Trois démonstrations du petit théorème de Fermat
Mémoire sur une aventure mathématique

T.D-V

Mémoire dirigé par Pr. Mohamed Atouani

Décembre 2017 - Janvier 2018

Remerciements

Je tiens à remercier :
— Le professeur Mohamed Atouani, pour le temps qu'il a pris d'avoir dirigé mon mémoire et tous ses conseils utiles.
— Mes parents, pour m'avoir encouragé et soutenu.
— Tous ceux qui m'ont fait aimer les mathématiques, en particulier mes oncles François et Hung.

Table des matières

Introduction

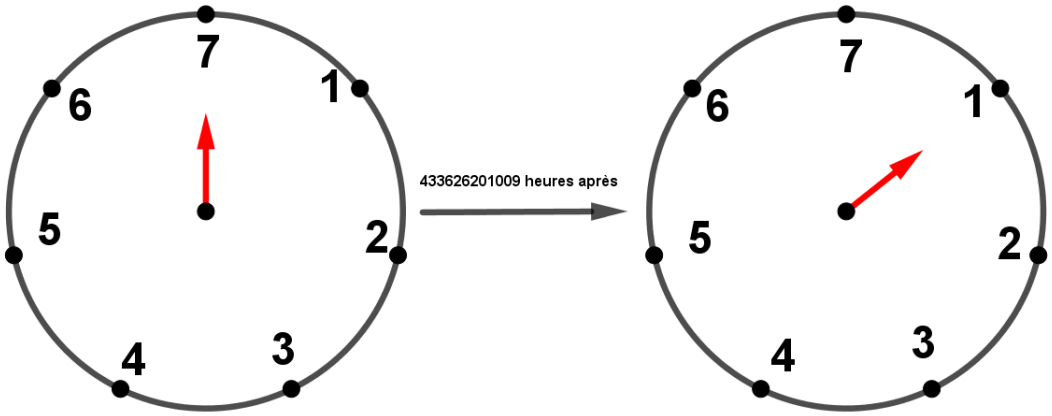
Pierre de Fermat est un grand mathématicien français (amateur) du 17è siècle. Il a travaillé notamment en théorie des nombres. Beaucoup de théorèmes et de conjectures portent son nom. Cependant, les plus connus sont de loin le petit théorème de Fermat (démontré peu de temps après Fermat par Leonhard Euler, le plus grand mathématicien de son temps) et le grand théorème de Fermat, démontré récemment, à la toute fin du 20è siècle par Andrew Wiles. C'est sur le petit que nous allons nous attarder dans ce mémoire.

Nous en verrons trois démonstrations : la première avec les congruences, la deuxième avec la récurrence et la formule du binôme de Newton et la dernière avec la théorie des groupes, les relations d'équivalences ainsi que les théorèmes de factorisation et de Lagrange. Nous introduirons chaque notion de manière claire (sauf ceux qui sont en appendice). Pour les pré-requis, il faut simplement avoir des notions de logique, de démonstrations et un peu de bagage mathématique.

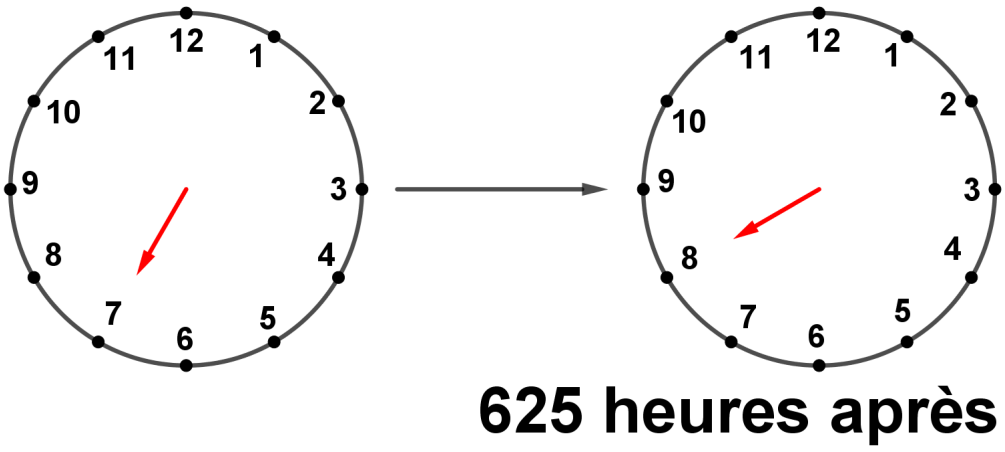
Au tout début du 19è siècle, le grand mathématicien allemand Carl Friedrich Gauss a inventé un outil très puissant pour aborder le problème. Cet outil est similaire à une horloge. On dit, par exemple, que "19 heures" est équivalent à "7 heures du soir". C'est cette idée que Gauss applique d'une manière plus formalisée en mathématiques. En fait, l'horloge que l'on utilise tous les jours représente l'arithmétique modulo 12. On tourne autour d'un cycle de 12 heures et c'est pour cela que lorsqu'il est 13 heures, la petite aiguille est pointée vers le 1, soit $13 - 12$.

Si l'on raisonne uniquement en termes d'heures, le petit théorème de Fermat stipule que si on a une horloge de p heures (pas forcément de 12), avec p étant un nombre premier, si a est un nombre non multiple de p et si l'horloge est pointé vers de le nombre p, alors après, a^{p-1} heures, la petite aiguille (des heures) sera pointée vers le 1. De la même manière, si l'aiguille est pointée vers le p, et si a^p heures s'écoulent (cette fois ci, peu importe a), l'aiguille sera pointée vers la même heure comme si seulement a heures s'étaient écroulées.

Par exemple, si on a une horloge fictive de 7 heures, et si l'aiguille des heures est pointée vers le 7, alors 433626201009 heures après ($87^{7-1} = 87^6$), la même aiguille sera tournée vers le 1. Dans la page suivante vous verrez deux illustrations de ce théorème.



Ce théorème est réservé aux nombres premiers mais on peut le généraliser pour n'importe quel entier. Par exemple, avec nos horloges habituelles. Cette fois, il faut élever un nombre n'ayant aucun diviseur commun avec 12 (premier avec 12). Nous avons pris 5. Il ne faut pas élever ce nombre n'importe comment, il faut élever à la puissance $\varphi(12)$. Si vous voulez savoir ce qu'est ce mystérieux nombre et pourquoi celui-ci, lisez la suite de ce mémoire...



1 Démonstration avec l'arithmétique modulaire

1.1 Bases sur les congruences

Définition 1. *Soient $n \in \mathbb{N}^*$ [1] et $a, b \in \mathbb{Z}$. On dit que $a \equiv b[n]$ (se lit "a est congru à b modulo n") si $a - b$ est un multiple de n dans $\mathbb{Z}$.*

Proposition 1. *(définition équivalente) Soient n, a et b définis comme ci-dessus. Alors, $a \equiv b \pmod{n}$ (écriture alternative) si et seulement si a et b ont le même reste de la division euclidienne par n.*

Démonstration. $\boxed{\Rightarrow}$ Supposons que $a \equiv b[n]$ et montrons que a et b ont le même reste de la division euclidienne par n.
Le théorème de la division euclidienne [2] affirme que l'on peut écrire a et b de façon unique sous la forme $a = a_1 n + r_1$ et $b = b_1 n + r_2$, avec $0 \leq r_1 < n$ et $0 \leq r_2 < n$. Montrons que si $a \equiv b \ (mod\ n)$, alors $r_1 = r_2$. On a $a - b = (a_1 n + r_1) - (b_1 n + r_2) = (a_1 - b_1)n + (r_1 - r_2)$, $a - b$ étant multiple de n par hypothèse, on en déduit que $r_1 - r_2$ l'est aussi. Sans perte de généralité, on peut supposer que $r_2 \geq r_1$. On a alors $0 \leq r_2 - r_1 < n$ (l'écart entre deux nombres entre 0 et n est plus petit que n) car $0 \leq r_1 \leq r_2 < n$. L'entier $r_2 - r_1$ étant multiple de n, l'inégalité précédente implique que $r_2 - r_1 = 0$. D'où le résultat.
$\boxed{\Leftarrow}$ Supposons que a et b ont le même reste de la division euclidienne par n et montrons que $a - b$ est un multiple de n.
De la même manière, le théorème de la division euclidienne affirme que l'on peut écrire a et b de manière unique sous la forme $a_1 n + r_1$ et $b_1 n + r_2$, soit $a_1 n + r$ et $b_1 n + r$ car a et b ont le même reste de la division euclidienne par n (par hypothèse). Alors, $a - b = (a_1 n + r) - (b_1 n + r) = a_1 n - b_1 n + r - r = n(a_1 - b_1)$. L'entier $a - b$ est donc bien un multiple de n et l'implication inverse est bien démontrée. □

Maintenant, on va montrer que les congruences se comportent en quelque sorte comme des vraies égalités, en montrant leurs propriétés d'addition et de multiplication.

Lemme 1. *(lemme des combinaisons linéaires) Soient a, $b \in \mathbb{Z}$ et soit n un entier $\in \mathbb{N}^*$. Dans ce cas, si n divise a et b, alors quelque soient $\alpha, \beta \in \mathbb{Z}$, n divise $\alpha a + \beta b$. On dit alors que n divise toute combinaison linéaire de a et b.*

1. $\mathbb{N}^*$ est l'ensemble des entiers strictement positifs, 0 exclu.
2. Voir premier appendice

Démonstration. Supposons que n divise a et b et montrons que $\alpha a+\beta b$ est de la forme nk, $k \in \mathbb{Z}$. D'après ce que l'on a supposé, on peut écrire a et b sous la forme $a_1 n$ et $b_1 n$, avec $a_1, b_1 \in \mathbb{Z}$. Alors, $\alpha a+\beta b = \alpha a_1 n+\beta b_1 n = n(\alpha a_1+\beta b_1)$. D'où le lemme.
En particulier, ce lemme implique que si n divise a et b, il divise $a+b$ et $a-b$. Ce sont les cas où $\alpha = 1$ et $\beta = \pm 1$ □

Proposition 2. *Soient a, b, c et d des entiers. Si $a \equiv b[n]$ et si $c \equiv d[n]$ (avec $n \in \mathbb{N}^*$), alors $a+c \equiv b+d[n]$.*

Démonstration. Cela équivaut à montrer que $(a+c)-(b+d)$ est un multiple de n. Par définition, n divise $a-b$ et $c-d$, il divise donc leur somme , d'après le lemme précédent. L'entier n divise $(a-b)+(c-d) = (a+c)-(b+d)$, ce qui démontre la proposition. □

Proposition 3. *Soient a, b, c et d des entiers Si $a \equiv b[n]$ et si $c \equiv d[n]$ (avec $n \in \mathbb{N}^*$), alors $ac \equiv bd[n]$*

Démonstration. Montrons que $ac-bd$ est un multiple de n. Par définition n divise $a-b$ et $c-d$. D'après le lemme des combinaisons linéaires, il divise donc également $d(a-b)+a(c-d)$. Or, $d(a-b)+a(c-d) = da-db+ac-ad = ac-bd$. L'entier n divise donc $ac-bd$. Par définition des congruences, $ac \equiv bd[n]$. □

1.2 Le petit théorème de Fermat et sa première démonstration

Lemme 2. *Soit p un nombre premier et a un entier non divisible par p. Soient i et j deux entiers tels que $0 < j \leq i < p$ Alors, si $ai \equiv aj[p]$, $i = j$.*

Démonstration. Si $ai \equiv aj[p]$, par définition, p divise donc $a(i-j)$. p et a sont premiers entre eux donc d'après le lemme d'Euclide [3], p divise $i-j$. Or, $0 \leq i-j < p$, d'après l'inégalité supposée. L'entier $i-j$ étant multiple de p, $i-j = 0$. On conclut donc que $i = j$. D'où le lemme. □

Théorème 1. *(petit théorème de Fermat) Soit p un nombre premier et soit a un entier non divisible par p. Alors,*

$$a^{p-1} \equiv 1[p]$$

3. Une démonstration de ce lemme est donnée dans la sous-section 3.4, mais nous vous conseillons d'aller la voir plus tard si vous n'avez pas beaucoup de bagage mathématique car cette dernière requiert d'autres notions comme les groupes ou les sous-groupes.

