N1MA4M11 Algèbre 3

Examen Session 2 du 22 Juin 2012

Durée 3h, documents interdits.

EXERCICE 1 Dans tout l'exercice, p et q sont deux nombres premiers impairs et distincts.

1. Soit K un corps, et soit $P(X) \in K[X]$ un polynôme non nul de degré d.
   (a) Montrez que, si $P(a) = 0$ avec $a \in K$, alors il existe $Q(X) \in K[X]$ tel que $P(X) = (X - a)Q(X)$.
   (b) Montrez que $P(X)$ a au plus d racines dans K (indication : procédez par récurrence sur d et utilisez la question précédente).
2. Montrez que l'application :
$$\begin{aligned} f : (\mathbb{Z}/p\mathbb{Z})^* &\to (\mathbb{Z}/p\mathbb{Z})^* \\ x &\mapsto x^2 \end{aligned}$$
   est un homomorphisme du groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^*$.
3. Montrez que $\mathrm{Ker}(f) = \{\pm 1\}$ et montrez que son image est un sous-groupe de $(\mathbb{Z}/p\mathbb{Z})^*$ d'ordre $(p-1)/2$ que nous noterons Q.
4. Montrez que les éléments de Q sont racines du polynôme $X^{(p-1)/2} - 1 \in (\mathbb{Z}/p\mathbb{Z})[X]$.
5. En déduire l'équivalence, pour $x \in (\mathbb{Z}/p\mathbb{Z})^*$:
$$x \in Q \iff x^{(p-1)/2} = 1.$$
6. Utilisez le résultat précédent pour déterminer si 2 est un carré dans $\mathbb{Z}/41\mathbb{Z}$.
7. Quel est l'ordre du groupe $(\mathbb{Z}/pq\mathbb{Z})^*$?
8. Montrez que le noyau de l'homomorphisme :
$$\begin{aligned} g : (\mathbb{Z}/pq\mathbb{Z})^* &\to (\mathbb{Z}/pq\mathbb{Z})^* \\ x &\mapsto x^2 \end{aligned}$$
   est d'ordre 4. (Indication : utilisez le théorème chinois).
9. Soit Q l'image de g ; montrez que Q est un groupe d'ordre $(p-1)(q-1)/4$.
10. En déduire l'équivalence, pour $x \in (\mathbb{Z}/pq\mathbb{Z})^*$:
$$x \in Q \iff \big(x^{(p-1)/2} = 1 \bmod p \quad \text{et} \quad x^{(q-1)/2} = 1 \bmod q\big).$$
11. Utilisez les questions précédentes pour déterminer si 2 est un carré modulo 1517.

EXERCICE 2 Dans cet exercice p est un nombre premier. On définit :

$$GL(2,p) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z}/p\mathbb{Z} \text{ et } ad - bc \neq 0 \right\}$$

$$SL(2,p) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z}/p\mathbb{Z} \text{ et } ad - bc = 1 \right\}$$

$$Z := \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} : a \in (\mathbb{Z}/p\mathbb{Z})^* \right\}$$

$$B := \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : a, b, d \in \mathbb{Z}/p\mathbb{Z} \text{ et } ad = 1 \right\}$$

$$U := \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{Z}/p\mathbb{Z} \right\} \qquad L := \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} : a, d \in \mathbb{Z}/p\mathbb{Z} \text{ et } ad = 1 \right\}.$$

1. Étant donné $(a,b) \in (\mathbb{Z}/p\mathbb{Z})^2$, $(a,b) \neq (0,0)$, montrez qu'il existe $p^2 - p$ vecteurs $(c,d) \in (\mathbb{Z}/p\mathbb{Z})^2$ tels que $\{(a,b),(c,d)\}$ forme une base du $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel $(\mathbb{Z}/p\mathbb{Z})^2$. En déduire que $GL(2,p)$ est un groupe d'ordre $(p^2-1)(p^2-p)$.
2. Montrez que Z est le centre de $GL(2,p)$ (indication : si M est dans le centre, M commute avec les matrices $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ et $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$).
3. En déduire que le quotient $PGL(2,p) := GL(2,p)/Z$ est un groupe d'ordre $p(p^2-1)$.
4. Montrez que l'application :
$$\begin{aligned} \det : GL(2,p) &\to (\mathbb{Z}/p\mathbb{Z})^* \\ M &\mapsto \det(M) \end{aligned}$$
est un homomorphisme de groupes et que $SL(2,p)$ est son noyau.
5. En déduire que $SL(2,p)$ est un sous-groupe distingué de $GL(2,p)$ d'ordre $p(p^2-1)$.
6. Montrez que B est un sous-groupe de $SL(2,p)$ et calculez son ordre.
7. Montrez que U est isomorphe au groupe $(\mathbb{Z}/p\mathbb{Z}, +)$ (indication : calculez le produit de deux éléments de U).
8. Montrez que L est un sous-groupe de B et montrez que L est isomorphe au groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^*$.
9. Montrez que U est distingué dans B (on pourra montrer que U est le noyau d'un homomorphisme de groupes à déterminer), que $L \cap U = \{\mathrm{Id}\}$ et que $B = \{MN : M \in U, N \in L\}$. (On dit que B est le produit semi-direct de U et L).
10. Dans cette question $p = 2$. Montrez que $|GL(2,2)| = 6$ et que l'action naturelle de $GL(2,2)$ sur l'ensemble $X = \{(1,0),(0,1),(1,1)\}$ par $M \cdot (a,b) = M\left(\begin{smallmatrix} a \\ b \end{smallmatrix}\right)$ induit un isomorphisme de $GL(2,2)$ sur le groupe des permutations S_3.
11. Dans cette question $p = 3$. Montrez que $|PGL(2,3)| = 24$, que $PGL(2,3)$ opère sur l'ensemble des quatre droites vectorielles de l'espace vectoriel $(\mathbb{Z}/3\mathbb{Z})^2$, et que cette action induit un isomorphisme de $PGL(2,3)$ sur le groupe des permutations S_4.