# HX3 Mathématiques

# Devoir surveillé N$^o$2

Mercredi 12 octobre 2005

- Durée : 3 heures -

*On prendra bien soin de préciser toute notation non donnée dans l'énoncé. Toute affirmation devra être justifiée. Les récurrences ne sauraient être commencées sans une formulation claire de l'hypothèse de récurrence.*

*On laissera une marge à gauche.*

*Il est demandé de ne pas recopier l'énoncé, on mettra seulement en évidence les numéros des questions traitées. Il est recommandé par contre d'annoncer ce qui va être démontré et éventuellement par quel type de raisonnement (récurrence, absurde, contraposée...). Seules les conclusions et les résultats mis en valeur seront pris en compte.*

*Enfin, les solutions doivent être rédigées et le formalisme utilisé avec parcimonie.*

## Actions de groupes

Soient $G$ un groupe dont la loi est notée multiplicativement, 1 son élément neutre et $E$ un ensemble non vide. On dit qu'une application $\varphi$ :

$$\varphi : \begin{array}{ccc} G \times E & \longrightarrow & E \\ (g,x) & \longmapsto & g_\bullet x \end{array}$$

est une *opération du groupe $G$ sur l'ensemble $E$* si les deux conditions suivantes sont vérifiées :

1. Pour tout $(g,g') \in G^2$ et tout $x \in E$, $g_\bullet(g'_\bullet x) = (gg')_\bullet x$.
2. Pour tout $x \in E$, $1_\bullet x = x$.

On prendra bien garde de ne pas confondre le produit de deux éléments $g$ et $g'$ de $G$, que l'on notera par simple juxtaposition, avec l'opération de $G$ sur $E$ que l'on notera avec un point $g_\bullet x$ (notation préférée à celle avec $\varphi$ qui ne sera pas utilisée car elle est moins bien adaptée à la situation).

Soit $p \in \mathbb{N}$. $p$ est un *nombre premier* si $p \neq 0$, $p \neq 1$ et 1 et $p$ sont les seuls entiers naturels divisant $p$. On admettra que les seuls entiers naturels divisant $p^m$, ($m \geqslant 1$) sont 1, $p$, $p^2$,..., $p^m$.

Les parties **III.** et **IV.** sont indépendantes entre elles et doivent être traitées après une bonne étude des deux premières parties.

### I. Généralités :

Soient $G$ un groupe et $E$ un ensemble et une opération de $G$ sur $E$.

**1)** On note pour $g \in G$, $\gamma_g : x \in E \longmapsto \gamma_g(x) = g_\bullet x \in E$.

**a.** Montrer que pour tout $g \in G$, $\gamma_g$ est une permuation de $E$.

**b.** Montrer que

$$\gamma : \begin{array}{ccc} G & \longrightarrow & \mathcal{S}_E \\ g & \longmapsto & \gamma_g \end{array}$$

définit un morphisme de groupes.

Réciproquement, on notera sans plus de justifications que se donner un morphisme $\gamma$ de $G$ dans $\mathcal{S}_E$ revient à se donner une opération de groupe : pour $x \in E$ et $g \in G$, on pose $g_\bullet x = \gamma(g)(x)$.

**c.** Préciser ${\gamma_g}^{-1}$.

**2)** On se propose d'étudier dans cette question quelques exemples.

**a.** On suppose $G$ quelconque et $E = G$. Montrer qu'on définit une opération de $G$ sur lui-même en posant pour tout $(g, x) \in G^2$, $g_\bullet x = gx$. Cette opération s'appelle *translation à gauche*.

**b.** On suppose $G$ quelconque et $E = G$. Montrer qu'on définit une opération de $G$ sur lui-même en posant pour tout $(g, x) \in G^2$, $g_\bullet x = gxg^{-1}$. On dit alors que $G$ *opère sur lui-même par conjugaison*.

**c.** On prend $G = \mathcal{S}_n$ et $E = \{1, 2, \ldots, n\}$ avec $n \in \mathbb{N}^*$. Montrer qu'on définit une opération de $G$ sur $E$ en posant pour tout $\sigma \in G$ et tout $i \in E$, $\sigma_\bullet i = \sigma(i)$.

**3)** On reprend les notations de la question **1)**. On dit que l'opération de $G$ sur $E$ est *fidèle* si le morphisme $\gamma : G \longrightarrow \mathcal{S}_E$ est injectif.

