université de BORDEAUX	**Année universitaire 2016-2017** S1 DE PRINTEMPS **Parcours :** Mathématiques Fondamentales **Code UE :** Mathématiques et Informatique 4TMQ401 **Épreuve : Structures Algébriques 1** 4 mai 2017 : 14h30 (durée : 3h) *Documents interdits* Responsable de l'épreuve : Renaud Coulangeon	**Collège Sciences et Technologies**

L'épreuve se compose de cinq exercices indépendants. Toutes les réponses doivent être justifiées.

Exercice 1. On rappelle que pour tout entier naturel non nul n, l'ensemble $(\mathbb{Z}/n\mathbb{Z})^\times$ des éléments de l'anneau $\mathbb{Z}/n\mathbb{Z}$ qui sont inversibles pour la multiplication est un groupe, la loi de groupe étant induite par la multiplication de $\mathbb{Z}/n\mathbb{Z}$.

1. Soit n un entier naturel non nul. Montrer que pour tout entier naturel a les propriétés suivantes sont équivalentes :
   (a) a et n sont premiers entre eux,
   (b) la classe de a dans $\mathbb{Z}/n\mathbb{Z}$ est inversible pour la multiplication,
   (c) il existe un entier naturel non nul k tel que $a^k \equiv 1 \mod n$.

   (a)⇒(b) Si a et n sont premiers entre eux, alors il existe u et v dans $\mathbb{Z}$ tels que $au + bv = 1$ (Bézout), ce qui implique entre autres que la classe de a est inversible, d'inverse la classe de u.
   (b)⇒(c) Si la classe $\overline{a}$ de a dans $\mathbb{Z}/n\mathbb{Z}$ est inversible pour la multiplication, alors $\overline{a}$ appartient au groupe $(\mathbb{Z}/n\mathbb{Z})^\times$, qui est fini d'ordre $\varphi(n)$, moyennant quoi $\overline{a}^{\varphi(n)} = \overline{1}$, grâce au théorème de Lagrange.
   (c)⇒(a) Si $a^k \equiv 1 \mod n$ alors il existe un entier q tel que $a^k - 1 = qn$ ou autrement dit

   $$aa^{k-1} - qn = 1$$

   d'où l'on conclut que a et n sont premiers entre eux en vertu du théorème de Bézout.

2. Montrer que le groupe $(\mathbb{Z}/10\mathbb{Z})^\times$ est cyclique.

   Le groupe $(\mathbb{Z}/10\mathbb{Z})^\times$ est d'ordre $\varphi(10) = 4$ Pour prouver qu'il est cyclique, il suffit donc de trouver un élément d'ordre 4, ce qui est le cas, par exemple, de la classe de 3, comme le montre un calcul immédiat ($3^2 \equiv -1$ et $3^4 \equiv 1 \mod 10$).

3. Quel est le chiffre des unités du développement en base 10 de

   $$1234567^{1234567} \text{ ?}$$

   Il s'agit de déterminer la classe de $1234567^{1234567} \mod 10$. On remarque tout d'abord que $1234567 \equiv 7 \mod 10$ est inversible modulo 10, moyennant quoi $1234567^k \equiv 1, 7, 9$ ou 3 modulo 10 selon que k est congru à $0, 1, 2$ ou 3 modulo 4. On est ici dans le dernier cas, et le chiffre des unités de $1234567^{1234567}$ est donc égal à 3.

Exercice 2.

1. Si K est un corps, montrer qu'un polynôme $P(X) \in K[X]$ de degré 2 ou 3 est irréductible dans $K[X]$ si et seulement s'il n'a pas de racine dans K. Le résultat est-il vrai pour les polynômes de degré 4 ?

