4.5 Les théorèmes de Fermat et de Wilson

4.5.1 Théorème

Soit p un nombre premier.
Alors $p\mathbb{Z}$, l'idéal de $\mathbb{Z}$ engendré par p est maximal, c'est à dire :
Il n'existe pas d'idéal $I \neq \mathbb{Z}$ tel que $p\mathbb{Z} \subsetneqq I \subsetneqq \mathbb{Z}$

Démonstration

Supposons que l'idéal $p\mathbb{Z}$ ne soit pas maximal.
Il existe alors $x \in \mathbb{Z}$ tel que $p\mathbb{Z} \subsetneqq x\mathbb{Z}$; en particulier $p \in x\mathbb{Z}$ et il existe $c \in \mathbb{Z}$ tel que $p = cx$, ce qui signifie que $c \mid p$; il y a donc contradiction avec le fait que p soit premier.
Donc $p\mathbb{Z}$ est maximal

4.5.2 Théorème

Soit $a \in \mathbb{Z}/n\mathbb{Z}$. Alors, a est inversible si et seulement a et n sont premiers entre eux

Démonstration

1. Supposons a et n premiers entre eux
   Alors, il existe $u \in \mathbb{Z}$ et $v \in \mathbb{Z}$ tels que $au + nv = 1$, ce qui veut dire que $au \equiv 1\,[n]$
   Donc, dans $\mathbb{Z}/n\mathbb{Z}$, a admet un inverse qui est u modulo n
2. Supposons a inversible dans $\mathbb{Z}/n\mathbb{Z}$
   Il existe donc $u \in \mathbb{Z}/n\mathbb{Z}$ tel que $au \equiv 1\,[n]$, c'est à dire que $au = 1 + kn$ avec $k \in \mathbb{Z}$. Or, $au = 1 + kn \iff au - kn = 1$, ce qui traduit, d'après Bachet-Bezout que a et n sont premiers entre eux

4.5.3 Corollaire

Les générateurs du groupe additif $(\mathbb{Z}/n\mathbb{Z}, +)$ sont les entiers a tels que a et n sont premiers entre eux ($a \wedge n = 1$)

Démonstration

1. Soit $a \in \mathbb{Z}$ tel que $a \wedge n = 1$.
   Alors, il existe $u \in \mathbb{Z}$ et $v \in \mathbb{Z}$ tels que $au + vn = 1$, et donc, $au \equiv 1\,[n]$.
   Ainsi, pour tout $k \in \mathbb{Z}/n\mathbb{Z}$, $kau \equiv k\,[n]$, c'est à dire $(ku)\,a \equiv k\,[n]$
   a est donc un générateur du groupe additif $(\mathbb{Z}/n\mathbb{Z}, +)$
2. Réciproquement, soit a un générateur du groupe additif $(\mathbb{Z}/n\mathbb{Z}, +)$.
   Alors, pour tout $p \in \mathbb{Z}/n\mathbb{Z}$, il existe $k \in \mathbb{N}$ tel que $ka \equiv p\,[n]$. En particulier si $p = 1$, nous avons $ka \equiv 1\,[n]$, ce qui est équivalent à :

   $$ka - 1 = \lambda n \iff ka - \lambda n = 1$$

   Ce qui traduit que a et n sont premiers entre eux.

4.5.4 Théorème

Soit $n \in \mathbb{N}$

1. **L'ensemble des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ noté $(\mathbb{Z}/n\mathbb{Z})^\star$ est un groupe commutatif pour la multiplication.**

2. **On appelle $\varphi(n)$ la fonction indicatrice d'Euleur qui désigne le nombre d'entiers positifs compris entre 1 et n qui sont premiers avec n, c'est à dire :**

$$\varphi(n) = \text{Card } \{m \in \mathbb{N}^* \text{ tels que } m \leqslant n \text{ et } \text{pgcd}(m,n) = 1\}$$

Alors, Card $(\mathbb{Z}/n\mathbb{Z})^\star = \varphi(n)$

Démonstration

— Que Card $(\mathbb{Z}/n\mathbb{Z})^\star = \varphi(n)$ est complètement évident puisque les éléments inversibles de $(\mathbb{Z}/n\mathbb{Z})$ sont les entiers premiers avec n ; ils sont donc en nombre $\varphi(n)$

— Démontrons donc que $(\mathbb{Z}/n\mathbb{Z})^\star$ est un groupe commutatif pour la multiplication.

