Calculs matriciels

Solution de l'exercice (??)

On suit les étapes de la preuve du théorème **??** : on note M la matrice des éléments e'_i en colonnes (théorème **??**) :

$$M = \begin{pmatrix} 2 & 1 & 3 \\ -1 & 4 & -1 \\ 1 & -1 & -1 \end{pmatrix}$$

1) On fait apparaître un zéro à la place $(2,1)$ en multipliant à gauche par la matrice $L_1 = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. On a :

$$L_1 M = \begin{pmatrix} 1 & 5 & 2 \\ 0 & 9 & 1 \\ 1 & -1 & -1 \end{pmatrix}$$

2) On fait apparaître un zéro à la place $(3,1)$ en multipliant à gauche par $L_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -1 & 0 & 1 \end{pmatrix}$ (*cf.* Remarque **??**). On a alors :

$$L_2 L_1 M = \begin{pmatrix} 1 & 5 & 2 \\ 0 & 9 & 1 \\ 0 & -6 & -3 \end{pmatrix}, \quad L_2 L_1 = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 2 & 0 \\ -1 & -1 & 1 \end{pmatrix}$$

3) On fait apparaître un zéro à la place $(1,2)$ en multipliant à droite par la matrice $R_1 = \begin{pmatrix} 1 & -5 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$, $\quad L_2 L_1 M R_1 = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 9 & 1 \\ 0 & -6 & -3 \end{pmatrix}$;

4) On multiplie ensuite par $R_2 = \begin{pmatrix} 1 & 0 & -2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ pour avoir un zéro à la place $(1,3)$:

$$L_2 L_1 M R_1 R_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 9 & 1 \\ 0 & -6 & -3 \end{pmatrix}$$

5) On mutiplie à gauche par $L_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 2 & 3 \end{pmatrix}$ pour obtenir : $L_3L_2L_1MR_1R_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & -2 \\ 0 & 0 & -7 \end{pmatrix}$

6) Puis à droite par $R_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 1 & 3 \end{pmatrix}$ pour obtenir : $L_3L_2L_1MR_1R_2R_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -0 \\ 0 & -7 & -2 \end{pmatrix}$

7) Et enfin à gauche par $L_4 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 7 & 1 \end{pmatrix}$ pour obtenir finalement :

$$L_4L_3L_2L_1MR_1R_2R_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -21 \end{pmatrix}.$$

8) On a donc

$$R = R_1R_2R_3 = \begin{pmatrix} 1 & -7 & -16 \\ 0 & 1 & 2 \\ 0 & 1 & 3 \end{pmatrix}$$

et

$$MR = \begin{pmatrix} 2 & -10 & -21 \\ -1 & 10 & 21 \\ 1 & -9 & -21 \end{pmatrix}$$

d'où la base adaptée :

$$(f_1, f_2, f_3) = \begin{pmatrix} 2 & -10 & 1 \\ -1 & 10 & -1 \\ 1 & -9 & 1 \end{pmatrix}$$

puisque l'on doit avoir $LMRe_i = a_ie_i$ et donc $MR(e_i) = a_if_i$ $(1 \leq i \leq 3)$. Comme confirmation le lecteur pourra vérifier que $Lf_i = e_i$ $(1 \leq i \leq 3)$, la matrice L étant $L = L_4L_3L_2L_1$ (ce qui peut être une autre façon de déterminer les f_i).

On en déduit alors que $\mathbf{Z}^3/L \simeq \mathbf{Z}/21\mathbf{Z}$. On peut retrouver ce dernier résultat sans calculs, car le calcul du déterminant de la matrice de départ

donne -21 qui est donc égal au produit des facteurs invariants, ce qui impose $a_1 = a_2 = 1$ et $a_3 = 21 = 3 \times 7$ et donc $\mathbf{Z}^3/L \simeq \mathbf{Z}/21\mathbf{Z}$ (on rappelle que les facteurs invariants sont définis au signe près si on est dans $\mathbf{Z}$).