Démonstration. Supposons que p est un nombre premier ne divisant pas a et montrons que $a^{p-1} \equiv 1[p]$.
On pose $N = a \times 2a \times 3a \times ... \times (p-1)a = (p-1)!a^{p-1}$.
$a, 2a, 3a, ..., (p-1)a$ ont tous un reste différent par la division euclidienne par p, d'après le lemme ayant précédé ce théorème. Tous les facteurs de ce produit ont un reste différent modulo p.
De plus, aucun de ces restes n'est nul : si pour un certain i, $ai \equiv 0[p]$, alors p divise ai. Étant premier, il divise soit a, soit i. Or, il ne divise aucun des nombres strictement positifs inférieurs à lui et ne divise pas a par hypothèse. Il y a donc $(p-1)$ restes différents non nuls dans ce produit. Ces restes sont alors $1, 2, 3, 4, ..., p-1$.

On a donc, par la proposition 3 :

$$\begin{aligned} a \times 2a \times 3a \times ... \times (p-1)a &\equiv (p-1)![p] \\ a^{p-1}(p-1)! &\equiv (p-1)![p] \end{aligned}$$

Cela donne, par la proposition 2 :

$$\begin{aligned} a^{p-1}(p-1)! - (p-1)! &\equiv (p-1)! - (p-1)![p] \\ (p-1)!\left(a^{p-1} - 1\right) &\equiv 0[p] \end{aligned}$$

Cependant, p étant premier, il ne divise pas $(p-1)!$ (puisqu'il ne divise aucun des facteurs de ce produit). D'après le lemme d'Euclide, p divise donc $a^{p-1} - 1$.

$$a^{p-1} - 1 \equiv 0[p]$$

On a donc, par la proposition 2 :

$$a^{p-1} - 1 + 1 \equiv 0 + 1[p]$$

Cela donne :

$$a^{p-1} \equiv 1[p]$$

D'où le théorème. □

2 Démonstration par récurrence

N.B : Cette démonstration est séparée, les parties suivantes ne dépendent donc pas de notions abordées ici, mis à part la démonstration par récurrence, que le lecteur peut dès maintenant consulter dans le premier appendice. Le lecteur est donc libre de passer cette démonstration.

2.1 Démonstration de l'énoncé équivalent

Lemme 3. *Soit p un nombre premier et k un entier tel que $1 \leq k < p$. Alors, p divise $\binom{p}{k} = \frac{p!}{k!(p-k)!}$.*

Démonstration. $\binom{p}{k} = \frac{p!}{k!(p-k)!}$. On a donc $k!\binom{p}{k} = \frac{p!}{(p-k)!}$. Or, $\frac{p!}{(p-k)!} = p\,\frac{(p-1)!}{(p-k)!}$. L'entier p divise donc $k!\binom{p}{k}$. Or, il ne divise pas $k!$, puisqu'il est premier et $k < p$. D'après le lemme d'Euclide, il divise $\binom{p}{k}$. D'où le lemme.

□

Théorème 2. *(énoncé équivalent du petit théorème de Fermat) Si p est un nombre premier , alors pour tout $a \in \mathbb{Z}$,*

$$a^p \equiv a[p]$$

Notons que nous sommes obligés d'utiliser cet énoncé équivalent. En effet, l'autre énoncé se restreignait les entiers a à ceux qui ne sont pas divisibles par p, or celui-là est vrai pour tout entier a, ce qui nous permet de faire une récurrence sur a.

Démonstration. Montrons que la proposition $P(a)$ est vraie pour $a = 0$ et montrons que si elle est vraie pour a, elle l'est pour $a + 1$ aussi.

Initialisation : Montrons que $P(0)$ est vraie. Posons $a = 0$. On a alors $0^p = 0$. De plus, on a bien $0 \equiv 0[p]$.

Hérédité Supposons que $a^p \equiv a[p]$ et montrons que $(a+1)^p \equiv a+1[p]$. Pour démontrer l'hérédité, nous allons également avoir besoin de la formule

du binôme de Newton [4] :

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$$

Dans le cas où $b = 1$ et $n = p$, on a :

$$(a+1)^p = \sum_{k=0}^{p} \binom{p}{k} a^k$$

Ce qui est égal à

$$\binom{p}{0} + \binom{p}{1} a + \binom{p}{2} a^2 + ... + \binom{p}{p-1} a^{p-1} + \binom{p}{p} a^p$$

Or, d'après le lemme 3, p divise $\binom{p}{1}$, $\binom{p}{2}$, $\binom{p}{3}$,...$\binom{p}{p-1}$

De plus, $n \equiv 0 \pmod{p} \iff p|n$ On a donc :

$$(a+1)^p \equiv \binom{p}{0} + \binom{p}{p} a^p [p]$$

Or, $\binom{p}{0} = \binom{p}{p} = 1$. Avec l'égalité précédente, cela donne :

$$(a+1)^p \equiv 1 + a^p [p]$$

On a supposé que $a^p \equiv a[p]$.
On obtient finalement, par addition des congruences,

$$(a+1)^p \equiv a + 1[p]$$

.
On a bien démontré que si $a^p \equiv a[p]$, alors $(a+1)^p \equiv a+1[p]$, avec p premier et a un entier quelconque de $\mathbb{N}$. Par le principe de récurrence [5], $P(a)$ est vraie pour tout $a \in \mathbb{N}$. □

4. Le lecteur en trouvera la signification et la démonstration dans le deuxième appendice s'il en a besoin.

5. Voir premier appendice

Démonstration pour $a < 0$ *:* On a démontré que ce théorème est vrai pour $a \in \mathbb{N}$. Montrons qu'il est aussi vrai pour les nombres négatifs, car le principe de récurrence ne marche que sur $\mathbb{N}$ (les entiers positifs).

Lemme 4. *Si a est un entier positif, p est un nombre premier, alors $(-a)^p \equiv -a[p]$.*

Démonstration. Soit $a \in \mathbb{N}$, et soit p un nombre premier. Montrons que $(-a)^p \equiv -a[p]$

- Si p est pair, alors $p = 2$ (seul nombre premier pair). Montrons que $(-a)^2 \equiv -a[2]$ Dans ce cas, $2a \equiv 0[2]$ pour tout a. On a donc $2a - a \equiv 0 - a[2]$ d'après la proposition 2, ce qui donne $a \equiv -a[2]$. Or, $(-a)^2 = a^2 \equiv a[2]$ [6]. $(-a)^2 \equiv a[2]$ et $a \equiv -a[2]$. On a alors $(-a)^2 \equiv -a[2]$. [7]
- Si p est impair, alors on a : $a^p \equiv a[p]$ et $-1 \equiv -1[p]$
  En multipliant les congruences, on a $-a^p \equiv -a[p]$.Or, $(-a)^p = -a^p$, car p est impair. On obtient donc finalement $(-a)^p \equiv -a[p]$.

On a montré que pour tout $a \in \mathbb{N}$ et pour tout p premier, on a $(-a)^p \equiv -a[p]$. La démonstration par récurrence et le lemme prouvent l'énoncé équivalent du petit théorème de Fermat. On l'a donc démontré pour tout entier. □

2.2 Démonstration de l'équivalence des deux énoncés

Montrons que les deux énoncés sont équivalents, montrons que pour tout p premier :

$$\forall a \in \mathbb{Z}, a^p \equiv a \pmod{p} \iff \begin{cases} a^{p-1} \equiv 1 \pmod{p} & \text{si } p \nmid a \\ a^p \equiv a \pmod{p} & \text{sinon} \end{cases}$$

- Soit p un nombre premier et soit a un entier quelconque. Si $p \nmid a$, alors, d'après le premier énoncé, $a^{p-1} \equiv 1 \pmod{p}$. On obtient le résultat attendu en multipliant par a des deux côtés (car pour tout entier relatif a et pour tout entier n strictement positif, $a \equiv a[n]$). Sinon, $a^p \equiv a \equiv 0 \pmod{p}$.
- Montrons que si $a^p - a$ est un multiple de p et si $p \nmid a$, alors $a^{p-1} - 1$ l'est. En effet, $a^p - a = a(a^{p-1} - 1)$. Si p ne divise pas a, alors d'après le lemme d'Euclide, il divise $a^{p-1} - 1$.

6. En effet, si a est impair, a^2 l'est et si a est pair, a^2 l'est aussi, d'après le théorème de Fermat que l'on a démontré pour les entiers positifs.

7. Si $a \equiv -a[2]$, alors $-a \equiv a[2]$. Par transitivité des congruences ,on obtient bien le résultat final.

3 Préliminaires à la troisième démonstration

3.1 Lois de compositions internes

Définition 2. *Une application $f : E \to F$ (de E dans F) est la donnée d'un sous ensemble f de $E \times F$ tel que*

$$\forall x \in E,\ \exists! y \in F \ \text{ tel que } \ (x, y) \in f$$

Une loi de composition interne est une application de $E \times E$ (ensemble des couples d'éléments de E) dans E.

Exemple 1. Par exemple, la loi de composition interne $+$ est définie de cette manière dans $\mathbb{N}$.

$$+ : \left| \begin{array}{ccc} \mathbb{N} \times \mathbb{N} & \longrightarrow & \mathbb{N} \\ (x, y) & \longmapsto & x + y \end{array} \right.$$

Remarque 1. Notons que la définition donnée ci dessus est un peu contradictoire (définir l'addition à partir de l'addition n'est pas très solide). En fait, dans $\mathbb{N}$, l'addition est définie d'une manière plus astucieuse, en définissant d'abord les nombres :

$$\begin{aligned} 0 &= \emptyset \\ 1 = s(0) &= 0 \cup \{0\} = \emptyset \cup \{\emptyset\} = \{\emptyset\} \\ &... \\ n + 1 = s(n) &= n \cup \{n\} \end{aligned}$$

Le symbole $\emptyset$ est l'ensemble vide, défini par l'axiome suivant :

$$\exists E, \forall x, \neg(x \in E)$$

En jouant sur les implications de propositions fausses, on démontre qu'il est unique (on ne le fait pas ici, ce serait partir en hors-sujet). On ne va pas définir $\mathbb{N}$ non plus, car c'est trop compliqué sans rentrer vraiment dans la théorie des ensembles ZFC. On définit ici l'addition de la manière suivante : *Pour tout $n \in \mathbb{N}$, il existe une application $m \longmapsto n + m$ de $\mathbb{N}$ dans $\mathbb{N}$ telle que :*

1. $n + 0 = n$
2. $\forall m \in \mathbb{N},\ n + s(m) = s(n + m)$

Ce que l'on peut prouver par récurrence (mais nous le ferons pas ici). La première partie de la définition définit 0 comme l'élément neutre de l'addition. Quand à la seconde, elle dit en quelque sorte que $n + (m + 1) = (n + m) + 1$. On ne rentrera pas plus dans les détails.

3.2 Groupes et sous groupes

Définition 3. *Un groupe est la donnée d'un couple $(G, \star)$ où G est un ensemble non vide et $\star$ est une loi de composition interne sur G telle que :*

1. *G a un élément neutre : il y a un élément de G, appelons le e_G tel que quelque soit x appartenant à G, $x \star e_G = e_G \star x = x$*
2. *Quelque soient x, y et z appartenant à G, $(x \star y) \star z = x \star (y \star z)$. On dit dans ce cas que la loi $\star$ est associative.*
3. *Chaque élément a un inverse par la loi de composition interne. Pour tout élément x de G, il existe un élément de G, appelons le y tel que $y \star x = x \star y = e_G$ où e_G est l'élément neutre de G.*

   Un groupe $(G, \star)$ dit est abélien (commutatif) si pour tous x et y appartenant à G : $x \star y = y \star x$. On note en général les groupes abéliens par $(G, +)$.

Exemple 2. $(\mathbb{R}, +)$ est un groupe. La loi $+$ est associative :$(a + b) + c = a + (b + c)$, admet un élément neutre : 0 et tout élément x a un inverse $-x$ (que l'on appelle aussi *opposé*).

Exemple 3. On peut de même montrer que $(\mathbb{R}\backslash\{1\}, \star)$ est un groupe abélien où $\mathbb{R}\backslash\{1\}$ est l'ensemble des réels dont aucun n'est égal à 1 et où l'on définit $x \star y = x + y - xy$.

