17.03.2021

Amphi 7

Proposition : Soit G un groupe fini, $x \in G$.
alors l'ordre de x divise l'ordre du groupe.

Applicat° à l'arithmétique

Si $x \in ((\mathbb{Z}/n\mathbb{Z})^\times, \times)$ (élément inversible)

Alors il existe un plus petit entier $k \in \mathbb{N}$ que $x^k = \bar{1}$

Si $x \in \mathbb{Z}$ est premier avec k, k s'appelle l'ordre multiplicatif de x modulo n.

Déf Soit $n \in \mathbb{N}$.
On appelle caractéristiQ d'Euler de n, noté $\varphi(n)$ le nb d'entiers entre 1 et n qui sont premiers avec n.

Rmq : $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$

Ex : Si p premier, $\varphi(p) = p-1$
$\varphi(p^\alpha) = p^{\alpha-1}(p-1)$

$\varphi(6) = \#\{1, 5\} = 2$ $\Rightarrow$ difficile à calculer pour les nb pas premiers.

Th : Soient a et n 1ers entre eux.
Alors $a^{\varphi(n)} \equiv 1 \mod n$
} Théorème d'Euler

Corollaire : Petit th. de Fermat
Si p premier, a entier
$a^p \equiv a \mod p$
Si $p \nmid a$ $a^{p-1} \equiv 1 \mod p$

Prop : Si a et b 1ers entre eux $\varphi(ab) = \varphi(a)\varphi(b)$

Hors-programme : RSA (voir page Wikipédia)

idée : Il est facile de multiplier 2 nombres mais difficile de factoriser

Homomorphismes et isomorphismes

Déf : Un homomorphisme (ou juste morphisme) d'un groupe $(G, \cdot)$ vers $(H, *)$ est une application
$f : G \to H$

Prop : Si $f : (G, \cdot) \to (H, *)$ est un morphisme de groupe, alors :

1) $f(e_G) = e_H$

2) $\underbrace{f(x^{-1})}_{\text{dans } G} = \underbrace{f^{-1}(x)}_{\text{dans } H}$

Preuve : 1) $f(e_G) = f(e_G \cdot e_G) = f(e_G) * f(e_G)$

$$e_H = f(e_G) * f(e_G)^{-1} = f(e_G) * \cancel{f(e_G) * f^{-1}(e_G)}$$
$$= f(e_G)$$

2) $e_H = f(e_G) = f(x \cdot x^{-1}) = f(x) * f(x^{-1})$ donc $f(x^{-1})$ est l'inverse de $f(x)$, qui est unique

donc $f(x^{-1}) = f^{-1}(x)$

Exemples :

1) $f : \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$

$f(\bar{0}) = \bar{0}$, $f(\bar{1}) = \bar{3}$, $f(\bar{2}) = \bar{0}$, $f(\bar{3}) = \bar{3}$

est un morphisme de groupe.

! $f(\bar{x}) = \bar{y}$ c'est x mod 4 et y mod 6
→ abus de langage pour simplifier l'écriture

$f(\bar{1} + \bar{3}) = f(\bar{0}) = \bar{0}$

$f(\bar{1}) + f(\bar{3}) = \bar{3} + \bar{3} = \bar{6} = \bar{0}$

$f(\bar{2} + \bar{3}) = f(\bar{1}) = \bar{3}$

$f(\bar{2}) + f(\bar{3}) = \bar{0} + \bar{3} = \bar{3}$

2) Soit $m \geq 1$, l'application $(\mathbb{Z}, +) \to (\mathbb{Z}/m\mathbb{Z}, +)$, $x \mapsto \bar{x}$ est un morphisme de groupe.

3) Si m divise n, morphisme $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$, $\bar{x} \mapsto \bar{x} \bmod m$

4) Si H est un sous-groupe de G, $x \in H \mapsto x \in G$ est un morphisme.

5) Soit G un groupe cyclique de cardinal n, et g un générateur de G.

$\mathbb{Z}/n\mathbb{Z} \to G$, $\bar{a} \mapsto g^a$ est un isomorphisme de groupe.
$(a \in \mathbb{Z},\ a \equiv \bar{a} \bmod n)$

Par ex $(\underbrace{(\mathbb{Z}/5\mathbb{Z})^\times}_{= \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}}, \times)$ est cyclique d'ordre 4 engendré par $\bar{2}$.

$\bar{1} \to \bar{2}^0$, $\bar{2} \to \bar{2}^1$, $\bar{3} \to \bar{2}^3$, $\bar{4} \to \bar{2}^2$

$(\mathbb{Z}/4\mathbb{Z}, +) \to ((\mathbb{Z}/5\mathbb{Z})^\times, \times)$, $a \mapsto \bar{2}^a$ est un isomorphisme

Définition : L'image d'un morphisme $f : (G, \cdot) \to (H, *)$ est $\mathrm{Im}(f) = \{ y \in H \text{ tq } \exists x \in G, f(x) = y \}$

Le noyau de f est $\mathrm{Ker}(f) = \{ x \in G, f(x) = e_H \}$

Exemple : $(\mathbb{Z}/4\mathbb{Z}, +) \longrightarrow (\mathbb{Z}/6\mathbb{Z}, +)$ de l'exemple d'avant

$\mathrm{Im}(f) = \{ \bar{0}, \bar{3} \} \subset \mathbb{Z}/6\mathbb{Z}$

$\mathrm{Ker}(f) = \{ \bar{0}, \bar{2} \} \subset \mathbb{Z}/4\mathbb{Z}$ car $f(\bar{0}) = f(\bar{2}) = \bar{0} = e_{\mathbb{Z}/6\mathbb{Z}}$

Proposition Soit $f : (G, \cdot) \to (H, *)$ un morphisme

1) $\mathrm{Im}(f)$ et $\mathrm{Ker}(f)$ sont des sous-groupes de H et de G respectivement.

2) Un morphisme est injectif ssi $\mathrm{Ker}(f) = \{ e_G \}$