Corrigé de l'entraînement écrit *Polynômes, extensions de corps*

D. Harari

Agrégation

1. a) Supposons x algébrique sur K. Alors il existe une famille finie $(a_0, ..., a_{k-1})$ d'éléments de K tellle que

$$x^k + a_{k-1}x^{k-1} + ... + a_0 = 0.$$

On vérifie alors immédiatement par récurrence sur n que pour tout $n \geq k$, x^n est dans le K-espace vectoriel engendré par $1, x, ...x^{k-1}$, ce qui prouve que le K-espace vectoriel $K[x]$ engendré par tous les x^n est de dimension au plus k. En sens inverse, si $K[x]$ est de dimension finie, alors la famille infinie des x^n est liée, ce qui donne immédiatement qu'il existe un polynôme non nul P (qu'on peut supposer unitaire, quitte à diviser par le coefficient dominant) P de $K[X]$ tel que $P(x) = 0$.

b) Il est immédiat que $K[x]$ est un sous-anneau de L. Si $x \neq 0$ est algébrique, alors son polynôme minimal π est irréductible et $K[x]$ est isomorphe à $K[X]/(\pi)$, donc est un corps puisque $K[X]$ est principal (autre formulation : $K[x]$ est une algèbre intègre de dimension finie sur K, donc c'est un corps). En sens inverse, si x n'est pas algébrique, alors on voit tout de suite que $P \mapsto P(x)$ est un isomorphisme de K-algèbres de $K[X]$ sur $K[x]$, donc $K[x]$ ne peut pas être un corps.

c) Il est clair que 0 et 1 sont dans E. Si x est dans E, le K-ev engendré par les x^n est clairement le même que celui engendré par les $(-x)^n$, donc $(-x)$ est dans E d'après a). De même, si $x \neq 0$ est dans E, il vérifie une équation du type

$$x^k + a_{k-1}x^{k-1} + ... + a_0 = 0,$$

donc $1 + a_{k-1}x + ... + a_0/x^k = 0$, ce qui montre que $1/x$ est encore dans E, vu qu'il annule un polynôme non nul à coefficients dans K. Il reste à montrer que si $x, y \in E$, alors $(x + y)$ et xy sont dans E. Or, le K-espace vectoriel $K[x + y]$ engendré par $x + y$ est un sous-ev du K-espace vectoriel

$K[x,y] = (K[x])[y]$ (constitué des polynômes en y à coefficients dans $K[x]$). On a vu en b) que $K[x]$ est un corps ; comme y est algébrique sur K, il l'est a fortiori sur $K[x]$, donc $K[x,y]$ est de dimension finie sur $K[x]$. Comme $K[x]$ est de dimension finie sur K puisque x est algébrique sur K, le théorème de la base télescopique donne que $K[x,y]$ est de dimension finie sur K, donc aussi $K[x+y]$ qui en est un sous-espace. De même pour $K[xy]$. On conclut avec a)

d) On applique a). On a que $K(a_0)$ est un K-ev de dimension finie car a_0 est algébrique sur K. Chaque a_i est algébrique sur K, donc a fortiori sur $K(a_0, ..., a_{i-1})$. Par récurrence sur i, on obtient alors (en utilisant toujours la base télescopique) que $K(a_0, ..., a_i)$ est de dimension finie sur K. En particulier $K(a_0, a_1, ..., a_{n-1})$ est de dimension finie sur K.

e) Soit $P = X^n + a_{n-1}X^{n-1} + ... + a_0$ un polynôme unitaire à coefficients dans E. Soit x une racine de P, alors x est algébrique sur $F := K(a_0, ..., a_{n-1})$ par définition, donc $F(x)$ est de dimension finie sur F, et finalement aussi sur K puisque F est de dimension finie sur K d'après d). Comme $K(x)$ est un sous-espace de $F(x)$, il est également de dimension finie sur K, ce qui signifie que x est algébrique sur K d'après a), i.e. $x \in E$ comme on voulait.

f) Pour tout $n \in \mathbf{N}$, l'ensemble $\mathbf{Q}_n[X]$ des polynômes de degré au plus n est dénombrable, car en bijection avec $\mathbf{Q}^{n+1}$. L'ensemble Z_n des éléments de E qui annulent un polynôme non nul de $\mathbf{Q}_n[X]$ est donc dénombrable, puisque chaque polynôme non nul de $\mathbf{Q}_n[X]$ n'a qu'un nombre fini de racines. On en déduit que E, qui est réunion dénombrable des Z_n pour $n \in \mathbf{N}$, est dénombrable.

2. a) Une telle extension est un corps de cardinal q^d, donc est unique à isomorphisme près. Réciproquement, il existe un corps L de cardinal q^d (puisque q^d est une puissance de p), qui est bien une extension de K vu que K et L sont les corps de décomposition respectifs sur $\mathbf{F}_p$ des polynômes $X^q - X$ et $X_X^{q^d}$ et qu'une racine de la première équation est clairement racine de la deuxième.

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 sur K (il existe car L est fini, donc de dimension finie sur K). 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, et on sait qu'il est irréductible.

d) 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.

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

Comme F est un automorphisme de corps de L qui induit l'identité sur K, on observe que $a, F(a), F^2(a), ..., F^{d-1}(a)$ sont des racines de R, et elles sont deux à deux distinctes d'après ce qu'on vient de voir. Ainsi R est scindé sur L, et son corps de rupture L est bien son corps de décomposition.

f) Comme $16 = 4^2$, on a bien que le corps fini $\mathbf{F}_{16}$ est une extension de degré 2 de $\mathbf{F}_4$. Comme $\mathbf{F}_{16}^*$ est cyclique de cardinal 15, il contient un élément β d'ordre 5. On observe que $\beta^4 \neq \beta$ (sinon β serait d'ordre divisant 3), ce qui montre que $\beta \notin \mathbf{F}_4$. En particulier le degré de $\mathbf{F}_4[\beta]$ sur $\mathbf{F}_4$ est ≥ 2, ce qui montre finalement (comme $\mathbf{F}_4[\beta] \subset \mathbf{F}_{16}$) que $\mathbf{F}_{16} = K[\beta]$ par égalité des dimensions sur $\mathbf{F}_4$.

3. a) Le polynôme 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, par exemple via l'algorithme d'Euclide). Ainsi P ne peut avoir une racine multiple dans L.

b) Un corps fini est parfait car le morphisme de corps $x \mapsto x^p$ est injectif, donc bijectif (application d'un ensemble fini dans lui-même). Le corps $\mathbf{F}_p(T)$ est imparfait, car T n'est pas une puissance p-ième dans ce corps (pour des raisons de degré).

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

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

Si K est parfait, 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.

Si par contre K est imparfait et $a \in K$ n'est pas une puissance p-ième, alors le polynôme $P = X^p - a$ 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) 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.