L3 algèbre effective - Corrigé de l'examen du 10 janvier 2020

Ex1
```
def facto(P):
    if f(P) == P: L = [P]
    else: L = facto(f(P)) + facto(P//f(P))
    return(L)
```

On ne sait pas ce que rend $f(P)$ si $P=0$. Pour $P\neq 0$ facto(P) rend une liste de polynômes irréductibles d'une certaine extension de k dont P est le produit. On peut tester ce dernier fait par

print P == prod(facto(P))

Ex2 a) $|(\mathbb{Z}/15\mathbb{Z})^\times| = \varphi(15) = \varphi(3\times 5) = 2\times 4 = 8$. Explication : $(\mathbb{Z}/15\mathbb{Z})^\times \xrightarrow{\sim} (\mathbb{Z}/3\mathbb{Z})^\times \times (\mathbb{Z}/5\mathbb{Z})^\times$ par le lemme chinois et $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z}$ sont des corps

b) Il suffit de montrer que l'image de $y^a - y$ par l'application $\mathbb{Z}/15\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ est nulle, puisque cette application est bijective (lemme chinois) $x \mapsto (x \bmod 3, x \bmod 5)$

On écrit $a = 1+8k$. Si $y = 0 \bmod 3$ alors $y^{1+8k} = 0 = y \bmod 3$

Sinon $y \in (\mathbb{Z}/3\mathbb{Z})^\times$ d'ordre 2 donc $y^2 = 1$ puis $y^{1+8k} = y(y^2)^{4k} = y$ donc $y^a - y = 0$ dans $\mathbb{Z}/3\mathbb{Z}$

De même si $y = 0 \bmod 5$ alors $y^{1+8k} = 0 = y \bmod 5$

si $y \neq 0 \bmod 5$ $y \in (\mathbb{Z}/5\mathbb{Z})^\times$ d'ordre 4 donc $y^4 = 1$ puis $y^{1+8k} = y(y^4)^{2k} = y$ dans $\mathbb{Z}/5\mathbb{Z}$

Rq On voit que si $a = y \bmod 15$ dès que $a = 1 \bmod 4$

c) algorithme d'Euclide appliqué à $(13, 8)$: $\left.\begin{array}{l} 13 = 8\times 2 - 3 \\ 8 = 3\times 3 - 1 \end{array}\right\} \rightsquigarrow 1 = 3\times 3 - 8 = (8\times 2 - 13)\times 3 - 8 = 8\times 5 - 13\times 3$

donc $13 \times (-3) = 1 = 13 \times 5 \bmod 8$

On a $(y^{13})^5 = y^{13\times 5} = y \bmod 15$ d'après b) donc $y = 3^5 \bmod 15$

$= 243 \bmod 15 = 6\times 30 + 3 \bmod 15 = 3 \bmod 15$

Rq Avec l'observation $y^a = y \bmod 15$ si $a = 1 \bmod 4$ on a $13 = 1 \bmod 4$ donc $y^{13} = y = 3 \bmod 15$

Ex3 a) Si X^3+X+1 admet un facteur non trivial alors il admet un facteur de degré 1 donc une racine

ni 0 ni 1 ne sont racines de X^3+X+1 dans $\mathbb{F}_2$ donc X^3+X+1 est irréductible dans $\mathbb{F}_2[X]$

1 est racine dans $\mathbb{F}_3$ donc $(X-1)$ divise X^3+X+1 dans $\mathbb{F}_3[X]$

Si X^3+X+1 était réductible dans $\mathbb{Z}[X]$ il le serait aussi dans $\mathbb{F}_2[X]$ ce qui n'est pas.

b) Posons $k = \mathbb{F}_2[X]/X^3+X+1$. k est un $\mathbb{F}_2$-espace vectoriel de dim 3 (de base $(1, X, X^2)$) donc $|k| = 2^3 = 8$.

Puisque X^3+X+1 est irréductible, k est un corps donc $|k^\times| = |k| - 1 = 7$

3c) On calcule

$$\begin{array}{r|l} X^5+X^4+1 & X^3+X+1 \\ \hline X^5+X^3+X^2 & X^2+X+1 \\ \cline{1-1} X^4+X^3+X^2+1 & \\ X^4+X^2+X & \\ \cline{1-1} X^3+X+1 & \\ X^3+X+1 & \\ \cline{1-1} 0 & \end{array}$$

$X^5+X^4+1 = (X^3+X+1)(X^2+X+1)$

Puisque X^3+X+1 est irréductible et ne divise pas X^2+X+1 (pour une raison de degré déjà) il est premier avec X^2+X+1.

