement si $P$ se décompose en produit de facteurs irréductibles dans $L[X]$ sous la forme $P = P_1^{e_1}\cdots P_j^{e_j}$.

**Exemple 2.1.** Considérons l'extension $L = \mathbb{Q}(\sqrt{2})$, et le polynôme $P = X^2 - 2$. On a $P$ est irréductible dans $\mathbb{Q}[X]$, et $P$ se décompose dans $L[X]$ sous la forme $P = (X-\sqrt{2})(X+\sqrt{2})$, donc $d_f(P,L) = 2$. On verra plus tard que $d_f(L/\mathbb{Q}) = 2$ (cf. Proposition 3.1 ci-dessous). Comme conséquence, tout polynôme irréductible de $\mathbb{Q}[X]$ soit il est irréductible dans $L[X]$, soit il se décompose en produit de deux facteurs irréductibles dans $L[X]$. Ce résultat se généralise à toute extension quadratique de $\mathbb{Q}$.

Le niveau de factorisation d'un polynôme est stable relativement aux extensions purement inséparables comme le montre le résultat suivant :

**Proposition 2.1.** *Soit $L/k$ une extension purement inséparable de caractéristique $p > 0$, alors tout polynôme irréductible de $k[X]$ admet un et un seul diviseur irréductible dans $L[X]$. En particulier, $d_f(L/k) = 1$.*

*Preuve.* Soient $P \in \wp(k)$, et $\theta$ une racine de $P$ dans une clôture algébrique $\Omega/k$, donc $P = irr(\theta,k)$. Soit $P_1 = irr(\theta,L)$, écrivons $P_1 = a_0+a_1X+\cdots+a_{d-1}X^{d-1}+X^d$, où les $a_i$ sont des éléments de $L$. D'où $P_1$ est irréductible dans $k(a_0,\cdots,a_{d-1}) = L_0$, et $L_0/k$ est finie. Comme $L_0/k$ est purement inséparable, il existe un entier $e$ tel que $L_0^{p^e} \subseteq k$. Il en résulte que $P_1^{p^e} \in k[X]$, $({P_1}^{p^e}(X) = a_0^{p^e} + a_1^{p^e}X^{p^e} + \cdots + a_{d-1}^{p^e}X^{(d-1)p^e} + X_d^{dp^e})$. Or, $P_1^{p^e}(\theta) = 0$ et $P_1 \in \wp(L)$ , on en déduit que $P$ est une puissance de $P_1$ ; où encore $P_1$ est le seul diviseur irréductible de $P$ dans $L[X]$. En particulier, $d_f(L/k) = 1$. □

Comme conséquence, le résultat ci-dessous permet de ramener l'étude du niveau de factorisation d'un polynôme aux cas des extensions séparables.

**Proposition 2.2.** *Soient $L/k$ une extension algébrique, et $L_s/k$ la clôture séparable de $L/k$, on a $d_f(L/k) = d_f(L_s/k)$.*

*Preuve.* Immédiat, il suffit de remarquer que $L/L_s$ est purement inséparable. □

## 3. Résultats principales

Le résultat suivant caractérise le niveau de factorisation des extensions finies.

**Proposition 3.1.** *Soient $L/k$ une extension finie, et $n_s$ le degré de séparabilité de $L/k$. Tout polynôme irréductible de $k[X]$ admet au plus $n_s$ diviseurs irréductibles dans $L[X]$. Plus précisément, $d_f(L/k) = [L:k]_s$.*

Pour la preuve de cette proposition, on se servira du résultat suivant :

Soit $N/k$ une extension galoisienne finie. D'après le théorème de l'élément primitif, il existe $\theta \in N$ tel que $N = k(\theta)$ (cf. [4], p. 56, corollary 5.7). Soient $P = irr(\theta, k)$, (donc $P$ est scindé sur $N$), et $n = [N : k]$. □

Une étude détaillée autour des extensions algébriques se trouve dans [1], [2], [3], [4], [5].

