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 $K[T]$; on peut aussi utiiliser l'argument général de la question d) ci-dessous).

d) Si K est parfait, la mêm méthode exactement que quand K est fini donne le résultat. Supposons K imparfait, soit $a \in K^*$ tel que a ne s'écrive pas $a = x^p$ avec $x \in K^*$. Soit $P \in K[X]$ défini par $P = X^p - a$. Comme $P' = 0$, toute racine de P dans un corps de décomposition est multiple (d'ordre p), il suffit donc de vérifier que P est irréductible sur K. Soit L un corps de décomposition de P sur K et soit $b \in L$ tel que $b^p = a$. Soit π le polynôme minimal de b sur K (qui est irréductible), il suffit de montrer que $\pi = P$. Comme $P(b) = 0$, on sait que π divise P. Mais comme $P = (X - b)^p$ dans $L[X]$, on a alors que π s'écrit $(X - b)^r$ dans $L[X]$ avec $1 \leq r \leq p$. En regardant le terme constant, on obtient $b^r = a \in K$. Mais si on avait $r < p$, r serait premier avec p et par Bezout on aurait $u, v \in \mathbf{Z}$ avec $ur + vp = 1$, ce qui impliquerait que

$$b = b^{ur+vp} = a^u.a^v$$

serait dans K, ce qui est absurde car a n'est pas une puissance p-ième. Finalement $\pi = P$ comme on voulait.

4. a) Posons $\alpha \bullet x = \sigma(\alpha).x$. Comme σ est un morphisme de corps, on vérifie alors immédiatement les quatre axiomes requis :

$1 \bullet x = x$ pour tout $x \in L$.

$\alpha \bullet (\beta \bullet x) = (\alpha\beta) \bullet x$ pour tous $\alpha, \beta \in K$ et tout $x \in L$.

$\alpha \bullet (x + y) = \alpha \bullet x + \alpha \bullet y$ pour tout $\alpha \in K$ et tous $x, y \in L$.

$(\alpha + \beta) \bullet x = \alpha \bullet x + \beta \bullet x$ pour tous $\alpha, \beta \in K$ et tout $x \in L$.

b) Soit $(e_1, ..., e_d)$ une base du K-ev L, montrons que c'est aussi une base de L'. Si $\lambda_1, ..., \lambda_d$ dans K vérifient

$$\sum_{i=1}^{d} \lambda_i \bullet e_i = 0,$$

alors

$$\sum_{i=1}^{d} \sigma(\lambda_i).e_i = 0$$

d'où $\sigma(\lambda_i) = 0$ pour tout i, puis $\lambda_i = 0$ puisque σ est injectif. Ainsi $(e_1, ..., e_d)$ est libre dans L'. Si maintenant $x \in L'$, on écrit $x = \sum_{i=1}^{d} \mu_i.e_i$ dans L avec $\mu_i \in K$, d'où $x = \sum_{i=1}^{d} \sigma^{-1}(\mu_i) \bullet e_i$ dans L', ce qui montre que la famille $(e_1, ..., e_d)$ est également génératrice dans L'.

c) Par hypothèse, le morphisme de corps σ défini par $\sigma(x) = x^p$ est un automorphisme de K. Soit L une extension finie de K, qu'on peut voir comme un K-ev, notons L' le K-ev défini comme en a). Alors l'application $u : x \mapsto x^p$ est un morphisme du K-ev L dans le K-ev L' : en effet $u(x+y) = u(x) + u(y)$ résulte de ce qu'on est en caractéristique p; si $\alpha \in K$ et $x \in L$, on a

$$u(\alpha.x) = \alpha^p x^p = \sigma(\alpha).u(x) = \alpha \bullet x.$$

Comme il est immédiat que $\ker u = 0$, u est injective et elle est donc bijective car $\dim L = \dim L'$ est finie. Ceci signifie exactement que $x \mapsto x^p$ est bijective de L dans L, et donc que L est parfait.

d) Mais oui ! Si F est une extension algébrique de K et si $x \in F$, alors $L := K[x]$ est une extension finie de K puisque x est algébrique sur K. Appliquant alors c) à L, on obtient qu'il existe $y \in L \subset F$ tel que $y^p = x$. Ainsi, F est parfait.