Université Pierre & Marie Curie 2007-2008

M1 ALGÈBRE COMMUTATIVE ET THÉORIE DE GALOIS **Devoir 2 - corrigé**

P.-V Koseleff

Corrigé du devoir 2

SOLUTION 1. —

1. Déterminer le rang et les facteurs invariants de E et F.

On fait des opérations élémentaires sur les lignes et les colonnes de la matrice $\begin{pmatrix} \boxed{1} & 2 & 3 \\ -1 & 1 & -3 \\ 2 & -3 & 1 \\ 1 & -13 & -3 \end{pmatrix}$.

On obtient

$$\begin{pmatrix} \boxed{1} & 0 & 0 \\ -1 & 3 & 0 \\ 2 & -7 & -5 \\ 1 & -15 & -6 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & \boxed{3} & 0 \\ 0 & -7 & -5 \\ 0 & -15 & -6 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & \boxed{-1} & -5 \\ 0 & 0 & -6 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -15 \\ 0 & \boxed{-1} & -5 \\ 0 & 0 & -6 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & \boxed{1} & -10 \\ 0 & -1 & -5 \\ 0 & 0 & -6 \end{pmatrix} \mapsto$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \boxed{1} & 0 \\ 0 & -1 & -15 \\ 0 & 0 & -6 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -15 \\ 0 & 0 & \boxed{-6} \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \boxed{3} \\ 0 & 0 & -6 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 3 \\ 0 & 0 & 0 \end{pmatrix}$$

Le rang de E est 3 et les facteurs invariants sont $1, 1, 3$.

Pour F, on fait la même chose avec la matrice

$$\begin{pmatrix} \boxed{1} & 3 \\ 1 & -2 \\ 0 & 3 \\ -2 & 1 \end{pmatrix} \mapsto \begin{pmatrix} \boxed{1} & 0 \\ 1 & -2 \\ 0 & 3 \\ -2 & 1 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -2 \\ 0 & 3 \\ 0 & \boxed{1} \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 1 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Le rang de E est 2 et les facteurs invariants sont $1, 1$.

2. Déterminer le rang et les facteurs invariants de $E+F$.

Pour $E+F$, on fait la même chose sur la matrice $\begin{pmatrix} 1 & 2 & 3 & 1 & 3 \\ -1 & 1 & -3 & 1 & -2 \\ 2 & -3 & 1 & 0 & 3 \\ 1 & -13 & -3 & -2 & 1 \end{pmatrix}$ *et on obtient* $\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 19 & 0 \end{pmatrix}$.

Le rang est 4 et les facteurs invariants $1, 1, 1, 19$.

3. *(a)* Montrer que $E\cap F=(A_1A_2A_3)\circ p_1(\mathrm{Ker}\phi)=(A_4A_5)\circ p_2(\mathrm{Ker}\phi)$.
On a $\mathrm{Ker}\phi=\{(X,Y)\in\mathbb{Z}^3\times\mathbb{Z}^2;(A_1A_2A_3)X+(A_4A_5)Y=0\}$. *Mais alors* $Z\in E\cap F$ *ssi il existe* $(X,Y)\in\mathbb{Z}^3\times\mathbb{Z}^2$ *tels que* $Z=(A_1A_2A_3)X=-(A_4A_5)Y$*, c'est-à-dire,* $(X,Y)\in\mathrm{Ker}\phi$ *et* $Z=(A_1A_2A_3)X=-(A_4A_5)Y$*. On a donc le résultat annoncé.*

(b) En déduire une base de $E\cap F$.
On échelonne en colonnes la matrice $(A_1A_2A_3A_4A_5)$*, c'est-à-dire, on cherche* R *dans* $\mathbf{SL}_5(\mathbb{Z})$*, telle que* $(A_1A_2A_3A_4A_5)\cdot R$ *soit échelonnée en colonne. Echelonnons donc*

$$\begin{pmatrix} 1 & 2 & 3 & 1 & 3\\ -1 & 1 & -3 & 1 & -2\\ 2 & -3 & 1 & 0 & 3\\ 1 & -13 & -3 & -2 & 1\\ 1 & 0 & 0 & 0 & 0\\ 0 & 1 & 0 & 0 & 0\\ 0 & 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}\mapsto\begin{pmatrix} 1 & 0 & 0 & 0 & 0\\ 0 & 1 & 0 & 0 & 0\\ 0 & 0 & 1 & 0 & 0\\ 4 & 13 & 5 & 19 & 0\\ -2 & -5 & 0 & -9 & 2\\ -1 & -2 & -1 & -2 & -1\\ 1 & 1 & 1 & 0 & 2\\ 2 & 3 & 2 & 1 & 3\\ 0 & 1 & -1 & 4 & -3 \end{pmatrix}.$$

