Université de Tours **L3 2017-2018**

Contrôle Continu terminal de l'UE 5.3 Algèbre

Jeudi 11 Janvier 2018

Les notations sont celles du cours. Documents et matériels électroniques interdits.

Durée : 3h

Questions brèves :

1) Parmi les ensembles ci-dessous, indiquez (et justifiez) lesquels sont des sous-groupes de $G = \mathbb{G}L_2(\mathbb{R})$ et parmi ceux-ci lesquels sont distingués dans G ?

$$F = \{M \in \mathbb{M}_2(\mathbb{R}), M = \begin{bmatrix} a & b \\ b & a \end{bmatrix}, a^2 - b^2 \neq 0\},\ H = \{M \in \mathbb{M}_2(\mathbb{R}), M = \begin{bmatrix} \lambda & 0 \\ 0 & \lambda \end{bmatrix}, \lambda > 0\},$$

$$S = \{M \in \mathbb{M}_2(\mathbb{R}) /\ {}^tM = M, \det(M) = 1\}.$$

2) Quel est l'ordre maximal d'un élément de $\mathfrak{S}_7$? Justifiez votre réponse.

3) Etablir que le polynôme $X^2 + X + 1$ n'a pas de racine dans $\mathbb{Z}/5\mathbb{Z}$. Qu'en déduit-on en terme d'irréductibilité pour ce polynôme dans $\mathbb{Z}/5\mathbb{Z}[X]$? Argumentez en précisant le résultat utilisé.

Exercice 1

Pour tout entier $n \geq 1$, on considère les ensembles C_n où $C_n := \{z \in \mathbb{C} \mid z^n = 1\}$ est l'ensemble des racines $n-$ièmes de l'unité.

1) Redémontrer brièvement que C_n est un sous-groupe du groupe multiplicatif $\mathbb{C}^*$.

2) a) Etablir que l'application $f(z) = z^3$ définit un morphisme entre les groupes C_6 et C_2.

b) En déduire que C_6/C_3 est isomorphe au groupe C_2.

3) Démontrer que si m et n sont deux entiers naturels non nuls , le groupe C_{mn}/C_n est isomorphe au groupe C_m.

Exercice 2

Soit p un nombre premier, $p > 3$. On note $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ et $\mathbb{M}(2, \mathbb{F}_p)$ l'anneau des matrices 2×2 à coefficients dans $\mathbb{F}_p$. Soient $I, J \in \mathbb{M}(2, \mathbb{F}_p)$ les matrices

$$I = \begin{bmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{bmatrix} J = \begin{bmatrix} \bar{0} & \bar{3} \\ \bar{1} & \bar{0} \end{bmatrix}.$$

Soit A l'ensemble des matrices $x\,I + y\,J = \begin{bmatrix} x & \bar{3}y \\ y & x \end{bmatrix}$, pour $x, y \in \mathbb{F}_p$.

1. Montrer que $(A, +\times)$ est un sous-anneau de $M(2, \mathbb{F}_p)$. Combien y-a-t-il d'éléments dans A ?
2. Soit $M = x\,I + y\,J \in A$. Montrer que M est inversible si et seulement si $x^2 - \bar{3}y^2$ est non nul dans $\mathbb{F}_p$. Dans ce cas donnez l'inverse de M en fonction de w inverse de $x^2 - \bar{3}y^2$ dans $\mathbb{F}_p$.
3. Supposons que l'équation $z^2 = \bar{3}$ n'admet pas de solution z dans $\mathbb{F}_p$. Montrer que A est un corps.
   En déduire qu'on a $M^{p^2-1} = I$ pour tout élément $M \in A \setminus \{0\}$.
4. Dans la suite, on suppose que $p = 5$.
   a)Vérifier que l'équation $z^2 = \bar{3}$ n'admet pas de solution z dans $\mathbb{F}_5$. En déduire les valeurs possibles pour l'ordre d'une matrice de $A \setminus \{0\}$.
   b) Déterminer les ordres des éléments $M \in A \setminus \{0\}$ de la forme $M = xI$.

Exercice 3

1) a) Un groupe à 11 éléments agit sur un ensemble X de cardinal 3. Etablir que toutes les orbites sont réduites à un élément.

b) Un groupe G à 33 éléments agit sur un ensemble X à 19 éléments. Démontrer qu'il y a nécessairement un point fixe sous l'action de G.