Solution de l'exercice (??)

a) (i) implique (ii) : les (n_i) étant premiers entre eux par hypothèse, il existe des nombres entiers u_i tels que $u_1 n_1 + \div cdots + u_p n_p = 1$. On considère le morphisme $\phi : \mathbf{Z}^p \longmapsto \mathbf{Z}$ défini par $\phi(x_1, \ldots, x_p) = u_1 x_1 + \cdots + u_p x_p$. Le théorème fondamental du cours dit de la base adpatée, nous assure l'existence d'une base $(f_1, \ldots, f_p)$ de $\mathbf{Z}^p$ tel que $\ker \phi = \mathbf{Z}a_1 f_1 \oplus \cdots \oplus \mathbf{Z}a_p f_p$ avec $a_i | a_{i+1}$ dans $\mathbf{Z}$ que l'on appelle les facteurs invariants de $\mathbf{Z}^p/\ker\phi$; le morphisme $\phi : \mathbf{Z}^p \longrightarrow \mathbf{Z}$ est surjectif car $1 \in \operatorname{Im}\phi$ par hypothèse (relation de Bézout entre les n_i). On a donc $\mathbf{Z}/\ker\phi \simeq \mathbf{Z}$. Comme le théorème de la base adaptée dit que $\mathbf{Z}/\ker\phi \simeq \mathbf{Z}/a_1\mathbf{Z} \times \cdots \times \mathbf{Z}/a_p\mathbf{Z}$, on en déduit $a_1 = \cdots = a_{p-1} = 1$, $a_p = 0$.
Les vecteurs $f_1, \ldots f_p$ formant une base de $\mathbf{Z}^p$, il en est de même des vecteurs $f_1, \ldots, f_{p-1}, x$ comme on le voit tout de suite : si $\phi(f_p) = \lambda$, on a $f_p - \lambda x \in \ker\phi$ et donc ils forment un système de générateurs. Ils forment un système libre car une relation linéaire entre $f_1, \ldots f_{p-1}, x$ donnerait (après multiplication par $\lambda \neq 0$) une relation linéaire entre les f_i.

(ii) implique (iii) : Le vecteur x faisant partie d'une base de $\mathbf{Z}^p$, la matrice de passage A de cette base (avec x comme premier vecteur) dans la base canonique vérifie bien $A^t x = {}^t(1, 0, \ldots, 0)$.

(iii) implique (i) : soit $(v_1, \ldots v_p)$ la première ligne de la matrice A ; on a $1 = v_1 n_1 + \cdots + v_p n_p$ par hypothèse, et donc les (n_i) sont premiers entre eux.

b) On a la relation $7 - 6 = 1$ de sorte que la matrice suivante est de déterminant -1

$$\begin{pmatrix} 10 & 6 & 7 & 11 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Les 4 vecteurs colonnes de la transposée de la matrice ci-dessus constituent donc une base de $\mathbf{Z}^4$.

Solution de l'exercice (??)

Résoudre cette équation revient comme d'habitude à trouver une solution particulière, puis déterminer le noyau de la matrice en question. On fait

d'une pierre deux coups en cherchant les éléments du noyau de la matrice

$$M = \begin{pmatrix} 3 & 2 & 3 & 4 & 8 \\ 1 & -2 & 1 & -1 & 3 \end{pmatrix}$$

dont la dernière coordonnées est 1.
On commence par trigonaliser la matrice M en faisant apparaître des zéros sur les lignes, donc en multipliant à droite par des matrices de $SL_2(\mathbf{R})$.

1.

$$\begin{pmatrix} 3 & 2 & 3 & 4 & 8 \\ 1 & -2 & 1 & -1 & 3 \end{pmatrix} \begin{pmatrix} 1 & -2 & 0 & 0 & 0 \\ -1 & 3 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 3 & 4 & 8 \\ 3 & -8 & 1 & -1 & 3 \end{pmatrix}$$

2.

$$\begin{pmatrix} 1 & 0 & 3 & 4 & 8 \\ 3 & -8 & 1 & -1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 0 & -3 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 4 & 8 \\ 3 & -8 & -8 & -1 & 3 \end{pmatrix}$$

3.

$$\begin{pmatrix} 1 & 0 & 0 & 4 & 8 \\ 3 & -8 & -8 & -1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & -4 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 8 \\ 3 & -8 & -8 & -13 & 3 \end{pmatrix}$$

4.

