Corps de décomposition, élément primitif... : correction

Exercice 1.

1. Si $n = \operatorname{car} \mathrm{A}$, on a

$$\begin{aligned} n \cdot 1_{\mathrm{A}'} &= 1_{\mathrm{A}'} + \cdots + 1_{\mathrm{A}'} \\ &= f(1_{\mathrm{A}}) + \cdots + f(1_{\mathrm{A}}) \\ &= f(1_{\mathrm{A}} + \cdots + 1_{\mathrm{A}}) \\ &= f(n \cdot 1_{\mathrm{A}}) = f(0_{\mathrm{A}}) = 0_{\mathrm{A}'} \end{aligned}$$

   donc $n \in \ker \iota = (\operatorname{car} \mathrm{A}')$ et $\operatorname{car} \mathrm{A}'$ divise $n = \operatorname{car} \mathrm{A}$.

2. Si la caractéristique de A n'est pas nulle, le théorème de factorisation fournit un morphisme injectif

$$\begin{aligned} \overline{\iota} : \mathbf{Z}/(\operatorname{car} \mathrm{A}) &\to \mathrm{A} \\ [k] &\mapsto k \cdot 1_{\mathrm{A}}. \end{aligned}$$

   Si A est intègre, il doit en être de même de tous ses sous-anneaux, et en particulier de $\mathbf{Z}/(\operatorname{car} \mathrm{A}) \simeq \mathbf{Z}/(\operatorname{car} \mathrm{A})\mathbf{Z}$. Or, on sait que $\mathbf{Z}/n\mathbf{Z}$ est intègre si et seulement si n est un nombre premier (et que dans ce cas $\mathbf{Z}/n\mathbf{Z} \simeq \mathbf{F}_n$ est un corps).

3. En général, dans un anneau commutatif, on a la formule du binôme de Newton

$$(x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{n-k}.$$

   Comme le coefficient binomial $\binom{p}{k}$ est divisible par p dès que p est premier et $1 \leq k \leq p-1$, l'élement

$$\binom{p}{k} = \binom{p}{k} \cdot 1_{\mathrm{A}}$$

   est nul dans tout anneau de caractéristique p. Dans un tel anneau, la formule du binôme de Newton donne donc simplement

$$(x+y)^p = x^p + y^p.$$

   Les autres axiomes de morphismes d'anneaux étant évidents pour $x \mapsto x^p$, celui-ci est bien un morphisme, le *morphisme de Frobenius*.

Exercice 2.

1. Une clôture algébrique d'un corps M est simplement un surcorps M′ de M algébriquement clos tel que l'extension M′/M soit algébrique.

   Dans les hypothèses de l'énoncé, puisque K^a/K est une extension algébrique, on a déjà que K^a est un corps algébriquement clos. Par ailleurs, l'extension K^a/K étant algébrique, les éléments de K^a sont algébriques sur K et *a fortiori* sur L. Le corps K^a est donc bien une clôture algébrique de K.

2. Par définition, tous les éléments de $\overline{\mathbf{Q}}$ sont algébriques sur $\mathbf{Q}$. Il reste à voir pourquoi $\overline{\mathbf{Q}}$ est algébriquement clos. (Après tout, on a « rajouté » les solutions d'équations à coefficients rationnels, mais pourquoi les équations à coefficients algébriques ne rajoutent-elles pas de nouvelles racines ?)

   On va en fait démontrer un résultat plus général : *si* M/L/K *est une tour d'extensions, l'extension* M/K *est algébrique si et seulement si* M/L *et* L/K *le sont.*

   On dit parfois que les extensions algébriques forment une classe distinguée d'extensions. Notons que l'on connait un autre exemple de telle classe : les extensions finies (dans un sens, c'est particulièrement évident, et l'autre provient du théorème de la base télescopique). On va d'ailleurs s'appuyer sur ce résultat et sur les affinités qui existent entre extensions finies et algébriques.

   Déjà, si M/K est algébrique, tous les éléments de M sont algébriques sur K et donc sur L. Cela donne directement que M/L et L/K sont algébriques.

