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) Si K est fini de caractéristique p, alors le morphisme de corps $x \mapsto x^p$ de K dans K, est injectif, donc bijectif; ainsi K est parfait. Par contre, dans $\mathbf{Z}/p\mathbf{Z}(T)$, l'élément T n'est pas une puissance p-ième (pour raison de degré).

b) Si P n'était pas irréductible dans $K[X]$, on pourrait écrire $X^p - a = QR^\alpha$ avec R irréductible unitaire ne divisant pas Q et $\alpha \geq 1$; posons alors $S = R^\alpha$, alors comme $X^p - a$ est de dérivée nulle, on aurait $QS' + Q'S = 0$ donc S divise $S' = \alpha R^{\alpha-1}R'$ puisqu'il est premier avec Q. Cela impose $S' = 0$, donc ou bien $R' = 0$, auquel cas R (qui n'est pas constant) est de degré un multiple non nul de p, ce qui implique $\alpha = 1$ et $Q = 1$, et dans ce cas $X^p - a$ est bien irréductible; ou bien $R' \neq 0$ d'où $\alpha = p$ (car α est multiple de p et $\leq p$ pour des raisons de degré) et $Q = 1$, mais ceci est exclu par le fait que a n'est pas une puissance p-ième dans K.

Maintenant, comme la dérivée de P est nulle, P n'a qu'une racine (de multiplicité p) dans un corps de décomposition.

c) D'après b), si K est imparfait, alors on sait que le polynôme $X^p - a$ (où a n'est pas une puissance p-ième) est irréductible. Dans l'extension finie $L = K[X]/(X^p - a)$, ce polynôme acquiert alors une racine multiple, dont le polynôme minimal sur K est $X^p - a$. Réciproquement, si K est parfait, on a vu dans la leçon que le polynôme minimal de tout x algébrique sur K (qui est irréductible) est à racines simples.

Si maintenant K est parfait et L est une extension finie de K, soit M une extension finie de L. Pour tout $x \in M$, le polynôme minimal π de x sur K n'a que des racines simples dans un corps de décomposition puisque K est parfait. Mais alors, le polynôme minimal π_L de x sur L a la même propriéte, car il divise π dans $L[X]$. D'après le critère de b), L est encore un corps parfait.

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.