Le Lemme chinois dit alors que l'application

$$K = \mathbb{F}_2[X]/_{X^5+X^4+1} \longrightarrow \mathbb{F}_2[X]/_{X^3+X+1} \times \mathbb{F}_2[X]/_{X^2+X+1}$$
$$P \longmapsto (P \bmod X^3+X+1,\ P \bmod X^2+X+1)$$

est un isomorphisme d'anneaux. Elle induit un isomorphisme entre les groupes multiplicatifs $K^\times \longrightarrow \left(\mathbb{F}_2[X]/_{X^3+X+1} \times \mathbb{F}_2[X]/_{X^2+X+1}\right)^\times$. Or le groupe multiplicatif (le groupe des éléments inversibles) d'un produit d'anneaux est le produit des groupes multiplicatifs.

d) On sait déjà $\left|\left(\mathbb{F}_2[X]/_{X^3+X+1}\right)^\times\right| = 7$.

X^2+X+1 est sans racine dans $\mathbb{F}_2$ donc irréductible (même argument que pour X^3+X+1) donc $\mathbb{F}_2[X]/_{X^2+X+1}$ est un corps et son groupe multiplicatif est de cardinal $2^2-1=3$.

On obtient avec (3c) $d = 7\times 3 = 21$

X^3+X+1 est non nul dans K (il ne peut être multiple de X^5+X^4+1 pour une raison de degré). Il n'est pas inversible dans K car il est nul dans $\mathbb{F}_2[X]/_{X^3+X+1}$

e) Tout élément de $\left(\mathbb{F}_2[X]/_{X^3+X+1}\right)^\times$ est d'ordre 1 ou 7, de même tout élément de $\left(\mathbb{F}_2[X]/_{X^2+X+1}\right)^\times$ est d'ordre 1 ou 3

Tout élément de $K^\times$ d'image $\neq 1$ dans $\left(\mathbb{F}_2[X]/_{X^3+X+1}\right)^\times$ et dans $\left(\mathbb{F}_2[X]/_{X^2+X+1}\right)^\times$ est d'ordre divisant 21, $\neq 1,3,7$ donc est d'ordre 21 donc $K^\times$ est cyclique. $P = X$ remplit ces critères donc est un générateur de $K^\times$

f) On détermine $\ker(F-\mathrm{id})$ dans $\underbrace{\mathbb{F}_2[X]/_{X^3+X+1}}_{K_1} \times \underbrace{\mathbb{F}_2[X]/_{X^2+X+1}}_{K_2}$. K_1 et K_2 sont des corps contenant $\mathbb{F}_2$ sur lequel $F=\mathrm{id}$.

le polynôme X^2-X ne peut y avoir plus de deux racines. On obtient $\ker(F-\mathrm{id}: K_1\to K_2) = \mathbb{F}_2$; $\ker(F-\mathrm{id}: K_2\to K_2) = \mathbb{F}_2$

puis $\ker(F-\mathrm{id}: K_1\times K_2 \to K_1\times K_2) = \mathbb{F}_2\times\mathbb{F}_2 = \mathrm{Vect}_{\mathbb{F}_2}\left((1,0),(0,1)\right)$ de dimension 2

On choisit P d'image $(1,0)$ dans $K_1\times K_2$ alors $P = 0 \bmod X^2+X+1$ donc X^2+X+1 divise P et comme X^2+X+1 divise X^5+X^4+1 on a $X^2+X+1 \mid \mathrm{pgcd}(X^5+X^4+1, P)$.

Par ailleurs $(1,0) \in \ker(F-\mathrm{id}: K_1\times K_2 \circlearrowleft)$ donc $P \in \ker(F-\mathrm{id}: K\to K)$

Calcul de P : On écrit $P = (X^2+X+1)Q$. $P = 1 \bmod X^3+X+1$ donc Q est inverse de $(X^2+X+1) \bmod X^3+X+1$.

On détermine Q par l'algorithme d'Euclide :

$$\left.\begin{array}{l} X^3+X+1 = (X^2+X+1)(X+1)+X \\ X^2+X+1 = X(X+1)+1 \end{array}\right\} \rightsquigarrow 1 = (X^2+X+1)+X(X+1) \quad (\text{modulo } 2 !)$$
$$= (X^2+X+1)+((X^3+X+1)+(X^2+X+1)(X+1))(X+1)$$
$$= (X^3+X+1)(X+1)+(X^2+X+1)(1+(X+1)^2)$$

$Q = 1+(X+1)^2 = X^2$ convient puis $P = (X^2+X+1)X^2 = X^4+X^3+X^2$

Ex4 a) $\mathrm{Im}(D) = \mathrm{Vect}\big((1,0,0,0),(0,2,0,0),(0,0,0,3)\big)$ comme $\mathbb{Q}$-espace vectoriel ou comme $\mathbb{Z}$-module.