   Réciproquement, supposons que M/L et L/K soient des extensions algébriques. Soit $x \in \mathrm{M}$. Cet élément est annulé par un polynôme $\mathrm{P} = \mathrm{X}^d + a_{d-1}\mathrm{X}^{d-1} + \cdots + a_0 \in \mathrm{L}[\mathrm{X}]$. Par hypothèse, tous les éléments $a_i \in \mathrm{L}$ sont algébriques sur K. Par récurrence, le sous-anneau $\mathrm{K}' = \mathrm{K}[a_1, \ldots, a_{d-1}]$ est donc une extension finie de K. L'élément x étant algébrique sur K′, les extensions $\mathrm{K}'[x]/\mathrm{K}'$ et K′/K sont toutes deux finies, ce qui entraîne que $\mathrm{K}'[x]/\mathrm{K}$ est encore une extension finie, et donc que $\mathrm{K}[x] \subset \mathrm{K}'[x]$ soit lui aussi de K-dimension finie. Bref, x est algébrique sur K et l'extension M/K est algébrique.

3. On a vu en cours que si $\sigma : \mathrm{K} \to \mathrm{M}$ est un plongement dans un corps algébriquement clos, le nombre d'extensions de σ à une extension algébrique $\mathrm{L} = \mathbf{Q}(\alpha)$ de K est égal au nombre de racines distinctes du polynôme minimal P_α dans M.

   Appliquons ce résultat à $\mathrm{K} = \mathbf{Q}$, $\mathrm{L} = \mathrm{K}(\alpha)$, $\mathrm{M} = \mathbf{C}$ et à l'inclusion $\sigma : \mathbf{Q} \to \mathbf{C}$.

   Déjà, tout plongement de $\mathbf{Q}(\alpha)$ dans $\mathbf{C}$ doit envoyer 1 sur 1 et donc coïncider avec σ sur $\mathbf{Q}$. Le nombre de plongements de $\mathbf{Q}(\alpha)$ dans $\mathbf{C}$ est donc bien égal au nombre de racines de P_α dans $\mathbf{C}$. Mais comme nous sommes en caractéristique nulle et que P_α est irréductible, ce nombre n'est autre que le degré $\deg \mathrm{P} = [\mathbf{Q}(\alpha) : \mathbf{Q}]$.

   Notons que ces morphismes sont en fait aisément constructibles : si β est une racine de P_α, le morphisme d'évaluation

$$\begin{aligned} \mathrm{év}_\beta : \mathbf{Q}[\mathrm{X}] &\to \mathbf{C} \\ \mathrm{P} &\mapsto \mathrm{P}(\beta) \end{aligned}$$

   vérifie évidemment $\mathrm{év}_\beta \mathrm{P}_\alpha = \mathrm{P}_\alpha(\beta) = 0$, donc passe au quotient en un morphisme $\mathbf{Q}[\mathrm{X}]/(\mathrm{P}_\alpha) \to \mathbf{C}$, dont l'anneau de départ est bien isomorphe au corps $\mathbf{Q}(\alpha)$.

4. Si $d \in \{2, 4, 8\}$, le polynôme $\mathrm{X}^d - 2$ est irréductible sur $\mathbf{Z}$ (et donc sur $\mathbf{Q}$) en vertu du critère d'Eisenstein. C'est donc le polynôme minimal de $\sqrt[d]{2}$, qui est donc bien de degré d. Il s'ensuit que $\mathbf{Q}(\sqrt[d]{2})$ a d plongements dans $\mathbf{C}$, déterminés par l'image de $\sqrt[d]{2}$ qui doit être une autre racine de $\mathrm{X}^d - 2$, c'est-à-dire un nombre de la forme $\zeta_d^k \sqrt[d]{2}$, où $\zeta_d = e^{2i\pi/d}$ et k décrit l'ensemble $\{1, 2, \ldots, d\}$.