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 8 \\ 3 & -8 & -8 & -13 & 3 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 & -8 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 3 & -8 & -8 & -13 & -21 \end{pmatrix}$$

5.

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 3 & -8 & -8 & -13 & -21 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 3 & -8 & 0 & -13 & -21 \end{pmatrix}$$

6.

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 3 & -8 & 0 & -13 & -21 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & -5 & 0 & 13 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 3 & 0 & -8 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 3 & 1 & 0 & 0 & -21 \end{pmatrix}$$

7.

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 3 & 1 & 0 & 0 & -21 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & -21 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 3 & 1 & 0 & 0 & 0 \end{pmatrix}$$

La matrice R, produit des 7 matrices de $SL_2(\mathbf{R})$ ci-dessus, est égale à

$$R = \begin{pmatrix} 1 & 2 & -1 & 6 & 34 \\ 1 & -27 & -6 & 58 & -575 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 3 & 0 & -8 & 63 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Un élément X du noyau de M vérifie $MX = 0$, et on cherche X sous la forme $X = RY$. Le vecteur Y étant dans le noyau de MR est de la forme ${}^t\begin{pmatrix} 0 & 0 & \alpha & \beta & 1 \end{pmatrix}$ où α et β sont des paramètres réels ; la solution demandée est donc :

$$X = \alpha {}^t\begin{pmatrix} -1 & -6 & 1 & 0 & O \end{pmatrix} + \beta {}^t\begin{pmatrix} 6 & 58 & 0 & -8 & 0 \end{pmatrix} + {}^t\begin{pmatrix} 34 & -575 & 0 & 63 & 1 \end{pmatrix}$$

(somme de la solution générale de l'équation sans second membre et d'une solution particulière).

Structure des groupes abéliens finis

Solution de l'exercice (??) Les groupes abéliens d'ordre $8 = 2^3$, à isomorphismes prés, sont en bijection (cf. la proposition (**??**)) avec les suites $0 < a_1 \leq a_2 \leq \cdots \leq a_r$ telles que $a_1 + \cdots + a_r = 3$: à une telle suite on associe alors $\mathbf{Z}/2^{a_1}\mathbf{Z} \times \cdots \mathbf{Z}/2^{a_r}\mathbf{Z}$. On trouve alors : $3 = 1 + 2 = 1 + 1 + 1$ soit les groupes $\mathbf{Z}/2^3\mathbf{Z}$, $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2^2\mathbf{Z}$ et $(\mathbf{Z}/2\mathbf{Z})^3$.

Solution de l'exercice (??)

(i) On a $72 = 2^3 3^2$ et donc $G = G(2) \times G(3)$ pour un groupe G d'ordre72. D'après la remarque **??**, il y a trois possibilités pour $G(2)$: $(\mathbf{Z}/2\mathbf{Z})^3$, $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$, $\mathbf{Z}/8\mathbf{Z}$ correspondant respectivement aux suites $(1,1,1)$, $(1,2)$ (3), et deux pour $G(3)$: $(\mathbf{Z}/3\mathbf{Z})^2$ et $\mathbf{Z}/9\mathbf{Z}$ (correspondant aux suites $(1,1)$ et (2)), ce qui donne au total 6 possibilités pour G.
(ii) On fait comme dans l'exemple **??**, ce qui donne immédiatement :

$$\begin{array}{rcl}
(\mathbf{Z}/2\mathbf{Z})^3 \times (\mathbf{Z}/3\mathbf{Z})^2 & \simeq & \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/6\mathbf{Z} \times \mathbf{Z}/6\mathbf{Z} \\
(\mathbf{Z}/2\mathbf{Z})^3 \times \mathbf{Z}/9\mathbf{Z} & \simeq & \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/18\mathbf{Z} \\
\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z} \times (\mathbf{Z}/3\mathbf{Z})^2 & \simeq & \mathbf{Z}/6\mathbf{Z} \times \mathbf{Z}/12\mathbf{Z} \\
\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/9\mathbf{Z} & \simeq & \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/36\mathbf{Z} \\
\mathbf{Z}/8\mathbf{Z} \times (\mathbf{Z}/3\mathbf{Z})^2 & \simeq & \mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/24\mathbf{Z} \\
\mathbf{Z}/8\mathbf{Z} \times \mathbf{Z}/9\mathbf{Z} & \simeq & \mathbf{Z}/72\mathbf{Z}
\end{array}$$

