

ALGEBRE¹

Examen du 02 juin 2005

durée : 2 heures

Nota bene. Le barème (approximatif) est I : 2 pts, II : 9 pts et III : 9 pts. Les notes de cours sont autorisées. L'usage de tout autre document est interdit.

I.

- (1) Résoudre l'équation $x^2 = -\bar{1}$ dans $\mathbb{Z}/17\mathbb{Z}$.
 - (2) Montrer que l'équation $x^2 = -\bar{1}$ n'a pas de solution dans $\mathbb{Z}/7\mathbb{Z}$.
-

II. On considère les éléments suivants du groupe de permutation \mathbf{S}_4 : $\sigma_1 = (12)(34)$, $\sigma_2 = (13)(24)$, $\sigma_3 = (14)(23)$. On rappelle que e désigne l'élément neutre de (\mathbf{S}_4, \cdot) , autrement dit e est la bijection *identité*.

- (1) Déterminer l'ordre de chaque élément de $H := \{e, \sigma_1, \sigma_2, \sigma_3\}$.
 - (2) Montrer que H est un sous-groupe de \mathbf{S}_4 . (On pourra construire une table.) H est-il commutatif?
 - (3) Déterminer tous les sous-groupes de H . (Justifier votre réponse.)
 - (4) (a) Soit $f \in \mathbf{S}_4$. Montrer que
$$f \cdot (12)(34) \cdot f^{-1} = (f(1)f(2))(f(3)f(4)).$$
(b) Montrer que H est un sous-groupe *distingué* de \mathbf{S}_4 .
 - (5) Montrer que H est isomorphe à $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +)$. (On pourra construire un isomorphisme explicite entre H et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.)
-

III. On appelle A l'ensemble des matrices 2×2 à coefficients dans $\mathbb{Z}/3\mathbb{Z}$,

$$A = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z}/3\mathbb{Z} \right\}.$$

On munit A des lois $+$ et \cdot définies par

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} a + a' & b + b' \\ c + c' & d + d' \end{pmatrix}$$
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} a \cdot a' + b \cdot c' & a \cdot b' + b \cdot d' \\ c \cdot a' + d \cdot c' & c \cdot b' + d \cdot d' \end{pmatrix}$$

Par exemple, on a

$$\begin{pmatrix} \bar{0} & \bar{2} \\ \bar{1} & \bar{0} \end{pmatrix} + \begin{pmatrix} \bar{1} & \bar{2} \\ \bar{1} & \bar{1} \end{pmatrix} = \begin{pmatrix} \bar{1} & \bar{1} \\ \bar{2} & \bar{1} \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} \bar{2} & \bar{1} \\ \bar{1} & \bar{2} \end{pmatrix} \cdot \begin{pmatrix} \bar{2} & \bar{0} \\ \bar{1} & \bar{2} \end{pmatrix} = \begin{pmatrix} \bar{2} & \bar{2} \\ \bar{1} & \bar{1} \end{pmatrix}.$$

On remarquera que, formellement, ce sont exactement les mêmes règles de calculs que pour les matrices usuelles. Il faut cependant prendre garde que tous les coefficients sont des éléments de $\{\bar{0}, \bar{1}, \bar{2}\}$.

1. Licence de mathématiques (2-ième année), *Université Paul Sabatier (Toulouse III)*. Année scolaire 2003-2004

On **admet** que $(A, +, \cdot)$ est un anneau unitaire. On a

$$0_A = \begin{pmatrix} \bar{0} & \bar{0} \\ \bar{0} & \bar{0} \end{pmatrix} \quad \text{et} \quad 1_A = \begin{pmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{pmatrix}.$$

Nota Bene. Nous ne définissons pas d'application déterminant sur A . L'emploi d'une telle application dans l'exercice est interdit.

(1) Propriétés élémentaires de l'anneau A .

(a) Montrer que A contient 81 éléments.

(b) Soit $M = \begin{pmatrix} \bar{1} & \bar{1} \\ \bar{1} & \bar{1} \end{pmatrix}$. Vérifier que $M^3 = M$. A t-on $M \in A^*$?

(c) Montrer que A n'est pas intègre.

(2) On considère B le sous-ensemble de A formé des matrices de la forme $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ avec a, b quelconques dans $\mathbb{Z}/3\mathbb{Z}$.

(a) Montrer que B est un sous-anneau de $(A, +, \cdot)$.

(b) Donner la liste des éléments de B .

(c) Déterminer l'ensemble des couples $(a, b) \in (\mathbb{Z}/3\mathbb{Z})^2$ tels que $a^2 + b^2$ soit non inversible.

(d) Soient $a, b \in \mathbb{Z}/3\mathbb{Z}$. Calculer

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \cdot \begin{pmatrix} a & -b \\ b & a \end{pmatrix}.$$

(e) En déduire que B est un corps.

(f) Existe-t-il $n \in \mathbb{N}^*$ tel que B soit isomorphe à $\mathbb{Z}/n\mathbb{Z}$?

FIN