On interprète cela en

$$\begin{pmatrix} 1 & 2 & 3 & 1 & 3\\ -1 & 1 & -3 & 1 & -2\\ 2 & -3 & 1 & 0 & 3\\ 1 & -13 & -3 & -2 & 1\\ 1 & 0 & 0 & 0 & 0\\ 0 & 1 & 0 & 0 & 0\\ 0 & 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}\cdot\begin{pmatrix} -2 & -5 & 0 & -9 & 2\\ -1 & -2 & -1 & -2 & -1\\ 1 & 1 & 1 & 0 & 2\\ 2 & 3 & 2 & 1 & 3\\ 0 & 1 & -1 & 4 & -3 \end{pmatrix}=\begin{pmatrix} 1 & 0 & 0 & 0 & 0\\ 0 & 1 & 0 & 0 & 0\\ 0 & 0 & 1 & 0 & 0\\ 4 & 13 & 5 & 19 & 0\\ -2 & -5 & 0 & -9 & 2\\ -1 & -2 & -1 & -2 & -1\\ 1 & 1 & 1 & 0 & 2\\ 2 & 3 & 2 & 1 & 3\\ 0 & 1 & -1 & 4 & -3 \end{pmatrix}.$$

ce qui est équivalent à

$$\begin{pmatrix} 1 & 2 & 3 & 1 & 3\\ -1 & 1 & -3 & 1 & -2\\ 2 & -3 & 1 & 0 & 3\\ 1 & -13 & -3 & -2 & 1 \end{pmatrix}\cdot\begin{pmatrix} -2 & -5 & 0 & -9 & 2\\ -1 & -2 & -1 & -2 & -1\\ 1 & 1 & 1 & 0 & 2\\ 2 & 3 & 2 & 1 & 3\\ 0 & 1 & -1 & 4 & -3 \end{pmatrix}=\begin{pmatrix} 1 & 0 & 0 & 0 & 0\\ 0 & 1 & 0 & 0 & 0\\ 0 & 0 & 1 & 0 & 0\\ 4 & 13 & 5 & 19 & 0 \end{pmatrix}$$

A ce stade, on retrouve les facteurs invariants de $E+F$*. Poursuivons en interprétant : une base du noyau de* Φ *est donc* $\begin{pmatrix} 2\\ -1\\ 2\\ 3\\ -3 \end{pmatrix}$ *et une base de* $E+F$ *est donnée par* $\begin{pmatrix} 1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\\ 4 & 13 & 5 & 19 \end{pmatrix}$*. Une base de*

$p_1(\mathrm{Ker}\phi)$ est donc $\begin{pmatrix} 2 \\ -1 \\ 2 \end{pmatrix}$ et une base de $E \cap F$ est par conséquent $G_6 = 2A_1 - A_2 + 2A_3 = \begin{pmatrix} 6 \\ -9 \\ 9 \\ 9 \end{pmatrix}$.

(c) Donner une base de E adaptée à $E \cap F$.

Partons d'une base de E, qu'on obtient en échelonnant la matrice $(A_1 A_2 A_3)$. On obtient $\begin{pmatrix} 1 & 0 & 0 \\ 2 & 3 & 0 \\ 0 & 3 & 5 \\ -8 & -3 & 6 \end{pmatrix}$.

Dans cette base (E_1, E_2, E_3), on remarque que $G_6 = 6E_1 - 7E_2 + 6E_3$. Les coefficients de G_6 dans cette dernière base sont premiers dans leur ensemble donc G_6 peut-être complété en une base de E. Par exemple $(E_1 E_2 E_3)\begin{pmatrix} 6 & 1 & 0 \\ -7 & -1 & 0 \\ 6 & 0 & 1 \end{pmatrix}$ puisque le déterminant de la matrice de droite vaut 1. On obtient une base adaptée $e_1 = 6E_1 - 7E_2 + 6E_3, e_2 = E_1 - E_2, e_3 = E_3$. On a $E \cap F = \mathbb{Z}e_1$. $E = \mathbb{Z}e_1 \oplus \mathbb{Z}e_2 \oplus \mathbb{Z}e_3$.

(d) Existe-t'il une base de $E + F$ adaptée à la fois à E, à F et à $E \cap F$?

