

1. Théorème de Lagrange

1.1. Théorème de Lagrange

Soient G un groupe d'ordre **fini** et H un sous groupe de G .

L'ordre de H divise l'ordre de G .

Démonstration :

a) Notons multiplicativement la loi de G .

Définissons, sur G , une relation $\mathcal{R}$ par :

$$\forall (x, y) \in G^2, (x \mathcal{R} y \Leftrightarrow x^{-1}y \in H)$$

Montrons que $\mathcal{R}$ est une relation d'équivalence :

- $x^{-1}x = 1 \in H$ donc $x \mathcal{R} x$, **$\mathcal{R}$ est réflexive.**
- $x \mathcal{R} y \Leftrightarrow x^{-1}y \in H \stackrel{H \text{ sous groupe}}{\Leftrightarrow} (x^{-1}y)^{-1} \in H \Leftrightarrow y^{-1}x \in H \Leftrightarrow y \mathcal{R} x$, donc **$\mathcal{R}$ est symétrique.**
- $(x \mathcal{R} y \text{ et } y \mathcal{R} z) \Rightarrow (x^{-1}y \in H \text{ et } y^{-1}z \in H) \Rightarrow (x^{-1}y y^{-1}z = x^{-1}z \in H) \Rightarrow (x \mathcal{R} z)$, **$\mathcal{R}$ est transitive.**

Donc $\mathcal{R}$ est bien une **relation d'équivalence**.

La classe d'équivalence d'un élément a de G est, par définition :

$$\{y \in G \mid a \mathcal{R} y\} = \{y \in G \mid a^{-1}y \in H\} = \{y \in G \mid \exists h \in H, a^{-1}y = h\} = \{y \in G \mid \exists h \in H, y = ah\} = aH$$

Cet ensemble est appelé **classe à gauche (de a) modulo H** .

Montrons que toutes les classes à gauche ont $|H|$ éléments :

Pour cela, on considère, pour tout $a \in G$, l'application

$$\begin{aligned} \varphi_a : H &\rightarrow aH \\ h &\mapsto ah \end{aligned}$$

- $\varphi_a(h_1) = \varphi_a(h_2) \Rightarrow ah_1 = ah_2 \Rightarrow h_1 = h_2$, donc φ_a est **injective**.
- $\forall y \in aH, \exists h \in H$ tel que $y = ah$ donc φ_a est **surjective**.

φ_a étant **bijjective**, on déduit :

$$\forall a \in G, |aH| = |H|$$

Montrons que toutes les classes à gauche sont disjointes :

Considérons deux classes aH et bH (a et b dans G) et supposons $aH \cap bH \neq \emptyset$.

Soit $g \in aH \cap bH$. Alors :

$$\exists h \in H \text{ tel que } g = ah \text{ et } \exists h' \in H \text{ tel que } g = bh'$$

On a alors :

$$ah = bh'$$

$$a = bh'h^{-1}$$

Tout élément ah'' de aH s'écrit donc :

$$bh'h^{-1}h''$$

Or, $h'h^{-1}h'' \in H$, donc tout élément ah'' de aH est aussi élément de bH , d'où :

$$aH \subset bH$$

On montre, de même :

$$bH \subset aH$$

On a donc :

$$aH = bH$$

Ceci prouve que **les classes à gauches sont disjointes**.

Remarque : on pouvait affirmer ce résultat directement car les classes d'équivalences forment une partition de G .

Concluons :

En notant m le nombre de classes à gauches, on a donc :

$$G = \coprod_{n=1}^m a_n H$$

$$D'où : |G| = \sum_{n=1}^m |a_n H| = \sum_{n=1}^m |H| = m|H|$$

L'ordre du sous groupe H divise donc l'ordre du groupe G .

Notons que cette démonstration peut se faire aussi en raisonnant sur les classes à droite Ha et, qu'en cas de groupe commutatif, les classes à gauche et à droite coïncident ($aH = Ha$).