Montrons que cette donnée satisfait les axiomes d'un groupe abélien : La loi $\star$ a bien un élément neutre : 0. En effet, pour tout $x \in \mathbb{R}\backslash\{1\}$: $x \star 0 = x + 0 - x \times 0 = x$ et $0 \star x = 0 + x - 0 \times x = x$.
Cette loi est commutative : $x \star y = x + y - xy$ et $y \star x = y + x - yx$. Par commutativité de l'addition et de la multiplication dans $\mathbb{R}\backslash\{1\}$, $x \star y = y \star x$

Elle est associative :
Remarquons que $x \star y = (x - 1)(y - 1) + 1$.
$(x \star y) \star z = (((x - 1)(1 - y) + 1) - 1)(z - 1) + 1 = (x - 1)(1 - y)(z - 1) + 1$.
De plus, $x \star (y \star z) = (y \star z) \star x = (y - 1)(1 - z)(x - 1) + 1$, car on a montré que cette loi est commutative.
$(x \star y) \star z = (x-1)(1-y)(z-1)+1 = (x-1)((-1)\times(1-y))((-1)\times(z-1))+1 = (y - 1)(1 - z)(x - 1) + 1 = x \star (y \star z)$

Elle est inversible : si $x \star y = 0$, pour un x donné, alors on a : $x + y - xy = 0$, ce qui est équivalent à l'équation $x + (1 - x)y = 0$. Dans ce cas, $y = \frac{x}{x-1}$ et on a alors $y \in \mathbb{R}\backslash\{1\}$, car $1 \notin \mathbb{R}\backslash\{1\}$

Proposition 4. *Soit $(G, \star)$ un groupe d'élément neutre e_G et soit x un élément de G. Alors, e_G est unique et x a un unique inverse y.*

Démonstration. Supposons que $(G, \star)$ est un groupe d'éléments neutres e_G et $e_{G'}$. Montrons alors que $e_G = e_{G'}$. Par hypothèse, $e_G = e_G \star e_G = e_G \star e_{G'}$, car ce sont des éléments neutres de G. On en déduit que $e_G = e_{G'}$, car $e_G \star e_G = e_G$ et $e_G \star e_{G'} = e_{G'}$

Soient y et z deux inverses de x (défini comme ci-dessus). Alors, $x \star y = x \star z = e_G$. En composant les deux membres par y, on obtient $y \star x \star y = y \star x \star z$. Cela donne $y = z$. □

Définition 4. *Soit $(G, \star)$ un groupe et H un sous ensemble de G, on dit que $(H, \star)$ est un sous groupe de G si*

1. *$H \neq \varnothing$ (H a au moins un élément)*
2. *$\forall x \in H, \forall y \in H$, $x \star y \in H$*
3. *$\forall x \in H$, $x^{-1} \in H$, où x^{-1} est l'inverse de x par la loi de composition interne $\star$.*

Définition 5. *Ces conditions sont équivalentes à :*

1. *$e_G \in H$, où e_G est l'élément neutre de G.*
2. *$\forall x \in H, \forall y \in H$, alors $x \star y^{-1} \in H$, où y^{-1} est l'inverse de y par la loi de composition $\star$.*

Démonstration. $\boxed{\Rightarrow}$ Montrons que la définition 4 implique la définition 5. Supposons que $(H, \star)$ est un sous-groupe de $(G, \star)$. D'après le premier axiome, $H \neq \varnothing$, il existe donc un élément, appelons le x, appartenant à H. x^{-1} appartient donc à H, d'après le troisième axiome. D'après le deuxième axiome, $x \star x^{-1} \in H$ et donc, par définition de x^{-1}, $e_G \in H$. De plus, si $x, y \in H$, alors $y^{-1} \in H$. Posons $z = y^{-1}$. On a alors $x \star z \in H$, donc $x \star y^{-1} \in H$.

$\boxed{\Leftarrow}$ Montrons que la définition 5 implique la définition 4. Supposons que $(H, \star)$ est un sous-groupe de $(G, \star)$. Par l'axiome 1, $e_G \in H$ donc H est non vide. Si $x \in H$, alors $e_G \star x^{-1} \in H$, avec l'axiome 2. Par définition de e_G, $x^{-1} \in H$. Supposons que $x, y \in H$. On a alors $y^{-1} \in H$. Cela implique que $x \star ((y)^{-1})^{-1} \in H$, et donc $x \star y \in H$. □

3.3 Sous groupes de $\mathbb{Z}$

Définition 6. *On définit $n\mathbb{Z}$ (avec $n \in \mathbb{N}$) comme suit :*

$$n\mathbb{Z} = \{x \in \mathbb{Z}, \exists k \in \mathbb{Z} | n \times k = x\}$$

On peut dire que c'est l'ensemble des multiples de n dans $\mathbb{Z}$.

Proposition 5. *Soit $n \in \mathbb{N}^*$. Alors, $n\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$.*

Démonstration. Montrons que $n\mathbb{Z}$ satisfait toutes les conditions pour être un sous groupe de $(\mathbb{Z}, +)$.

1. Par sa définition, on voit que $n\mathbb{Z}$ est inclus dans $\mathbb{Z}$.
2. $0 \in \mathbb{Z}$ car $0 \times n = 0$ et $0 \in \mathbb{Z}$
3. Si x et y appartiennent à $n\mathbb{Z}$, alors n divise x et y.
   D'après le lemme des combinaisons linéaires, il divise aussi leur différence, qui appartient donc à $n\mathbb{Z}$.

□

Théorème 3. *(théorème des sous groupes de $\mathbb{Z}$) Tout sous-groupe de $\mathbb{Z}$ est de la forme $n\mathbb{Z}$ où $n \in \mathbb{N}$.*

Démonstration. Soit H un sous groupe de $\mathbb{Z}$. Montrons qu'il existe $n \in \mathbb{N}$ tel que $H = n\mathbb{Z}$. Il y a deux cas possibles :

— H est trivial ($H = \{0\}$). Dans ce cas, H est bien de la forme $n\mathbb{Z}$ avec $n \in \mathbb{N}$ car $H = 0\mathbb{Z}$, 0 étant le seul multiple de 0.

— H n'est pas trivial. Il a donc plusieurs éléments. On raisonne donc par double-inclusion. Montrons qu'il existe $n \in \mathbb{N}$ tel que $H \subset n\mathbb{Z}$ et $n\mathbb{Z} \subset H$

1. L'ensemble $H \cap \mathbb{N}^*$ a donc un plus petit élément, car il est non vide [8], (en effet, il contient forcément un entier non nul. Si cet entier est positif, il contient bien au moins un entier strictement positif. Si cet entier est strictement négatif, alors son opposé strictement positif appartient à H puisque c'est un sous groupe) appelons le n. Tous les multiples de n appartiennent à H. Montrons le par récurrence.

   Initialisation $0 \in H$, puisque $0 = 0 \times n$

8. Voir premier appendice

Hérédité Montrons que si $kn \in H$, où $k \in \mathbb{N}$, alors $(k+1)n \in H$. H étant un sous groupe de $\mathbb{Z}$ et $n \in H$, cela implique que $kn+n \in H$ et donc $(k+1)n \in H$. On a montré que tous les multiples positifs de n appartiennent à H. H étant un sous groupe, tous les opposés de ces multiples appartiennent à H. Tous les multiples de n appartiennent donc à H. Cela montre que $n\mathbb{Z} \subset H$ pour un certain $n \in \mathbb{N}$.

2. Montrons que pour ce même entier, $H \subset n\mathbb{Z}$
   Soit $k \in H$. Montrons que $k \in n\mathbb{Z}$ D'après le théorème de la division euclidienne[9], il existe un unique couple d'entiers $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que $k = qn + r$ et $0 \leq r < n$. L'entier r appartient à H, car H est un sous-groupe.
   $0 \leq r < n$, mais n est sensé être le plus petit élément de $H \cap \mathbb{N}^*$.
   r est donc forcément égal à 0, impliquant que k est un multiple de n.

Cela termine la démonstration. □

3.4 Théorème de Bachet - Bézout

Proposition 6. *Soit $(G, +)$ un groupe abélien muni de l'addition. Si $(H_1, +)$ et $(H_2, +)$ sont deux sous groupes de $(G, +)$, alors $(H_1 + H_2, +)$ en est un aussi.* On définit $H_1 + H_2$ comme suit : $H_1 + H_2 = \{u + v, u \in H_1 \text{ et } v \in H_2\}$

Démonstration. Supposons que H_1 et H_2 sont des sous-groupes de $(G, +)$ et que ce dernier est abélien.
Montrons que les trois conditions pour être un sous-groupe sont satisfaites.

1. Soit $x \in H_1 + H_2$. Montrons que $x \in G$.
   On pose $x = u_1 + v_1$, avec $u_1 \in H_1$ et $v_1 \in H_2$
   H_1 et H_2 étant inclus dans G, $u_1 \in G$ et de même pour v_1.
   $u_1 + v_1 \in G$, car G est muni d'une loi de composition interne.
2. Montrons que 0 est de la forme $u + v$, où $u \in H_1$ et $v \in H_2$.
   $0 \in H_1$ et $0 \in H_2$ car ce sont des sous groupes de G.
   0+0=0.
   0 appartient donc à $H_1 + H_2$.
3. Soient x et y deux éléments de H_1+H_2. Montrons que $x-y \in H_1+H_2$.
   Posons $x = u_1 + v_1$ et $y = u_2 + v_2$, avec u_1, u_2 appartenant à H_1 et v_1, v_2 appartenant à H_2.
   H_1 et H_2 sont deux sous-groupes de G. On a donc (par définition des

9. Là aussi, voir premier appendice

sous groupes) :
$u_1 - u_2 \in H_1$ et $v_1 - v_2 \in H_2$.
On a alos :
$u_1 + v_1 - (u_2 + v_2) = u_1 + v_1 - u_2 - v_2$.
Par commutativité,
$u_1 + v_1 - u_2 - v_2 = u_1 - u_2 + v_1 - v_2$
$= (u_1 - u_2) + (v_1 - v_2)$ par associativité.
$x - y$ est bien de la forme $u + v$, où $u \in H_1$ et $v \in H_2$

Les trois conditions sont bien démontrées. $H_1 + H_2$ est donc bien un sous groupe de G. □

Cette proposition va permettre de démontrer l'un des théorèmes les plus importants de l'arithmétique : le théorème de Bachet-Bézout (ou identité de Bézout, car le théorème de Bézout est le nom donné à un autre théorème de géométrie algébrique). Maintenant, on peut voir la créativité hors du commun des mathématiciens : on va appliquer cette proposition aux sous groupes de $\mathbb{Z}$!

Définition 7. *Le pgcd de deux nombres non tous les deux nuls est le plus grand nombre divisant ces deux nombres.*

Proposition 7. *Deux nombres non tous les deux nuls ont toujours un et un seul pgcd.*

Démonstration. Montrons que tout sous-ensemble fini non vide de $\mathbb{N}$ admet un plus grand élément.

Initialisation : Soit A un tel sous ensemble. Si $\#A = 1$, alors il a un unique élément qui est donc le plus grand.

Hérédité : Supposons que tout sous ensemble A de $\mathbb{N}$ a un plus grand élément lorsqu'il en a n ou moins. Montrons que cette propriété est aussi vraie pour $n + 1$. Posons $B = A - \{a_0\}$, où a_0 est le plus petit élément de A (qui existe, d'après l'axiome du plus petit élément, voir appendice). Alors, B a 1 élément de moins que A. L'ensemble B contient n éléments et admet donc un plus grand élément, qui est aussi le plus grand de A.
On a démontré cette propriété pour tout sous-ensemble de $\mathbb{N}$ fini par récurrence. Maintenant, posons

$$A = \{x \in \mathbb{N} \mid x|n \text{ et } x|m\} \qquad (n, m) \in \mathbb{Z} \times \mathbb{Z}^*$$

. Ce sous ensemble est fini et non vide, car n et m n'ont qu'un nombre fini de diviseurs, et 1 fait partie de cet ensemble. Alors, A a un plus grand élément,

et ce plus grand élément est unique, car si d est le plus grand élément de A, alors pour tout $x \in A$, $d \geq A$. Maintenant, supposons que d et d_1 sont deux plus grands éléments de A. Alors, $d_1 \geq d$ et $d \geq d_1$. Autrement dit, $d = d_1$. On a prouvé son unicité. □

Théorème 4. *(Théorème de Bachet-Bézout) Soient n et m deux entiers non tous les deux nuls, alors, il existe un couple d'entiers (u, v) tel que*

$$nu + mv = pgcd(n, m)$$

Démonstration. $n, m \in \mathbb{Z}$ donc $|n|\mathbb{Z}$ et $|m|\mathbb{Z}$ sont deux sous-groupes de $\mathbb{Z}$ [10] D'après la proposition 6, $|n|\mathbb{Z} + |m|\mathbb{Z}$ est un sous groupe de $\mathbb{Z}$. Il est évident que ce sous groupe est non trivial, car l'un des deux ne l'est pas. Dans ce cas, d'après le théorème des sous-groupes de $\mathbb{Z}$, $|n|\mathbb{Z} + |m|\mathbb{Z}$ est de la forme $d\mathbb{Z}$, où $d \in \mathbb{N}^*$

$$d\mathbb{Z} = \{x + y |\ x \in |n|\mathbb{Z} \ \ et \ \ y \in |m|\mathbb{Z}\} = \{|n|u + |m|v,\ u, v \in \mathbb{Z}\}$$

$= \{nu + mv |\ u, v \in \mathbb{Z}\}$, car si $x = |n|u + |m|v$, alors $x = n(\pm u) + m(\pm v)$. On a bien $-u, -v \in \mathbb{Z}$ car $u, v \in \mathbb{Z}$ par hypothèse.