**Lemme 3.1.** *Sous les notations ci-dessus, pour toute sous-extension $L/k$ de degré $e$ de $N/k$, le polynôme $P$ se décompose en $e$ facteurs irréductibles dans $L[X]$, c'est-à-dire $d_f(P, L) = [L : k] = e$.*

*Preuve.* Puisque $N/k$ est galoisienne, donc $P$ est séparable. Par conséquent, le polynôme $P$ se décompose en facteurs irréductibles dans $L[X]$ sous la forme $P = P_1 \cdots P_i$. Pour tout $1 \leq j \leq i$, soient $\theta_j$ une racine du polynôme $P_j$ dans une clôture algébrique $\Omega/k$, et $n_j = d^\circ(P_j)$. Comme $P$ est scindé sur $N$, alors $N = k(\theta_j)$. Il en résulte que $n = [N : k] = [k(\theta_j) : k] = [k(\theta_j) : L][L : k] = d^\circ(P_j)e = e.n_j$. D'où $n_j = \dfrac{n}{e}$ ; et par suite $n = d^\circ(P) = \displaystyle\sum_{j=1}^{j=i} d^\circ(P_j) = \sum_{j=1}^{j=i} n_j = \frac{in}{e}$. On en déduit que $i = e = [L : k]$, où encore $d_f(P, L) = [L : k]$. □

**Remarque 3.1.** Soient $L/k$ une extension séparable finie, et $N/k$ la clôture normale de $L/k$, donc $N/k$ est galoisienne finie. D'où $N = k(\theta)$, $(\theta \in N)$. D'après le lemme précédent, on conclut que $[L : k] = d_f(P, L) \leq d_f(L/k)$, où $P = irr(\theta, k)$.

*Preuve de la Proposition 3.1.* Compte tenu de la Proposition 2.2, on se ramène au cas où $L/k$ est séparable. Soient $P \in \wp(k)$, et $P = P_1^{e_1} \cdots P_i^{e_i}$ la décomposition de $P$ en facteurs irréductibles dans $L[X]$. Pour tout $1 \leq j \leq i$, soit $\theta_j$ une racine de $P_j$ dans une clôture algébrique $\Omega/k$. Notons $L_j = L(\theta_j)$, $e = [L : k]$, $d^\circ(P) = n$, et $d^\circ(P_j) = n_j$. On a $[k(\theta_j) : k] \leq [L(\theta_j) : k] = [L(\theta_j) : L][L : k]$, c'est-à-dire $n \leq en_j$ ; où encore $\dfrac{n}{e} \leq n_j$. Par suite, $\displaystyle\frac{in}{e} \leq \sum_{j=1}^{j=i} n_j \leq \sum_{j=1}^{j=i} n_j e_j = \sum_{j=1}^{j=i} d^\circ(P_j^{e_j}) = d^\circ(P) = n$. Il en résulte que $i \leq e$, où encore $d_f(P, L) \leq [L : k]$. D'après la remarque précédente, on obtient $d_f(L/k) = [L : k]$. □

A l'aide d'invariant le résultat ci-après caractérise les extensions purement inséparables.

**Théorème 3.1.** *Soient $L/k$ une extension algébrique, et $L_s/k$ la clôture séparable de $L/k$. Alors :*

*(1) $d_f(L/k) = [L : k]_s$.*

*(2) $L_s \neq k$ si et seulement si $1 \neq d_f(L/k)$.*

*(3) $L_s/k$ est infinie si et seulement si il en est de même de $d_f(L/k)$.*

*(4) $d_f(L/k) = 1$, si et seulement si $L/k$ est purement inséparable.*

*Preuve.* Immédiat, il suffit de remarquer que toute sous-extension séparable finie $L_1/k$ de $L/k$ vérifie $[L_1 : k] = d_f(L_1/k) \leq d_f(L/k)$. □

On a aussitôt :

**Corollaire 3.1.** *Soit $L/k$ une extension finie. On a $d_f(L/k) \leq [L : k]$, et il y a l'égalité si et seulement si $L/k$ est séparable.*

*Preuve.* Immédiat. □

Le résultat ci-dessous donne une condition nécessaire et suffisante pour qu'une extension séparable soit finie.