1.2. Corollaire

- a) Dans tout groupe G d'ordre fini, l'ordre d'un élément a divise l'ordre de G .
- b) Si G est un groupe d'ordre n , alors, pour tout a dans G , on a : $a^n = 1$.
- c) Tout groupe d'ordre un nombre premier est cyclique.

Commençons par quelques rappels sur l'ordre d'un élément dans un groupe.

Soient G un groupe (quelconque) et $a \in G$.

Notons : $\langle a \rangle = \{a^n, n \in \mathbb{Z}\} \subset G$

Cet ensemble $\langle a \rangle$ est un sous groupe de G . (Il est non vide (il contient a) et $a^n \times a^{-m} \in \langle a \rangle$)

On l'appelle "le groupe engendré par a ". Un tel groupe est dit "monogène" (engendré par un seul élément).

Montrons que $\langle a \rangle$ est soit infini et isomorphe à $(\mathbb{Z}, +)$ soit d'ordre m et isomorphe à $\mathbb{Z}/m\mathbb{Z}$.

Pour cela, on considère l'application :

$$\begin{aligned} \varphi_a : \mathbb{Z} &\rightarrow \langle a \rangle \\ n &\mapsto a^n \end{aligned}$$

- $\text{Im}(\varphi_a) = \langle a \rangle$ donc φ_a est **surjectif**.
- $\varphi_a(n + n') = a^{n+n'} = a^n \times a^{n'} = \varphi_a(n) \times \varphi_a(n')$ donc φ_a est un **morphisme de groupes**.

On sait que le noyau d'un morphisme de groupe est un sous-groupe, donc :

$$\text{Ker}(\varphi_a) = \{n \in \mathbb{Z} \mid a^n = 1\} \text{ est un sous-groupe de } \mathbb{Z}$$

Par conséquent, il existe $m \in \mathbb{N}$ tel que : $\text{Ker}(\varphi_a) = m\mathbb{Z}$

Deux cas se présentent alors :

$m = 0$: et alors $\text{Ker}(\varphi_a) = \{0\}$, φ_a est injective et donc bijective. Donc $\langle a \rangle$ est infini et isomorphe à $(\mathbb{Z}, +)$.

$m \in \mathbb{N}^*$: dans ce cas, φ_a n'est pas injective. Mais :

$$\varphi_a(n) = \varphi_a(n') \Rightarrow a^n = a^{n'} \Rightarrow a^{n-n'} = 1 \Rightarrow n - n' \in \text{Ker}(\varphi_a) \Rightarrow n - n' \in m\mathbb{Z} \Rightarrow n = n' [m]$$

$\varphi_a(n)$ ne dépend donc que de la classe $\bar{n}$ de n modulo m .

Définissons alors :

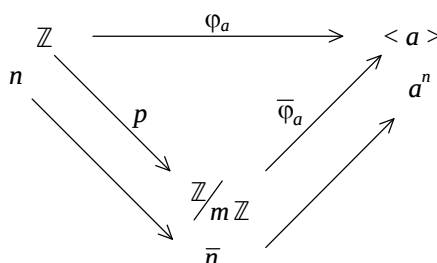
$$\bar{\varphi}_a : \mathbb{Z} / \text{Ker}(\varphi_a) = \mathbb{Z} / m\mathbb{Z} \rightarrow \langle a \rangle$$

$$\bar{n} \mapsto a^n$$

Ainsi, ce nouveau morphisme $\bar{\varphi}_a$ est injectif (puisque $\bar{\varphi}_a(\bar{n}) = \bar{\varphi}_a(\bar{n}') \Rightarrow \bar{n} = \bar{n}'$) et surjectif.

Donc $\langle a \rangle$ est isomorphe à $\mathbb{Z} / m\mathbb{Z}$.

On dit que l'on a factorisé le morphisme φ_a :



L'entier $m \in \mathbb{N}^*$ vérifie donc $a^m = 1$ et c'est le plus petit. (En effet : $a^k = 1 \Rightarrow k \in \text{Ker}(\varphi_a) \Rightarrow k \in m\mathbb{Z}$)

Cet entier m s'appelle **l'ordre de l'élément a** .

