**L3 Mathématiques**

**Epreuve du 3 Février 2006**

*Les téléphones portables et les calculettes sont interdits*

Les exercices ne sont pas classés par ordre de difficulté croissante, si $p$ désigne un nombre premier on rappelle que $\mathbf{Z}/p\mathbf{Z}$ et $\mathbf{F}_p$ désignent le même objet.

**1.1.** Décrire toutes les classes de conjugaison des groupes symétriques $\mathcal{S}_4$ et $\mathcal{S}_5$. On donnera le nombre d'éléments de chacune de ces classes. (Remarque : la description des classes de conjugaison est une question de cours on ne demande pas de faire la démonstration mais seulement d'énoncer le résultat). Donner à chaque fois un exemple d'élément dans la classe.
**1.2.** Soit $f$ un automorphisme de $\mathcal{S}_4$. Démontrer que l'image d'une classe de conjugaison de $\mathcal{S}_4$ par $f$ est une classe de conjugaison de $\mathcal{S}_4$. Montrer que l'image d'une transposition par $f$ est une transposition. On pourra utiliser le fait que si $x$ est d'ordre $k$, $f(x)$ est aussi d'ordre $k$.
**1.3.** Faire le même exercice pour $\mathcal{S}_5$.
Puis montrer que le groupe $\mathcal{S}_6$ contient une classe de conjugaison, dont les éléments sont d'ordre 2, qui est distincte de la classe des transpositions, et qui a autant d'éléments que cette dernière classe. (Cette sous-question est hors barème).

Cet exercice a été détaillé dans des notes précédentes. Voici quelques éléments pour la correction. D'abord si on a un homomorphisme $f$ d'un groupe $G$ dans un groupe $H$ un élément conjugué à $x \in G$ est envoyé sur un élément conjugué à $f(x) \in H$. Donc la classe de conjugaison de $x$ est envoyée sur un sous-ensemble de la classe de conjugaison de $f(x)$. Maintenant si $G = H$ et si $f$ est un isomorphisme on peut appliquer la même remarque à $f^{-1}$ et $f(x)$ d'où on déduit que la classe de conjugaison de de $f(x)$ est envoyée par $f^{-1}$ sur un sous-ensemble de la classe de conjugaison de $x$. Donc si $G = H$ et $f$ est un isomorphisme on en déduit que la classe de conjugaison de $x$ est envoyée bijectivement sur celle de $f(x)$.
De plus on sait que si $x$ est d'ordre $k$ et si $f$ est un isomorphisme $f(x)$ est d'ordre $k$.
Donc si $f$ est un isomorphisme de $\mathcal{S}_n$ ($n$ quelconque), et $\tau$ une transipostion on sait que $f(\tau)$ est d'ordre 2. Mais on ne sait pas tout de suite que $f(\tau)$ est une transposition. Par contre on sait que le cardinal de la classe de conjugaison de $f(x)$ est le même que celui de celle de $x$. Or si $n = 4$ il y a 6 transpositions, les seuls éléments d'ordre 2 par ailleurs sont les produits de transpositions à supports disjoints, il y en a 3, ils forment une classe de conjugaison. Il est donc impossible que que $f(\tau)$ soit de cette forme, donc c'est une transposition puis que c'est un élément d'ordre 2.
Pour $n = 5$ l'argument est identique, il y a cette fois ci 10 transpositions et 15 produits de deux transpostions à supports disjoints (seuls éléments d'ordre 2 à part les transpositions).

Pour $n = 6$ il y a 15 transpostions et 15 produits de 3 transpositions à supports disjoints (exercice!). L'argument précédent est défaillant.

**2.1.** Donner la liste des polynômes irréductibles sur le corps $\mathbf{F}_3$ de degré inférieur ou égal à 2. Montrer que les polynômes $X^3 + 2X^2 + 1$, $X^3 + 2X^2 + X + 1$ sont irréductibles.

Cet exercice a été fait en cours. Rappelons qu'il fallait énoncer qu'en degré inférieur ou égal à 3 pour vérifier qu'un polynôme à coefficients dans un corps $L$ est irréductible il suffit de montrer qu'il n'a pas de racines dans le corps $L$. En l'occurence si $L = \mathbf{F}_3$ il suffit de considérer les racines potentielles $\bar{0}$, $\bar{1}$, $\bar{2}$.