**a.** Soit $G$ un groupe. Montrer que la translation à gauche est une opération fidèle de $G$ dans $G$ (cf **2) a.**).

**b.** En déduire le *théorème de Cayley* : "*tout groupe fini $G$ de cardinal $n$ est isomorphe à un sous-groupe de $\mathcal{S}_n$*".

**4)** Soit $n \geqslant 2$. Pour $f : \mathbb{Q}^n \longrightarrow \mathbb{Q}$ et $\sigma \in \mathcal{S}_n$, on pose

$$\sigma_\bullet f : (x_1, \ldots, x_n) \in \mathbb{Q}^n \longmapsto f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) \in \mathbb{Q}.$$

**a.** Montrer que l'on définit ainsi une action du groupe $\mathcal{S}_n$ sur l'ensemble des fonctions de $\mathbb{Q}^n$ dans $\mathbb{Q}$.

On considère l'application

$$\Delta : \begin{array}{ccc} \mathbb{Q}^n & \longrightarrow & \mathbb{Q} \\ (x_1, \ldots, x_n) & \longmapsto & \displaystyle\prod_{1 \leqslant i < j \leqslant n} (x_j - x_i) \end{array}.$$

**b.** Démontrer que si $\tau$ est la transposition $[k, n]$ avec $k < n$, alors $\tau_\bullet \Delta = -\Delta$.

**c.** En déduire par récurrence que $\tau_\bullet \Delta = -\Delta$ pour toute transposition $\tau$.

**d.** Démontrer à l'aide de la question précédente que si $\sigma \in \mathcal{S}_n$, la signature de $\sigma$ vaut

$$\varepsilon(\sigma) = \frac{\prod_{1 \leqslant i < j \leqslant n} (\sigma(j) - \sigma(i))}{\prod_{1 \leqslant i < j \leqslant n} (j - i)}.$$

## II. Equation aux classes :

Soit $G$ un groupe opérant sur un ensemble $E$.

**1)** On munit $E$ d'une relation binaire $\mathcal{R}$ définie pour tout $(x, y) \in E^2$ par : $x \,\mathcal{R}\, y$ si, et seulement s'il existe $g \in G$ tel que $y = g_\bullet x$.

**a.** Montrer que $\mathcal{R}$ est une relation d'équivalence.

La classe d'équivalence de $x \in E$ s'appelle *orbite de $x$ pour l'action de $G$* et sera noté $\Omega_x$.

**b.** Soit $H$ un sous-groupe de $G$. On fait opérer $H$ sur $G$ par translation à gauche : pour $h \in H$ et $x \in G$, $h_\bullet x = hx$. Décrire l'orbite de $a$ dans $G$. En déduire une démonstration du théorème de Lagrange : "*si $G$ est un groupe fini de cardinal $n$ et $H$ un sous-groupe de $G$ de cardinal $d$, alors $d$ divise $n$*".

**c .** Soient $n \in \mathbb{N}^*$, $\sigma \in \mathcal{S}_n$ et $H$ le sous-groupe de $\mathcal{S}_n$ engendré par $\sigma$. On considère l'opération de $H$ sur $E = \{1, 2, \ldots, n\}$ définie par $\tau_\bullet x = \tau(x)$ où $\tau \in H$ et $x \in E$. Quelle est l'orbite de $x \in E$ ?

**2)** On définit pour tout $x \in E$ le *stabilisateur de* $x$ : $G_x = \{g \in G,\ g_\bullet x = x\}$.

**a.** Montrer que si $x \in E$, $G_x$ est un sous-groupe de $G$.

**b.** Soient $(x, y) \in E$ et $g_0 \in G$ tel que $y = g_{0\bullet} x$. Montrer que $G_y = g_0 G_x g_0^{-1}$.

Soit $x \in E$. On note alors

$$F_x : \begin{array}{ccc} G & \longrightarrow & E \\ g & \longmapsto & g_\bullet x \end{array}$$

**c.** On considère la relation $\mathcal{S}_x$ définie par $g\mathcal{S}_x g' \iff F_x(g) = F_x(g')$ pour tout $(g, g') \in G^2$. Montrer qu'il s'agit d'une relation d'équivalence.

**d.** Montrer que la classe de $a \in G$ est $aG_x$.

**e.** Montrer que l'application $\overline{F_x}$ qui à $\omega = aG_x \in G/\mathcal{S}_x$ associe $a.x \in \Omega_x$ est bien définie.