Prouvons maintenant le corollaire 1.2. :

- Comme G est fini, le sous groupe $\langle a \rangle$ est aussi fini d'ordre m . On applique alors le théorème de Lagrange au sous groupe $\langle a \rangle$.
- Soit m l'ordre a . (On a donc : $a^m = 1$). On sait que m divise n : $n = km$. Donc $a^n = (a^m)^k = 1$.
- Soit G un groupe d'ordre un nombre premier p . Soit $a \neq 1$ dans G . Notons m son ordre ($m > 1$ car $a \neq 1$). Comme m divise p , on a nécessairement $m = p$ donc $G = \langle a \rangle$.

2. Théorème d'Euler

Étudions, pour commencer, les éléments inversibles (pour $\times$) de l'anneau commutatif :

$$(\mathbb{Z} / n\mathbb{Z}, +, \times), \quad n \in \mathbb{N} \setminus \{0; 1\}$$

2.1. Théorème

Soit $\bar{x} \in \mathbb{Z} / n\mathbb{Z}$. Alors : $\bar{x}$ est inversible $\Leftrightarrow (x, n) = 1$

Démonstration : les conditions suivantes sont équivalentes

$$\bar{x} \text{ est inversible dans } \mathbb{Z} / n\mathbb{Z}$$

$$\exists \bar{y} \in \mathbb{Z} / n\mathbb{Z}, \quad \bar{x} \bar{y} = \bar{1}$$

$$\exists y \in \mathbb{Z}, xy = 1 [n]$$

$$\exists (y, k) \in \mathbb{Z}^2, xy - kn = 1$$

$$(x, n) = 1$$

(Le lien entre les deux dernières lignes étant le théorème de Bézout)

Pour la suite, on note $(\mathbb{Z}/n\mathbb{Z})^*$ l'ensemble des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$.

2.2. Théorème

L'ensemble $(\mathbb{Z}/n\mathbb{Z})^*$ est un groupe multiplicatif.

Démonstration :

- Comme $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif, la loi $\times$ est **associative** et admet **un élément neutre 1** qui est élément de $(\mathbb{Z}/n\mathbb{Z})^*$.

- Soit $\bar{x}$ dans $(\mathbb{Z}/n\mathbb{Z})^*$. Donc $\bar{x}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$:

$$\exists \bar{x}' \in \mathbb{Z}/n\mathbb{Z} \text{ tel que : } \bar{x} \bar{x}' = 1$$

Donc l'inverse $\bar{x}'$ de $\bar{x}$ est aussi **inversible**. Autrement dit : $\bar{x}^{-1} \in (\mathbb{Z}/n\mathbb{Z})^*$.

Donc $(\mathbb{Z}/n\mathbb{Z})^*$ est muni d'une loi associative ($\times$), admet un élément neutre (1) et tout élément admet un symétrique. Donc, c'est un groupe (commutatif, car la loi $\times$ l'est).

Remarque : inverse d'un produit dans $(\mathbb{Z}/n\mathbb{Z})^*$:

Soient $\bar{x}$ et $\bar{y}$ des éléments de $(\mathbb{Z}/n\mathbb{Z})^*$.

Il existe $\bar{x}'$ et $\bar{y}'$ dans $(\mathbb{Z}/n\mathbb{Z})^*$ tels que :

$$\bar{x} \bar{x}' = 1 \text{ et } \bar{y} \bar{y}' = 1$$

On a alors : $(\bar{x} \bar{y})(\bar{y}' \bar{x}') = \bar{x}(\bar{y} \bar{y}') \bar{x}' = \bar{x} \bar{x}' = 1$

Donc $\bar{x} \bar{y}$ est inversible d'inverse $\bar{y}^{-1} \bar{x}^{-1}$.

