

## L3 Mathématiques

### Interrogation 10-2006

**1.** Soient  $n$  un entier positif non nul et  $k \in \mathbf{Z}$  non divisible par  $n$ . Montrer que l'ordre de  $\bar{k} \in \mathbf{Z}/n\mathbf{Z}$  est égal à  $\frac{n}{\text{pgcd}(n,k)}$ .

Pour ce faire on pourra poser  $\mu = \text{pgcd}(n, k)$ , puis on définira  $n'$  et  $k'$  par  $n = n'\mu$ ,  $k = k'\mu$ . On montrera que l'ordre de  $\bar{k}$  divise  $n'$ . Montrer que le plus petit entier positif non-nul  $\ell$  tel que  $n$  divise  $\ell k'\mu$  est  $n'$ . Puis montrer que l'ordre de  $\bar{k}$  est égal à  $n'$ .

L'ordre de  $\bar{k}$  est le plus petit entier  $\ell > 0$  tel que  $\ell\bar{k} = 0$ . Soit tel que  $\ell k$  soit divisible par  $n$ . Avec les notations introduites plus haut cela veut dire le plus petit entier  $\ell$  tel que  $n'\mu$  divise  $\ell k'\mu$ , donc que  $n'$  divise  $\ell k'$ . Il faut donc, comme  $n'$  est premier avec  $k'$ , que  $n'$  divise  $\ell$ . Le plus petit entier pour lequel cette condition a lieu est  $n' = \frac{n}{\text{pgcd}(n,k)}$ . par ailleurs on vérifie facilement que  $n'\bar{k} = 0$ .

**1.2.** Soit  $G$  et  $H$  deux groupes,  $f$  un endomorphisme de  $G$  dans  $H$ . Soit  $x \in G$  d'ordre  $k$ . Que peut-on dire de l'ordre de  $f(x)$ ? Montrer que si  $f$  est un automorphisme et l'ordre de  $x$  est  $k$ , alors  $f(x)$  est d'ordre  $k$ .

On a par hypothèse  $x^k = e$ . En appliquant l'homomorphisme  $f$  on obtient  $f(x^k) = f(x)^k = e$ , donc l'ordre de  $f(x)$  divise  $k$ .

(On applique le lemme qui dit que si  $x^n = e$  alors l'ordre de  $x$  divise  $n$ )

Si  $f$  est un automorphisme et si  $\ell$  est l'ordre de  $f(x)$ , l'ordre de  $f^{-1}(f(x))$  divise  $\ell$ . Mais cet élément est égal à  $x$  dont l'ordre est  $k$ . Donc  $k$  divise  $\ell$ , or  $\ell$  divise  $k$ , donc  $k = \ell$ .

On en déduira que si deux groupes sont isomorphes, pour tout entier  $k$  ils ont nécessairement le même nombre d'éléments d'ordre  $k$ .

**1.3.** Etant donné un groupe  $G$  on dira que deux éléments  $x$  et  $y$  de  $G$  sont conjugués si il existe  $z \in G$  tel que  $x = zyz^{-1}$ . Montrer que c'est une relation d'équivalence. Les classes d'équivalence seront appelées les classes de conjugaison.

On a évidemment la réflexivité :  $x = exe$ ; la symétrie : si on a  $x = zyz^{-1}$  alors  $y = z^{-1}xz$ , la transitivité : si  $x = yzy^{-1}$  et si  $y = vzw^{-1}$  alors  $x = vzw(vz)^{-1}$ .

Quelle est la classe de conjugaison de l'élément neutre, quelle est la classe de conjugaison d'un élément du centre de  $G$ ?

Quelles sont les classes de conjugaison dans un groupe abélien?

La classe de conjugaison de l'élément neutre  $e$  est réduite comme plus généralement la classe de conjugaison de tout élément du centre car si  $x$  est dans le centre alors  $uxu^{-1} = xuu^{-1} = x$ .

La classe de conjugaison d'un élément  $x$  dans un groupe abélien sont donc réduites est donc réduite à  $x$ .