Montrons que d est le pgcd de n et m. Pour cela, remarquons que si $d|n$, $d|m$ et que $pgcd(n, m)|d$, alors $d = pgcd(n, m)$ [11]. Notons que dire que $d|n$ est équivalent à dire que $n \in d\mathbb{Z}$.
$n \times 1 + 0 \times m \in d\mathbb{Z}$ donc d divise n (le cas où $u = 1$ et $v = 0$). De la même manière, $d|m$.
Montrons maintenant que le *pgcd* de n et m divise d. Il divise n et m par définition.
$d\mathbb{Z} = \{nu + mv \mid u, v \in \mathbb{Z}\}$. Or, $d \in d\mathbb{Z}$, ce qui implique que d est de la forme $nu + mv$. Par le lemme des combinaisons linéaires, $pgcd(n, m)|d$.
Les conditions pour que d soit le *pgcd* de n et m sont satisfaites. D'où le théorème. □

Corollaire 1. *Si n et m sont deux entiers de $\mathbb{N}$ premiers entre eux non tous les deux nuls, alors il existe au moins un couple d'entiers (u, v) tel que*

$$nu + mv = 1$$

10. On notera simplement $\mathbb{Z}$ et non pas $(\mathbb{Z}, +)$ car l'addition est la seule loi de composition interne intéressante faisant de $\mathbb{Z}$ un groupe.

11. Supposons que $d|n$, $d|m$ et que $pgcd(n, m)|d$ et montrons que $d = pgcd(n, m)$, avec n, m et d strictement positifs. $pgcd(n, m)|d$ et $d > 0$ donc $d \geq pgcd(n, m)$ $d|n$ et $d|m$ donc d est un diviseur commun de n et m. Il est donc égal ou inférieur au *pgcd* de n et m. $d \geq pgcd(n, m)$ et $d \leq pgcd(n, m)$ donc $d = pgcd(n, m)$

Inversement, si n, m, u et v sont des entiers tels que $nu + mv = 1$, alors

$$pgcd(n, m) = pgcd(n, v) = pgcd(u, v) = pgcd(m, u) = 1$$

Démonstration. La première implication se démontre directement par le théorème 3, en plus de la définition de deux nombres premiers entre eux (deux nombres sont premiers entre eux si leur *pgcd* est égal à 1).

Pour démontrer l'implication inverse, supposons que $nu + mv = 1$ et supposons que d est un diviseur commun de n et m, n et v, u et m ou u et v. D'après le lemme des combinaisons linéaires, d divise 1. En conséquent, $d = \pm 1$. Les seuls diviseurs communs de ces couples d'entiers sont alors -1 et 1. Leur *pgcd* est donc 1. □

Exemple 4. On a : $pgcd(7, 4) = 1$. D'après le théorème de Bézout, il existe au moins deux entiers, appelons les x et y tels que :

$$7 \times x + 4 \times y = 1$$

On pourra même voir qu'il y a une infinité de couples d'entier (x, y) satisfaisant cette condition. Il y a des méthodes pour les trouver. En voici une :
$7 \times x + 4 \times y = 1$
Posons $z = x + y$. Par conséquent on a $4z + 3x = 1$.
Cette équation admet un couple de solutions évident : $(z, x) = (1, -1)$
Il faut donc résoudre l'équation :

$$-7 + 4 \times y = 1$$

Cette équation a pour solution $y = 2$.
On a donc : $(x_0, y_0) = (-1, 2)$ (on les appelle ainsi car on va montrer que ce couple de solution n'est pas l'unique). Les solutions sont donc toutes de la forme (où $t \in \mathbb{Z}$) :

$$\begin{cases} x = -1 + 4t \\ y = 2 - 7t \end{cases}$$

Dans le cas général, étant donné une équation diophantienne (où l'on cherche des solutions entières) de la forme $ax + by = 1$, a et b donnés avec $a \wedge b = 1$ (une autre manière d'écrire le fait que a et b sont premiers entre eux).
Si (x_0, y_0) est une solution particulière de cette équation, et si l'on cherche à trouver une solution générale à cette équation (x, y), on aura :

$$ax_0 + by_0 = 1$$

$$ax + by = 1$$

ce qui implique que $a(x - x_0) + b(y - y_0) = 0$, en conséquent on a $a(x - x_0) = b(y_0 - y) = 0$.
L'entier a ne divise pas b donc a divise $y_0 - y$. Il existe donc un entier t tel que $at = y_0 - y$. En substituant par at dans l'équation $a(x - x_0) + b(y - y_0 = 0)$, on a $a(x - x_0) - b \times at$, soit $x - x_0 = bt$. Pour le même t, $x - x_0 = bt$

Exemple 5. $pgcd(343, 1001) = 7$ D'après le théorème de Bézout, il existe deux entiers u et v tels que $343u + 1001v = 7$.
Il va cette fois nous falloir une méthode bien plus rapide pour trouver une solution : l'algorithme d'Euclide étendu.
Si $343u + 1001v = 7$, alors $49u + 143v = 1$. Dans ce cas, utilisons l'algorithme d'Euclide classique pour trouver le *pgcd* de 49 et 143 (il va nous être utile même si on sait qu'il est égal à 1).

$$\begin{aligned} 143 &= 49 \times 2 + 45 \\ 49 &= 45 \times 1 + 4 \\ 45 &= 11 \times 4 + 1 \\ 4 &= 4 \times 1 \end{aligned}$$

L'égalité $45 = 11 \times 4 + 1$ nous servira comme point de départ.

$$\begin{aligned} 1 = 45 - 11 \times 4 &= (143 - 2 \times 49) - 11 \times (49 - 45) \\ &= 143 - 2 \times 49 - 11 \times (49 - (143 - 2 \times 49)) \\ &= 143 - 2 \times 49 - 11 \times (-143 + 3 \times 49) \\ &= 143 - 2 \times 49 + 11 \times 143 - 33 \times 49 \\ &= 143 \times 12 - 49 \times 35 = 1 \end{aligned}$$

Les solutions sont donc de la forme :

$$\begin{cases} x = -35 + 143t \\ y = 12 - 49t \end{cases}$$

où $t \in \mathbb{Z}$

Lemme 5. *(lemme de Gauss) Soient p, a et b trois entiers. Si p divise ab, et si p et a sont premiers entre eux, p divise b. En particulier, si p est premier et si p ne divise pas a, ils sont forcément premiers entre eux et p divise donc b. Ce cas particulier est le lemme d'Euclide.*

Démonstration. Le *pgcd* de p et a est 1. D'après le lemme 1, il existe donc deux entiers x et y tels que $px + ay = 1$. Alors, $b(px + ay) = pxb + aby = b$. Posons c l'entier tel que $pc = ab$, car d'après notre supposition, $p|ab$. $p(xb + cy) = b$. p divise donc bien b. □

Le lecteur pourra vérifier que le lemme d'Euclide utilisé pour les deux premières démonstrations du théorème de Fermat n'est jamais intervenu dans la démonstration du théorème de Bachet-Bézout. Voici une autre démonstration de ce dernier :

Démonstration. Soit l'ensemble A défini comme suit, où p est un nombre premier et a un entier quelconque non divisible par p :

$$A = \{n \in \mathbb{Z} \mid p|an\}$$

On va montrer que c'est un sous-groupe de $\mathbb{Z}$.

- Il est inclus dans $\mathbb{Z}$, par définition.
- 0 appartient à cet ensemble, car p divise $0 = 0 \times a$.
- Si x et y appartiennent à A, alors x et y s'écrivent sous la forme px_1 et py_1. $px_1 - py_1 = p(x_1 - y_1)$. p divise donc leur différence, qui du coup s'écrit également comme un facteur de a.
  Cet ensemble étant un sous-groupe de $\mathbb{Z}$, il y a forcément un élément, appelons-le d divisant tous les autres (on dit que A est le sous groupe de $\mathbb{Z}$ engendré par d). Cet élément est égal ou supérieur à 2 :
  - $d \neq 0$, car $p \in A$ et $p \neq 0$.
  - $d \neq 1$, car $1 \notin A$, par hypothèse.

  Cet élément est donc supérieur ou égal à 2. Or, p appartient à A (car p divise ap), ce qui implique que d divise p. Il n'y a que deux possibilités : $d = 1$ ou $d = p$. L'entier d est supérieur ou égal à 2 donc il est égal à p. Tous les nombres appartenant à A sont des multiples de p. Si $p|ab$ et si p ne divise pas a, alors $b \in A$, impliquant que p divise b.

□

3.5 $\mathbb{Z}/n\mathbb{Z}$: Définition et propriétés

Définition 8. *On définit* $\mathbb{Z}/n\mathbb{Z}$, $n \in \mathbb{N}^*$ *comme suit :*

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{x} \mid x \in \mathbb{Z}\}$$

$$\text{où } \overline{x} = \{a \in \mathbb{Z} \ \textit{ tels que } \ a \equiv x[n]\}$$

$\overline{x}$ se lit "classe d'équivalence de x". Lorsque l'on parlera des relations d'équivalences nous verrons que ce n'est pas un hasard.

Remarque 2. Dans l'ensemble $\mathbb{Z}/n\mathbb{Z}$, il n'y a en fait que n classes d'équivalences différentes.

Remarque 3. Notons que pour tout $a \in \mathbb{Z}$, $\overline{a} = \overline{r}$ où r est le reste de la division euclidienne par n.

Nous allons voir ci dessous comment définir les opérations dans cet ensemble. D'abord, définissons l'addition.

Le problème majeur de cet ensemble (pour y inclure l'addition) est le choix des représentant des classes. À priori, on ne peut pas définir l'addition par :

$$\overline{a} + \overline{b} = \overline{a+b}$$

Il faut trouver un moyen de contourner cette difficulté, car pour trouver une loi de composition interne. Cela peut poser des problèmes. Pour cela, revenons en à la définition de $\overline{x}$:

$$\overline{x} = \{a \in \mathbb{Z} \ \ tels\ que \ \ a \equiv x[n]\}$$

Il faut remarquer que si $a \equiv x[n]$, alors $\overline{a} = \overline{x}$. Cette remarque nous permet de contourner la difficulté. On définit donc l'addition comme ci-dessous :

$$\overline{a} + \overline{b} = \overline{a+b}$$

Montrons qu'elle est bien définie : si $\overline{x} = \overline{a}$ et si $\overline{y} = \overline{b}$, alors $\overline{a+b} = \overline{x+y}$.

Si $\overline{x} = \overline{a}$, alors $a \equiv x[n]$. De même, si $\overline{y} = \overline{b}$, alors $b \equiv y[n]$.

Par addition des congruences, on a $a + b \equiv x + y[n]$. On a donc bien $\overline{a+b} = \overline{x+y}$, par définition des classes d'équivalences.

Exemple 6. Prenons par exemple $\mathbb{Z}/7\mathbb{Z}$. Par exemple, on a : $\overline{3} + \overline{2} = \overline{5}$. Remarquons que $\overline{3} = \overline{10}$ et que $\overline{2} = \overline{9}$. De plus, $\overline{10} + \overline{9} = \overline{19}$. Or, $19 \equiv 5[7]$ donc $\overline{19} = \overline{5}$.

De la même manière, on définit la multiplication comme suit : $\overline{a} \times \overline{b} = \overline{a \times b}$. Montrons de la même manière que si $\overline{a} = \overline{x}$ et si $\overline{b} = \overline{y}$, alors $\overline{a \times b} = \overline{x \times y}$. On a $a \equiv x[n]$ et $b \equiv y[n]$. On a donc $a \times b \equiv x \times y[n]$, ce qui est donc équivalent à $\overline{x \times y} = \overline{a \times b}$. La multiplication est donc également bien définie.

