Université Mohammed Premier
Faculté Pluridisciplinaire de Nador
Département de Mathématiques
Nador

Deuxième Année Universitaire

Semestre 3

Filière : SMC

COURS ET TRAVAUX DIRIGÉS DE MATHÉMATIQUES POUR LA CHIMIE

Année universitaire :
2021-2022

Préparé par le Professeur :
Rachid MESSAOUDI

Décembre 2021

Table des matières

Chapitre 1

Compléments d'Analyse

1.1 Suites et séries de fonctions

1.1.1 Suite de fonctions

Définition 1.1.1

Une suite de fonctions $(f_n)_{n\in\mathbb{N}}$ définie sur $I = [a;b]$ (en général une partie de $\mathbb{R}$) est la donnée, pour tout entier $n \in \mathbb{N}$, d'une fonction f_n définie sur $[a;b]$ à valeurs dans $\mathbb{R}$ (ou $\mathbb{C}$ ou plus généralement vectorielle) :

- *Si on fixe n, on a la fonction $f_n : x \longmapsto f_n(x)$;*
- *si on fixe x, on a la suite numérique $(f_n(x))_n$.*

Exemples 1.1.2

- *Soit pour tout entier $n \in \mathbb{N}^*$, $f_n(x) = x^n$, donc $(f_n)_n$ est une suite de fonctions définie sur $\mathbb{R}$;*
  il en est de même pour :
- $n \in \mathbb{N}, g_n(x) = \sqrt{nx+1}$ *sur* $\mathbb{R}^+$;
- $n \in \mathbb{N}, h_n(x) = \frac{1}{nx+1}$ *sur* $\mathbb{R}^+$;
- $n \in \mathbb{N}^*, k_n(x) = ln(1+\frac{x}{n})$ *sur* $\mathbb{R}^+$.

Définition 1.1.3 *Convergence simple / uniforme d'une suite de fonctions :*

- *La suite $(f_n)_n$ converge **simplement** sur $[a;b]$ vers une fonction f si on a une convergence point par point dans $[a;b]$, i.e pour tout $x \in [a;b]$, la suite $(f_n(x))_n$ converge vers $f(x)$. On note $f_n \underset{n\to+\infty}{\longrightarrow} f$ simplement ;*
- *la suite $(f_n)_n$ converge **uniformément** vers une fonction f sur $[a;b]$ si :*

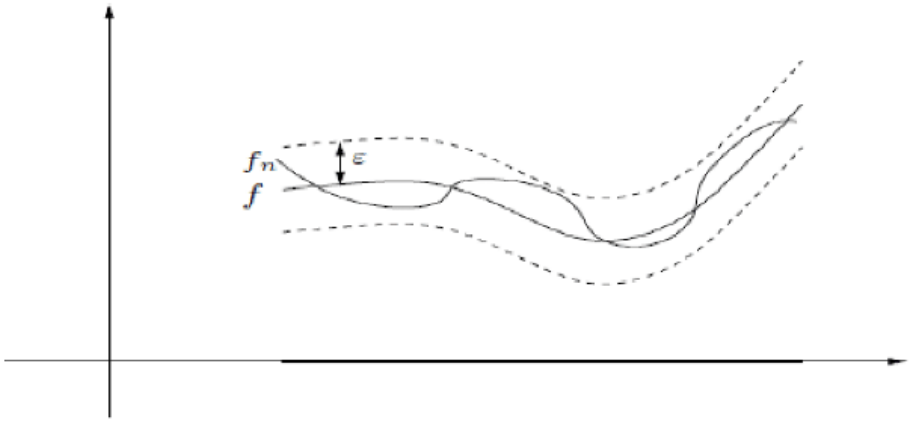
$$\sup_{x\in[a;b]} |f_n(x) - f(x)| \underset{n\to+\infty}{\longrightarrow} 0.$$

On note $f_n \underset{n\to+\infty}{\longrightarrow} f$ uniformément. Dans ce cas, la convergence est globale pour tout l'intervalle $[a;b]$;

