Devoir maison 1 – Indications

Exercice 1.

1. Si L/K est séparable, alors il existe $x \in L$, de polynôme minimal $\mu_{x,K}$ sur K, tel que :

$$L = K(x) \simeq K[X]/(\mu_{x,K})$$

par le théorème de l'élément primitif. Alors, pour toute extension E de K, on a les isomorphismes de K-algèbres :

$$L \otimes_K E \simeq K[X]/(\mu_{x,K}) \otimes_K E \simeq E[X]/(\mu_{x,K}).$$

Comme $\mu_{x,K}$ est séparable, il est à racines simples dans E, et en particulier sans facteur carré dans $E[X]$: si on note Q_i les facteurs irréductibles de $\mu_{x,K}$, alors le théorème des restes chinois montre que $E[X]/(\mu_{x,K})$ est isomorphe (comme K-algèbre) au produit cartésien des $E[X]/(Q_i)$, qui sont des corps car Q_i est irréductible pour tout i, donc sans éléments nilpotents. Donc $E[X]/(\mu_{x,K})$ est réduit. Ceci montre que (a) implique (b). En prenant $E = L$, on voit trivialement que (b) implique (c).

Si L/K n'est pas séparable, alors il existe $x \in L$ tel que $\mu_{x,K}$ ne soit pas séparable ; par un raisonnement classique, ceci implique que $\mu'_{x,K} = 0$. Dériver la relation $\mu_{x,K} = (X-x)P$ montre que $X - x$ divise P, et donc que $(X-x)^2$ divise $\mu_{x,K}$: la racine x est multiple (c'est, en fait, le cas de toutes les racines de $\mu_{x,K}$), et on peut écrire $\mu_{x,K} = (X-x)^m Q$ où $m \geqslant 2$ et $Q \in L[X]$ est premier à $X - x$.
Ceci étant dit, on en déduit un élément nilpotent de $L \otimes_K K(x)$: ce produit tensoriel est en effet isomorphe, d'après ce qui précède, à $L[X]/(\mu_{x,K}) \simeq L[X]/(X-x)^m \times L[X]/(Q)$ d'après le théorème des restes chinois, et cet anneau contient l'élément nilpotent non nul $(X-x,0)$. On conclut en remarquant que $L \otimes_K L$ contient $L \otimes_K K(x)$, et donc contient un élément nilpotent non nul. On a en effet :

Lemme *Le K-module L est plat. Plus généralement, tout module sur un corps est plat.*

C'est immédiat à partir du théorème 3.15 du cours : il suffit de remarquer que $0 = 0 \otimes_K L \to L$ et $L = K \otimes_K L \to L$ sont des injections.

Ainsi, comme $K(x)$ s'injecte dans L et L est plat, on a $L \otimes_K K(x) \hookrightarrow L \otimes_K L$, et $L \otimes_K L$ n'est pas réduit. Ceci montre que (c) implique (a).

2. Si L/K est galoisienne (donc en particulier séparable), on peut écrire $L = K(x) \simeq K[X]/(\mu_{x,K})$ et $\mu_{x,K}$ se décompose totalement dans L. Par le théorème des restes chinois, $L \otimes_K L \simeq L[X]/(\mu_{x,K})$ est isomorphe à un produit de n corps de la forme $L[X]/(X - x_i) \simeq L$, donc est isomorphe à L^n.

Réciproquement, si $L \otimes_K L \simeq L^n$, alors en particulier cette algèbre est réduite, et L/K est séparable d'après la question précédente : on peut écrire $L = K(x)$ et il reste à prouver que $\mu_{x,K}$ est scindé dans L. Or, si on a la décomposition en irréductibles $\mu_{x,K} = \prod_{i=1}^{r} Q_i$ dans L alors, notant $L_i = L[X]/(Q_i)$, on a l'isomorphisme :

$$L \otimes_K L \simeq \prod_{i=1}^{r} L_i \simeq L^n. \tag{1}$$

Il suffit de montrer que le dernier isomorphisme n'est possible que si $r = n$ et $L_i \simeq L$, sachant que L_i est une extension finie de L. Ainsi, $\mu_{x,K}$ admettrait n facteurs irréductibles dans L, donc serait scindé car $n = \dim_K(L) = \deg(\mu_{x,K})$ (ou encore : on aurait $\dim_L(L_i) = 1 = \deg(Q_i)$).