Equations : $(y_1,y_2,y_3,y_4) \in \mathrm{Im}(D) \Leftrightarrow y_2 = 0$ dans $\mathbb{Q}^4$

$$\Leftrightarrow \begin{cases} y_2 = 0 & \text{dans } \mathbb{Z}^4 \\ y_3 = 0 \bmod 2 \\ y_4 = 0 \bmod 3 \end{cases}$$

b) $A = P^{-1} D Q^{-1}$ alors $\mathrm{Im}(A) = \mathrm{Im}(P^{-1} D Q^{-1}) = \mathrm{Im}(P^{-1} D)$ car Q^{-1} est inversible

or $P^{-1}D = \big(c_1 \mid 0 \mid 2c_3 \mid 3c_4\big)$ où $c_1,\dots,c_4$ sont les colonnes de P^{-1}

donc $\mathrm{Im}(A) = \mathrm{Vect}(c_1, 2c_3, 3c_4)$. $c_1, 2c_3, 3c_4$ ne sont pas liés puisque P^{-1} est inversible, donc forme une base de $\mathrm{Im}(A)$ dans $\mathbb{Q}^4$ ou $\mathbb{Z}^4$

Equations : $\begin{pmatrix} y_1 \\ \vdots \\ y_4 \end{pmatrix} \in \mathrm{Im}\,A \Leftrightarrow P\begin{pmatrix} y_1 \\ \vdots \\ y_4 \end{pmatrix} \in \mathrm{Im}(PA) = \mathrm{Im}(PAQ) = \mathrm{Im}(D)$

$\Leftrightarrow L_2 \begin{pmatrix} y_1 \\ \vdots \\ y_4 \end{pmatrix} = 0$ dans $\mathbb{Q}^4$ où $L_1,\dots,L_4$ sont les lignes de P

$$\Leftrightarrow \begin{cases} L_2 \begin{pmatrix} y_1 \\ \vdots \\ y_4 \end{pmatrix} = 0 & \text{dans } \mathbb{Z}^4 \\ L_3 \begin{pmatrix} y_1 \\ \vdots \\ y_4 \end{pmatrix} = 0 \bmod 2 \\ L_4 \begin{pmatrix} y_1 \\ \vdots \\ y_4 \end{pmatrix} = 0 \bmod 3 \end{cases} \qquad \begin{cases} -10y_1 - 14y_2 - 6y_3 - 15y_4 = 0 \\ 7y_1 + 9y_2 + 4y_3 + 10y_4 = 0 \bmod 2 \\ -21y_1 - 26y_2 - 12y_3 - 30y_4 = 0 \bmod 3 \end{cases}$$

Ex5 $D = \begin{pmatrix} 1 & & & \\ & 0 & & \\ & & 2 & \\ & & & 3 \end{pmatrix} \xrightarrow[L_2 \leftrightarrow L_4]{C_2 \leftrightarrow C_4} \begin{pmatrix} 1 & & & \\ & 3 & & \\ & & 2 & \\ & & & 0 \end{pmatrix} \xrightarrow{C_2 + C_3 \to C_2} \begin{pmatrix} 1 & & & \\ & \boxed{\begin{matrix} 3 & 0 \\ 2 & 2 \end{matrix}} & & \\ & & & 0 \end{pmatrix} \xrightarrow{L_2 - L_3 \to L_2} \begin{pmatrix} 1 & & & \\ & \boxed{\begin{matrix} 1 & -2 \\ 2 & 2 \end{matrix}} & & \\ & & & 0 \end{pmatrix} \xrightarrow{L_3 - 2L_2 \to L_3} \begin{pmatrix} 1 & & & \\ & \boxed{\begin{matrix} 1 & -2 \\ 0 & 6 \end{matrix}} & & \\ & & & 0 \end{pmatrix}$

$$\downarrow C_3 + 2C_2 \to C_3$$

$$\begin{pmatrix} 1 & & & \\ & \boxed{\begin{matrix} 1 & 0 \\ 0 & 6 \end{matrix}} & & \\ & & & 0 \end{pmatrix}$$

d'où $(d_1,\dots,d_4) = (1,1,6,0)$

$P = I_4$ transformée par les opérations sur les lignes seulement $= \left(\begin{array}{c|ccc} 1 & 0 & & \\ \hline 0 & 0 & -1 & 1 \\ 0 & 3 & -2 & \\ 1 & 0 & 0 & \end{array}\right)$

$Q = I_4$ transformée par les opérations sur les colonnes seulement $= \left(\begin{array}{c|ccc} 1 & 0 & & \\ \hline 0 & 0 & 0 & 1 \\ 0 & 1 & 3 & 0 \\ & -1 & 2 & 0 \end{array}\right)$