# N1MA4M11 Algèbre 3

## Examen du 11 mai 2012. Durée 3h, documents interdits.

$\boxed{1}$ Soit $\sigma \in S_{11}$ la permutation définie par :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 10 & 7 & 9 & 11 & 2 & 1 & 3 & 5 & 8 & 4 & 6 \end{pmatrix}$$

1. Décomposez $\sigma$ en produit de cycles à supports disjoints.
2. Calculez l'ordre de $\sigma$.
3. Calculez la signature de $\sigma$.
4. Calculez $\sigma^2$ et $\sigma^3$.
5. Calculez $\sigma^{-1}$.

$\boxed{2}$ Dans cet exercice $p$ est un nombre premier.

1. Montrez qu'un groupe d'ordre $p$ est nécessairement cyclique.
2. Dans cette question $G$ est un groupe commutatif d'ordre $p^2$ et son neutre est noté 1.
   (a) Montrez que, si $G$ n'est pas cyclique, alors tout élément de $G$ différent de 1 est d'ordre $p$.
   (b) On suppose que $G$ n'est pas cyclique. Soit $x \in G$, $x \neq 1$ et soit $y \in G$, $y \notin \langle x \rangle$. Montrez que l'application :

   $$\begin{array}{llll} f : & \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} & \to G \\ & (a\ ,\ b) & \mapsto x^a y^b \end{array}$$

   est un isomorphisme de groupes.
3. Dans cette question on démontre que le centre $Z(G)$ d'un groupe $G$ dont l'ordre est une puissance de $p$ est non trivial (i.e. non réduit à $\{1\}$). Pour cela, on considère l'action de $G$ sur lui-même par conjugaison, définie par :

   $$g \in G,\ x \in G,\ g \cdot x = gxg^{-1}.$$

   On rappelle que les orbites de $G$ pour cette action s'appellent les classes de conjugaison de $G$.
   (a) Rappelez la définition de $Z(G)$. En déduire que $x \in Z(G)$ si et seulement si son orbite $O_x = \{x\}$.
   (b) Rappelez la relation qui lie, pour $x \in G$, les cardinaux de $G$, du stabilisateur $G_x$ de $G$, et de l'orbite $O_x$ de $x$. En déduire que, pour tout $x \in G$, $|O_x|$ est une puissance de $p$.
   (c) Utilisez l'équation aux classes pour montrer que $|Z(G)| > 1$.

4. Dans cette question on montre qu'un groupe d'ordre $p^2$ est toujours commutatif. On suppose par l'absurde que $G$ est un groupe d'ordre $p^2$ non commutatif.
   (a) Utilisez la question 3. pour montrer que $|Z(G)| = p$.
   (b) Montrez que $Z(G)$ est un sous-groupe distingué de $G$ et que le groupe quotient $G/Z(G)$ est cyclique.
   (c) En déduire qu'il existe $y \in G$ tel que
   $$G = Z(G) \cup Z(G)y \cup Z(G)y^2 \cup \cdots \cup Z(G)y^{p-1}$$
   puis que $G$ est commutatif. Conclure.
5. Dans cette question, $G$ est un groupe d'ordre $p^3$ non commutatif.
   (a) Procédez comme dans la question 4. pour montrer que $|Z(G)| \neq p^2$. En déduire que $|Z(G)| = p$.
   (b) On considère à nouveau l'action de $G$ sur lui-même par conjugaison ; montrez que, si $x \notin Z(G)$, $|G_x| = p^2$ (indication : on pourra remarquer que $x \in G_x$).
   (c) En utilisant l'équation aux classes, montrez que le nombre de classes de conjugaisons de $G$ est $p^2 + p - 1$.

$\boxed{3}$ Soit $P(X) = X^2 - 2 \in \mathbb{Z}/5\mathbb{Z}[X]$ et $K = \mathbb{Z}/5\mathbb{Z}[X]/(P(X))$.

1. Montrez que $P(X)$ est un polynôme irréductible de $\mathbb{Z}/5\mathbb{Z}[X]$. Montrez que $K$ est un corps.
2. Soit $\alpha = X \bmod P(X) \in K$. Montrez que
   $$K = \{a\alpha + b : a, b \in \mathbb{Z}/5\mathbb{Z}\}.$$
   En déduire le cardinal de $K$ ainsi que l'ordre de son groupe multiplicatif $K^*$.
3. Montrez que $\alpha$ est d'ordre 8 dans $K^*$.
4. Montrez que $(1 + \alpha)$ est d'ordre 12 dans $K^*$.
5. En déduire que $\beta := \alpha + 2$ est d'ordre 24 dans $K^*$.
6. En déduire que $K^*$ est cyclique. Quel est le nombre de ses générateurs ?