Remarques 1.1.4

- *Si la suite $(f_n)_n$ converge simplement, alors la limite est unique ;*
- *($f_n \underset{n\to+\infty}{\longrightarrow} f$ uniformément) $\Longrightarrow$ ($f_n \underset{n\to+\infty}{\longrightarrow} f$ simplement). La réciproque est fausse ! (voir exemples ci-dessous) ;*
- *la convergence uniforme de la suite de fonctions vers f signifie qu'à partir d'un certain rang, la distance entre les fonctions f_n et la fonction f tendra vers 0 i.e. toutes les suites $(f_n(x))_{n\in\mathbb{N}}$ avancent vers leur limite respective avec une sorte de « mouvement d'ensemble ». Géométriquement, les graphes des fonctions f_n s'insèrent dans une bande de largeur 2ϵ autour du graphe de f (2ϵ est l'écart maximal autorisé pour la distance entre $f_n(x)$ et f (cf. graphe ci-dessous).*

FIGURE 1.1 – *convergence*



Exemples 1.1.5 *(Elémentaires)*

- $f_n(x) = x^n$ *sur* $]-1;1]$ *: Conditions de convergence d'une suite géométrique de raison x ;*
  - *Convergence simple :* $f_n(1) = 1$ *et pour tout* $x \in]-1;1[$, *on a* $f_n(x) \underset{n\to+\infty}{\longrightarrow} 0$, *donc :*

$$f_n \underset{n\to+\infty}{\longrightarrow} f \text{ simplement sur }]-1;1] \; avec \; f(1) = 1 \; et \; f(x) = 0 \; si \; x \in]-1;1[;$$

  - *convergence uniforme :* (f_n) *ne converge pas uniformément sur* $]-1;1]$ *car f est discontinue au point 0 même si les fonctions f_n sont continues (cf. propositions suivante) .*
- $f_n(x) = (1-x)^n$ *sur* $[0;2[$ *: Conditions de convergence d'une suite géométrique de raison* $(1-x)$ *;*
  - *Convergence simple :* $f_n(0) = 1$ *et pour tout* $x \in]0;2[$, *on a* $f_n(x) \underset{n\to+\infty}{\longrightarrow} 0$, *donc :*

$$f_n \underset{n\to+\infty}{\longrightarrow} f \text{ simplement sur } [0;2[\; avec \; f(0) = 1 \; et \; f(x) = 0 \; si \; x \in]0;2[;$$

- *convergence uniforme :* (f_n) *ne converge pas uniformément sur* $[0;2[$ *(cf. propositions suivante).*

- $g_n(x) = \sqrt{nx+1}$ *sur* $\mathbb{R}^+$ *:*
  - *Convergence simple :* $g_n(0) = 1$ *et pour tout* $x \in \mathbb{R}^{+*}$, $\sqrt{nx+1} \geq \sqrt{nx} \underset{n\to+\infty}{\longrightarrow} +\infty$, *donc,* (g_n) *diverge sur* $\mathbb{R}^+$ *;*
  - $h_n(x) = \dfrac{1}{nx+1}$ *sur* $\mathbb{R}^+$ *:*
    - *Convergence simple :* $h_n(0) = 1$ *et pour tout* $x \in \mathbb{R}^{+*}$, *on a* $h_n(x) \underset{n\to+\infty}{\longrightarrow} 0$, *donc :*

$$h_n \underset{n\to+\infty}{\longrightarrow} h \text{ simplement, telle que } h(0) = 1 \; et \; h(x) = 0 \; si \; x \in \mathbb{R}^{+*};$$

    - *convergence uniforme :* (h_n) *ne converge pas uniformément sur* $\mathbb{R}^+$ *(cf. propositions suivante).*
  - $k_n(x) = ln(1 + \frac{x}{n})$ *sur* $\mathbb{R}^+$ *:*
    - *Convergence simple :* $k_n(0) = 0$ *et pour tout* $x \in \mathbb{R}^{+*}$ *on a* $k_n(x) \underset{n\to+\infty}{\longrightarrow} 0$, *donc :*

$$k_n \underset{n\to+\infty}{\longrightarrow} 0 \text{ simplement sur } \mathbb{R}^+;$$