Dans tout ce qui suit G est un groupe à 33 éléments de neutre e.

2) a) Démontrer, en énonçant précisément le résultat utilisé, qu'il existe x et y tels que $o(x) = 3$ et $o(y) = 11$. On désigne dans la suite $H = < x >$ et $K = < y >$.

b) Démontrer que $H \cap K = \{e\}$.

3)a) Montrer que l'on définit une action de K sur l'ensemble des classes d'équivalences à gauche $X = (G/K)_g$ en posant pour tout $k \in K$ et $g \in G$, $k \bullet gK = (kg)K$.

b) Quel est le cardinal de X ? Déduire grâce à la question 1) que toutes les orbites sont réduites à une classe d'équivalence ie $\mathcal{O}_{gK} = \{gK\}$.

c) En déduire que K est distingué dans G ; on considèrera l'élément kgk' de kgK.

3) a) Trouver tous les automorphismes du groupe $(\mathbb{Z}/11\mathbb{Z}, +)$ et en déduire que le groupe des automorphismes de K, $\mathrm{Aut}(K)$, est isomorphe à $\mathbb{U}(\mathbb{Z}/11\mathbb{Z}) = (\mathbb{Z}/11\mathbb{Z})^*$.

b) Quels sont les ordres possibles des éléments de $(\mathbb{Z}/11\mathbb{Z})^*$? Montrer qu'il est cyclique en montrant, avec un minimum d'étapes, que $o(\overline{2}) = 10$.

4) On considère α_x l'automorphisme intérieur associé à un générateur x de H. Etablir que $o(\alpha_x)$ dans $\mathrm{Aut}(K)$ divise 3 puis que $\alpha_x = Id$ sur K.

5) En déduire que x et y commutent et que G est commutatif car cyclique.

Exercice 4 (voir Exercice de cours)

On désigne par $\mathcal{P}$ le demi-plan complexe $\mathcal{P} = \{z \in \mathbb{C}$ tels que $\mathrm{Im}(z) > 0\}$.

1. Etablir que l'ensemble $SL_2(\mathbb{Z}) = \{M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} / ad - bc = 1\}$ est un sous-groupe distingué du groupe des matrices inversibles à coefficients entiers $GL_2(\mathbb{Z})$.
2. A chaque matrice $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ de $SL_2(\mathbb{Z})$, on associe la transformation f_M de $\mathcal{P}$ dans $\mathbb{C}$ en posant $f_M(z) = \frac{az+b}{cz+d}$
   (a) Déterminer les réels X et Y de sorte que $f(z) = \frac{1}{|cz+d|^2}(X + iY)$ et en déduire que f est bien définie et que pour tout $z \in \mathcal{P}$, $f_M(z) \in \mathcal{P}$.
   (b) Démontrer que pour tout couple de matrices (M, N) de $SL_2(\mathbb{Z})$, $f_M \circ f_N = f_{MN}$.
   (c) En déduire que f_M est une bijection de $\mathcal{P}$ dans $\mathcal{P}$.
3. On considère l'application $\psi : SL_2(\mathbb{Z}) \mapsto \mathfrak{S}(\mathcal{P})$ ($\mathfrak{S}(\mathcal{P})$ est l'ensemble des bijections de $\mathcal{P}$ dans $\mathcal{P}$) définie par $\psi(M) = f_M$. Etablir que ψ est un morphisme et que $Ker(\psi) = \{\pm I_2\}$. A quel groupe $G = Im(\psi)$ est-il isomorphe ?
4. (a) Démontrer que l'on fait agir $SL_2(\mathbb{Z})$ sur $\mathcal{P}$ en posant $M \bullet z = f_M(z)$.
   (b) On note $U = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et H_U le sous-groupe de $SL_2(\mathbb{Z})$ engendré par U. Décrire H_U et montrer qu'il est d'ordre infini. A quel groupe est-il isomorphe ?
   (c) H_U agit sur $\mathcal{P}$ par l'action $\bullet$ ci-dessus . Déterminer l'orbite de $z \in \mathcal{P}$ (on demande une figure) . Cette action est-elle transitive ?