UNIVERSITÉ DE PARIS 7 — **Samedi 9 décembre 2000**
Année 2000-2001, DEUG 2ème année — **8h30 – 11h30**
Groupes et arithmétique (MT282)

Partiel

L'utilisation de calculatrice, téléphone portable et de tout document est interdite.

Exercice 1

Le but de l'exercice est de déterminer tous les entiers k tels que $k^k - 3$ est divisible par 7.

1. Résoudre le système de congruences : $\begin{cases} x \equiv 3 & (mod\ 7) \\ x \equiv 1 & (mod\ 6) \end{cases}$
2. Quel est l'ensemble des éléments inversibles dans l'anneau $\mathbf{Z}/7\mathbf{Z}$? On note $(\mathbf{Z}/7\mathbf{Z})^\times$ cet ensemble.
3. Pour $x \in (\mathbf{Z}/7\mathbf{Z})^\times$, que vaut x^6 ?
4. Soient a et b les restes dans la division euclidienne de l'entier k respectivement par 7 et 6. On suppose que a est non nul. Montrer que $k^k \equiv a^b (mod\ 7)$.
5. Quels sont les entiers k tels que $k^k - 3$ est divisible par 7 ?

Exercice 2

On considère l'ensemble

$$\mathbf{Z}[\sqrt{7}] = \{a + b\sqrt{7} \mid (a,\, b) \in \mathbf{Z}\}$$

muni de l'addition et de la multiplication des réels.

1. Montrer que $(\mathbf{Z}[\sqrt{7}],\, +,\, *)$ est un sous-anneau de $\mathbf{R}$.
2. Montrer que l'application
$$t: \begin{array}{rcl} \mathbf{Z}[\sqrt{7}] & \longrightarrow & \mathbf{Z}[\sqrt{7}] \\ a + b\sqrt{7} & \longmapsto & a - b\sqrt{7} \end{array}$$
est un homomorphisme d'anneaux.
3. Montrer que l'élément $8 + 3\sqrt{7}$ est inversible dans $\mathbf{Z}[\sqrt{7}]$.
4. On note $(\mathbf{Z}[\sqrt{7}])^\times$ le groupe des éléments inversibles de $\mathbf{Z}[\sqrt{7}]$. Montrer que $8 + 3\sqrt{7}$ est d'ordre infini dans $(\mathbf{Z}[\sqrt{7}])^\times$.
5. Si $c \in \mathbf{Z}$, on note $\bar{c}$ sa classe dans $\mathbf{Z}/3\mathbf{Z}$. Montrer que l'application
$$f: \begin{array}{rcl} \mathbf{Z}[\sqrt{7}] & \longrightarrow & \mathbf{Z}/3\mathbf{Z} \\ a + b\sqrt{7} & \longmapsto & \overline{a + 2b} \end{array}$$
est un homomorphisme d'anneaux.

T.S.V.P.

Problème

Dans tout ce problème on considère un groupe fini $(G, \cdot)$, et un sous-groupe H de G. Si $x \in G$, on pose $xH = \{xh \mid h \in H\}$ et $xHx^{-1} = \{xhx^{-1} \mid h \in H\}$. Si X est un ensemble fini alors $|X|$ désigne le cardinal de X.

1. Montrer au moyen de bijections que $|xH| = |H| = |xHx^{-1}|$.

2. On rappelle que l'on a une relation d'équivalence $\mathcal{R}$ sur G définie par

$$\forall x, y \in G \qquad x\mathcal{R}y \iff y^{-1}x \in H.$$

   (a) Démontrer que xH est la classe d'équivalence de x pour la relation $\mathcal{R}$.

   (b) On note G/H l'ensemble quotient $G/\mathcal{R}$. Démontrer que

$$|G| = |G/H| \cdot |H|.$$

3. On définit le *normalisateur* de H dans G :

$$N_G(H) = \{x \in G \mid xHx^{-1} = H\}.$$

   (a) Montrer que $H \subset N_G(H)$, et que $N_G(H)$ est un sous-groupe de G.

   (b) Montrer que H est distingué dans $N_G(H)$.

   (c) Montrer que H est distingué dans G si et seulement si $N_G(H) = G$.

4. On suppose dans cette question que G/H est de cardinal 2. Le but de cette question est de montrer que H est alors distingué dans G.

   (a) Montrer que $|G/N_G(H)| \leq |G/H|$. Quelles valeurs peut donc prendre $|G/N_G(H)|$?

   (b) Supposons que $|G/N_G(H)| = 2$. Montrer que $H = N_G(H)$.

   (c) (On suppose toujours que $|G/N_G(H)| = 2$.) Montrer qu'il existe $g \in G$ tel que $G/H = \{H, gH\}$. Peut-on avoir $gHg^{-1} = H$?

   (d) (On suppose toujours que $|G/N_G(H)| = 2$.) Montrer que

$$gHg^{-1} \cap gH \neq \emptyset.$$

   En déduire que l'hypothèse $|G/N_G(H)| = 2$ est une absurdité.

   (e) Conclure.