    - *convergence uniforme : On a pour* n *fixé,*

$$\sup_{x\in\mathbb{R}^+} |k_n(x) - 0| = \sup_{x\in\mathbb{R}^+} ln(1 + \frac{x}{n}) = +\infty;$$

      donc, (k_n) *ne converge pas uniformément sur* $\mathbb{R}^+$ *;*
    - *d'autre part, on a pour* n *fixé :*

$$\sup_{x\in[0;a]} |k_n(x) - 0| = ln(1 + \frac{a}{n}) \underset{n\to+\infty}{\longrightarrow} 0;$$

      donc, (k_n) *converge uniformément sur tout intervalle compact (fermé et borné) de type* $[0;a]$
  - $f_n(x) = \frac{nx^3}{1+nx^2}$ *sur* $\mathbb{R}$, *on a :*
    - *Convergence simple :* $f_n(0) = 0$ *et pour tout* $x \in \mathbb{R}^*$ *on a* $f_n(x) \underset{n\to+\infty}{\longrightarrow} x$, *donc :*

$$f_n \underset{n\to+\infty}{\longrightarrow} id_{\mathbb{R}} \text{ simplement sur } \mathbb{R};$$

    - *convergence uniforme : tout d'abord on a*

$$|f_n(x) - id_{\mathbb{R}}(x)| = \left|\frac{nx^3}{1+nx^2} - x\right| = \frac{|x|}{1+nx^2} \leq \inf(|x|, \frac{1}{n|x|})$$

      distinguons deux cas :
      - *Si* $|x| \leq \dfrac{1}{\sqrt{n}}$ *:*

$$|f_n(x) - id_{\mathbb{R}}(x)| \leq \frac{1}{\sqrt{n}}.$$

– *Si* $|x| \geq \dfrac{1}{\sqrt{n}}$:

$$|f_n(x) - x| \leq \frac{1}{n\,|x|} \leq \frac{\sqrt{n}}{n} \leq \frac{1}{\sqrt{n}}.$$

Dans tous les cas :

$$|f_n(x) - x| \leq \frac{1}{\sqrt{n}} \text{ pour tout } x \in \mathbb{R};$$

et

$$\sup_{x\in\mathbb{R}} |f_n(x) - x| \leq \frac{1}{\sqrt{n}} \underset{n\to+\infty}{\longrightarrow} 0,$$

donc,

$$f_n \underset{n\to+\infty}{\longrightarrow} id_{\mathbb{R}} \text{ uniformément sur } \mathbb{R}.$$

Proposition 1.1.6 *(Propriétés fondamentales) :*

Soit $(f_n)_n$ *une suite de fonctions telle que* $f_n : I \longrightarrow \mathbb{R}$ *avec* $I = [a, b]$ *. Si* $f_n \underset{n\to+\infty}{\longrightarrow} f$ *uniformément sur* I *alors, on a les propriétés suivantes :*

– *Si les fonctions* f_n *sont continues sur* I *alors* f *est aussi continue sur* I *;*

– *si les fonctions* f_n *sont intégrables sur* I *alors* f *est aussi intégrable sur* I*, et :*

$$\int_a^b f_n(t)dt = \int_a^b \lim_n f_n(t)dt = \int_a^b f(t)dt;$$

– *On pose :* $F_n(x) = \displaystyle\int_a^x f_n(t)dt$ *(resp.* $F(x) = \displaystyle\int_a^x f(t)dt$*) la primitive de* f_n *(resp.* f*) qui s'annule en* a*. Alors*

$$F_n \underset{n\to+\infty}{\longrightarrow} F \text{ uniformément sur } I.$$

– *La propriété n'est vraie que sur un intervalle fermé borné* $[a, b]$*. Prenons par exemple* $(f_n)_{n\in\mathbb{N}^*}$ *la suite de fonction telle que :*

$$f_n(x) = \begin{cases} \dfrac{1}{n} & \text{si } \ x \in [0, n] \ ; \\ \\ 0 & \text{sinon .} \end{cases}$$

On a bien $f_n \underset{n\to+\infty}{\longrightarrow} f = 0$ *uniformément sur* $\mathbb{R}^+$*, mais* $\displaystyle\int_0^{+\infty} f_n(t)dt = 1 \neq 0 = \int_0^{+\infty} f(t)dt$ *;*