   Un tel plongement $\sigma : \mathbf{Q}(\sqrt[d]{2}) \to \mathbf{C}$ est un isomorphisme si et seulement si $\sigma(\sqrt[d]{2}) \subset \mathbf{Q}(\sqrt[d]{2})$: c'est évidemment une condition nécessaire et, si elle est remplie, l'image de σ est un sous-corps de $\mathbf{Q}(\sqrt[d]{2})$ de même $\mathbf{Q}$-dimension, donc c'est bien $\mathbf{Q}(\sqrt[d]{2})$. Dans notre cas, cela implique en particulier que $\sigma(\sqrt[d]{2})$ soit encore dans $\mathbf{R}$, c'est-à-dire que $\sigma(\sqrt[d]{2}) = \pm\sqrt[d]{2}$.

   Ainsi, $\mathbf{Q}(\sqrt[d]{2})$ a d plongements dans $\mathbf{C}$, mais seuls deux d'entre eux sont des automorphismes.

   Remarque. Le résultat resterait le même pour d pair quelconque. Si d est impair, $\mathbf{Q}(\sqrt[d]{2})$ a toujours d plongements dans $\mathbf{C}$, mais l'identité devient le seul automorphisme.

Exercice 3. Les racines de X^3-2 dans $\mathbf{C}$ sont $\sqrt[3]{2}$, $j\sqrt[3]{2}$ et $j^2\sqrt[3]{2}$, où $j=e^{2i\pi/3}=\zeta_3$. Le corps de décomposition est donc

$$\mathbf{Q}(\sqrt[3]{2}, j\sqrt[3]{2}, j^2\sqrt[3]{2}) = \mathbf{Q}(j, \sqrt[3]{2}).$$

Comme $\sqrt[3]{2}$ (resp. j) est algébrique sur $\mathbf{Q}$ de degré 3 (resp. 2), la deuxième question de l'exercice 1 du TD 1 montre que $[\mathbf{Q}(j, \sqrt[3]{2}) : \mathbf{Q}] = 6$.
Pour trouver un élément primitif, on peut remarquer par exemple que la preuve donnée en cours est constructive : est élément primitif d'une extension séparable finie L/K tout élément $x \in L$ n'appartenant pas à

$$\bigcup_{i\neq j} \left\{ x \in L \,\middle|\, \sigma_i(x) = \sigma_j(x) \right\},$$

où les $(\sigma_i)_i$ sont les plongements de K dans une clôture algébrique.
Dans notre cas, $\mathbf{Q}(\sqrt[3]{2})$ a 3 plongements dans $\mathbf{C}$ (en envoyant $\sqrt[3]{2}$ sur lui-même, $j\sqrt[3]{2}$ ou $j^2\sqrt[3]{3}$), et chacun de ces plongements s'étend de 2 façons à $\mathbf{Q}(j, \sqrt[3]{2})$ (en envoyant j sur lui-même ou sur j^2). On vérifie que $\sqrt[3]{2}+j$, par exemple n'appartient à aucun $\left\{ x \in L \,\middle|\, \sigma_i(x) = \sigma_j(x) \right\}$:

image de $\sqrt[3]{2}$	image de j	image de $j+\sqrt[3]{2}$
$\sqrt[3]{2}$	j	$j+\sqrt[3]{2}$
$\sqrt[3]{2}$	j^2	$j^2+\sqrt[3]{2}$
$j\sqrt[3]{2}$	j	$j+j\sqrt[3]{2}$
$j\sqrt[3]{2}$	j^2	$j^2+j\sqrt[3]{2}$
$j^2\sqrt[3]{2}$	j	$j+j^2\sqrt[3]{2}$
$j^2\sqrt[3]{2}$	j^2	$j^2+j^2\sqrt[3]{2}$

(les éléments de la colonne de droite sont tous différents, ce que l'on vérifie facilement en comparant par exemple leurs expressions dans la $\mathbf{Q}$-base $(1, \sqrt[3]{2}, \sqrt[3]{4}, j, j\sqrt[3]{2}, j\sqrt[3]{4})$ de $\mathbf{Q}(j, \sqrt[3]{2})$.)

Exercice 4.

