10.03.2021 Maths 4 : Amphi 6

Théorème de Lagrange

Soit G un groupe fini et H un sous-groupe de G.
Alors l'ordre de H divise l'ordre de G.

Preuve :

$\forall x \in G$, on pose $xH = \{x.h, h \in H\}$

$\forall x, y \in G$, de deux choses l'une :

→ soit il existe $h \in H$ tq $x = y.h \iff y^{-1}.x \in H$

alors $xH = yH$ car • si $z \in xH$, $\exists h' \in H$ tq $z = x.h'$ donc $z = y.h.h'$ $\in yH$ ($h.h' \in H$ car H est un sous-groupe)

• réciproquement, on a $y = x h^{-1}$
par le même raisonnement $z \in yH \Rightarrow z \in xH$

→ donc $xH = yH$

→ soit un tel h n'existe pas, autrement dit $y^{-1}x \notin H$ alors $xH \cap yH = \emptyset$

car si ces ensembles avaient un élément commun z
$z = xh_1$, $h_1 \in H$
$z = yh_2$, $h_2 \in H$

$xh_1 = yh_2$
$x = y(h_2 h_1^{-1})$ ($h_2 h_1^{-1} \in H$)

On peut choisir $(x_1, \dots, x_k) \in G$ tq tout élément de G appartient à un et un seul des $x_i H$

$\Rightarrow$ Une partition de G $\quad G = \coprod_{i=1,\dots,k} x_i H$

xH a le même nb d'éléments que H.

l'application $H \to xH$ est une bijection
$z \mapsto xz$
($\times x^{-1}$ pour aller dans l'autre sens)

Donc le nb d'éléments de G est un multiple du nb d'éléments de H.

Exemple : $G = (\mathbb{Z}/12\mathbb{Z}, +)$
$H = \{\bar{0}, \bar{4}, \bar{8}\}$

$H = \bar{0} + H = \{\bar{4}, \bar{8}, \bar{0}\}$
$\bar{1} + H = \{\bar{1}, \bar{5}, \bar{9}\}$
$\bar{2} + H = \{\bar{2}, \bar{6}, \bar{10}\}$
$\bar{3} + H = \{\bar{3}, \bar{7}, \bar{11}\}$
$= \bar{4} + H$

$x \in G$

On a partitionné G en 4 paquets obtenus en "décalant" H et qui ont tous 3 éléments.

$|G| = 12$ est bien un multiple de $|H|$

Proposition : Soit $(G, .)$ un groupe à p éléments avec p premier. Alors G est cyclique.

Preuve : Soit x un élément de G différent de l'élément neutre.
Soit H le sous-groupe engendré par x.

Th de Lagrange $\Rightarrow |H| \mid |G|$ donc $|H| = 1$ ou $|H| = p$
or H contient l'élément neutre et x
donc il a au moins 2 éléments.
Donc $|H| = p$ car p premier

Donc $H = G$

Définition Soit $x \in G$, G d'élément neutre e.
Si $k \in \mathbb{N}$, on note $x^k = \underbrace{x . x . \dots . x}_{k \text{ fois}}$

Le plus petit entier positif d, s'il existe, tq $x^d = e$ est appelé l'ordre de x.
Si d n'existe pas, x est d'ordre infini.

Exemple : dans $\mathbb{Z}/n\mathbb{Z}$, $\bar{1}$ est d'ordre n

dans $\mathbb{Z}/6\mathbb{Z}$, $\bar{3}$ est d'ordre 2 car $\bar{3} + \bar{3} = 0$

Proposition Soit G un groupe, $x \in G$

1) s'il existe n tq $x^n = e$, alors x est d'ordre fini, et n un multiple de l'ordre de x.

2) l'ordre de x est égal au nombre d'éléments du s-g engendré par x

3) dans un groupe fini, tout élément est d'ordre fini.

Proposition : Soit G un groupe fini, et x dans G.
Alors l'ordre de x divise l'ordre de G.