▷ Tout d'abord, $(\mathbb{Z}/n\mathbb{Z})^\star \neq \emptyset$ puisque $1 \in (\mathbb{Z}/n\mathbb{Z})^\star$

▷ Ensuite, si $u \in (\mathbb{Z}/n\mathbb{Z})^\star$, évidemment que $u^{-1} \in (\mathbb{Z}/n\mathbb{Z})^\star$ puisque $\left(u^{-1}\right)^{-1} = u$

▷ D'autre part, si $u \in (\mathbb{Z}/n\mathbb{Z})^\star$ et $v \in (\mathbb{Z}/n\mathbb{Z})^\star$, alors $uv \in (\mathbb{Z}/n\mathbb{Z})^\star$ puisque uv est inversible et nous avons : $(uv)^{-1} = v^{-1}u^{-1}$

Donc, $(\mathbb{Z}/n\mathbb{Z})^\star$ est un groupe pour la multiplication ; la commutativité découle de celle de la multiplication dans $\mathbb{Z}$

Remarque 15 :

1. Il y a donc $\varphi(n)$ générateurs du groupe additif $(\mathbb{Z}/n\mathbb{Z}, +)$
2. Si $(R, +, \times)$ est un anneau unitaire, l'ensemble des éléments inversibles de R noté $R^\star$ forme un groupe pour la multiplication (pas forcément commutatif).

4.5.5 Corollaire de 4.5.2

Soit $p \in \mathbb{Z}$ un nombre premier ; alors, $\mathbb{Z}/p\mathbb{Z}$ est un corps

Démonstration

La démonstration est une redite de 4.5.2
Soit $p \in \mathbb{Z}$ un nombre premier
On sait déjà que $(\mathbb{Z}/p\mathbb{Z}, +, \times)$ est un anneau commutatif ; il faut maintenant montrer que chacun des éléments non nuls de $\mathbb{Z}/p\mathbb{Z}$ est inversible.
Soit donc $a \in \mathbb{Z}$ tel que $0 < a < p$; alors, a et p sont premiers entre eux, et, d'après le théorème de Bezout, il existe $u \in \mathbb{Z}$ et $v \in \mathbb{Z}$ tels que $au + pv = 1$; or, $pv \equiv 0\,[p]$ et donc $ua \equiv 1\,[p]$; il existe un inverse à a ; donc $\mathbb{Z}/p\mathbb{Z}$ est un corps.

4.5.6 Théorème

La caractéristique d'un corps $\mathbb{K}$ est zéro ou un nombre premier

Remarque 16 :

Qu'est ce que la caractéristique d'un corps ?
La caractéristique d'un corps est le plus petit entier positif m tel que $m \times 1 = 0$
C'est donc en fait l'ordre additif de l'unité.

Démonstration

Soit m la caractéristique du corps $\mathbb{K}$
Supposons que la caractéristique du corps $\mathbb{K}$ soit non nulle et non premier, et on écrit $m = hk$. Nous avons, évidemment, $h < m$ et $k < m$; donc, $m \times 1 = 0$ est équivalent à $hk \times 1 = 0$, c'est à dire $(h \times 1)(k \times 1) = 0$; comme $\mathbb{K}$ est un corps, $\mathbb{K}$ est intègre, donc $h \times 1 = 0$ ou $k \times 1 = 0$; il y a donc contradiction ; donc m est premier.