Première méthode. Définissons l'inclusion $\iota_j : L_j \hookrightarrow \prod_{i=1}^{r} L_i$, l'isomorphisme $\varphi : \prod_{i=1}^{r} L_i \simeq L^n$, et les projections $\pi_i : L^n \to L$. Alors $f_{i,j} = \pi_i \circ \varphi \circ \iota_j : L_j \to L$ est un morphisme de corps, donc est soit nul, soit injectif. Or, pour $j \in [\![1, r]\!]$ fixé, les morphismes $f_{i,j}$ ne sont pas tous simultanément nuls, car $\bigcap_{i=1}^{n} \ker(f_{i,j}) \hookrightarrow \bigcap_{i=1}^{n} \ker(\pi_i) = \{0\}$. Il existe donc $i \in [\![1, n]\!]$ tel que $f_{i,j}$ ne soit pas nul, et définisse un isomorphisme $L_j \simeq f_{i,j}(L_j) \subseteq L \subseteq L_j$. On en déduit que $L_j \simeq L$.
Deuxième méthode. Un produit de s corps contient 2^s solutions à l'équation $x^2 = x$. Ainsi, l'isomorphisme de (1) impose $r = n$.

Exercice 2.

1. Cette question a été correctement traitée par tout le monde.
2. De même.
3. Soit $\psi : \mathbb{Z}^N \to \mathbb{Z}$ s'annulant sur $\mathbb{Z}^{(\mathbb{N})}$, et soit $(u_n)_{n\in\mathbb{N}} \in \mathbb{Z}^{\mathbb{N}}$. Comme 2^n et 3^n sont premiers entre eux pour tout n, il existe $a_n, b_n \in \mathbb{Z}$ tels que $u_n = 2^n a_n + 3^n b_n$. Si on montre que $\psi\left((2^n a_n)_{n\in\mathbb{N}}\right) = \psi\left((3^n a_n)_{n\in\mathbb{N}}\right) = 0$, alors on aura montré que $\psi\left((u_n)_{n\in\mathbb{N}}\right) = 0$.

   Si, pour toute suite $(v_n)_{n\geqslant 0}$ et tout entier N, on note

   $$v_n^{\geqslant N} = \begin{cases} 0 & \text{si } n < N \\ v_n & \text{si } n \geqslant N \end{cases} \quad \text{et } v_n^{<N} = \begin{cases} v_n & \text{si } n < N \\ 0 & \text{si } n \geqslant N \end{cases},$$

   alors $\psi\left((v_n)_{n\in\mathbb{N}}\right) = \psi\left(\left(v_n^{<N}\right)_{n\in\mathbb{N}}\right) + \psi\left(\left(v_n^{\geqslant N}\right)_{n\in\mathbb{N}}\right) = \psi\left(\left(v_n^{\geqslant N}\right)_{n\in\mathbb{N}}\right)$ par hypothèse sur ψ, donc en particulier pour $(v_n)_{n\in\mathbb{N}} = (2^n a_n)_{n\in\mathbb{N}}$:

   $$\forall N \in \mathbb{N}, \quad \psi\left((2^n a_n)_{n\in\mathbb{N}}\right) = 2^N \psi\left(\left(2^{n-N} a_n^{\geqslant N}\right)_{n\in\mathbb{N}}\right),$$

   et donc 2^N divise l'entier $\psi\left((2^n a_n)_{n\in\mathbb{N}}\right)$ pour tout N, ce qui impose $\psi\left((2^n a_n)_{n\in\mathbb{N}}\right) = 0$. De même pour montrer la nullité de $\psi\left((3^n b_n)_{n\in\mathbb{N}}\right)$, d'où le résultat.