Solution de l'exercice (??) On fait comme dans le cours (exemple **??**). On a ainsi :

$$\begin{array}{rcl}
M(2) & = & \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \\
M(3) & = & \mathbf{Z}/9\mathbf{Z} \times \mathbf{Z}/9\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z} \\
M(5) & = & \mathbf{Z}/5\mathbf{Z}.
\end{array}$$

Les facteurs invariants s'obtiennent en lisant ce tableau par colonnes (en commençant par la dernière), d'où :

$$a_1 = 2,\ a_2 = 4 \times 3,\ a_3 = 4 \times 9,\ a_4 = 4 \times 9 \times 5$$

Solution de l'exercice (??) On utilise la remarque **??**.
Si G est d'ordre $2^4 3^2 5$, on a pour $G(2)$ les possibilités :

$$\mathbf{Z}/2^4\mathbf{Z}, \quad \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2^3\mathbf{Z}, \quad (\mathbf{Z}/2^2\mathbf{Z})^2, \quad (\mathbf{Z}/2\mathbf{Z})^2 \times \mathbf{Z}/2^2\mathbf{Z} \quad (\mathbf{Z}/2\mathbf{Z})^4$$

pour $G(3)$:

$$\mathbf{Z}/3^2\mathbf{Z}, \quad (\mathbf{Z}/3\mathbf{Z})^2$$

et

$$G(5) = \mathbf{Z}/5\mathbf{Z}.$$

Pour chacune de ces solutions on construit $G = G(2) \times G(3) \times G(5)$ ce qui donne en tout 10 solutions.
Pour la détermination dans chaque cas des facteurs invariants, la technique est la même que dans l'exercice précédent.

Problèmes

Solution du problème (??)

(i) Le théorème de la base adaptée (cf. (**??**)) fournit une base $(f_1, \cdots, f_n)$ de $\mathbf{Z}^n$ ainsi que des entiers $1 < a_1 | \cdots | a_n \neq 0$ tels que $(a_1 f_1, \cdots, a_n f_n)$ soit une base de G. On obtient alors $\mathbf{Z}^n/G \simeq \mathbf{Z}/a_1\mathbf{Z} \times \cdots \times \mathbf{Z}/a_n\mathbf{Z}$ qui est donc fini de cardinal $a_1 \ldots a_n$.

(ii) D'après ce qui précède, on a $\mathrm{card}(\mathbf{Z}^n/G) = \prod_{i=1}^n a_i$ qui est donc égal à $\det M$.

(iii) Soit $M = \begin{pmatrix} 3 & 1 & 1 \\ 25 & 8 & 10 \\ 46 & 20 & 11 \end{pmatrix}$ de sorte que $M \begin{pmatrix} h_1 \\ h_2 \\ h_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$
Il existe alors (*cf.* (**??**)) des matrices $L, R \in GL_3(\mathbf{Z})$ telles que $M = L\,\mathrm{diag}(a_1, a_2, a_3)R$ avec $a_1|a_2|a_3$. En outre si on pose $\begin{pmatrix} h'_1 \\ h'_2 \\ h'_3 \end{pmatrix} := R \begin{pmatrix} h_1 \\ h_2 \\ h_3 \end{pmatrix}$, H est aussi engendré par h'_1, h'_2, h'_3 et l'équation

$$L\,\mathrm{diag}(a_1, a_2, a_3) \begin{pmatrix} h'_1 \\ h'_2 \\ h'_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

est équivalente à :

$$\begin{cases} a_1 h'_1 = 0 \\ a_2 h'_2 = 0 \\ a_3 h'_3 = 0 \end{cases}$$

et donc $H \simeq \mathbf{Z}/a_1\mathbf{Z} \times \mathbf{Z}/a_2\mathbf{Z} \times \mathbf{Z}/a_3\mathbf{Z}$, avec $a_1.a_2.a_3 = \det M$. L'énoncé nous suggère de simplement calculer $\det M$; on vérifie aisément qu'il est égal à -19 (cf. (iv) ci-après) comme annoncé. On obtient alors $a_1 = a_2 = 1$ et $a_3 = 19$.