– *la première propriété est souvent utilisée pour démontrer qu'une suite de fonctions, qui converge simplement vers une fonctions* f*,* ***ne converge pas uniformément****, de la façon suivante :*

$$\begin{cases} f_n(x) \text{ est continue sur un intervalle } I \text{ pour tout } n; \\ f_n \underset{n\to+\infty}{\longrightarrow} f \text{ simplement sur } I; \\ f \text{ n'est pas continue sur } I; \end{cases} \Longrightarrow f_n \textbf{ ne converge pas uniformément } \text{sur } I.$$

Proposition 1.1.7 *(Propriétés fondamentales) :*

Soit $(f_n)_n$ une suite de fonctions telle que $f_n : I \longrightarrow \mathbb{R}$ avec $I = [a, b]$. Si
- *Chaque fonction f_n est dérivable sur I ;*
- *$f'_n \underset{n\to+\infty}{\longrightarrow} g$ uniformément sur tout intervalle fermé borné contenu dans I ;*
- *il existe $x_0 \in I$ tel que la suite numérique $(f_n(x_0))_n$ converge ;*

alors :

$$f_n \underset{n\to+\infty}{\longrightarrow} f \text{ uniformément sur tout intervalle fermé borné contenu dans } I;$$

où la fonction f est dérivable et vérifie : $f' = g$ sur I.

1.1.2 Série de fonctions

Définition 1.1.8

Soit $(f_n)_n$ une suite de fonctions définie sur I. La série de fonctions notée $\sum f_n$ de terme général f_n est, par définition, la suite de fonctions $(S_n)_n$ définie par :

$$\forall x \in I : S_n(x) = \sum_{k=0}^{n} f_k(x);$$

où S_n est appelée la $n^{ième}$ somme partielle de la série de fonctions $\sum f_n$.

Définition 1.1.9 *(Convergence d'une série de fonctions) :*
- *La série $\sum f_n$ converge simplement sur I si la suite de fonctions $(S_n)_n$ converge simplement sur I vers une fonction S notée $\sum_{k=0}^{+\infty} f_k$ et définie comme suivant :*

$$\forall x \in I : \left(\sum_{k=0}^{+\infty} f_k\right)(x) = \sum_{k=0}^{+\infty} f_k(x),$$

  dans ce cas, la fonction $R_n = S - S_n : x \longmapsto \sum_{k=n+1}^{+\infty} f_k(x)$ s'appelle reste d'ordre (ou de rang) n de la série $\sum f_p(x)$;
- *la série $\sum f_n$ converge uniformément sur I si la suite de fonctions $(S_n)_n$ converge uniformément sur I vers une fonction S, i.e. :*

$$\sup_{x\in I} |S_n(x) - S(x)| \underset{n\to+\infty}{\longrightarrow} 0;$$

- *la série $\sum f_n$ converge absolument sur I si la série $\sum |f_n|$ converge simplement sur I ;*
- *la série $\sum f_n$ converge normalement sur I si la série numérique $\sum \sup_{x\in I} |f_n(x)|$ est convergente .*

Proposition 1.1.10 *(Critères de convergence) :*

- *Convergence normale $\Longrightarrow$ convergence uniforme $\Longrightarrow$ convergence simple ;*
- *la série $\sum f_n$ converge normalement sur $I \Longleftrightarrow$ il existe une série $\sum u_n$ à termes positifs et convergente telle que :*

$$\sup_{x\in I} |f_n(x)| \leq u_n.$$

Exemple 1.1.11

Soit $f_n(x) = \dfrac{sin(nx)}{n!}$, on a :

$$|f_n(x)| \leq \frac{1}{n!} \ \forall x \in \mathbb{R}.$$

On pose $u_n = \dfrac{1}{n!}$, la série de terme général u_n converge (règle de d'Alembert), donc $\sum f_n$ converge normalement.