Cet ensemble, muni de l'addition, est un groupe.

— $\overline{0}$ est l'élément neutre de l'addition : $\overline{x} + \overline{0} = \overline{x+0} = \overline{x}$.
— L'addition est associative : $\overline{a+b} + \overline{c} = \overline{a} + \overline{b+c} = \overline{a+b+c}$, donc on a bien $(\overline{a} + \overline{b}) + \overline{c} = \overline{a} + (\overline{b} + \overline{c})$.
— Chaque élément admet un inverse (opposé) : Si $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$, alors $\overline{x} + \overline{n-x} = \overline{n} = \overline{0}$.

Cette multiplication admet un élément neutre : $\overline{1}$.

Elle est associative : $\overline{a \times b} \times \overline{c} = \overline{a} \times \overline{b \times c}$, donc on a bien $(\overline{a} \times \overline{b}) \times \overline{c} = \overline{a} \times (\overline{b} \times \overline{c})$. Cela nous servira pour transformer cela en groupe.

3.6 Inversibilité dans $\mathbb{Z}/n\mathbb{Z}$

On va appliquer le théorème de Bachet-Bézout de manière un peu spéciale. Cependant, cela, avec beaucoup de travail et de créativité encore, sera crucial pour démontrer le petit théorème de Fermat.
On veut absolument transformer l'ensemble $(\mathbb{Z}/n\mathbb{Z}, \times)$ en un groupe, et pour cela, il lui manque l'inversibilité des éléments (c'est à dire le troisième axiome pour qu'un ensemble soit un groupe), pour qu'il ait en quelque sorte des bonnes propriétés (indispensables pour l'application du théorème de Lagrange) , pour lui appliquer tout ce que l'on a vu et pour démontrer le théorème. Là encore, vous verrez l'imagination spectaculaire des mathématiciens, qui inventent (ou découvrent) des manières de résoudre les problèmes absolument incroyables.

Proposition 8. *Soit $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$. $\overline{a}$ admet un inverse par la loi $\times$ dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si le pgcd de ce nombre et de n est 1.*

Démonstration.
— Supposons que $\overline{a}$ admet un inverse par la loi $\times$ dans $\mathbb{Z}/n\mathbb{Z}$. Montrons que $pgcd(n, a) = 1$.
Si $\overline{a}$ admet un inverse (appelons le b) dans $\mathbb{Z}/n\mathbb{Z}$: $\overline{a \times b} = \overline{1}$, ce qui est équivalent $ab \equiv 1[n]$ Il existe donc $k \in \mathbb{Z}$ tel que, $ab = nk + 1$, et donc $ab + n(-k) = 1$. D'après le théorème de Bézout (le corollaire 1 plus précisément), $pgcd(a, n) = 1$.
— Supposons que $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ et que $pgcd(a, n) = 1$. Montrons que $\overline{a}$ admet un inverse dans $\mathbb{Z}/n\mathbb{Z}$. D'après le même corollaire, il existe au moins un couple d'entiers (u, v) tels que $au + nv = 1$ ou encore : $\overline{1} = \overline{au + nv} = \overline{au}$ car $nv \equiv 0[n]$. Au final, on a l'égalité $\overline{1} = \overline{au}$ qui termine la preuve de la proposition.

□

3.7 Fonction indicatrice d'Euler

Définition 9. *On définit* $(\mathbb{Z}/n\mathbb{Z})^\times$, $n \in \mathbb{N}^*$ *de la manière suivante :*

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{x} \in \mathbb{Z}/n\mathbb{Z} |\ \exists\, \overline{b} \in \mathbb{Z}/n\mathbb{Z} \ \ tel \ \ que \ \ \overline{ab} = 1\}$$

$((\mathbb{Z}/n\mathbb{Z})^\times, \times)$ est donc un groupe, car on a vu que la multiplication admet un élément neutre, est associative et d'après la proposition 8, chaque élément est inversible. Pour tout $n \in \mathbb{N}^*$, $(\mathbb{Z}/n\mathbb{Z}, \times)$ n'est pas un groupe. En fait, aucun d'entre eux n'en est un. $\overline{0} \in \mathbb{Z}/n\mathbb{Z}$ quelque soit n. Il n'est pas inversible car il ne satisfait pas les conditions pour l'être.

Définition 10. *On note*

$$\varphi(n) = \#\{1 \leq x \leq n \mid pgcd(x, n) = 1\}$$

est le symbole indiquant le cardinal, c'est à dire le nombre d'éléments d'un ensemble. $\varphi(n)$ se lit "phi de n" : c'est la fonction indicatrice d'Euler, indiquant le nombre de nombres entiers positifs premiers avec n et inférieurs à n. Ce n'est pas par hasard qu'elle porte le nom du plus grand mathématicien du 18è siècle, car ce dernier a travaillé là-dessus.
D'après la proposition 8 (à la page précédente), on a : $\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times$
Ce résultat sera d'une grande importance pour la dernière démonstration du petit théorème de Fermat.

3.8 Morphismes de groupes, images et noyaux

Soient $(G, \star)$ et $(G', *)$ deux groupes.
Soit f une application de G dans G'.

Définition 11. *On dit que* f *est un morphisme de groupes si :*
$\forall x \in G$ *et* $\forall y \in G, \quad f(x \star y) = f(x) * f(y)$.

Exemple 7. Par exemple si $(G, \star) = (\mathbb{R}, +)$ et $(G', *) = (\mathbb{R}_+^*, \times)$
L'application $f : \ x \mapsto e^x$ est un morphisme de groupes de $(\mathbb{R}, +)$ dans $(\mathbb{R}_+^*, \times)$.
En effet, $e^{x+y} = e^x \times e^y$.

Soit $f : \ G \longrightarrow G'$ un morphisme de groupes.

Définition 12. *On note ker* $f = \{x \in G \mid f(x) = e_{G'}\}$ *(se lit "noyau de* f *")*

Proposition 9. *ker f est un sous groupe de G (muni de la même loi)*

Démonstration. Montrons que $ker\ f$ satisfait toutes les conditions pour être un sous groupe de G.

1. Par sa définition, on voit directement que $kerf \subset G$.
2. Montrons que $e_G \in ker\ f$.
   $f(e_G \star e_G) = f(e_G) * f(e_G) \Rightarrow f(e_G) = f(e_G) * f(e_G)$
   Notons $f(e_G)^{-1}$ l'inverse de $f(e_G)$ pour la loi $*$.
   L'égalité précédente a pour conséquence $f(e_G)^{-1} * f(e_G) = f(e_G)^{-1} * f(e_G) * f(e_G)$. Cela implique finalement que $e_{G'} = f(e_G)$
   Par définition, $e_{G'} \in ker\ f$.
3. Supposons que $x \in ker\ f$ et $y \in ker\ f$ et montrons que $x \star y^{-1} \in ker\ f$, où y^{-1} est l'inverse de y par la loi $\star$. Alors,
   $f(x \star y^{-1}) = f(x) * f(y^{-1}) = e_{G'} * f(y^{-1}) = f(y^{-1})$.
   De plus, $e_{G'} = f(e_G) = f(y * y^{-1}) = f(y) * f(y^{-1}) = f(y^{-1})$, car $y \in ker\ f$. On a alors $f(y^{-1}) = f(e_G) = e_{G'}$, donc $f(y^{-1}) \in ker\ f$. On obtient bien le résultat attendu : $x \star y^{-1} \in ker\ f$

□

Proposition 10. *Si on définit Im f de la manière suivante :*

$$Im\ f = \{y \in G', |\ \exists x \in G \text{ tel que } f(x) = y\}$$

alors, Im f est un sous groupe de $(G', *)$.

Démonstration. Montrons que $Im\ f$ statisfait toutes les conditions pour être un sous groupe de G'.

1. Par sa définition, on voit instantanément que $Im\ f \subset G'$.
2. Montrons que $e_{G'} \in Im\ f$.
   $e_{G'} = f(e_G)$ et $e_G \in G$.
3. Supposons que $x, y \in Im\ f$ et montrons que $x * y \in Im\ f$.
   Posons $x = f(x_1)$ et $y = f(y_1)$.$x * y = f(x_1) * f(y_1) = f(x_1 \star y_1)$, car f est un morphisme de groupes. G étant un groupe, $x_1 \star y_1 \in G$.
4. Supposons que $x \in Im\ f$ et montrons que $x^{-1} \in Im\ f$.
   Posons $x = f(x_1)$. Notons que $x^{-1} = f(x_1)^{-1}$. On a alors, car f est

un morphisme de groupes :

$$\begin{aligned} f(x_1 \star x_1^{-1}) &= f(x_1) * f(x_1^{-1}) \\ &= e_{G'}, \text{ car } x_1 \star x_1^{-1} = e_G \text{ et } f(e_G) = e_{G'} \\ f(x_1)^{-1} * (f(x_1) * f(x_1^{-1})) &= f(x_1)^{-1} * e_{G'} \\ (f(x_1)^{-1} * f(x_1)) * f(x_1^{-1}) &= f(x_1)^{-1}, \text{ par associativité} \\ f(x_1)^{-1} * f(x_1) = e_{G'} &\Rightarrow f(x_1^{-1}) = f(x_1)^{-1} \\ &\Rightarrow f(x_1^{-1}) = x^{-1} \end{aligned}$$

$x_1 \in G$ donc $x_1^{-1} \in G$, car G est un groupe. Au final, $x^{-1} \in Im\ f$

□

3.9 Injections, surjections, bijections

Définition 13. *Soit $f : E \longrightarrow F$ une application de E dans F.*

- *On dit que f est surjective si pour tout élément y de F, il y a au moins un élément x de E tel que y = f(x).*
- *On dit que f est injective si pour tous $x, y \in E$ la condition $f(x_1)=f(x_2)$ implique que $x_1 = x_2$.*
- *On dit que f est bijective si elle est à la fois surjective et injective.*

Soit Y un sous-ensemble de F. On note $f^{-1}(Y)$ (ensemble image réciproque de Y par f) l'ensemble défini comme suit :

$$f^{-1}(Y) = \{x \in E \text{ tel que } f(x) \in Y\}$$

Proposition 11. *Si f est un morphisme de groupes :*

- *f est surjective si et seulement si Im f = F*
- *f est injective si et seulement si ker $f = \{e_E\}$*

Démonstration.

- Supposons que f est surjective. Montrons que $Imf = F$. Par définition, $Im\ f = \{f(x) \in F \mid x \in E\}$. Or, d'après la définition de la surjectivité, si $x \in F$, alors $x \in Im\ f$. $F \subset Im\ f$. Si $F = Im\ f$, alors $F \subset Im\ f$. Tout élément de f a donc un antécédent par f.
- Si f est injective, il y a un seul élément $x \in E$ tel que $f(x) = e_F$. La proposition 9 (voir page 24) nous indique que cet élément x est e_E.

  Maintenant, supposons que $ker\ f = \{e_E\}$ et montrons que f est injective. Supposons qu'il existe deux éléments x, y de F tel que $f(x) = f(y)$. Montrons que $x = y$.
  $f(x) = f(y)$ donc on a $f(x) * f(x)^{-1} = f(y) * f(x)^{-1}$. Cela donne

$e_F = f(x \star y^{-1})$, car $f(y^{-1}) = f(y)^{-1}$ (voir démonstration de la proposition 10, page 24). D'après ce que l'on a supposé, on a forcément $x \star y^{-1} = e_E$. On obtient finalement $x = y$. f est donc bien injective.

□

Proposition 12. *Soient E et F deux ensembles finis. Soit $f : E \longrightarrow F$ une application de E dans F. Si f est injective, alors $\# F \geq \# E$.*

Démonstration. Supposons que f est injective.
Dans ce cas, deux éléments de E ont forcément deux images distinctes par f. On a alors $\#Im\ f = \#E$.
Or, $Im\ f \subset F$ donc on a $\#Im\ f \leq \#F$.
On en déduit finalement que $\#E \leq \#F$.

□

Pour la surjectivité, la démonstration est un peu plus technique, et si vous n'y comprenez rien, vous pouvez l'admettre pour revenir dessus plus tard.

Lemme 6. *Si l'on définit f de la même manière que dans la proposition 12 alors $f^{-1}(\bigcup_{y\in F}\{y\}) = \bigcup_{y\in F} f^{-1}(\{y\})$*

Démonstration. Montrons que $f^{-1}(\bigcup_{y\in F}\{y\}) \subset \bigcup_{y\in F} f^{-1}(\{y\})$ et que $\bigcup_{y\in F} f^{-1}(\{y\}) \subset f^{-1}(\bigcup_{y\in F}\{y\})$ (raisonnement par double-inclusion).