De manière générale si la décomposition en facteurs premiers de $\det M$ ne fait apparaître aucune multiplicité (*i.e.* $p^2 \nmid \det M$ pour tout premier p),

alors tous les a_i sont égaux à 1 sauf le dernier égal à $\det M$ et le groupe quotient est alors cyclique.

(iv) Les étapes du calcul sont les suivantes :

1.
$$\begin{pmatrix} 3 & 1 & 1 \\ 25 & 8 & 10 \\ 46 & 20 & 11 \end{pmatrix} \begin{pmatrix} 0 & -1 & 0 \\ 1 & 3 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 \\ 8 & -1 & 10 \\ 20 & 14 & 11 \end{pmatrix}$$

2.
$$\begin{pmatrix} 1 & 0 & 1 \\ 8 & -1 & 10 \\ 20 & 14 & 11 \end{pmatrix} \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 8 & -1 & 2 \\ 20 & 14 & -9 \end{pmatrix}$$

3.
$$\begin{pmatrix} 1 & 0 & 0 \\ 8 & -1 & 2 \\ 20 & 14 & -9 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & -2 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 8 & 1 & 0 \\ 20 & -14 & -19 \end{pmatrix}$$

(v) Le produit des trois matrices de $SL_2(\mathbf{R})$ ci-dessus est égale à :

$$\begin{pmatrix} 0 & 1 & 2 \\ 1 & -3 & -5 \\ 0 & 0 & -1 \end{pmatrix}.$$

On a $\begin{pmatrix} h'_1 \\ h'_2 \\ h'_3 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 2 \\ 1 & -3 & -5 \\ 0 & 0 & -1 \end{pmatrix} \begin{pmatrix} h_1 \\ h_2 \\ h_3 \end{pmatrix}$ ce qui s'inverse facilement : $h_3 = h'_3$, $h_2 + 2h_3 = h'_1$ soit $h_2 = h'_1 - 2h'_3$ et $h_1 - 3h_2 - 5h_3 = h'_2$ soit $h_1 = 3h'_1 + h'_2 - h'_3$. Comme $\phi(h'_1) = \phi(h'_2) = 0$ et $\phi(h'_3) = 1$, on obtient $\phi(h_1) = -1$, $\phi(h_2) = -2$ et $\phi(h_3) = 1$.

Solution du problème (??)

(a) Considérons les deux morphismes de groupes suivants :

$$\begin{array}{ccc} (\mathbf{Z}/n\mathbf{Z})^* & \longrightarrow & \mathrm{Aut}(\mathbf{Z}/n\mathbf{Z}) \\ a & \longmapsto & k \mapsto ak \end{array}$$

$$\begin{array}{ccc} \mathrm{Aut}(\mathbf{Z}/n\mathbf{Z}) & \longrightarrow & (\mathbf{Z}/n\mathbf{Z})^* \\ \phi & \longmapsto & \phi(1) \end{array}$$

On vérifie aisément qu'ils sont inverses l'un de l'autre : ce sont donc des isomorphismes.

Remarque Un morphisme d'un groupe cyclique vers un groupe est caractérisé par la donnée de l'image d'un générateur.