   Remarque. Comme $\mathbb{Z}^{(\mathbb{N})}$ admet $(e_i)_{i\in\mathbb{N}} = \left((\delta_{i,j})_{j\in\mathbb{N}}\right)_{i\in\mathbb{N}}$ pour base, dire que ψ s'annule sur $\mathbb{Z}^{(\mathbb{N})}$ revient à dire que $\Psi(\psi) = 0$. Cette question démontre que Ψ est injective.
4. Par l'absurde, supposons $\mathrm{Im}(\Psi) \not\subseteq \mathbb{Z}^{(\mathbb{N})}$. Il existe alors $\psi : \mathbb{Z}^{\mathbb{N}} \to \mathbb{Z}$ et une suite strictement croissante $(i_n)_{n\geqslant 0} \in \mathbb{N}^{\mathbb{N}}$ telle que $\psi(e_{i_n}) \neq 0$ pour tout $n \in \mathbb{N}$.
   Considérons alors la suite u dont le support est exactement $\{i_n \mid n \in \mathbb{N}\}$ et pour laquelle $u_{i_n} = 2^n$. Alors pour tout $N \geqslant 0$, l'entier $\psi\left(\left(u^{\geqslant i_{N+1}}\right)\right)$ est divisible par 2^{N+1}, tandis que $\psi\left(\left(u^{<i_{N+1}}\right)\right)$ est divisible au plus par 2^N. Si on prend $N = N_0$ la puissance de 2 dans la décomposition en facteurs premiers de l'entier $\psi(u)$, alors la différence $\psi(u) - \psi(u^{<i_{N_0+1}}) = \psi(u^{\geqslant i_{N_0}+1})$ est à la fois divisible et non divisible par 2^{N_0+1} : impossible. Donc le support de $(\psi(e_i))_{i\in\mathbb{N}}$ est fini, et $\mathrm{Im}(\Psi) \subseteq \mathbb{Z}^{(\mathbb{N})}$.
5. L'injectivité est déjà montrée en question 2. Par définition de Φ et Ψ, et par la question précédente, la composée $\Phi \circ \Psi$ coïncide clairement avec $\mathrm{Id}_{\mathbb{Z}^{\mathbb{N}}}$ sur $\mathbb{Z}^{(\mathbb{N})}$, et donc sur $\mathbb{Z}^{\mathbb{N}}$, et donc Φ est surjective.
6. Si $\mathbb{Z}^{\mathbb{N}}$ est un $\mathbb{Z}$-module libre, alors on a $\mathbb{Z}^{\mathbb{N}} \simeq \mathbb{Z}^{(I)}$ pour un certain ensemble I. Reproduisant l'isomorphisme de la première question, et celui qu'on vient de montrer, on a :

   $$\mathbb{Z}^{(\mathbb{N})} \simeq \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}^{\mathbb{N}}, \mathbb{Z}) \simeq \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}^{(I)}, \mathbb{Z}) \simeq \mathbb{Z}^I,$$

   et donc $\mathbb{Z}^{(\mathbb{N})} \simeq \mathbb{Z}^I$. Or $\mathbb{Z}^{(\mathbb{N})}$ s'injecte dans l'ensemble dénombrable $\bigcup_{n=1}^{\infty} \mathbb{Z}^n$, donc est dénombrable, ce qui n'est possible que si I est fini : c'est clairement absurde.

Exercice 3.

1. Observation préliminaire : si $P_1|\cdots|P_s$ est la suite des invariants de similitude d'un endomorphisme $f \in \mathrm{L}(K^6)$ de polynôme caractéristique $\chi_f = (X^2+1)(X^2+X+1)^2$, on sait que $\prod_{i=1}^{s} P_i$ égale χ_f, donc chaque facteur irréductible de χ_f divise nécessairement l'un des P_i, et même P_s (puisque $P_i|P_s$).

   Si $K = \mathbb{Q}$: alors X^2+1 et X^2+X+1 sont les facteurs irréductibles de χ_f, et d'après l'observation précédente : $P_s = (X^2+1)(X^2+X+1)^\beta$ avec $1 \leqslant \beta \leqslant 2$. Ceci ne laisse que deux possibilités :
   – si $\beta = 1$, alors $P_1 = X^2+X+1$ et $P_2 = (X^2+1)(X^2+X+1)$ (et donc $s=2$) ;
   – si $\beta = 2$, alors $P_1 = (X^2+1)(X^2+X+1)^2$ (et $s=1$).
   Les matrices compagnons de ces polynômes permettent d'écrire simplement un représentant de chaque classe de similitude, caractérisée par ses invariants de similitude en figure 1.

Figure 1 – Classes de similitude des endomorphismes de $\mathbb{Q}^6$ dont le polynôme caractéristique est égal à $(X^2+1)(X^2+X+1)^2$.