2.3. Définition Indicateur d'Euler

L'indicateur d'Euler, noté $\varphi(n)$ est l'ordre du groupe $(\mathbb{Z}/n\mathbb{Z})^*$.

Par exemple, avec $n = 24$, on a :

$$(\mathbb{Z}/24\mathbb{Z})^* = \{ \bar{1}; \bar{5}; \bar{7}; \bar{11}; \bar{13}; \bar{17}; \bar{19}; \bar{23} \} \text{ et } \varphi(24) = 8.$$

Si p est un nombre premier, alors $(\mathbb{Z}/p\mathbb{Z})^* = \{ \bar{1}; \bar{2}; \dots; \overline{p-1} \}$ et $\varphi(p) = p - 1$.

2.4. Théorème d'Euler

Soit n un entier supérieur ou égal à 2.

Soit $a \in \mathbb{Z}^*$ que $(a, n) = 1$.

Alors :
$$a^{\varphi(n)} = 1 [n]$$

Démonstration :

Puisque a est premier avec n , d'après 2.1. : $\bar{a} \in \left(\mathbb{Z}/n\mathbb{Z}\right)^*$.

Notons d l'ordre de $\bar{a}$. D'après le corollaire 1.2.a) du théorème de Lagrange : d divise $\varphi(n)$.

Donc il existe $k \in \mathbb{N}^*$ tel que : $\varphi(n) = kd$.

Dans $\left(\mathbb{Z}/n\mathbb{Z}\right)^*$, on a donc l'égalité :
$$\bar{a}^{\varphi(n)} = (\bar{a}^d)^k = 1$$

Donc :
$$a^{\varphi(n)} = 1 [n]$$

Application : calcul de l'inverse d'un élément $\bar{x}$ de $\left(\mathbb{Z}/n\mathbb{Z}\right)^*$.

Le théorème d'Euler permet d'affirmer que, dans $\left(\mathbb{Z}/n\mathbb{Z}\right)^*$, on a l'égalité :

$$\bar{x}^{\varphi(n)} = 1$$

Ce qui peut encore s'écrire :
$$\bar{x} \bar{x}^{\varphi(n)-1} = 1$$

D'où :
$$\bar{x}^{-1} = \bar{x}^{\varphi(n)-1}$$

Par exemple, voici dans $\left(\mathbb{Z}/10\mathbb{Z}\right)^*$, la table des inverses : ($\varphi(10) = 4$)

Élément	$\bar{1}$	$\bar{3}$	$\bar{7}$	$\bar{9}$
Inverse	$\bar{1}$	$\bar{7}$	$\bar{3}$	$\bar{9}$

3. Petit théorème de Fermat

3.1. Petit théorème de Fermat

Soit p un nombre premier.

1) Pour tout $a \in \mathbb{Z}$, on a :
$$a^p = a [p]$$

2) Pour tout $a \in \mathbb{Z}^*$ tel que $(a, p) = 1$:
$$a^{p-1} = 1 [p]$$

Première démonstration utilisant ce qui précède :

Commençons par prouver le deuxième point :

Comme $(a, p) = 1$, le théorème d'Euler permet d'affirmer : $a^{\varphi(p)} = 1 [p]$

Et comme p est premier, $\varphi(p) = p - 1$, d'où : $a^{p-1} = 1 [p]$

Prouvons maintenant le premier point :

si $(a, p) = 1$ alors il suffit de multiplier l'égalité ci-dessus par a pour obtenir : $a^p = a [p]$

si $(a, p) \neq 1$ alors p divise a . Donc a et a^p sont des multiples de p , donc : $a^p = a = 0 [p]$

Seconde démonstration à l'aide d'une récurrence et de la formule du binôme de Newton :

Déjà, prouvons le résultat suivant :

si p est premier, alors pour tout $k \in \{1 ; 2 ; \dots ; p-1\}$, $p \mid C_p^k$

En effet, on a : $p! = k! (p-k)! C_p^k$

Donc : $p \mid k! (p-k)! C_p^k$

Or, pour tout $k \in \{1 ; 2 ; \dots ; p-1\}$ on a $(p, k) = 1$ et $(p, p-k) = 1$ donc $(p, k! (p-k)!) = 1$.