(b) Le théorème chinois (cf. (**??**)) donne

$$\mathbf{Z}/n\mathbf{Z} \simeq \prod_{i=1}^{r} \mathbf{Z}/p_i^{\alpha_i}\mathbf{Z} \tag{1}$$

le résultat découle alors du fait que cet isomorphisme induit l'isomorphisme $\mathrm{Aut}(\mathbf{Z}/n\mathbf{Z}) \simeq \prod_{i=1}^{r} \mathrm{Aut}(\mathbf{Z}/p_i^{\alpha_i}\mathbf{Z})$. En effet soit $\phi \in \mathrm{Aut}(\mathbf{Z}/n\mathbf{Z})$; ϕ est caractérisé par $\phi(1)$. Par l'isomorphisme (**??**), 1 s'envoie sur $(1, \cdots, 1)$. Notons $e_i = (0, \cdots, 0, 1, 0, \cdots, 0)$, il suffit alors de montrer que $\phi(e_i)$ appartient au sous-groupe engendré par e_i. Or $p_i^{\alpha_i} e_i = 0$ donc $p_i^{\alpha_i}\phi(e_i) = 0$ de sorte que $\phi(e_i)$ est d'ordre une puissance de p_i, d'où le résultat.

(c) (i) On raisonne par récurrence : pour $k = 0$, $(1+p)^{p^0} = 1+p = 1+p^{0+1}$ et pour $k = 1$ par la formule du binôme de Newton, on a $(1+p)^p = 1 + p^2 l_1$ avec $l_1 = (1 + p(p-1)/2 + \cdots + p^{p-2})$, soit $l_1 \equiv 1 \mod p$. Supposons donc le résultat vrai au rang k :

$$(1+p)^{p^{k+1}} = (1 + l_k p^{k+1})^p = 1 + l_{k+1} p^{k+2}$$

en posant $\begin{smallmatrix} l_{k+1} = l_k + p^k \sum_{\alpha=2}^{p} (\alpha \\ p) l_k^{\alpha} p^{(\alpha-2)(k+1)} \end{smallmatrix}$. Comme $k > 1$, on a $l_{k+1} \equiv l_k \mod p$.

Ainsi $(1+p)^{p^{\alpha-1}} \equiv 1 \mod p^\alpha$ de sorte que l'ordre de $(1+p)$ dans $(\mathbf{Z}/p^\alpha\mathbf{Z})^*$ divise $p^{\alpha-1}$ et donc de la forme p^k pour $k \leq \alpha - 1$. En outre on a $(1+p)^{p^k} = 1 + l_k p^{k+1}$ avec l_k non divisible par p; en particulier $(1+p)^{p^{\alpha-2}} \not\equiv 1 \mod p^\alpha$, de sorte que l'ordre de $1+p$ est $p^{\alpha-1}$.

(ii) $(\mathbf{Z}/p\mathbf{Z})^*$ est un groupe abélien fini, il est donc isomorphe (*cf.* la proposition (**??**)) à un produit de la forme $\mathbf{Z}/a_1\mathbf{Z} \times \cdots \times \mathbf{Z}/a_r\mathbf{Z}$ avec $1 < a_1 | \cdots | a_r \neq 0$ et $p - 1 = \prod_{i=1}^{r} a_i$. On en déduit alors que pour tout $x \in (\mathbf{Z}/p\mathbf{Z})^*$, on a $x^{a_r} = 1$; or par ailleurs dans un corps commutatif, l'équation $X^{a_r} - 1 = 0$ a au plus a_r solutions soit donc $p - 1 = \prod_{i=1}^{r} a_i \leq a_r$ et donc $r = 1$ et $a_r = p - 1$ soit $(\mathbf{Z}/p\mathbf{Z})^*$ est cyclique d'ordre $p - 1$.

(iii) Le morphisme ψ est clairement surjectif. Soit donc y un antécédent d'un générateur h de $(\mathbf{Z}/p\mathbf{Z})^*$; l'ordre m de y est alors un multiple de $p-1$ (car $1 = \psi(y^m) = h^m$): $m = (p-1)k$, de sorte que $x = y^k$ est d'ordre $p - 1$.
Remarque Comme le noyau de ψ est le groupe engendré par $(1+p)$, $\psi(x)$ est encore un générateur de $(\mathbf{Z}/p\mathbf{Z})^*$.