   Un polynôme P est *réductible* si et seulement si il est produit de deux polynômes A et B de degrés strictement positifs. Comme par ailleurs $\deg P = \deg A + \deg B$, les deux facteurs A et B ne peuvent pas être l'un et l'autre de degré ≥ 2 si $\deg P = 2$ ou 3. Par conséquent, un polynôme P de degré 2 ou 3 est réductible si et seulement si il admet un facteur $A = aX + b$ de degré 1 ($a \neq 0$), c'est-à-dire si et seulement si il admet une racine $x = -a^{-1}b$ dans K. Le résultat est faux pour les polynômes de degré 4 : par exemple, $X^4 + 1 = (X^2 - \sqrt{2}X + 1)(X^2 + \sqrt{2}X + 1)$ est réductible dans $\mathbb{R}[X]$ mais sans racine dans $\mathbb{R}$ (exemple vu en cours). Le polynôme $X^4 + X^2 + 1$ étudié à la question suivante fournit un autre exemple. Plus simplement encore, $(X^2 + 1)^2$ fournit un contre-exemple évident dans $\mathbb{R}[X]$.

2. Déterminer les racines dans $\mathbb{C}$ des polynômes $A = X^2 + X + 1$ et $B = X^4 + X^2 + 1$.

   Les racines de A dans $\mathbb{C}$ sont $j = e^{2i\pi/3}$ et $\bar{j} = j^2 = e^{4i\pi/3}$. Celles de B sont obtenues en remarquant que $B(X) = A(X^2)$, moyennant quoi

   $$x \text{ est racine de } B \Leftrightarrow x^2 \text{ est racine de } A.$$

   Les racines de B sont donc :

   $$j,\ j^2 = \bar{j},\ -j \text{ et } -j^2 = -\bar{j}.$$

3. En déduire la factorisation de A et B en produit de polynômes irréductibles respectivement dans $\mathbb{C}[X]$ et $\mathbb{R}[X]$.

   On a :

   $$\begin{aligned} A &= (X - j)(X - j^2) \text{ dans } \mathbb{C}[X] \\ &= X^2 + X + 1 \text{ dans } \mathbb{R}[X] \end{aligned}$$

   et

   $$\begin{aligned} A &= (X - j)(X - \bar{j})(X + j)(X + \bar{j}) \text{ dans } \mathbb{C}[X] \\ &= (X^2 + X + 1)(X^2 - X + 1) \text{ dans } \mathbb{R}[X]. \end{aligned}$$

4. Soit $K = \mathbb{Z}/2\mathbb{Z}$ le corps à deux éléments. Quelle est la factorisation en produits d'irréductibles dans $K[X]$ du polynôme $X^4 + X^2 + 1$?

   $X^4 + X^2 + 1 = (X^2 + X + 1)^2$ dans $K[X]$.

Exercice 3.

1. Quel est le plus petit entier naturel n tel qu'il existe un groupe non commutatif d'ordre n ? Justifiez votre réponse.

   Le groupe trivial réduit à un élément est évidemment commutatif. Les groupes d'ordre p premiers sont cycliques, donc également commutatifs. Si G est un groupe d'ordre 4, alors, soit il contient un élément d'ordre 4, auquel cas il est cyclique, donc commutatif, soit tous ses éléments, à part le neutre, sont d'ordre 2, auquel cas il est commutatif. La première valeur de n à tester est donc $n = 6$; or il existe bien un groupe non commutatif d'ordre 6, à savoir S_3.

2. Montrer que S_3 et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ ne sont pas isomorphes.

   L'un – $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ – est commutatif et l'autre pas, donc ces deux groupes ne sont pas isomorphes. Autre argument possible : $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ contient des éléments d'ordre 6 et pas S_3.

Exercice 4. Soient $R = \mathscr{M}_2(\mathbb{Z})$ l'anneau des matrices carrées de taille 2 à coefficients dans $\mathbb{Z}$. On note $R^\times$ l'ensemble de ses éléments inversibles pour la multiplication.

