141. Polynômes irréductibles, corps de rupture : éléments de solutions

1. a) Un tel L doit être de cardinal q^d puisqu'isomorphe à K^d comme K-ev. On sait (théorème au programme) qu'il existe un tel corps, unique à isomorphisme près. C'est bien alors une extension de K, puisqu'on sait qu'un corps fini K_2 est extension d'un corps fini K_1 si et seulement si le cardinal de K_2 est une puissance de celui de K_1 (ce qui résulte par exemple de ce que dans une clôture algébrique, le corps de cardinal p^k (où $k \in \mathbf{N}^*$) est l'ensemble des solutions de l'équation $x^{p^k} = x$).

b) On a clairement $K[\alpha] \subset L$. Réciproquement, comme α engendre le groupe fini L^*, tout élément de L^* s'écrit α^m avec $m \in \mathbf{N}$, ce qui montre que $L^* \subset K[\alpha]$, d'où le résultat puisque bien entendu $0 \in K[\alpha]$.

c) Soit P le polynôme minimal de α. Comme $L = K[\alpha]$, le corps L est un corps de rupture de α sur K. Comme $[L : K] = d$, le polynôme P est de degré d.

2. a) Soit p la caractéristique de K (et de L). On sait qu'on peut écrire $q = p^m$ avec $m \in \mathbf{N}$. Ainsi F est le m-ième itéré de $F_0 : x \mapsto x^p$; or F_0 est un morphisme de corps (le seul point non trivial est de voir que $(x+y)^p = x^p+y^p$, ce qui est vrai dans tout corps de caractéristique p car p divise le coefficient binomial C_p^k pour tout $k \in \{1, ..., p-1\}$). En particulier F_0 est injectif, et comme L est fini il est aussi bijectif, donc c'est bien un automorphisme de L. Par conséquent c'est aussi le cas de $F = F_0 \circ ... \circ F_0$. Enfin, pour tout $x \in K$, on a $x^q = x$ puisque K est un corps de cardinal q.

b) Supposons que $F^m(\alpha) = \alpha$ avec $0 < m < d$. Cela signifie que $\alpha^{q^m} = \alpha$, et on sait alors que α est dans un corps de cardinal q^m, qui est de degré m sur K. Ceci implique $[K[\alpha] : K] \leq m$, ce qui contredit le fait que $L = K[\alpha]$ est de degré d.

c) Soit P le polynôme minimal de α sur K. Comme F est un automorphisme de corps de L qui induit l'identité sur K, on observe que $\alpha, F(\alpha), F^2(\alpha), ..., F^{d-1}(\alpha)$ sont des racines de P, et elles sont deux à deux distinctes d'après b). Ainsi P est scindé sur L comme on voulait. Ainsi,

sur un corps fini, corps de rupture coïncide avec corps de décomposition, phénomène aussi vrai sur $\mathbf{R}$ mais pas sur $\mathbf{Q}$ par exemple.

d) Comme $16 = 4^2$, on a bien que le corps fini L est une extension de degré 2 de K. Comme L^* est cyclique de cardinal 15, il contient un élément α d'ordre 5. Alors, $\alpha^4 \neq \alpha$ (sinon α serait d'ordre divisant 3), ce qui montre que $\alpha \notin K$. En particulier le degré de $K[\alpha]$ sur K est ≥ 2, ce qui montre finalement (comme $K[\alpha] \subset L$) que $L = K[\alpha]$ par égalité des dimensions sur K. Ainsi on peut avoir $L = K[\alpha]$ sans que α soit un générateur de L^*.

3. a) a déjà été vu dans l'exercice précédent.

b) Ici P' n'est pas nul car P n'est pas constant et K est de caractéristique zéro. Ainsi, le degré de P' est $< \deg P$, ce qui implique que comme P est irréductible, P et P' sont premiers entre eux dans $K[X]$ ou $L[X]$ (rappelons que le pgcd ne dépend pas du corps de base). Ainsi P ne peut avoir une racine multiple dans L.

c) D'après ce qu'on a vu en b), le seul problème est quand $P' = 0$, ce qui signifie que P s'écrit

$$P = a_0 + a_1 X^p + ... + a_k X^{pk}.$$

D'après a), on peut écrire $a_i = b_i^p$ avec $b_i \in K$. Alors $P = (b_0 + b_1 X + ... + b_k X^k)^p$ ne peut pas être irréductible.

Par contre, sur $K = \mathbf{Z}/p\mathbf{Z}(T)$, le polynôme $P = X^p - T$ vérifie $P' = 0$ (donc il a une racine de multiplicité P sur son corps de décomposition), bien que P soit irréductible sur K (clair si $p = 2$, en général résulte du critère d'Eisenstein en regardant P comme à coefficients dans l'anneau factoriel $K[T]$).

4. a) Notons déjà que F n'est pas constant. Supposons que $F = GH$ avec G et H de degré au moins 1. Alors $\overline{F} = \overline{G}.\overline{H}$, et comme $\overline{F}$ est irréductible, on a par exemple $\overline{G}$ constant non nul, i.e. $G = a + pQ$ avec $a \in \mathbf{Z}$ et $Q \in \mathbf{Z}[X]$. Ceci implique que le coefficient dominant de F est divisible par p, ce qui contredit le fait que F est unitaire.

b) Non, prendre par exemple $F = X^2 + p$.

c) Non, prendre par exemple $F = pX^2 + X$.

5. Pour $d = 1$, c'est évident. Supposons le résultat vrai jusqu'à $d-1$. Soit F un facteur irréductible de P, il est de degré au plus d. Soit K_1 un corps de rupture de F sur K, alors P a au moins une racine a sur K_1, donc s'écrit $P = (X-a)Q$ avec $Q \in K_1[X]$. Comme L est le corps engendré sur K par les racines de P, c'est aussi le corps de décomposition de Q sur L. L'hypothèse

de récurrence donne $[L : K_1] \leq (d-1)!$, et comme $[K_1 : K] = \deg F \leq d$, on obtient

$$[L : K] \leq d(d-1)! = d!.$$

Sur $\mathbf{Q}$, le corps de décomposition de $X^3 - 2$ est $\mathbf{Q}(j, \sqrt[3]{2})$, qui est bien de degré 6 sur $\mathbf{Q}$.