

Devoir 4

Exercice 1 — Élément primitif.

- a) On suppose que $[K : k] \leq n$. Pour $x \in K$, on a $[k(x) : k] \leq [K : k(x)][k(x) : k] \leq n$ et donc $[k(x) : k] \leq n$. Réciproquement, K est une extension finie de k qui est de caractéristique nulle. C'est donc une extension séparable et par conséquent monogène. Ainsi il existe $x \in K$ tel que $k(x) = K$. Ainsi $[K : k] = [k(x) : k] \leq n$.
- b) L'hypothèse utilisée dans la question a est la séparabilité pour obtenir le fait que l'extension est monogène.
- c) Soit $x \in K$ tel que $[k(x) : k]$ soit maximal. Par hypothèse, un tel x existe et vérifie $[k(x) : k] \leq n$. Soit $y \in K$, on considère alors $k(x, y) \subset K$. Comme l'extension $k \rightarrow K$ est séparable, l'extension $k \rightarrow k(x, y)$ l'est aussi. Le théorème de l'élément primitif assure alors qu'il existe $z \in k(x, y)$ tel que $k(z) = k(x, y)$. En particulier, on a $[k(z) : k] = [k(x, y) : k(x)][k(x) : k] \geq [k(x) : k]$. Par maximalité, on en déduit que $[k(x) : k] = [k(z) : k]$. L'inclusion $k(x) \subset k(z)$ assure alors que $k(x) = k(z)$ et donc $y \in k(x)$. Finalement $K = k(x)$ et donc $[K : k] \leq n$.
- d) L'équivalence est évidemment fautive. En effet, l'hypothèse $[k(x) : k] < +\infty$ pour tout $x \in K$ est exactement synonyme du fait que K est une extension algébrique de k . Or il existe des extensions algébriques de degré infini. Par exemple l'extension

$$\overline{\mathbb{Q}} = \{x \in \mathbb{Q}, \quad x \text{ algébrique sur } \mathbb{Q}\} \subsetneq \mathbb{C}$$

est une extension algébrique de $\mathbb{Q}$ (puisque formées d'éléments algébriques) de degré infini. Le degré de cette extension est infini puisque par exemple $\sqrt[n]{2} \in \overline{\mathbb{Q}}$ est de degré n (puisque $X^n - 2$ est un polynôme irréductible sur $\mathbb{Q}$ d'après le critère d'Eisenstein).

- e) Montrons que $[K : L] = p^2$. Le polynôme $P(T) = T^p - X^p \in L[T]$ est irréductible sur L . En effet, dans $K[T]$, on a, grâce au morphisme de Frobenius $P(T) = (T - X)^p$. Ainsi si $P(T)$ était réductible sur L , on aurait $P = QR$ avec $Q, R \in L[T]$ et $\deg Q \geq 1$ et $\deg R \geq 1$. On aurait donc $Q = (T - X)^q$ et $R = (T - X)^r$ avec $q, r \geq 1$ et $q + r = p$. La formule du binôme montre alors que le coefficient qX de T^{q-1} de Q est dans L . Comme $1 \leq q < p$ est inversible dans L , on en déduit que $X \in L$. Montrons que ceci est absurde. On aurait alors

$$X = P(X^p, Y^p)/Q(X^p, Y^p) \quad \text{avec} \quad P, Q \in k[T_1, T_2] \quad \text{et} \quad Q(X^p, Y^p) \neq 0.$$

En réduisant au même dénominateur, on obtient $XQ(X^p, Y^p) = P(X^p, Y^p)$. En comparant les puissances de X qui interviennent, on obtient une contradiction. Ainsi P est irréductible et X est de degré p sur L . De même, Y est de degré p sur L .

En fait, pour montrer que $[L : K] = p^2$, il faut montrer que Y est de degré p sur $L(X) = k(X, Y^p)$ ce qui s'obtient presque de la même façon. Détaillons l'adaptation. Le polynôme $P(T) = T^p - Y^p \in L(X)[T]$ est irréductible sur $L(X)$. En effet, dans $K[T]$, on a, grâce au morphisme de Frobenius $P(T) = (T - Y)^p$. Ainsi si $P(T)$ était réductible sur $L(X)$, on aurait $P = QR$ avec $Q, R \in L(X)[T]$ et $\deg Q \geq 1$ et $\deg R \geq 1$. On aurait donc $Q = (T - Y)^q$ et $R = (T - Y)^r$ avec $q, r \geq 1$ et $q + r = p$. La formule du binôme montre alors que le coefficient qY de T^{q-1} de Q est dans L . Comme $1 \leq q < p$ est inversible dans $L(X)$, on en déduit que $Y \in L(X)$. Montrons que ceci est absurde. On aurait alors

$$Y = P(X, Y^p)/Q(X, Y^p) \quad \text{avec} \quad P, Q \in k[T_1, T_2] \quad \text{et} \quad Q(X^p, Y^p) \neq 0.$$