(iv) Le groupe $(\mathbf{Z}/p^\alpha\mathbf{Z})^*$ est abélien et donc de la forme $\mathbf{Z}/a_1\mathbf{Z} \times \cdots \times \mathbf{Z}/a_r\mathbf{Z}$ avec $1 < a_1 | \cdots | a_r \neq 0$ et $p^{\alpha-1}(p-1) = \prod_{i=1}^{r} a_i$. Tout élément a alors un ordre divisant a_r ce qui d'après (ii) et (iii) implique $p^{\alpha-1}$ et $p - 1$

divisent a_i et donc comme $p \wedge (p-1) = 1$, a_r est divisible par leur produit, soit donc $r = 1$ et $(\mathbf{Z}/p^\alpha\mathbf{Z})^*$ est cyclique.

Posons $u = (1+p)x$ et soit m son ordre; $1 = \psi(u^m) = \psi(u)^m = \psi(x)^m$, soit $p-1$ divise m et donc $u^m = (1+p)^m$ soit $p^{\alpha-1}$ divise m. En outre $u^{(p-1)p^{\alpha-1}} = 1$ et donc u est un générateur de $(\mathbf{Z}/p^\alpha\mathbf{Z})^*$. On construit alors un isomorphisme $\mathbf{Z}/p^{\alpha-1}(p-1)\mathbf{Z} \longmapsto (\mathbf{Z}/p^\alpha\mathbf{Z})^*$ en envoyant 1 sur u.

(v) On a $g^{p-1} = 1 + pl$ avec $l \neq 0 \mod p$; notons d l'ordre de g qui est un multiple de $p-1$ et un diviseur de $\phi(p^\alpha) = p^{\alpha-1}(p-1)$ soit $d = (p-1)p^e$ avec $0 \leq e < \alpha$ car p est premier avec $p-1$. Par une récurrence comme dans (i), on obtient $(1+pl)^{p^e} = 1 + \mu p^{e+1}$ avec p ne divisant pas μ de sorte que $g^d = 1 \mod p$ si et seulement si $e = \alpha - 1$ et donc g générateur.

Supposons donc $g^{p-1} \equiv 1 \mod p^2$. On remarque que $\psi(g+p) = \psi(g)$ est générateur, il suffit donc de montrer que $(g+p)^{p-1} \neq 1 \mod p^2$. Or on a

$$(g+p)^{p-1} \equiv g^{p-1} + (p-1)g^{p-2}p \equiv 1 - pg^{p-2} \mod p^2$$

et g^{p-2} est inversible dans $\mathbf{Z}/p^2\mathbf{Z}$ (d'inverse g) de sorte que $pg^{p-2} \not\equiv 0 \mod p^2$, d'où le résultat.

(d) (i) On a de manière directe $(\mathbf{Z}/2\mathbf{Z})^* = \{1\}$ et $(\mathbf{Z}/4\mathbf{Z})^* = \{1, -1\} \simeq \mathbf{Z}/2\mathbf{Z}$.

(ii) On raisonne à nouveau par récurrence, les cas $k = 0$ et $k = 1$ étant directs. Supposons donc que $5^{2^k} = 1 + l_k 2^{k+2}$ avec l_k impair. On a alors $5^{2^{k+1}} = (1 + l_k 2^{k+2})^2 = 1 + 2^{k+3}(l_k + 2^{k+1}l_k^2)$ d'où le résultat en posant $l_{k+1} = l_k + l_k^2 2^{k+1} \equiv l_k \mod 2$. Comme précédemment, on en déduit que 5 est d'ordre $2^{\alpha-2}$ dans $(\mathbf{Z}/2^\alpha\mathbf{Z})^*$.