1. Si $P=\sum_{i=0}^n a_i X^i$, alors $P'=\sum_{i=0}^{n-1}(i+1)a_{i+1}X^i$. Donc si $P'=0$, $(i+1)a_i=0$ quel que soit $i\geq 0$ et donc $a_i=0$ pour tout $i\geq 1$, autrement dit, P est constant. La réciproque est évidente.
2. Supposons que $P'=0$. Comme dans la question précédente, on a $ia_i=0$ pour tout $i\geq 1$. Si i n'est pas divisible par p, i est inversible dans K, et donc $a_i=0$. Donc $P=\sum_{i=0}^n a_{pi}X^{pi}=\sum_{i=0}^n a_{pi}(X^p)^i$.
3. (a) C'est une propriété du cours : les extensions finies en caractéristique nulle sont séparables. (La preuve en est simple : si P est un polynôme irréductible de degré $n\geq 2$ ayant des racines multiples, il n'est pas premier avec sa dérivée P' ; par irréductibilité, cela entraîne que $P'=0$ et donc que P est constant, une contradiction).

   (b) Supposons dans un premier temps que K soit un corps de caractéristique p dans lequel le morphisme de Frobenius $x\mapsto x^p$ est surjectif et prenons P un polynôme irréductible non constant de K[X] ayant des racines multiples (ce qui entraîne que P et P' aient un facteur commun).

   Puisque le degré de P' est strictement inférieur à celui de P et que P est irréductible, P et P' ne peuvent avoir un facteur commun que si $P'=0$. Mais cela impose alors l'existence de $Q\in K[X]$ tel que $P=Q(X^p)$. Écrivons $Q=\sum_{i=0}^n a_i X^i$. Puisque le morphisme de Frobenius est surjectif, il existe $b_i\in K$ tel que $b_i^p=a_i$. On a alors $P=\left(\sum_{i=0}^n b_i X^i\right)^p$. Mais P est un polynôme irréductible non constant, donc une telle décomposition est absurde : P' est non nul et P est séparable.

   Observons maintenant qu'en caractéristique p, les factorisations d'un polynôme $P=X^p-t\in K[X]$ ne peuvent être que de deux types :

– soit le polynôme est irréductible (ce qui entraîne qu'il n'a pas de racine, c'est-à-dire que t n'est pas dans l'image du morphisme de Frobenius) ;
– soit t a une racine p-ième z et $X^p - t = (X-z)^p$.

En effet, t a une racine p-ième z dans la clôture algébrique $\overline{K}$ de K. Si elle n'appartient pas à K, aucune de ses puissances z^i, $1 \leq i \leq p-1$ n'est non plus dans K : on a une relation de Bézout $ui + vp = 1$, donc

$$z^i \in K \Rightarrow z = (z^i)^u \cdot (z^p)^v = z^i \cdot t^v \in K.$$

Mais les seuls facteurs de P dans $\overline{K}[X]$ sont les $(X-z)^i$, avec $0 \leq i \leq p$ (et leurs multiples). Ainsi, si P avait une factorisation non triviale $P = QR$ dans K[X], on aurait $P = u(X-z)^i$ avec $u \in K^\times$ et $1 \leq i \leq p-1$, ce qui entraînerait (en regardant le coefficient constant) $z^i \in K$, une contradiction.

Cela permet de conclure : si K est un corps parfait de caractéristique p, puisque les $X^p - t$ ne sont pas séparables, ils ne peuvent pas être irréductibles. D'après ce qui précède, ils ont donc une racine et t a une racine p-ième, ce qui signifie bien qu'il est dans l'image du morphisme de Frobenius.

Exercice 5.

1. Cela provient de la dernière question de la question précédente : en caractéristique p, le polynôme $X^p + t$ est irréductible sauf si $t \in K$ a une racine p-ième. Comme ce n'est clairement pas le cas de $T \in K(T)$, le polynôme $X^p + T$ est irréductible.

   Dans tout corps dans lequel $X^p + T$ a une racine Z (en particulier dans un corps de rupture), ce polynôme se scinde :

   $$X^p + T = (X+Z)^p.$$

   Pour lui, corps de rupture et de décomposition coïncident donc.