4.5.7 Le petit théorème de Fermat

Soit $p \in \mathbb{Z}$ un nombre premier ; alors, pour tout $a \in \mathbb{Z}$, $a^p \equiv a\,[p]$

Démonstration

1. Si $a = 0$, ou si a est multiple de p, c'est à dire $a \equiv 0\,[p]$, le théorème est démontré.
2. Supposons $a \neq 0$ et a non multiple de p
   On appelle $\mathcal{U} = \mathbb{Z}/p\mathbb{Z} - \{0\}$. $\mathcal{U}$ est l'ensemble des éléments inversibles de $\mathbb{Z}/p\mathbb{Z}$ qui est un groupe multiplicatif d'ordre $p-1$; alors, $a^{p-1} \equiv 1\,[p]$, c'est à dire $a^p \equiv a\,[p]$

Remarque 17 :

Voici une autre démonstration du théorème de Fermat 4.5.7 :

Nous appelons toujours $\mathcal{U}$ le groupe multiplicatif des éléments inversibles de $\mathbb{Z}/p\mathbb{Z}$.
Soit $a \in \mathcal{U}$. On appelle

$$\begin{cases} \Phi : \mathcal{U} & \longrightarrow & \mathcal{U} \\ x & \longmapsto & \Phi(x) = ax \end{cases}$$

Φ est un automorphisme *(homomorphisme bijectif)*. Alors :

$$\Phi(1) \times \Phi(2) \times \cdots \times \Phi(p-1) = 1 \times 2 \times \cdots \times (p-1)$$

Car Φ est une bijection. Or :

$$\Phi(1) \times \Phi(2) \times \cdots \times \Phi(p-1) = (a \times 1) \times (a \times 2) \times \cdots \times (a\,(p-1))$$

Or,

$$(a \times 1) \times (a \times 2) \times \cdots \times (a\,(p-1)) = (1 \times 2 \times \cdots \times (p-1))\,a^{p-1}$$

Et donc :

$$1 \times 2 \times \cdots \times (p-1) = (1 \times 2 \times \cdots \times (p-1))\,a^{p-1}$$

Et, par simplification, $a^{p-1} = 1$ dans $\mathcal{U}$

4.5.8 Le théoprème de Wilson

Soit p un nombre premier ; alors :

$$(p-1)! + 1 \equiv 0\,[p] \Longleftrightarrow (p-1)! \equiv -1\,[p] \Longleftrightarrow (p-1)! \equiv p-1\,[p]$$

Démonstration

On considère $\mathbb{Z}/p\mathbb{Z}$ et $\mathcal{U}$ le groupe multiplicatif des éléments inversibles de $\mathbb{Z}/p\mathbb{Z}$. p étant premier, $\mathbb{Z}/p\mathbb{Z}$ est un corps.
Donc, $(p-1)!$ est le produit de tous les éléments de $\mathcal{U}$. $\mathcal{U}$ ayant un nombre pair d'éléments, on peut les regrouper 2 à 2, c'est à dire chaque élément et son inverse. Il se peut que des éléments soient leur propre inverse.
Recherchons donc les éléments qui sont leur propre inverse. Il s'agit donc de résoudre l'équation

$$X^2 \equiv 1\,[p] \Longleftrightarrow X^2 - 1 \equiv 0\,[p]$$

Or, $X^2 - 1 = (X-1)(X+1)$. $\mathbb{Z}/p\mathbb{Z}$ étant un corps est intègre et nous avons :

$$\begin{cases} (X-1) \equiv 0\,[p] & \Longleftrightarrow & X \equiv 1\,[p] \\ & \text{ou} & \\ (X+1) \equiv 0\,[p] & \Longleftrightarrow & X \equiv -1\,[p] \Longleftrightarrow X \equiv p-1\,[p] \end{cases}$$

Donc, seuls 1 et $p-1$ sont leur propre inverse. Donc $(p-1)! \equiv p-1\,[p] \Longleftrightarrow (p-1)! \equiv -1\,[p]$
Ce que nous voulions.