Invariants de similitude	Représentant de la classe
$X^2+X+1, (X^2+1)(X^2+X+1)$	$\begin{pmatrix} 0 & -1 & 0 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 1 & 0 & -2 \\ 0 & 0 & 0 & 0 & 1 & -1 \end{pmatrix}$
$(X^2+1)(X^2+X+1)^2$	$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 & 0 & -2 \\ 0 & 1 & 0 & 0 & 0 & -4 \\ 0 & 0 & 1 & 0 & 0 & -4 \\ 0 & 0 & 0 & 1 & 0 & -4 \\ 0 & 0 & 0 & 0 & 1 & -2 \end{pmatrix}$

   Si $K = \mathbb{Z}/2\mathbb{Z}$: alors $X+1$ et X^2+X+1 sont les facteurs irréductibles de $\chi_f = X^6+1$, et cette fois-ci : $P_s = (X+1)^\alpha(X^2+X+1)^\beta$ avec $1 \leqslant \alpha, \beta \leqslant 2$. Ceci laisse quatre possibilités :
   – si $\alpha = \beta = 1$, alors $P_1 = P_2 = (X+1)(X^2+X+1) = X^3+1$;
   – si $\alpha = 1$, $\beta = 2$, alors $P_1 = X+1$ et

$$P_2 = (X+1)(X^2+X+1)^2 = (X+1)\frac{(X^3+1)^2}{(X+1)^2} = \frac{X^6+1}{X+1} = X^5+X^4+X^3+X^2+X+1;$$

   – si $\alpha = 2$, $\beta = 1$, alors $P_1 = X^2+X+1$ et

$$P_2 = (X+1)^2(X^2+X+1) = (X+1)(X^3+1) = X^4+X^3+X+1;$$

   – si $\alpha = \beta = 2$, alors $P_1 = X^6+1$.
   On en déduit un représentant de chaque classe de similitude en figure 2.

Figure 2 – Classes de similitude des endomorphismes de $(\mathbb{Z}/2\mathbb{Z})^6$ dont le polynôme caractéristique est égal à $(X^2+1)(X^2+X+1)^2$.

Invariants de similitude	Représentant de la classe
X^3+1, X^3+1	$\begin{pmatrix} 0&0&1&0&0&0\\ 1&0&0&0&0&0\\ 0&1&0&0&0&0\\ 0&0&0&0&0&1\\ 0&0&0&1&0&0\\ 0&0&0&0&1&0 \end{pmatrix}$
$X+1, \sum_{i=0}^{5} X^i$	$\begin{pmatrix} 1&0&0&0&0&0\\ 0&0&0&0&0&1\\ 0&1&0&0&0&1\\ 0&0&1&0&0&1\\ 0&0&0&1&0&1\\ 0&0&0&0&1&1 \end{pmatrix}$
X^2+X+1, X^4+X^3+X+1	$\begin{pmatrix} 0&1&0&0&0&0\\ 1&1&0&0&0&0\\ 0&0&0&0&0&1\\ 0&0&1&0&0&1\\ 0&0&0&1&0&0\\ 0&0&0&0&1&1 \end{pmatrix}$
X^6+1	$\begin{pmatrix} 0&0&0&0&0&1\\ 1&0&0&0&0&0\\ 0&1&0&0&0&0\\ 0&0&1&0&0&0\\ 0&0&0&1&0&0\\ 0&0&0&0&1&0 \end{pmatrix}$

2. Soit M la matrice de l'énoncé. On calcule les facteurs invariants de $X\mathrm{I}_3 - M$:

$$\begin{pmatrix} X-3 & -2 & 2\\ 1 & X & -1\\ -1 & -1 & X \end{pmatrix} \xrightarrow[L_1 \leftrightarrow L_2]{} \begin{pmatrix} 1 & X & -1\\ X-3 & -2 & 2\\ -1 & -1 & X \end{pmatrix}$$
$$\xrightarrow[\substack{L_2 \leftarrow L_2-(X-3)L_1\\ L_3 \leftarrow L_3+L_1}]{} \begin{pmatrix} 1 & X & -1\\ 0 & -2+3X-X^2 & X-1\\ 0 & X-1 & X-1 \end{pmatrix}$$
$$\xrightarrow[\substack{C_2 \leftarrow C_2-XC_1\\ C_3 \leftarrow C_3+C_1}]{} \begin{pmatrix} 1 & 0 & 0\\ 0 & -2+3X-X^2 & X-1\\ 0 & X-1 & X-1 \end{pmatrix}$$
$$\xrightarrow{L_2 \leftarrow L_2-L_3} \begin{pmatrix} 1 & 0 & 0\\ 0 & -(X-1)^2 & 0\\ 0 & X-1 & X-1 \end{pmatrix}$$
$$\xrightarrow{C_2 \leftarrow C_2-C_3} \begin{pmatrix} 1 & 0 & 0\\ 0 & -(X-1)^2 & 0\\ 0 & 0 & X-1 \end{pmatrix}.$$

On en déduit que ses invariants de similitude sont $X-1$ et $(X-1)^2$.