Soit $x \in f^{-1}(\bigcup_{y\in F}\{y\})$. Cela implique que $f(x) \in (\bigcup_{y\in F}\{y\})$ et donc il existe y tel que $f(x) \in \{y\}$. Alors, $x \in f^{-1}(\{y\})$. Il existe un élément $y \in F$ tel que $y \in f^{-1}(\{y\})$ donc $x \in \bigcup_{y\in F} f^{-1}(\{y\})$. x appartient donc à $\bigcup_{y\in F} f^{-1}(\{y\})$. Cela montre que $f^{-1}(\bigcup_{y\in F}\{y\}) \subset \bigcup_{y\in F} f^{-1}(\{y\})$

Soit $x \in \bigcup_{y\in F} f^{-1}(\{y\})$. Alors, il existe y_1 appartenant à F tel que $x \in f^{-1}(\{y_1\})$. Cela implique que $f(x) \in \{y_1\}$ et donc que $f(x) \in \bigcup_{y\in F}\{y\}$. x appartient donc à $f^{-1}(\bigcup_{y\in F}\{y\})$. On en conclut que
$\bigcup_{y\in F} f^{-1}(\{y\}) \subset f^{-1}(\bigcup_{y\in F}\{y\})$. D'où le fait que $f^{-1}(\bigcup_{y\in F}\{y\}) = \bigcup_{y\in F} f^{-1}(\{y\})$.

□

Proposition 13. *Si f est surjective et définie de la même manière que dans la proposition 12, alors $\# F \leq \# E$. De cette proposition et de la précédente, on en déduit que si il existe une bijection (application bijective) entre E et F, alors $\# E = \# F$.*

Démonstration. $F = \bigcup_{y\in F}\{y\}$ (propriété vraie peu importe l'ensemble F).
De plus, $E = f^{-1}(F)$, l'ensemble image réciproque de F, puisque f est une

application de E dans F, ce qui nous donne $E = f^{-1}(\bigcup_{y\in F}\{y\})$.

D'après le lemme précédent, On a $E = f^{-1}(F) = f^{-1}(\bigcup_{y\in F}\{y\}) = \bigcup_{y\in F} f^{-1}(\{y\})$. f est surjective donc $\#f^{-1}(\{y\}) \geq 1$ pour tout y. De plus, $\#\bigcup_{y\in F} f^{-1}(\{y\}) = \sum_{y\in F} \#f^{-1}(\{y\})$, car c'est une union disjointe (un élément est associé à un unique autre par une application).
On obtient finalement $\#E = \sum_{y\in F} \#f^{-1}(\{y\}) \geq \sum_{y\in F} 1 = \#F$. D'où le résultat.

□

4 La dernière ligne droite vers le théorème

4.1 Relations binaires

Définition 14. *Une relation binaire $\mathcal{R}$ sur un ensemble E est la donnée d'un sous ensemble R de $E \times E$. Le sous-ensemble R est appelé le graphe de la relation $\mathcal{R}$.*

Exemple 1. Par exemple, si $\mathcal{R}$ est la relation définie sur $\mathbb{R}$ telle que $x\Re y \iff x+y=2$, alors le graphe de $\mathcal{R}$ est la droite d'équation $y=-x+2$

4.2 Relations d'équivalence

Définition 15. *Une relation d'équivalence (notée $\mathcal{R}$) est une relation binaire satisfaisant les propriétés suivantes :*

1. *La réflexivité : $x\mathcal{R}x\ \forall x \in E$*
2. *La symétrie : $\forall x, \forall y \in E$, $x\mathcal{R}y$ si et seulement si $y\mathcal{R}x$*
3. *La transitivité : $\forall x \in E, \forall y \in E$ et $\forall z \in E$, si $x\mathcal{R}y$ et $y\mathcal{R}z$, alors $x\mathcal{R}z$.*

On note Cl(x) (classe d'équivalence de x) l'ensemble défini ci-dessous :

$$Cl(x) = \{y \in E \mid x\mathcal{R}y\}$$

Exemple 2. Les congruences forment une relation d'équivalence.
En effet, posons à titre d'exemple $x\mathcal{R}y$ si et seulement si $x \equiv y[n]$ pour $n \in \mathbb{N}^*$.

1. $x \equiv x[n]$, car $x - x = 0$ et $n|0$
2. Si $x \equiv y[n]$, alors $n|x-y$.

$$\begin{aligned} x - y \equiv 0[n] &\Rightarrow -(x-y) \equiv (-1) \times 0[n] \equiv 0[n] \\ &\Rightarrow y - x \equiv 0[n] \end{aligned}$$

   On a donc bien $y \equiv x[n]$
3. Posons $x \equiv y[n]$ et $y \equiv z[n]$

$$\begin{aligned} x \equiv y[n] \text{ et } y \equiv z[n] &\Rightarrow x - y \equiv 0[n] \\ &\Rightarrow (x-y) + y \equiv 0 + z[n] \\ &\Rightarrow x \equiv z[n] \end{aligned}$$

On a montré les trois conditions pour que les congruences soient une relation d'équivalence. Ce n'est d'ailleurs pas par hasard que dans l'ensemble $\mathbb{Z}/n\mathbb{Z}$, $\overline{x}$ se lit "classe d'équivalence de x".

$$\overline{x} = \{y \in E \mid x\mathcal{R}y\} = \{y \in \mathbb{Z} \mid x \equiv y[n]\}$$

4.3 Classes d'équivalence et partition d'un ensemble

Définition 16. *Soit E un ensemble quelconque. Une partition de E est un ensemble de parties (sous ensembles) non vides de E telle que l'union des parties est E et que ces parties sont deux à deux disjointes. Autrement dit, si $(A_i)_{i\in I}$ est une famille de parties de E, où I désigne un ensemble quelconque, on dit que $(A_i)_{i\in I}$ forme une partition de E, alors :*

1. $\forall i \in I,\ A_i \neq \emptyset$
2. $\forall i \in I, \forall j \in I,\ i \neq j \iff A_i \cap A_j = \emptyset$
3. $\bigcup_{i\in I} A_i = E$

Proposition 14. *Soit E un ensemble, $\mathcal{R}$ une relation d'équivalence définie sur cette dernière, et $Cl(x)$ la classe d'équivalence de x pour $x \in E$.*
On a alors :

$$E = \coprod_{x\in E} Cl(x)$$

E est l'union disjointe des classes d'équivalences de $\mathcal{R}$. Les classes d'équivalences de $\mathcal{R}$ forment donc une partition de l'ensemble E.

Démonstration. Montrons que $E \subset \coprod_{x\in E} Cl(x)$ et que $\coprod_{x\in E} Cl(x) \subset E$.

- Si $x \in E$, alors par réflexivité, $x \in Cl(x)$. Cela montre de plus qu'aucune classe d'équivalence est vide.
- Si $y \in Cl(x)$, où $x \in E$, alors par définition de $Cl(x)$, $y \in E$.
- Montrons à présent que cette union est disjointe, c'est à dire que pour tous x, y, si $Cl(x) \cap Cl(y) \neq \emptyset$, alors $Cl(x) = Cl(y)$. Autrement dit, si $Cl(x) \neq Cl(y)$, $Cl(x) \cap Cl(y) = \emptyset$.
  Supposons que $Cl(x) \cap Cl(y) \neq \emptyset$. Il existe donc un élément tel que $x\mathcal{R}z$ et $y\mathcal{R}z$. Cependant, si $y\mathcal{R}z$, par symétrie, $z\mathcal{R}y$. On a donc $x\mathcal{R}z$ et $z\mathcal{R}y$ Par transitivité, $x\mathcal{R}y$. Par définition de $Cl(x)$, $Cl(x) = Cl(y)$.

□

Exemple 3. On a vu que les congruences forment une relation d'équivalence. Soit $x \in \mathbb{Z}$, on pose $Cl(x) = \{y \in \mathbb{Z} \mid x \equiv y[3]\}$.
Alors, d'après la proposition 14,

$$\mathbb{Z} = \overline{1} \coprod \overline{2} \coprod \overline{3}$$

Cela ne marche pas que pour $n = 3$, mais pour tout $n \in \mathbb{N}^*$.

En fait, quelque soit $n \in \mathbb{N}^*$, si $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$

$$\mathbb{Z} = \coprod_{x \in \mathbb{Z}} \overline{x}$$

Exemple 4. Soit l'application définie par :

$$f : \left| \begin{array}{ccc} E & \longrightarrow & F \\ x & \longmapsto & f(x) \end{array} \right.$$

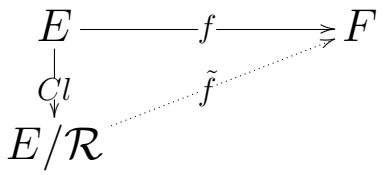
Alors, la relation binaire définie sur E par $x\mathcal{R}y \iff f(x) = f(y)$ est une relation d'équivalence. En effet, $f(x) = f(x)$, si $f(x) = f(y)$, alors $f(y) = f(x)$ et de même, si $f(x) = f(y)$ et $f(y) = f(z)$, alors $f(x) = f(z)$. Cela va nous servir pour le théorème de factorisation.

4.4 Théorème de factorisation

Théorème 5. *(théorème de factorisation) Soit $f : E \longrightarrow F$ une application. Soit la relation binaire $\mathcal{R}$ définie sur E par $x\mathcal{R}y \iff f(x) = f(y)$, c'est donc aussi une relation d'équivalence (voir exemple 4 ci dessus). Soit $E/\mathcal{R}$ l'ensemble des classes d'équivalences Cl(x) avec $x \in E$ de $\mathcal{R}$. Soit l'application définie par :*

$$Cl : \left| \begin{array}{ccc} E & \longrightarrow & E/\mathcal{R} \\ x & \longmapsto & Cl(x) \end{array} \right.$$

Alors, il existe une unique application injective, notons la $\tilde{f}$ (se lit "f tilde"), telle que $f = \tilde{f} \circ Cl$. Cette application est surjective si et seulement si f l'est. $f = \tilde{f} \circ Cl$ est une composition d'applications. On dit que $\tilde{f}$ rend le diagramme suivant commutatif :



Démonstration. Montrons que cette application existe et qu'elle est unique. Pour tout élément $\alpha \in E/\mathcal{R}$ tel que $\alpha = Cl(x)$, on pose $\tilde{f}(\alpha) = f(x)$.
Si $\alpha = Cl(x) = Cl(x')$, alors $x\mathcal{R}x'$, on a donc $f(x) = f(x')$, par la relation d'équivalence que l'on a défini. La fonction $\tilde{f}$ est donc bien définie.

Soit g une autre fonction qui satisfait les mêmes propriétés. Montrons que $g = \tilde{f}$. On a donc $f(x) = g(Cl(x))$. L'application g fait associer à la classe de x l'image de x, ce qui implique que $g(Cl(x)) = \tilde{f}(Cl(x))$, cette application est donc bien égale à $\tilde{f}$.

Montrons que cette application est injective :
Posons $\alpha = Cl(x)$ et $\beta = Cl(y)$, supposons que $\tilde{f}(\alpha) = \tilde{f}(\beta)$ et montrons que $\alpha = \beta$.
$\tilde{f}(\alpha) = \tilde{f}(\beta)$ donc on a $f(x) = f(y)$. On obtient par définition de $\mathcal{R}$, $x\mathcal{R}y$. Mais si $x\mathcal{R}y$, alors $Cl(x) = Cl(y)$, ce qui a pour conséquence que $\alpha = \beta$.
Cette injectivité est assez naturelle et intuitive. Après tout, la philosophie des relations d'équivalences est de considérer tous les éléments ayant une même propriété par un même élément. Ainsi, tous les éléments ayant la même image sont réduits à un seul élément. L'image de cet élément a donc un seul antécédent : la classe du représentant.