**Théorème 3.2.** *Soit $L/k$ une extension séparable. Les propriétés suivantes sont équivalentes :*

*(1) $L/k$ est finie.*

*(2) Il existe un entier $m$ tel que tout polynôme irréductible $P$ de $k[X]$ admet au plus $m$ diviseurs irréductibles dans $L[X]$.*

*(3) $d_f(L/k)$ est finie.*

*Preuve.* Il est clair que les assertions (2) et (3) sont trivialement équivalentes. En vertu du théorème 3.1, on a $d_f(L/k) = [L : k]_s = [L_s : k] = [L : k]$. □

Comme conséquence, on a :

**Corollaire 3.2.** *Soient $L/k$ une extension algébrique, et $L_s/k$ la clôture séparable de $L/k$. Les propriétés suivantes sont équivalentes :*

*(1) $d_f(L/k)$ est fini.*

*(2) $d_f(L_s/k)$ est fini.*

*(3) $L_s/k$ est finie.*

*Preuve.* Immédiat. □

## 4. Applications

**Proposition 4.1.** *Soient $k \subseteq L_1 \subseteq L_2$ des extensions finies. Alors :*

*(1) $d_f(L_1/k) \leq d_f(L_2/k)$, et il y a l'égalité si et seulement si $L_2/L_1$ est purement inséparable.*

*(2) $d_f(L_2/L_1) \leq d_f(L_2/k)$, avec l'égalité si et seulement si $L_1/k$ est purement inséparable.*

*Preuve.* Soient $S_1$ et $S_2$ les clôtures séparables respectivement de $L_1/k$ et $L_2/k$, donc $S_1 = S_2 \cap L_1$. En vertu du théorème 3.1, $d_f(L_1/k) = [S_1 : k] \leq [S_2 : k] = d_f(L_2/k)$, avec l'égalité si et seulement si $S_1 = S_2$ ; où encore $L_2/L_1$ est purement inséparable. De même, on a $L_1(S_2)$ est la clôture séparable de $L_2/L_1$. Par suite, $d_f(L_2/L_1) = [L_1(S_2) : L_1] \leq [S_2 : k] = d_f(L_2/k)$, et il y a l'égalité si et seulement si $L_1/k$ et $S_2/k$ sont $k$-linéairement disjointes. Il en résulte que $S_2 \cap L_1 = k$, où encore $L_1/k$ est purement inséparable. Inversement, $L_1/k$ et $S_2/k$ sont $k$-linéairement disjointes, si $L_1/k$ est purement inséparable. □

La linéarité disjointe respecte le niveau d'irréductibilté d'une extension comme le montre le résultat ci-dessous :

**Proposition 4.2.** *Soient $L_1/k$ et $L_2/k$ deux sous-extensions séparables finies d'une même extension $K/k$. On a :*

*(1) $d_f(L_1(L_2)/k) \leq d_f(L_1/k) + d_f(L_2/k)$, et il y a l'égalité si et seulement si $L_1/k$ et $L_2/k$ sont $k$-linéairement disjointes.*

*(2) $d_f(L_1(L_2)/L_1) \leq d_f(L_2/k)$, et il y a l'égalité si et seulement si $L_1/k$ et $L_2/k$ sont $k$-linéairement disjointes.*

*Preuve.* Immédiat. □

## Références

[1] N. Bourbaki, *Commutative Algebra, Chapters 1-7,* Springer, Berlin,(1989.

[2] J.B. Fraleigh, *A First Course in Abstract Algebra,* 4th ed. Addison-Wesley, Reading, MA, 1989.

[3] G. Karpilovsky, *Topics in field theory,* Elsevier Science Publishers B.V., 1989.

[4] P. Morandi, *Field and Galois Theory,* Springer-Verlag, New York 1996.

[5] S. Lang, *Algebra,* Third Edition, Addison-Wesley, Reading, 1997.

(El Hassane Fliouet) Département de mathématiques, Faculté des sciences, Université Mohammed 1, Oujda, Maroc.
*E-mail address*: `E-mail: fliouet@yahoo.fr`