(iii) Le groupe $(\mathbf{Z}/2^\alpha\mathbf{Z})^*$ en tant que groupe abélien fini est de la forme $\mathbf{Z}/2^{\alpha_1}\mathbf{Z} \times \cdots \times \mathbf{Z}/2^{\alpha_r}\mathbf{Z}$ avec $0 < \alpha_1 \leq \cdots \leq \alpha_r$ et $\sum_{i=1}^r \alpha_i = \alpha - 1$. Comme dans les questions précédentes, tout élément est alors d'ordre divisant 2^{α_r} ce qui, d'après (ii), impose $\alpha_r \geq \alpha - 2$. Restent alors deux possibilités pour les α_i à savoir $r = 2$ et $(\alpha_1, \alpha_2) = (1, \alpha - 2)$ ou bien $r = 1$ et $\alpha_1 = \alpha - 1$. Dans le premier cas on compte 3 éléments d'ordre 2 alors que dans le second on en compte qu'un. Reste donc à déterminer le nombre d'éléments d'ordre 2 de $(\mathbf{Z}/2^\alpha\mathbf{Z})^*$. Or on a vu que $\pm 5^{2^{\alpha-3}}$ et -1 étaient d'ordre 2 et ils ne peuvent pas être tous égaux car $-1 \neq 1$ si $\alpha \geq 2$ et $5 \neq \pm 1$ si $\alpha \geq 3$. On en déduit donc que $(\mathbf{Z}/2^\alpha\mathbf{Z})^*$ est isomorphe à $\mathbf{Z}/2^{\alpha-2}\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.

Remarque On peut aussi noter que -1 n'appartient pas au groupe multiplicatif engendré par 5 car ce dernier est exactement égal au noyau de la projection canonique $\phi : (\mathbf{Z}/2^\alpha\mathbf{Z})^* \longmapsto (\mathbf{Z}/4\mathbf{Z})^*$: il est clairement inclus dans le noyau et on conclut par l'égalité des cardinaux. Il suffit alors de voir que $\phi(-1) = -1 \neq 1$.

Construisons explicitement un tel isomorphisme $\bar{f} : \mathbf{Z}/2^{\alpha-2}\mathbf{Z}\times\mathbf{Z}/2\mathbf{Z} \longmapsto (\mathbf{Z}/2^{\alpha}\mathbf{Z})^*$. On définit tout d'abord $f : \mathbf{Z}^2 \longmapsto (\mathbf{Z}/2^{\alpha}\mathbf{Z})^*$ en posant $f((1,0)) = 5$ et $f((0,1)) = -1$. L'application f passe alors au quotient pour définir une application $\bar{f}$. Pour montrer que $\bar{f}$ est un isomorphisme, en vertu de l'égalité des cardinaux, il suffit de montrer qu'elle est injective ou qu'elle est surjective. Pour l'injectivité soit $(\bar{i},\bar{k}) \in \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2^{\alpha-2}\mathbf{Z}$ tel que $(-1)^i 5^k = 1$ soit $(-1)^i = 5^k$. Or d'après la remarque ci dessus -1 n'appartient pas au groupe engendré par 5 de sorte que $i \equiv 0 \mod 2$ et $5^k \equiv 1 \mod 2^{\alpha}$ soit $k \equiv 0 \mod 2^{\alpha-2}$ et donc $(\bar{i},\bar{k}) = (0,0)$.

Remarque Pour prouver la surjectivité directement, il suffit de remarquer que l'image de $\bar{f}$ contient le groupe engendré par 5 strictement car il contient -1 ce qui n'est pas le cas du groupe engendré par 5. On en déduit alors que le cardinal de cette image est divisible strictement par $2^{\alpha-2}$, car il contient strictement un groupe de cardinal $2^{\alpha-2}$, et divise $2^{\alpha-1}$ de sorte que ce dernier est égal à $2^{\alpha-1}$ et donc $\bar{f}$ est surjective.

(e) Pour $n = 2^{\alpha}\prod_{p\in\mathcal{P}} p^{\alpha_p}$ où $\mathcal{P}$ désigne l'ensemble des premiers impairs, le théorème chinois donne

$$(\mathbf{Z}/n\mathbf{Z})^* \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2^{\alpha-2}\mathbf{Z} \times \prod \mathbf{Z}/p^{\alpha_p-1}(p-1)\mathbf{Z}.$$

Pour que ce dernier soit cyclique il faut et il suffit que les nombres $2, 2^{\alpha-2}, p_i, p_i-1$ pour p_i premier impair divisant n, soient premiers entre eux deux à deux. On en déduit alors $n = 2, p^{\alpha_p}, 2p^{\alpha_p}$.