Montrons que si f est surjective, alors $\tilde{f}$ est surjective (et donc bijective).
Si f est surjective, alors pour tout $y \in F$, il existe un élément x de E tel que $f(x) = y$. Alors, on a $x \in Cl(x)$, par réflexivité. En conséquent, $Cl(x) \in E/\mathcal{R}$ et de plus, $\tilde{f}(Cl(x)) = y$ □

4.5 Derniers préliminaires

Proposition 15. *Soit $(G, *)$ un groupe. Soit $(H, *)$ un sous-groupe de G. Soit l'application*

$$f : \left| \begin{array}{ccc} G & \longrightarrow & \mathcal{P}(G) \\ g & \longmapsto & g * H \end{array} \right.$$

Où $\mathcal{P}(G)$ est l'ensemble des parties (sous-ensembles) de G. On pose la relation binaire suivante dans G : $g\mathcal{R}g'$ si et seulement si $f(g) = f(g')$. L'exemple 4, page 30, montre que c'est une relation d'équivalence. Soient $G/\mathcal{R} = \{Cl(g) \mid g \in G\}$ et $G/H = \{g * H \mid g \in G\}$. Alors, pour tout $g \in G$

$$Cl(g) = g * H \text{ , autrement dit, } G/\mathcal{R} = G/H$$

Démonstration. — Soit $g' \in Cl(g)$. Montrons que $g' \in g * H$. Si $g' \in Cl(g)$, alors $g' * H = g * H$. Il existe donc deux éléments de H, notons

les h et h', tels que $g * h = g' * h'$. Notons h'^{-1} l'inverse de h' par la loi $*$. $h^{-1} \in H$, car H est un sous-groupe de G.

$$\begin{aligned} g' * h' * h'^{-1} &= g * h * h'^{-1} \\ g &= g * h * h'^{-1} \\ g &= g * (h * h'^{-1}), \text{ par associativité} \end{aligned}$$

H étant un sous-groupe, $h' * h'^{-1} \in H$. g' est donc bien de la forme gh où $h \in H$.

— Soit $x \in gH$, montrons que $x \in Cl(g)$.
x est donc nécessairement de la forme $g * h$.
Montrons alors que $x * H = g * H$, ou encore que $g * h * H = g * H$ (par définition de $Cl(g)$).

1. Montrons que $g * h * H \subset g * H$.
   Soit $g * h * h' \in g * h * H$ et montrons que $g * h * h'$ est de la forme $g * h''$, avec $h \in H$
   $g * h * h' = g * (h * h')$, par associativité. $h * h' \in H$, car H est un sous-groupe de G. $g * h * h'$ est bien de la forme $g * h''$, où $h \in H$. On a donc $g * h * H \subset g * H$.
2. Montrons que $g * H \subset g * h * H$.
   Soit $g * h_1 \in g * H$, $h_1 \in H$ et montrons que $g * h_1$ est de la forme $g * h * h'$. Cherchons h' tel que $g * h_1 = g * h * h'$. Alors, $h' = (h^{-1} * h_1)$. Cet élément appartient bien à H, car $(H, *)$ est un sous-groupe. On a alors

   $$\begin{aligned} g * h * h' &= g * h * (h^{-1} * h_1) \\ &= g * h * h^{-1} * h_1, \text{ par associativité} \\ &= g * h_1 \end{aligned}$$

   On a montré que $g * h_1$ est bien de la forme $g * h * h'$.

□

4.6 Le théorème de Lagrange sur les groupes

Nous allons voir ici le théorème qui va permettre de démontrer notre résultat avec une facilité déroutante, d'où la puissance des groupes, permettant de résoudre un maximum de problèmes avec un minimum d'effort.

Lemme 7. *Soit $(G, *)$ un groupe, $(H, *)$ un sous groupe de G, g un élément de G et soit l'application φ_g définie par :*

$$\varphi_g : \left| \begin{array}{ccc} H & \longrightarrow & g * H \\ h & \longmapsto & g * h \end{array} \right.$$

Alors, cette application est bijective.

Démonstration. 1. Montrons qu'elle est injective.
Posons $\varphi_g(h) = \varphi_g(h')$ et montrons que $h = h'$.
On a donc $g * h = g * h'$
Soit g^{-1} l'inverse de g par la loi $*$ (cet inverse existe car $g \in G$ et G est un groupe).
$g^{-1} * g * h = g^{-1} * g * h'$ et donc finalement, $h = h'$

2. Montrons qu'elle est surjective. Supposons que $y \in g * H$ et montrons qu'il existe un élément x de H tel que $y = \varphi_g(x)$.
Si $y \in g * H$, alors y est de la forme $g * h$, $h \in H$.
$y = g * h$, ce qui nous donne au final $y = \varphi_g(h)$.

φ_g est donc une application bijective. Il y a donc une bijection entre H et $g * H$. En particulier, $\#H = \#g * H$. □

Théorème 6. *(théorème de Lagrange) Soit $(G, *)$ un groupe d'ordre (de cardinal) fini. Si $(H, *)$ est un sous-groupe de $(G, *)$, alors $\#H | \#G$*

Démonstration. Soit la relation d'équivalence définie sur G par
$g' \mathcal{R} g \iff gH = g'H$
Soit $G/H = \{g * H \mid g \in G\}$. Cet ensemble est fini, car G l'est.
Démontrons maintenant que $\#H | \#G$:
On a, d'après la proposition 14 (p.29) :

$$G = \coprod_{g \in R(G)} Cl(g)$$

où $R(G)$ est un ensemble des représentants des classes d'équivalence dans G (dans cet ensemble, aucun élément n'est en relation avec un autre).
Remarquons que $\#G/H = \#R(G)$. On a donc, d'après la proposition 15 (p.31) :

$$G = \coprod_{g \in R(G)} g * H$$

$$\#G = \# \coprod_{g \in R(G)} g * H$$

$$\#G = \sum_{g \in R(G)} \#g * H$$

car il s'agit d'une union disjointe.

$$\#G = \sum_{g \in R(G)} \#H = \#H + \#H + ... + \#H$$

d'après le résultat qu'on a montré ($\#H = \#g * H$). Il y a un H pour chaque $g \in R(G)$

$$\#G = \#R(G) \times \#H$$

$$\#G = \#G/H \times \#H$$

car $\#R(G) = \#G/H$. D'où le théorème $\square$

5 La troisième démonstration du théorème de Fermat

Nous voilà arrivés presque à la dernière étape de notre parcours. Il nous reste que deux notions à définir. Ensuite, tout ce que l'on verra ne sera qu'une application des propositions que l'on a vues. La seule chose dont on a encore besoin, c'est d'un peu de créativité et de courage. C'est le commencement de la fin.

5.1 Définitions et lemme

Définition 17. *Soit G un groupe multiplicatif d'élément neutre e_G et a un élément de G. Soit $A = \{r \in \mathbb{N}^* \mid a^r = e_G\}$, où a^r est défini par*

- *Si $r \geq 0$, $a^0 = e_G$ et $a^{r+1} = a^r \times a$*
- *Si $r < 0$, $a^r = (a^{-1})^{-r}$, où a^{-1} est l'inverse de a par la loi $\times$ (car $(G, \times)$ est un groupe).*

On définit $ord(a)$ comme suit :

$$ord(a) = \begin{cases} min\ A & si \quad A \neq \emptyset \\ +\infty & si \quad A = \emptyset \end{cases}$$

On définit $< a >$ comme suit :

$$< a >= \{a^r \mid r \in \mathbb{Z}\}$$

On démontre aisément que $(< a >, \times)$ est un groupe.

Proposition 16. *Soit f un morphisme de groupes de $(E, \star)$ dans $(F, *)$. Soit la relation d'équivalence $\mathcal{R}$ définie par $x\mathcal{R}y \iff f(x) = f(y)$. Alors, cette relation d'équivalence est équivalente à $x\mathcal{R}y \iff f(x \star y^{-1}) = e_F$*

Démonstration. Supposons que $f(x) = f(y)$. Alors,
$f(x) * f(y)^{-1} = e_F = f(x) * f(y^{-1}) = f(x \star y^{-1})$ (voir démonstration de la proposition 10, page 24), ce qui termine la démonstration. □

Lemme 8. *Le cardinal de $< a >$ est égal à $ord(a)$.*

Démonstration. Soit le morphisme de groupes suivant :

$$\phi : \left| \begin{array}{ccc} (\mathbb{Z}, +) & \longrightarrow & (< a >, \times) \\ r & \longmapsto & a^r \end{array} \right.$$

En effet, $\varphi(r_1 + r_2) = a^{r_1} \times a^{r_2}$

On voit facilement que ϕ est surjective : si $x \in < a >$, alors x s'écrit de la forme a^r, où $r \in \mathbb{Z}$ et donc $\phi(r) = x$.

1. Si ϕ est injective, alors $ker\ \phi = \{0\}$ et il y a une bijection entre $< a >$ et $\mathbb{Z}$. De plus, $A = \emptyset$. On a donc $\# < a >= +\infty = ord(a)$, car si $ker\ \phi = \{0\}$, alors $A = \emptyset$. Notons que $ker\ \phi = \{0\} \coprod A$
2. Si ϕ n'est pas injective, Posons $x\mathcal{R}y \iff a^x = a^y$
   D'après le théorème de factorisation, il y a une application $\tilde{\phi}$ injective de $\mathbb{Z}/\mathcal{R}$ à $< a >$, où $x\mathcal{R}y \iff \phi(x) = \phi(y)$, ou encore $\phi(x-y) = 1$, d'après la proposition 16, page précédente. Dans le dernier cas, $x - y \in ker\ \phi$ Le théorème nous indique que cette application est également surjective (puisque φ l'est).

   Cette application est donc bijective. Il y a alors une bijection entre $\mathbb{Z}/\mathcal{R}$ et $< a >$. De plus, la proposition 9 (page 24) nous indique que $ker\ \phi$ est un sous groupe de $\mathbb{Z}$, mais $ker\ \phi = \{x \in \mathbb{Z} \mid a^x = 1\}$. Le plus petit élément strictement positif de $ker\ f$ est donc $ord(a)$. D'après le théorème 3 (page 14), $ker\ f = ord(a)\mathbb{Z}$. On obtient donc, d'après les définitions dans la proposition 15 (page 31) :

$$\mathbb{Z}/\mathcal{R} = \{Cl(z) \mid z \in \mathbb{Z}\}$$

   Or,

$$\begin{aligned} Cl(z) &= \{x \in \mathbb{Z} \mid x - z \in ker\ \phi\} \\ &= \{x \in \mathbb{Z} \mid ord(a) | x - z\} \\ &= \{x \in \mathbb{Z} \,|x \equiv z[ord(a)]\} = \overline{z} \end{aligned}$$

   On a donc :

$$\begin{aligned} \mathbb{Z}/\mathcal{R} &= \{\overline{z} \,|z \in \mathbb{Z}\} \\ &= \mathbb{Z}/ord(a)\mathbb{Z} \end{aligned}$$

   Comme il y a une bijection entre $\mathbb{Z}/\mathcal{R}$ et $< a >$, alors

$$\#\mathbb{Z}/\mathcal{R} = \# < a > \iff \mathbb{Z}/ord(a)\mathbb{Z} = \# < a >$$

   De plus, $\#\mathbb{Z}/ord(a)\mathbb{Z} = ord(a)$, car il y a $ord(a)$ restes différents possibles de la division euclidienne par $ord(a)$: de 0 à $ord(a) - 1$. On a finalement l'égalité suivante finissant la démonstration :

$$\#\mathbb{Z}/ord(a)\mathbb{Z} = ord(a) = \# < a >$$

□

5.2 La troisième démonstration du petit théorème de Fermat

Théorème 7. *(théorème d'Euler) Soient a et n deux entiers premiers entre eux avec $n > 0$. Alors,*

$$a^{\varphi(n)} \equiv 1[n]$$

où φ est la fonction indicatrice d'Euler, que l'on a vu dans la sous-section 3.7 (p.23)

Démonstration. $< \overline{a} >$ est un sous-groupe de $(\mathbb{Z}/n\mathbb{Z})^\times$.

On a donc $ord(\overline{a})|\#(\mathbb{Z}/n\mathbb{Z})^\times$, d'après le théorème de Lagrange et le lemme que l'on vient de démontrer. Mais d'après la définition 10 (p.23), $\#(\mathbb{Z}/n\mathbb{Z})^\times = \varphi(n)$, et donc $ord(\overline{a})|\varphi(n)$. Ce qui implique que $\varphi(n) \in ker\ \phi$

$$a^{\varphi(n)} = \overline{1}$$

□

Maintenant, considérons l'ensemble $(\mathbb{Z}/p\mathbb{Z})^\times$, où p est un nombre premier. p étant premier, quelque soit $1 \leq n < p$, $pgcd(n, p) = 1$. C'est pour cette raison que $\varphi(p) = p - 1$. a étant premier avec p (par définition de $(\mathbb{Z}/p\mathbb{Z})^\times$), p ne divise pas a. D'après le théorème d'Euler, on a : $a^{\varphi(p)} = a^{p-1} = \overline{1}$ (Par définition de $\overline{1}$), et donc $a^{p-1} \equiv 1[p]$

Incroyable ! Le théorème d'Euler rend quasiment trivial le théorème de Fermat. Mieux encore, C'est une généralisation de ce dernier. Avec cela, le petit théorème de Fermat difficilement accessible jusqu'ici, ne devient qu'un cas particulier d'un théorème encore plus incroyable.