Donc, d'après le théorème de Gauss : $p \mid C_p^k$

Supposons $a \in \mathbb{N}$ et montrons par récurrence sur a la propriété : $\wp(a) : "a^p = a [p]"$

- Comme $0 = 0 [p]$, on a bien $\wp(0)$.
- Montrons, pour tout $a \in \mathbb{N}$, que : $\wp(a) \Rightarrow \wp(a+1)$

Supposons $\wp(a) : a^p = a [p]$

D'après la formule du binôme : $(a+1)^p = \sum_{k=0}^p C_p^k a^k [p]$

Or, on a vu plus haut que : $C_p^k = 0 [p]$ pour tout $k \in \{1 ; 2 ; \dots ; p-1\}$

D'où : $(a+1)^p = a^p + 1 [p]$

Et d'après $\wp(a) : (a+1)^p = a+1 [p]$

D'où $\wp(a+1)$.

Du principe de récurrence, on déduit : $\wp(a), \forall a \in \mathbb{N}$

Supposons maintenant $a \in \mathbb{N}^-$.

Si p est impair : $a^p = -(-a)^p = -(-a) = a [p]$

Si $p = 2 : a^2 = (-a)^2 = -a [2]$. Or, $a = -a [2]$ donc $a^2 = a [2]$.

Dans tous les cas, on a bien : $a^p = a [p]$

L'égalité ci-dessus peut encore s'écrire : $a(a^{p-1} - 1) = 0 [p]$

Or, p étant premier, $\mathbb{Z}/p\mathbb{Z}$ est intègre donc :

$$a = 0 [p] \text{ ou } a^{p-1} - 1 = 0 [p]$$

Or, $(a, p) = 1$ donc p ne divise pas a , on ne peut donc pas avoir $a = 0 [p]$, d'où :

$$a^{p-1} - 1 = 0 [p]$$

Exemple : démontrer que pour tout nombre premier $p \neq 3$, on a :

$$p^2 + 2 = 0 [3]$$

On applique le petit théorème de Fermat (version 2) avec $p = 3$ et $a = p$. Comme $(p, 3) = 1$ (puisque $p \neq 3$),

il vient : $p^2 = 1 [3]$

D'où : $p^2 + 2 = 0 [3]$

Existe-t-il une réciproque du petit théorème de Fermat ? Plus précisément :

Soit $n \in \mathbb{N}$ tel que pour tout $a \in \mathbb{Z}$ tel que $(a, n) = 1$ on ait : $a^{n-1} = 1 [n]$

Peut-on en déduire : n premier ?

La réponse est non. Il s'agit des nombres de Carmichael.

Un entier n est dit de Carmichael si pour tout entier $a \in \mathbb{Z}^*$ tel que $(a, n) = 1$: $a^{n-1} = 1 [n]$

Il existe une infinité de nombres de Carmichael (démontré en 1992). Le premier est $n = 561$.

En effet :
$$n = 561 = 3 \times 11 \times 17$$

Et
$$n - 1 = 560 = 2^4 \times 5 \times 7$$

Soit a un entier tel que $(a, n) = 1$.

Comme $(560, 3) = 1$, le petit théorème de Fermat (sens direct) permet d'affirmer :

$$a^{560} = 1 [3]$$

De même :
$$a^{560} = 1 [11]$$

$$a^{560} = 1 [17]$$

Les nombres 3, 11 et 17 sont des diviseurs de $a^{560} - 1$. Et comme ils sont premiers entre eux deux à deux, le produit $3 \times 11 \times 17$, c'est-à-dire 561 divise $a^{560} - 1$:

$$a^{560} = 1 [561]$$

Ce qui prouve que la réciproque du théorème de Fermat est fausse.