**2.2.** Montrer que l'anneau quotient $L = \mathbf{F}_3[X]/(X^3 + 2X^2 + 1)$ est un corps.
Le poilynôme est irréductible, donc puisque $\mathbf{F}_3[X]$ est prinicipal, l'idéal qu'il engendre est maximal, donc le quotient est un corps.
Précisez son nombre d'éléments.
C'est le cardinal du corps, soit 3 dans ce cas, à la puissance le degré du polynôme, soit aussi 3 dans ce cas.
Soit $R \in \mathbf{F}_3[X]$ quelconque, montrer que si $a \in L$ est racine de $R$ il en est de même de $a^3$.

Soit $R = \sum_i \alpha_i X^i$, $\alpha_i \in \mathbf{F}_3$, on a $R(a) = \sum_i \alpha_i a^i = 0$. Mais puisque l'on est en caractéristique 3 on a $(\sum_i \alpha_i a^i)^3 = \sum_i \alpha_i^3 a^{3i} = 0$, comme $\alpha_i \in \mathbf{F}_3$ on a (Fermat) $\alpha_i^3 = \alpha_i$, donc $\sum_i \alpha_i a^{3i} = 0$. Le résultat suit.

Dans le corps $L$ trouver les racines de $Q = X^3+2X^2+X+1$ (on pourra calculer $Q(X-1)$).

Notant $a$ la classe de $X$ dans $L$ on vérifie par le calcul indiqué que $a - 1$ est racine, puis $a^3 - 1$ et $a^9 - 1$ que l'on écrit en fonction de 1, $a$, $a^2$.

Donner les valeurs possibles de l'ordre d'un élément dans le groupe multiplicatif des éléments non nuls (inversibles) de $L$. Puis chercher un générateur de ce groupe.

Le groupe MULTIPLICATIF des éléments non nuls à $26 = 27 - 1$ éléments. Les ordres possibles sont 1, 2, 13, 26, $a$ n'est pas d'ordre 1 ou 2, on vérifie que l'ordre n'est pas 1" en calculant $a^3 = a^2 - 1$ (hypothèse) puis $a^6 = -a^2 - a$, $a^9 = -a^2 - a - 1$, $a^4 = a^2 - a - 1$, $a^5 = -a - 1$... Donc l'ordre de $a$ est 26.

**3.** On admet dans la suite que l'anneau $\mathbf{Z}[i]$ des entiers de Gauss est euclidien donc principal.

Factoriser les entiers 3, 7, 11, 15, en éléments irréductibles (on utilisera des théorèmes du cours dans cette partie).

Voir cours.

**4.** Quel est l'ordre de 3 dans le groupe des éléments inversibles de $\mathbf{Z}/16\mathbf{Z}$? Quel est l'ordre de 4 dans le groupe des éléments inversibles de $\mathbf{Z}/27\mathbf{Z}$?

Attention il s'agit du groupe des éléments inversibles donc la loi est la MULTIPLICATION. Pour trouver le nombre d'éléments inversibles on utilise l'indicatrice d'Euler.
Il ya 8 éléments inversibles dans $\mathbf{Z}/16\mathbf{Z}$, 3 est d'ordre soit 1 (non), soit 2 (également non car $3^2 = 9$ n'est pas congruent à 1 mod 16), soit 4 oui car $3^4 = 81 = 16x5 + 1$ est congru à 1 mod 16.
Il y a 18 éléments inversibles dans $\mathbf{Z}/27\mathbf{Z}$. L'ordre de 4 n'est pas 1 ni 2 (16 n'est pas congru à 1 mod 27, ni 3 car $4^3 = 64$ est congru à 10 modulo 27, ni 6 (à vérifier). L'ordre est donc 9 ou 18, or $4^9$ est congru à $(4^3)^3$ soit $10^3$, soit $100X10$, soit $19X10$, soit 190 mod 3, soit 1 mod 3. L'ordre est 9.

**5.** Enoncer le petit théorème de Fermat.