Dans la cas de F, on a comme base, par exemple en échelonnant la matrice $(A_4 A_5)$: $\begin{pmatrix} 1 & 0 \\ 1 & 5 \\ 0 & -3 \\ -2 & -7 \end{pmatrix}$

Dans cette base F_1, F_2, on a $e_1 = G_6 = 6F_1 - 3F_2$. On voit que cette base ne peut pas être complétée en une base de F. Posons $e_1 = 3f_1$, on obtient avec $e_1 = 3f_1$ et $f_2 = F_1$,

$$F = \mathbb{Z}f_1 \oplus \mathbb{Z}f_2, \quad E \cap F = 3\mathbb{Z}f_1, \quad E = 3\mathbb{Z}f_1 \oplus \mathbb{Z}e_2 \oplus \mathbb{Z}e_3.$$

On a aussi $E + F = \mathbb{Z}f_1 \oplus \mathbb{Z}f_2 \oplus \mathbb{Z}e_2 \oplus \mathbb{Z}e_3$, puisque les facteurs invariants du sous-module de $\mathbb{Z}^4$ à droite sont $1, 1, 1, 1, 19$.

□

SOLUTION 2. — *Posons $\Phi_p = X^{p-1} + \cdots + 1$. On a $X^p - 1 = (X-1)\Phi_p$. Donc ζ_p est une racine de Φ_p. On a*

$$\Phi_p(Y+1) = \frac{(Y+1)^p - 1}{Y} = \sum_{k=0}^{p-1} \binom{p}{k+1} Y^k.$$

Tous les coefficients de $\Phi_p(Y+1)$ sont divisibles par p sauf le coefficient dominant.

Rappel : *On a (voir Demazure, cours d'algèbre, Cassini) l'identité dans $\mathbb{F}_p[X]$:*

$$X^p - X = \prod_{\alpha \in \mathbb{F}_p} (X - \alpha) = \prod_{\alpha \in \mathbb{F}_p} (X + 1 - \alpha) = (X+1)^p - (X+1)$$

d'où l'on déduit que $(X+1)^p = X^p + 1$ et $p | \binom{p}{k}$.

Le coefficient constant de $\Phi_p(Y+1)$ vaut p qui n'est pas divisible par p^2. Donc, d'après le critère d'Eisenstein, $\Phi_p(Y+1)$ est irréductible et donc Φ_p l'est également.

Φ_p est donc le polynôme minimal de ζ_p, puisqu'il est irréductible.

Les autres racines de Φ_p sont les puissances de ζ, sauf ζ_p^p. Elles sont dans $\mathbb{Q}(\zeta_p)$ qui est donc un corps de décomposition.

On a $[Q(\zeta_p):\mathbb{Q}] = \deg \Phi_p = p-1$.

Posons $\xi_p = \zeta_p + \zeta_p^{-1}$.

On a $\zeta_p^2 - \xi_p\zeta_p + 1 = 0$ donc $[\mathbb{Q}(\zeta_p):\mathbb{Q}(\xi_p)] \leq 2$.

Dans le cas où $p = 2$, alors $\mathbb{Q}(\xi_p) = \mathbb{Q}(\zeta_p) = \mathbb{Q}$.

Dans les autres cas, remarquons que ξ_p est réel donc $\mathbb{Q}(\zeta_p) \neq \mathbb{Q}(\xi_p)$. On déduit que $[\mathbb{Q}(\zeta_p):\mathbb{Q}(\xi_p)] = 2$ et $[\mathbb{Q}(\xi_p):\mathbb{Q})] = \dfrac{p-1}{2}$.

Remarques :

1. *Le fait que ζ_p ne soit pas réel provient du fait que ζ_p est de module 1. Si ζ_p était réel, il serait égal à ± 1 donc d'ordre 1 ou 2.*
2. *En fait, on n'a pas besoin d'invoquer le caractère réel de ξ_p. On peut montrer directement que ξ_p est annulé par un polynôme de degré $(p-1)/2$. En effet, en écrivant $\Phi_p(x) = x^{(p-1)/2}\Psi(x, \dfrac{1}{x})$, on remarque que Ψ est un polynôme symétrique en x et $\dfrac{1}{x}$ donc s'exprime comme polynôme en $x + \dfrac{1}{x}$ et $x \cdot \dfrac{1}{x} = 1$ donc comme un polynôme en $x + \dfrac{1}{x}$ de degré $\dfrac{p-1}{2}$. Ce polynôme n'est autre que le polynôme de Chebychev de première espèce $\Psi_n(x) = 2\cos(n \arccos(x/2))$.*

$\square$