2. (a) Soit Z et W des racines des polynômes irréductibles $X^p - T$ et $X^p - U$ dans une clôture algébrique $\overline{K}$ de K. On a donc $L = K(Z,W) \subset \overline{K}$.

   Une simple considération de degré en T montre que T n'a pas de racine p-ième dans K et que le polynôme $X^p - T$ y est donc irréductible. On a donc bien $[K(Z) : K] = p$.

   De la même façon, un élément de K(Z) est une fraction rationnelle en U à coefficients dans K(Z) : U n'a donc pas de racine p-ième dans K(Z) et $X^p - U$ y est irréductible. On a donc $[K(Z,W) : K(Z)] = p$ et le théorème de la base télescopique montre que

   $$[L : K] = [K(Z,W) : K] = [K(Z,W) : K(Z)] \cdot [K(Z) : K] = p^2.$$

   (b) Tout élément $\alpha \in L = K(\sqrt[p]{T}, \sqrt[p]{U})$ s'écrit $\alpha = f(\sqrt[p]{T}, \sqrt[p]{U})$, avec $f(X,Y) \in K(X,Y)$. Comme $x \mapsto x^p$ est un morphisme de corps, on a

   $$\alpha^p = f(\sqrt[p]{T}, \sqrt[p]{U})^p = f((\sqrt[p]{T})^p, (\sqrt[p]{U})^p) = f(T,U) \in \mathbf{F}_p(T,U) = K.$$

   (c) L/K est donc une extension de degré p^2 dont tous les éléments sont algébriques de degré 1 ou p. Dans ces conditions L ne saurait être égal à un $K(\alpha)$, puisque ces K-espaces vectoriels n'ont pas la même dimension.

Exercice 6.

1. La partition en racines primitives $\mu_n = \bigsqcup_{d|n} \mu_d^*$ (où l'on a noté μ_d^* l'ensemble des racines d-ièmes primitives de l'unité) fournit une factorisation $X^n - 1 = \prod_{d|n} \Phi_d(X)$ (qui est d'ailleurs la décomposition en facteurs irréductibles dans $\mathbf{Z}[X]$ de ce polynôme). Si d divise n, on a donc
$$\frac{X^n - 1}{X^d - 1} = \prod_{\substack{d'|n \\ d' \nmid d}} \Phi_{d'}(X),$$
ce qui entraîne le résultat.
2. Par définition, $\Phi_n(X) = \prod_{\zeta \in \mu_n^*} (X - \zeta)$. Si $\zeta \in \mu_n^*$, on a $|\zeta| = 1$ et donc $\forall r \geq 1, |r - \zeta| \geq r - 1$. En outre, l'égalité est stricte dès que $\zeta \neq 1$. Ainsi, si $r \geq 2$ et $n \geq 2$, on a $\Phi_n(r) > (r-1)^{\phi(n)} \geq r - 1$.
3. Soit n un entier impair. On va montrer que $\zeta \mapsto -\zeta$ met en bijection μ_{2n}^* et μ_n^*.
En effet, si ζ est une racine primitive $2n$-ième de l'unité, ζ^n est un élément d'ordre 2 dans $\mathbf{C}^\times$, donc $\zeta^n = -1$. On a donc $(-\zeta^k) = (-1)^k \zeta^k = 1$ si et seulement si k est pair et $\zeta^k = 1$ ou k est impair et $\zeta^k = -1$, c'est-à-dire si et seulement si k est un multiple de n. La racine $-\zeta$ est donc bien d'ordre n.
Réciproquement, si ζ est d'ordre n, on a $(-\zeta)^k = 1$ si et seulement si k est pair et multiple de n (car on n'a $\zeta^k = -1$ pour aucun k) et $-\zeta$ est d'ordre $2n$. L'involution $\zeta \mapsto -\zeta$ réalise donc une bijection entre μ_{2n}^* et μ_n^*. Le polynôme cyclotomique $\Phi_{2n}(X)$ est donc le polynôme unitaire dont les racines, simples, sont les $-\zeta$ pour ζ parcourant μ_n^*, c'est-à-dire $\Phi_n(-X)$ (qui est unitaire car $\phi(n)$ est pair).
Supposons maintenant n pair. Le même genre de calcul montre que si ζ est une racine primitive $2n$-ième, $-\zeta$ est aussi une racine primitive $2n$-ième et leur carré commun ζ^2 est une racine primitive n-ième. Cela démontre que l'application $\zeta \mapsto \zeta^2$ envoie surjectivement μ_{2n}^* sur μ_n^* et que l'image réciproque de toute racine primitive n-ième contient exactement 2 racines primitives $2n$-ièmes.
Les racines de $\Phi_n(X^2)$ sont donc exactement les $\phi(2n) = 2\phi(n)$ racines primitives de l'unité, ce qui montre (les deux polynômes étant clairement unitaires), que $\Phi_{2n}(X) = \Phi_n(X^2)$.