En réduisant au même dénominateur, on obtient $YQ(X, Y^p) = P(X, Y^p)$. En comparant les puissances de Y qui interviennent, on obtient une contradiction. Ainsi P est irréductible et Y est de degré p sur $L(X)$. Finalement $[K : L] = p^2$.

Soit $x \in K \setminus L$, on a $[L(x) : L] \mid [K : L] = p^2$ et $[L(x) : L] \neq 1$. Ainsi $[L(x) : L] \in \{p, p^2\}$. On a

$$x = P(X, Y)/Q(X, Y) \in k(X, Y) \quad \text{avec} \quad P, Q \in k[T_1, T_2] \quad \text{et} \quad Q \neq 0$$

On a alors, grâce au morphisme de Frobenius, $x^p \in L$. En effet, si

$$P = \sum_{(i,j) \in \mathbb{N}^2} a_{ij} X^i Y^j \quad \text{et} \quad Q = \sum_{(i,j) \in \mathbb{N}^2} b_{ij} X^i Y^j$$

$$\text{on a} \quad x^p = \frac{\sum_{(i,j) \in \mathbb{N}^2} a_{ij}^p (X^p)^i (Y^p)^j}{\sum_{(i,j) \in \mathbb{N}^2} b_{ij}^p (X^p)^i (Y^p)^j} \in L$$

Ainsi x est racine du polynôme $T^p - x^p \in L(x)$ et donc $[L(x) : L] \leq p$. Finalement $[L(x) : L] = p$. L'extension $L \subset K$ n'est donc pas monogène sinon il existerait $x \in K$ tel que $L(x) = K$ et donc $[L(x) : L] = p$.

Si l'extension $L \subset K$ était séparable, elle serait monogène ce qui n'est pas le cas. Pour montrer que l'extension $L \subset K$ n'est pas séparable, on peut aussi trouver un élément non séparable de K . Par exemple, X n'est pas séparable puisque son polynôme minimal est $T^p - X^p$ (on a vu que $P = T^p - X^p$ est irréductible sur L et annule X) dont la dérivée est nulle ou dont X est l'unique racine (puisque $P = (T - X)^p$).

f) L'extension $L \subset K$ vérifie $[L(x) : L] \leq p$ pour tout $x \in K$ mais $[K : L] = p^2 > p$.

Exercice 2 – Un exemple d'extension non monogène.

a) Voir la question **e** de l'exercice ??

b) Voir la question **e** de l'exercice ??

c) Soit $x \in K \setminus L$. On a vu que $T^p - x^p$ est un polynôme à coefficients dans L qui annule x . Il est donc divisible par le polynôme minimal de x . Or $[L(x) : L] = p$ d'après la question précédente donc le polynôme minimal de x sur L est de degré p . Ainsi le polynôme minimal de x sur L est $T^p - x^p$ qui n'est pas séparable puisque sa dérivée est nulle ou alors que $T^p - x^p = (T - x)^p$ n'est pas à racine simple. Ainsi les seuls éléments de K qui sont séparable sur L sont les éléments de L .

d) Montrons que K est le corps de décomposition sur L de $P = (T^p - X^p)(T^p - Y^p) \in L[T]$. Dans $K[T]$, on a $P = (T - X)^p(T - Y)^p$ est scindé et $K = L(X, Y)$ est engendré par les racines de P . Ainsi $L \subset K$ est une extension normale.

Soient $\sigma \in \text{Aut}_L(K)$ et $x \in K \setminus L$. L'élément $\sigma(x)$ est donc une racine dans K du polynôme minimal de x sur L . Or d'après la question **c**, le polynôme minimal de x sur L est $T^p - x^p$ qui se factorise dans $K[T]$ en $(T - x)^p$. Ainsi x est l'unique racine dans K (et même dans toute extension) du polynôme minimal de x sur L . Ainsi $\sigma(x) = x$ et donc $\sigma = \text{id}_K$.