**f.** Montrer que $\overline{F_x}$ est bijective.

**3)** On suppose $G$ fini.

**a.** Montrer que si $x$ et $y$ sont dans la même orbite de $E$ alors $\mathrm{Card}G_x = \mathrm{Card}G_y$.

**b.** Soit $x \in E$. Montrer que $\Omega_x$ est fini et que :

$$\mathrm{Card}\Omega_x = \frac{\mathrm{Card}G}{\mathrm{Card}G_x}$$

**c .** On suppose de plus $E$ fini, et on note $\Omega_1$,..., $\Omega_r$ ses orbites ($r \geqslant 1$) deux à deux distinctes. Pour tout $i \in \{1, 2, \ldots, r\}$, on choisit $x_i$ dans $\Omega_i$. Etablir l'*équation aux classes* :

$$\mathrm{Card}E = \sum_{i=1}^{r} \frac{\mathrm{Card}G}{\mathrm{Card}G_{x_i}}$$

## III. Lemme de Cauchy :

Soient $G$ un groupe fini de cardinal $n$ et $p \in \mathbb{N}^*$ un nombre premier divisant $n$.

On note $E = \{(x_1, x_2, \ldots, x_p) \in G^p,\ x_1 x_2 \ldots x_p = 1\}$, $S$ le sous-groupe de $\mathcal{S}_p$ engendré par le cycle $\sigma_0 = [1, 2, \ldots, p]$ de longueur $p$.

**1) a.** Quelle est la signature de $[1, 2, \ldots, p]$ ?

**b.** Quel est le cardinal de $S$ ? $S$ est-il abélien ?

**2) a .** Soient $(x_1, x_2, \ldots, x_p) \in E$ et $\sigma \in S$. Montrer que $(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(p)}) \in E$ (on commencera à le prouver pour $\sigma_0$).

**b .** En déduire que l'on définit une opération de $S$ sur $E$ en posant pour $\sigma \in S$ et $(x_1, x_2, \ldots, x_p) \in E$ :

$$\sigma_\bullet(x_1, x_2, \ldots, x_p) = (x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(p)})$$

**c.** Soient $(x_1, \ldots, x_p) \in E$ et $G_{(x_1,\ldots,x_p)} = H = \{\sigma \in S,\ \forall i \in [\![ 1, p ]\!],\ x_i = x_{\sigma(i)}\}$. Montrer que $H = \{1\}$ ou $S$.

**d.** En déduire que les orbites de $E$ possèdent 1 ou $p$ éléments.

**3) a.** Calculer $\mathrm{Card}E$.

**b.** On note $r$ (resp. $s$) le nombre d'orbites de cardinal 1 (resp. $p$). Montrer que $n^{p-1} = r + sp$.

**4)** Montrer qur $r$ est non nul. En déduire l'existence d'un élément de $G$ d'ordre $p$.

**Conclusion :** *Ainsi, pour tout groupe fini de cardinal $n$ et tout diviseur premier $p$ de $n$, il existe un élément de $G$ d'ordre $p$. Ce résultat constitue le lemme de Cauchy.*

## IV. Théorème de Frobénius :

Soit $G$ un groupe. On dira qu'un sous-groupe $H$ est distingué lorsque pour tout $g \in G$, $gHg^{-1} \subset H$.

**1)** Soit $f : G \longrightarrow G'$ un morphisme de groupes. Montrer que $\ker f$ est un sous-groupe distingué de $G$.

**2)** Soient $H$ et $K$ deux sous-groupes de $G$. On suppose $K$ distingué. Montrer que $HK$ est un sous-groupe.

**3)** On suppose $G$ fini de cardinal $n$. On considère $H$ un sous-groupe de $G$ et on pose $p = \dfrac{\mathrm{Card} G}{\mathrm{Card} H}$. On suppose que $p$ est premier et que $p$ est le plus petit entier premier divisant $n$. On fait opérer $H$ sur $E = \{aH, a \in G\}$ par translation à gauche : pour $h \in H$ et $a \in G$, $h_\bullet(aH) = (ha)H$.

**a.** Quel est la cardinal de $E$ ?

**b.** Montrer que le stabilisateur de $aH \in E$ est $aHa^{-1} \cap H$. Quel est le stabilisateur de $1H = H$

**c.** A l'aide de l'équation aux classes (cf **II.**), montrer que $E$ a exactement pour cette action $p$ orbites et que chacune est réduite à un élément.

**d.** En déduire que $H$ est un sous-groupe distingué de $G$.

*Ce résultat constitue le théorème de Frobénius.*

**4)** On suppose $G$ fini de cardinal $2n$. Soit $H$ un sous-groupe de $G$ de cardinal $n$. Montrer que $H$ est un sous-groupe distingué de $G$.