Exercice 7.

1. D'après les relations coefficients-racines, le terme constant de Φ_n est, au signe près, le produit des racines primitives n-ièmes de l'unité. C'est donc lui-même une racine de l'unité. Comme $\Phi_n \in \mathbf{Z}[X]$, on a $\Phi_n(0) = \pm 1$.
2. Puisque p ne divise pas n, le polynôme $X^n - 1 \in \mathbf{F}_p[X]$ est séparable. Supposons que p divise $\Phi_n(a)$. Comme Φ_n est un diviseur de $X^n - 1$, cela entraîne $p | a^n - 1$ et a est donc un inversible modulo p, d'ordre d divisant n. Si on avait $d < n$, on aurait $\overline{\Phi_d(a)} = 0$ (la barre représentant la réduction modulo p). Dans $\mathbf{F}_p$, la classe de a annulerait donc à la fois Φ_d et Φ_n, ce qui contredit la séparabilité de $X^n - 1$ dans $\mathbf{F}_p[X]$. La classe de a modulo p est donc d'ordre exactement n.
Réciproquement, supposons que a est d'ordre n modulo p. Dans $\mathbf{F}_p[X]$, a annule donc le polynôme $X^n - 1$ et donc l'un des polynômes cyclotomiques $\Phi_d(X)$ pour d divisant n. Mais puisqu'il n'annule aucun des $X^d - 1$ pour d diviseur strict de n, il ne peut annuler aucun des Φ_d correspondant. On a donc bien $\overline{\Phi_n(a)} = 0$, soit p divise $\Phi_n(a)$.
3. Le groupe $\mathbf{F}_p^\times$, cyclique d'ordre $p - 1$, contient un élément d'ordre n si et seulement si n divise $p - 1$, c'est-à-dire si p est congru à 1 modulo n. D'après la question précédente, $p \equiv 1 \pmod{n}$ si et seulement s'il existe un entier relatif a tel que p divise $\Phi_d(a)$.

4. Supposons que l'ensemble des nombres premiers congrus à 1 modulo n soit fini, disons $\{p_1,\dots,p_k\}$. Comme $\Phi_n(\mathrm{X})$ a pour terme dominant $\mathrm{X}^{\phi(n)}$, on peut trouver un entier M suffisamment grand pour que $\Phi_n(\mathrm{M}\cdot p_1\cdots p_k)$ soit strictement supérieur à 1. Il admet donc un diviseur premier p. D'après la question précédente, on a $p\equiv 1\,(\mathrm{mod}\ n)$. Mais puisque le terme constant de Φ_n est ± 1, on a forcément

$$\forall i\in\{1,\dots,k\},\Phi_n(\mathrm{M}\cdot p_1\cdots p_k)\equiv\pm 1\,(\mathrm{mod}\ p_i),$$

donc $p\notin\{p_1,\dots,p_k\}$, ce qui constitue une contradiction. L'ensemble des nombres premiers congrus à 1 modulo n est donc infini.

Remarque. Le théorème de la progression arithmétique de Dirichlet (1837) affirme que si a et n sont premiers entre eux, il existe une infinité de nombres premiers congrus à a modulo n.

Exercice 8.

1. Les arguments ressemblent à ceux donnant de fortes contraintes sur la factorisation de X^p-t vus dans les exercices précédents.