5.3 La dernière démonstration

Ici, nous allons voir une démonstration spéciale. C'est une démonstration du théorème d'Euler qui a l'avantage d'être plus rapide et plus élégante. En fait, elle n'a même pas besoin du théorème de Lagrange ou de relations d'équivalences. Soit l'application

$$\varphi_a : \left| \begin{array}{ccc} (\mathbb{Z}/n\mathbb{Z})^\times & \longrightarrow & (\mathbb{Z}/n\mathbb{Z})^\times \\ \overline{x} & \longmapsto & \overline{ax} \end{array} \right. \quad \text{où } a \text{ est un élément de } (\mathbb{Z}/n\mathbb{Z})^\times.$$

Montrons que cette application est bijective :
Injectivité : Si $\overline{ax} = \overline{ay}$, alors $\overline{x} = \overline{y}$ dans $(\mathbb{Z}/n\mathbb{Z})^\times$. ($(\mathbb{Z}/n\mathbb{Z})^\times$ est un groupe donc $\overline{a}$ est inversible et on obtient le résultat en multipliant par cet inverse).
Surjectivité : Si $\overline{y} \in (\mathbb{Z}/n\mathbb{Z})^\times$, alors $\overline{y} = \varphi_a(a^{-1}y)$
Cela nous permet d'affirmer que :

$$\prod_{\overline{x}\in(\mathbb{Z}/n\mathbb{Z})^\times} \overline{x} = \prod_{\overline{x}\in(\mathbb{Z}/n\mathbb{Z})^\times} \overline{ax} = \prod_{\overline{x}\in(\mathbb{Z}/n\mathbb{Z})^\times} \overline{a} \times \prod_{\overline{x}\in(\mathbb{Z}/n\mathbb{Z})^\times} \overline{x} = \overline{a}^{\varphi(n)} \times \prod_{\overline{x}\in(\mathbb{Z}/n\mathbb{Z})^\times} \overline{x}$$

En multipliant par l'inverse de $\prod_{\overline{x}\in(\mathbb{Z}/n\mathbb{Z})^\times} \overline{x}$ des deux côtés de l'égalité, on arrive à la conclusion stupéfiante que

$$\overline{a}^{\varphi(n)} = \overline{1}$$

Magique ? Non, mathématique. Et cette merveilleuse démonstration clôt la partie principale de ce mémoire.

6 Appendice I

Dans le premier appendice, nous allons nous intéresser aux bases de l'arithmétique, c'est-à-dire que nous allons démontrer deux propriétés fondamentales sans lesquels tout ce mémoire tomberait à l'eau. En mathématiques, on ne parle pas de vrai ou de faux, mais plutôt de cohérent ou d'inconsistant. Leurs fondations sont en fait des assertions admises : des postulats ou encore des axiomes.

Axiome du plus petit élément *Tout sous-ensemble non vide de* $\mathbb{N}$ *a un plus petit élément, que l'on peut appeler minimum.*

Principe de récurrence *Soit P(n) une propriété sur un entier n.*
Si on montre que $P(0)$ *est vraie, et si on montre que pour tout* $n \in \mathbb{N}$*, si* $P(n)$ *est vraie, alors* $P(n+1)$ *est vraie, alors* $P(n)$ *est vraie pour tout* $n \geq 0$*.*

Démonstration. Supposons que $P(0)$ est vraie et que pour tout $n \in \mathbb{N}$,
$P(n)$ est vraie $\Longrightarrow P(n+1)$ est vraie. Montrons qu'il n'existe aucun nombre s supérieur ou égal à 1 tel que $P(s)$ est fausse, ou que si ce nombre existe, il y a contradiction.

Considérons l'ensemble $S = \{s \in \mathbb{N} \mid P(s) \text{ est fausse } \}$
Si $S = \emptyset$, alors la proposition est démontrée.
Si $S \neq \emptyset$, alors S étant inclus dans $\mathbb{N}$, il a un plus petit élément, appelons le s.
$s \neq 0$, car $P(0)$ est vraie.
On a donc $s \geq 1$.
Cela donne : $s - 1 \geq 0$. On a donc $s - 1 \in \mathbb{N}$. Mais s étant le plus petit élément de S, $s - 1 \notin S$.
Si $s - 1 \notin S$, alors $P(s-1)$ est vraie (car si $P(s-1)$ était fausse, alors $s-1$ appartiendrait à S).
Mais si $P(s-1)$ est vraie, d'après ce que l'on a supposé, $P(s)$ est vraie.
Or, comme $s \in S$, $P(s)$ est fausse.
Contradiction.

□

Théorème de la division euclidienne *Soient* $a \in \mathbb{Z}$ *et* $b \in \mathbb{N}^*$*. Alors, il existe un unique couple* $(q, r) \in \mathbb{Z} \times \mathbb{N}$ *tel que*

$$a = bq + r \quad et \quad 0 \leq r < b$$

Démonstration. — Montrons l'existence de q et r. Considérons l'ensemble

$$A = \{a - bm \geq 0 \mid m \in \mathbb{Z}\}$$

A est un sous-ensemble non vide de $\mathbb{N}$. En effet, si $a \geq 0$, il contient $a - b \times 0$. Sinon, il contient $a - ba$. Il contient un plus petit élément d'après l'axiome vu page précédente. Appelons cet élément r. Cet élément r vérifie l'égalité $r = a - bq$ pour un certain $q \in \mathbb{Z}$, par définition de A. De même, $r \geq 0$ par définition.
$r < b$, car si $r \geq b$, alors $a - b(q + 1) \in A$, ce qui est en contradiction avec le fait que r soit le plus petit élément de A.

— Montrons maintenant que (q, r) est unique. Soient (q', r') deux couples de la division euclidienne de a par b. Alors $|r' - r| < b$. Par ailleurs on sait que $b(q - q') = r' - r$. Au final, on obtient que que $|q - q'| < 1$, q et q' étant entiers, on en déduit que $q = q'$. Par conséquent $r = a - bq = a - bq' = r'$. D'où le théorème.

□

7 Appendice II

À la page 9, nous avons mentionné la formule du binôme de Newton. En fait, nous avons utilisé cette égalité :

$$(a+1)^p = \sum_{k=0}^{p} \binom{p}{k} a^k$$

. Dans cet appendice, nous allons en comprendre la signification et la démontrer.
Le symbole $\sum$ (sigma majuscule) représente la somme. $k = 0$ est la première valeur que prend k. On peut voir que k prend les valeurs de 0 à p.
Par exemple,

$$\sum_{n=1}^{5} n = 1 + 2 + 3 + 4 + 5 = 15$$

C'est la somme des n, avec n prenant successivement les valeurs $1, 2, 3, 4$ et 5 (de 1 à 5).

Dans le cas que l'on a vu, c'est la somme des $\binom{p}{k} a^k$, k prenant les valeurs de 0 à p.

Définition 18. *On note $n!$, pour $n \in \mathbb{N}$ le nombre égal à $n \times (n-1) \times ... \times 3 \times 2 \times 1$.*
$\binom{p}{k}$*, pour $p \geq k \geq 0$ est le nombre égal à*

$$\frac{p!}{k!(p-k)!}$$

.

On a donc :

$$(a+1)^p = \sum_{k=0}^{p} \frac{p!}{k!(p-k)!} a^k$$

Cette égalité n'est qu'un cas particulier de la formule plus générale ci-dessous, que l'on va démontrer :

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

Notez que la démonstration que vous allez voir ci dessous est assez astucieuse et que l'on ne l'a pas trouvé d'un claquement de doigts.

Lemme 9. *Soient k et n deux nombres entiers positifs tels que $n \geq k$, alors*

$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$$

Démonstration.

$$\begin{aligned}
\binom{n}{k} + \binom{n}{k-1} &= \frac{n!}{(n-k)!k!} + \frac{n!}{(n-(k-1))!(k-1)!} \\
&= \frac{n!}{(n-k)!k!} + \frac{n!}{(n-k+1))!(k-1)!} \\
&= \frac{((n+1)-k)n!}{((n+1)-k)(n-k)!k!} + \frac{n!k}{(n-k+1))!(k-1)! \times k} \\
&= \frac{((n+1)-k)n!}{((n+1)-k)(n-k)!k!} + \frac{n!k}{((n+1)-k))!k!} \\
&= \frac{((n+1)-k)n! + k \times n!}{((n+1)-k)(n-k)!k!} \\
&= \frac{n!((n+1)-k+k)}{((n+1)-k)(n-k)!k!} \\
&= \frac{(n!(n+1))}{((n+1)-k)!k!} \\
&= \frac{(n+1)!}{((n+1)-k)!k!} \\
&= \binom{n+1}{k}
\end{aligned}$$

□

Proposition 17. *Soient a et b deux réels. Soit n un entier positif. Alors,*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$$

Démonstration. Démontrons le par récurrence.

Initialisation Soient deux réels a et b. On note $P(n)$ la propriété qui dit que pour n entier,

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$$

Montrons que $P(0)$ est vraie :

$$(a+b)^0 = \sum_{k=0}^{n} \binom{n}{k} a^0 = 1$$

$P(0)$ est donc vraie.

Récurrence Supposons que $P(n)$ est vraie pour n et montrons qu'elle est vraie pour $n+1$.
On a :

$$\begin{aligned}(a+b)^{n+1} &= (a+b)(a+b)^n \\ &= (a+b)\sum_{k=0}^{n} \binom{n}{k} a^{n-k}b^n \\ &= a\sum_{k=0}^{n} \binom{n}{k} a^{n-k}b^n + b\sum_{k=0}^{n} \binom{n}{k} a^{n-k}b^n\end{aligned}$$

Remarquons que $\displaystyle\sum_{k=0}^{n} \binom{n}{k} a^{n-k}b^n = a^n + \sum_{k=1}^{n} \binom{n}{k} a^{n-k}b^n$

On a donc :

$$a\sum_{k=0}^{n} \binom{n}{k} a^{n-k}b^n = a^{n+1} + \sum_{k=1}^{n} \binom{n}{k} a^{n-k+1}b^k$$

De même,

$$\begin{aligned}b\sum_{k=0}^{n} \binom{n}{k} a^{n-k}b^n &= b\left(\sum_{k=0}^{n-1} \binom{n}{k} a^{n-k}b^n + b^n\right) \\ &= b^{n+1} + b\sum_{k=0}^{n-1} \binom{n}{k} a^{n-k}b^n \\ &= b^{n+1} + \sum_{k=0}^{n-1} \binom{n}{k} a^{n-k}b^{n+1} \\ &= b^{n+1} + \sum_{k=1}^{n} \binom{n}{k-1} a^{n-k+1}b^n\end{aligned}$$

On obtient donc :

$$\begin{aligned}a\sum_{k=0}^{n} \binom{n}{k} a^{n-k}b^n + b\sum_{k=0}^{n} \binom{n}{k} a^{n-k}b^n &= a^{n+1} + \sum_{k=1}^{n} \binom{n}{k} a^{n-k+1}b^k + \sum_{k=1}^{n} \binom{n}{k-1} a^{n-k+1}b^n + b^{n+1} \\ &= a^{n+1} + b^{n+1} + \sum_{k=1}^{n} \left[\binom{n}{k} + \binom{n}{k-1}\right] a^{n-k+1}b^k\end{aligned}$$

D'après le lemme vu précédemment, on obtient :

$$= a^{n+1} + \sum_{k=1}^{n} \binom{n+1}{k} a^{n-k+1} b^k + b^{n+1}$$

$$= \binom{n+1}{0} a^{n+1} + \sum_{k=1}^{n} \binom{n+1}{k} a^{n-k+1} b^k + \binom{n+1}{n+1} b^{n+1}$$

$$= \sum_{k=0}^{n+1} \binom{n+1}{k} a^{(n+1)-k} b^k = P(n+1)$$

On a prouvé que $P(0)$ est vraie et que si $P(n)$ est vraie, alors $P(n+1)$ l'est aussi.
$P(n)$ est vraie pour tout $n \geq 0$, d'après le principe de récurrence. □