4.5.9 Quelques exercices

Exercice 34 :

Encore une autre démonstration du théorème de Fermat 4.5.7

1. Soit $n \in \mathbb{N}^*$ et $k \in \mathbb{N}$ tel que $0 < k < n$.
   (a) Montrer que si n est premier, alors n divise C_n^k [1]
   (b) Démontrer que si n est premier, alors n divise $2^n - 2$
2. Soit $n \in \mathbb{N}^*$, premier et $a \in \mathbb{N}$. Montrer que $a^n - a$ est divisible par n

Exercice 35 :

La fonction indicatrice d'Euler
Cet exercice revient sur la fonction indicatrice d'Euler définie en 4.5.4. Nous allons en donner une forme explicite et travailler quelques unes de ses propriétés

1. Calculer $\varphi(8)$ et $\varphi(78)$
2. Démontrer que p est premier si et seulement si $\varphi(p) = p - 1$
3. Soit p un nombre premier supérieur ou égal à 2
   (a) Montrer que $k \wedge p^\alpha \neq 1 \iff p \mid k$
   (b) Démontrer qu'il y a $p^{\alpha-1}$ multiples de p entre 0 et $p^\alpha - 1$
   (c) En déduire $\varphi(p^\alpha)$
4. Soient $m \in \mathbb{N}^*$ et $n \in \mathbb{N}^*$ tels que $m \wedge n = 1$. On appelle $\mathcal{U}(\mathbb{Z}/mn\mathbb{Z})$, les éléments inversibles de $\mathbb{Z}/mn\mathbb{Z}$, tout comme on appelle $\mathcal{U}(\mathbb{Z}/n\mathbb{Z})$, les éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ et $\mathcal{U}(\mathbb{Z}/m\mathbb{Z})$, ceux de $\mathbb{Z}/m\mathbb{Z}$.
   (a) Pour $x \in \mathcal{U}(\mathbb{Z}/mn\mathbb{Z})$, on appelle r le reste de la division de x par m. Montrer que $r \in \mathcal{U}(\mathbb{Z}/m\mathbb{Z})$.

   De la même manière, si $x \in \mathcal{U}(\mathbb{Z}/mn\mathbb{Z})$ et s le reste de la division de x par n alors $s \in \mathcal{U}(\mathbb{Z}/m\mathbb{Z})$
   (b) Soit :
   $$\begin{cases} f : \mathcal{U}(\mathbb{Z}/mn\mathbb{Z}) & \longrightarrow & \mathcal{U}(\mathbb{Z}/m\mathbb{Z}) \times \mathcal{U}(\mathbb{Z}/n\mathbb{Z}) \\ x & \longmapsto & f(x) = (r, s) \end{cases}$$
   Montrer que f est un isomorphisme de groupe multiplicatif.
   (c) En déduire que si $m \in \mathbb{N}^*$ et $n \in \mathbb{N}^*$ sont tels que $m \wedge n = 1$, alors $\varphi(mn) = \varphi(m)\varphi(n)$
5. Soit $n \in \mathbb{N}^*$. Exprimer $\varphi(n)$ en fonction de la décomposition de n en un produit de facteurs premiers.
6. Montrer que, pour $n \geqslant 3$, nous avons $\varphi(n)$ est un nombre pair

Exercice 36 :

Démontrer que, pour $n \geqslant 3$, $\varphi(n) \geqslant \dfrac{n \ln 2}{\ln n + \ln 2}$

Exercice 37 :

On appelle $\mathcal{U}(\mathbb{Z}/n\mathbb{Z})$ l'ensemble des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$. On sait que $(\mathcal{U}(\mathbb{Z}/n\mathbb{Z}), \times)$ est un groupe commutatif *(voir4.5.4)* de cardinal $\varphi(n)$
Montrer que pour tout $a \in \mathcal{U}(\mathbb{Z}/n\mathbb{Z})$, nous avons $a^{\varphi(n)} = 1$

1. Rappel : $C_n^k = \binom{n}{k}$

Exercice 38 :

Soit $n \in \mathbb{N}^*$; en considérant les fractions $\left\{\frac{1}{n}, \frac{2}{n}, \cdots, \frac{k}{n}, \cdots, \frac{n}{n}\right\}$, montrer que :

$$n = \sum_{d|n} \varphi(d)$$

Exercice 39 :

Soit $n \in \mathbb{N}^\star$
Montrer que si $(n-1)$! est un multiple de n, alors, n n'est pas un nombre premier ; la réciproque est-elle vraie ?