1. En considérant le produit d'une matrice $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ par sa comatrice $\widetilde{A} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$, établir l'équivalence
$$A \in R^\times \Leftrightarrow \det A = \pm 1.$$

   En utilisant l'identité
$$A\widetilde{A} = \widetilde{A}A = \begin{pmatrix} ad-bc & 0 \\ 0 & ad-bc \end{pmatrix}$$
   on conclut que si $ad - bc = 1$ (resp. -1) alors A est inversible dans R, d'inverse $\widetilde{A}$ (resp. $-\widetilde{A}$). Inversement, si A est inversible dans R, c'est-à-dire s'il existe $B \in R$ tel que $AB = BA = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, alors $\det A \det B = \det AB = \det \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1$, ce qui signifie que $\det A$ est inversible dans $\mathbb{Z}$, c'est-à-dire $\det A = \pm 1$.

2. Soit $S = \left\{ \begin{pmatrix} a & 2b \\ b & a \end{pmatrix} \in R \mid a \in \mathbb{Z}, b \in \mathbb{Z} \right\}$.

   (a) Montrer que S est un sous-anneau commutatif de R.

   - C'est un sous-groupe additif : si $\begin{pmatrix} a & 2b \\ b & a \end{pmatrix}$ et $\begin{pmatrix} a' & 2b' \\ b' & a' \end{pmatrix}$ appartiennent à S, alors leur différence
$$\begin{pmatrix} a & 2b \\ b & a \end{pmatrix} - \begin{pmatrix} a' & 2b' \\ b' & a' \end{pmatrix} = \begin{pmatrix} a-a' & 2(b-b') \\ b-b' & a-a' \end{pmatrix}$$
     également.
   - C'est une partie stable pour la multiplication à cause de l'égalité
$$\begin{pmatrix} a & 2b \\ b & a \end{pmatrix} \begin{pmatrix} a' & 2b' \\ b' & a' \end{pmatrix} = \begin{pmatrix} aa'+2bb' & 2(ab'+ba') \\ ab'+ba' & aa'+2bb' \end{pmatrix}.$$

- L'élément neutre multiplicatif $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ de R appartient à S.
- Le produit de deux éléments quelconques de S est commutatif :

$$\begin{pmatrix} a & 2b \\ b & a \end{pmatrix}\begin{pmatrix} a' & 2b' \\ b' & a' \end{pmatrix} = \begin{pmatrix} aa'+2bb' & 2(ab'+ba') \\ ab'+ba' & aa'+2bb' \end{pmatrix} = \begin{pmatrix} a' & 2b' \\ b' & a' \end{pmatrix}\begin{pmatrix} a & 2b \\ b & a \end{pmatrix}.$$

(b) Montrer que S est intègre [*on pourra utiliser la propriété de multiplicativité du déterminant*].
Si $AB = 0$ alors le produit $\det A \det B = \det AB$ est nul, ce qui, dans l'anneau intègre $\mathbb{Z}$, n'est possible que si $\det A$ ou $\det B$ est nul. Or le déterminant de $A = \begin{pmatrix} a & 2b \\ b & a \end{pmatrix}$ vaut $a^2 - 2b^2$, et l'équation $a^2 - 2b^2 = 0$ n'a dans $\mathbb{Z}^2$ que la solution triviale $(a,b) = (0,0)$, à cause de l'irrationalité de $\sqrt{2}$. La conclusion en découle.

(c) Soit

$$\begin{array}{rccl} \phi : & S & \longrightarrow & \mathbb{Z}/2\mathbb{Z} \\ & \begin{pmatrix} a & 2b \\ b & a \end{pmatrix} & \longmapsto & a \mod 2 \end{array}$$

Montrer que ϕ est un morphismes d'anneaux surjectif et que son noyau est un idéal engendré par un élément que l'on déterminera.
Il est immédiat de vérifier que ϕ est un morphisme d'anneau, grâce à la propriété $aa' + 2bb' \equiv aa' \mod 2$. La surjectivité est également claire : les classes de 0 et 1 modulo 2 sont les images respectives de la matrice nulle et de la matrice identité.
Le noyau de ϕ est constitué des matrices de la forme

$$\begin{pmatrix} 2a & 2b \\ b & 2a \end{pmatrix}$$

avec a et b dans $\mathbb{Z}$. Comme $\begin{pmatrix} 2a & 2b \\ b & 2a \end{pmatrix} = \begin{pmatrix} b & 2a \\ a & b \end{pmatrix}\begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$, c'est donc l'idéal engendré par la matrice $\begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$.