   Soit β une racine de $\mathrm{X}^p-\mathrm{X}-a$ dans un corps K′ éventuellement plus grand que K. Puisque, pour tout $i\in\mathbf{F}_p$, on a $i^p=i$, il vient

   $$(\beta+i)^p=\beta^p+i^p=\beta^p+i=\beta+i+a$$

   et les $(\beta+i)_{i\in\mathbf{F}_p}$, qui appartiennent tous au corps K′, sont p racines distinctes de $\mathrm{X}^p-\mathrm{X}-a$. Ce polynôme se scinde donc sous la forme

   $$\mathrm{X}^p-\mathrm{X}-a=\prod_{i\in\mathbf{F}_p}(\mathrm{X}-(\beta+i))$$

   dans tout corps K′ sur lequel il a une racine. En particulier, ses corps de rupture sont ses corps de décomposition.

   Soit $a\notin\mathrm{S_K}$. Fixons nous maintenant un corps K′ dans lequel $\mathrm{X}^p-\mathrm{X}-a$ a une racine β et démontrons que P est irréductible sur K. Si ce n'était pas le cas, un facteur irréductible s'écrirait

   $$\prod_{i\in\mathrm{I}}\left(\mathrm{X}-(\beta+i)\right),$$

   pour un certain $\mathrm{I}\subset\mathbf{F}_p$ de cardinal $d\notin\{0,p\}$. Mais le coefficient en X^{d-1} de ce polynôme est $-(dx+\sum_{i\in\mathrm{I}}i)$: s'il était dans K, dx le serait aussi et, comme d est inversible modulo p, on aurait également $x\in\mathrm{K}$, ce qui apporterait $x^p-x=a$ et une contradiction.

   Il reste à déterminer le groupe des automorphismes du corps de rupture L/K de ce polynôme. Fixons $\beta\in\mathrm{L}$ une racine de $\mathrm{X}^p-\mathrm{X}-a$. L est le corps de rupture de $\mathrm{X}^p-\mathrm{X}-a$: les automorphismes de L sont donc déterminées par l'image de β, qui doit être une racine de $\mathrm{X}^p-\mathrm{X}-a$ (donc de la forme $\beta+i$ pour un certain élément $i\in\mathbf{F}_p$) et peut être n'importe laquelle. On a donc une bijection $\phi:\mathrm{Aut(L/K)}\to\mathbf{F}_p$ (ici, $\mathbf{F}_p$ est simplement le groupe additif) telle que f envoie β sur $\beta+\phi(f)$. En outre, la composée $g\circ f$ envoie β sur $g(\beta+\phi(f))=g(\beta)+\phi(f)=g(\beta)+\phi(g)+\phi(f)$, la première égalité étant justifiée par le fait que g est un morphisme de corps K-linéaire, donc en particulier $\mathbf{F}_p$-linéaire. On a donc bien $\phi(g\circ f)=\phi(g)+\phi(f)$, et ϕ est un isomorphisme de groupes $\mathrm{Aut(L/K)}\to\mathbf{F}_p$.

2. (a) C'est une propriété très importante des caractères, dont la preuve est classique.

   Supposons que les caractères soient linéairement liés et soit $c_1\chi_{i_1}+\cdots+c_n\chi_{i_k}=0$ une relation de liaison minimale (c'est-à-dire que k est minimal). En particulier, on a $n\geq 2$

et aucun c_i n'est nul. Puisque $\chi_1 \neq \chi_2$, on peut trouver $g_0 \in \mathrm{G}$ tel que $\chi_1(g_0) \neq \chi_2(g_0)$. On a alors

$$\begin{aligned} \forall g \in \mathrm{G}, \quad & c_1\chi_1(g) + c_2\chi_2(g) + \cdots + c_n(g)\chi_n(g) && = 0 \\ \forall g \in \mathrm{G}, \quad & c_1\chi_1(g_0)\chi_1(g) + c_2\chi_2(g_0)\chi_2(g) + \cdots + c_n(g)\chi_n(g_0)\chi_n(g) && = 0. \end{aligned}$$

On obtient donc une relation plus courte

$$c_2\left(\frac{\chi_2(g_0)}{\chi_1(g_0)} - 1\right)\chi_2 + \cdots + c_n\left(\frac{\chi_n(g_0)}{\chi_1(g_0)} - 1\right)\chi_n = 0,$$

ce qui contitue une contradiction.

(b) Puisque $\mathrm{Aut}(\mathrm{L}/\mathrm{K})$ est cyclique d'ordre p et que σ en est un générateur, on a $\mathrm{Aut}(\mathrm{L}/\mathrm{K}) = \{\mathrm{id}, \sigma, \sigma^2, \ldots, \sigma^{p-1}\}$. Ces automorphismes de corps sont en particulier des caractères $\mathrm{L}^\times \to \mathrm{L}^\times$. D'après ce qui précède,

$$\mathrm{id} + \sigma + \sigma^2 + \cdots + \sigma^{p-1} \neq 0 \text{ donc } \exists x \in \mathrm{L}^\times : x + \sigma(x) + \sigma^2(x) + \cdots + \sigma^{p-1}(x) \neq 0.$$

Si on note $z = \sigma(x) + \sigma^2(x) + \cdots + \sigma^{p-1}(x)$ cet élément non nul, on a donc

$$\begin{aligned} \sigma(y) &= \sigma\left((p-1)x + (p-2)\sigma(x) + \cdots + 2\sigma^{p-3}(x) + \sigma^{p-2}(x)\right) \\ &= (p-1)\sigma(x) + (p-2)\sigma^2(x) + \cdots + 2\sigma^{p-2}(x) + \sigma^{p-1}(x) \\ &= y + \left(x + \sigma(x) + \sigma^2(x) + \cdots + \sigma^{p-2}(x) + \sigma^{p-1}(x)\right) \\ &= y + z. \end{aligned}$$

(On a utilisé $p - 1 = -1$).

(c) D'après ce qui précède, $\sigma(y) = y + z$, avec $z \neq 0$. L'élément $\alpha = y/z$ vérifie donc $\sigma(\alpha) = \alpha + 1$. En particulier, $\sigma(\alpha) \neq \alpha$ donc $\alpha \notin \mathrm{K}$.

Dans la suite de l'exercice, il fallait ajouter une hypothèse absente de l'énoncé, à savoir que l'extension L/K **était elle-même de degré** p**.**

En particulier, puisque $\alpha \notin \mathrm{K}$ et que son degré doit diviser p, on a bien $[\mathrm{K}(\alpha) : \mathrm{K}] = p$ et $\mathrm{L} = \mathrm{K}(\alpha)$.

(d) Dans notre cas, l'hypothèse $\forall g \in \mathrm{Aut}(\mathrm{L}/\mathrm{K}), g(x) = x$ devient simplement $\sigma(x) = x$. Ainsi, x appartient au sous-corps

$$\mathrm{L}^\sigma = \left\{ x' \in \mathrm{L} \,\middle|\, \sigma(x') = x' \right\}.$$

Comme σ est K-linéaire et qu'il n'est pas l'identité, on a $\mathrm{K} \subset \mathrm{L}^\sigma \subsetneq \mathrm{L}$ et le théorème de la base télescopique implique que $\mathrm{L}^\sigma = \mathrm{K}$.

Dans notre cas, l'élément

$$\prod_{g \in \mathrm{Aut}(\mathrm{L}/\mathrm{K})} g(\alpha) = \prod_{i=0}^{p-1} \sigma^i(\alpha) = \prod_{i \in \mathbf{F}_p} (\alpha + i) = \alpha^p - \alpha$$

est donc bien un élément de $\mathrm{L}^\sigma = \mathrm{K}$.

Puisque $\alpha \notin \mathrm{K}$, on a $\forall i \in \mathbf{F}_p, \alpha + i \notin \mathrm{K}$ donc $a = \alpha^p - \alpha \notin \mathrm{S}_\mathrm{K}$ et $\mathrm{X}^p - \mathrm{X} - a$ est bien irréductible sur K. Comme ce polynôme annule α, c'en est bien le polynôme minimal.