Exercice 5. On note S_3 le groupe des permutations de l'ensemble $\{1,2,3\}$. Soit $\mathscr{B} = (e_1, e_2, e_3)$ la base canonique de $\mathbb{R}^3$. Pour tout $\sigma \in S_3$ et tout $x = x_1e_1 + x_2e_2 + x_3e_3 \in \mathbb{R}^3$, on pose

$$\sigma \cdot x = x_1 e_{\sigma(1)} + x_2 e_{\sigma(2)} + x_3 e_{\sigma(3)} \tag{1}$$

1. Montrer que ceci définit une action à gauche du groupe S_3 sur l'ensemble $\mathbb{R}^3$.
Pour tout $x = x_1e_1 + x_2e_2 + x_3e_3 \in \mathbb{R}^3$, et tous $(\sigma, \tau) \in S_3$, on a

$$\tau \cdot (\sigma \cdot x) = \tau \cdot (x_1 e_{\sigma(1)} + x_2 e_{\sigma(2)} + x_3 e_{\sigma(3)}) = x_1 e_{\tau\sigma(1)} + x_2 e_{\tau\sigma(2)} + x_3 e_{\tau\sigma(3)} = \tau\sigma \cdot x.$$

Comme par ailleurs $\mathrm{Id} \cdot x = x$ pour tout $x \in \mathbb{R}^3$, on a bien une action de S_3 sur $\mathbb{R}^3$.

2. Une action d'un groupe G sur un ensemble E non vide est dite *transitive* si elle possède une seule orbite, c'est-à-dire si

$$\forall (x,y) \in E \times E,\ \exists g \in G \mid g \cdot x = y$$

Est-ce le cas de l'action (1) ci-dessus ?

L'action étudiée n'est pas transitive : par exemple l'orbite du vecteur $e_1+e_2+e_3$ est réduite à un élément.

3. Déterminer l'ensemble des points fixes pour cette action, c'est-à-dire l'ensemble des éléments $x = x_1e_1 + x_2e_2 + x_3e_3$ de $\mathbb{R}^3$ qui sont tels que $\sigma \cdot x = x$ pour tout σ dans S_3.

   Un vecteur $x = x_1e_1 + x_2e_2 + x_3e_3$ de $\mathbb{R}^3$ est fixe par l'action considérée si et seulement si toutes ses composantes sont égales, c'est-à-dire ssi il appartient à la droite engendrée par $e_1+e_2+e_3$.

4. Plus généralement, déterminer le stabilisateur d'un élément $x = x_1e_1 + x_2e_2 + x_3e_3$ de $\mathbb{R}^3$ ainsi que le cardinal de son orbite sous cette action [*il y a plusieurs cas à distinguer*].

   Il y a trois cas à considérer :

   - si les trois composantes de x sont distinctes, son stabilisateur est réduit à Id, et le cardinal de son orbite vaut $6 = |S_3|$.
   - si les trois composantes de x sont égales, alors son stabilisateur est égal à S_3 tout entier et le cardinal de son orbite vaut 1.
   - si 2 des 3 composantes de x sont égales, la troisième étant distincte, alors le stabilisateur de x est constitué des permutations stabilisant l'indice de cette troisième composante. Autrement dit, si $x = a(e_i + e_j) + be_k$ avec $a \neq b$, alors le stabilisateur de x est égal au sous-groupe d'ordre 2 engendré par la transposition $(i\ j)$ et le cardinal de son orbite vaut $\dfrac{|S_3|}{2} = 3$.