Proposition 1.1.12 *(Fondamentale) :*

Soit $\sum f_n$ une série de fonctions définies sur $I = [a, b]$. Si $\sum f_n$ converge uniformément sur I et les fonctions f_n sont continues, alors :

- *La fonction $S = \sum_{k=0}^{+\infty} f_k$ est continue ;*
- *la série numérique $\sum \left(\int_a^b f_n(t)dt \right)$ converge et on a :*

$$\sum_{k=0}^{+\infty} \left(\int_a^b f_k(t)dt \right) = \int_a^b \left(\sum_{k=0}^{+\infty} f_k(t) \right) dt = \int_a^b S(t)dt.$$

Proposition 1.1.13

Soit $\sum f_n$ une série de fonctions de classe C^1 sur I et vérifiant :

- *$\sum f_n$ converge simplement sur I ;*
- *$\sum f'_n$ converge uniformément sur I.*

Alors :

- *$\sum f_n$ converge uniformément sur I ;*
- *$S = \sum_{k=0}^{+\infty} f_k$ est de classe C^1 sur I ;*
- *$S' = \left(\sum_{k=0}^{+\infty} f_k \right)' = \sum_{k=0}^{+\infty} f'_k$.*

1.2 Série entière et séries de Fourier

La classe des séries de fonctions est très large et ayant plusieurs applications. Parmi les séries les plus utilisées dans les applications en les sciences expérimentales on trouve les séries entières et les séries de Fourier.

1.2.1 Série entière

Définition 1.2.1

Une série entière est une série de fonctions de terme général $f_n(z) = a_n z^n$ où $a_n \in \mathbb{C}$. Une série entière est notée :

$$\sum a_n z^n.$$

Lemme 1.2.2 *(d'Abel) :*

Soit $\sum a_n z^n$ une série entière. S'il existe z_0 tel que $\sum |a_n z^n|$ converge, alors pour tout $z \in \mathbb{C}$ tel que $|z| \leq |z_0|$ la série entière $\sum a_n z^n$ est absolument convergente.

Définition 1.2.3 *(Rayon de convergence) :*

Soit $\sum a_n z^n$ une série entière. Il existe $R \in [0; +\infty[$ tel que :
– $\sum a_n z^n$ converge pour tout z tel que $|z| < R$;
– $\sum a_n z^n$ diverge pour tout z tel que $|z| > R$;
– Lorsque $|z| = R$ nous ne pouvons pas conclure et il faut utiliser une autre méthode.
R est appelé : Rayon de convergence de la série entière $\sum a_n z^n$.

Exemples 1.2.4
– La série entière $\sum z^n$ a pour rayon de convergence $R = 1$ et elle diverge lorsque $|z| = 1$;
– la série entière $\sum \dfrac{z^n}{n^2}$ a pour rayon de convergence $R = 1$ et elle converge lorsque $|z| = 1$.

Proposition 1.2.5 *(Règle de d'Alembert)*

Soit $\sum a_n z^n$ une série entière. On a :

$$\lim_n \left| \frac{a_{n+1}}{a_n} \right| = l \Longrightarrow R = \frac{1}{l} \text{ avec } \frac{1}{0^+} = +\infty \text{ et } \frac{1}{+\infty} = 0.$$

Proposition 1.2.6

Soit $\sum a_n x^n$ une série entière. Alors :
– La série entière dérivée $\sum n a_n x^{n-1}$ a le même rayon de convergence que $\sum a_n x^n$;
– la série entière $\sum a_n x^n$ converge normalement sur tout intervalle fermé borné inclus dans $]-R, R[$;
– la fonction limite $S(x) = \sum_{k=0}^{+\infty} a_k x^k$ est continue sur $]-R, R[$;
– $S(x)$ est de classe C^∞ sur $]-R, R[$ et on a :

$$S^p(x) = \sum_{k=p}^{+\infty} \frac{n!}{(n-p)!} a_k x^k;$$

où S^p est la dérivée d'ordre p de S.

Définition 1.2.7 *(Développement en série entière) :*

On dit qu'une fonction f est développable en série entière s'il existe une série entière $\sum a_n x^n$ de rayon de convergence R telle que :

$$f(x) = \sum a_n x^n \text{ pour tout } x \in]-R, R[;$$

dans ce cas f est de classe C^∞ et

$$a_n = \frac{f^{(n)}(0)}{n!}.$$

Proposition 1.2.8

- *Si f est développable en série entière avec $f(x) = \sum a_n x^n$, alors :*
  - *f paire $\Longrightarrow a_{2k+1} = 0$;*
  - *f impaire $\Longrightarrow a_{2k} = 0$;*
- *soit $f :]-a, a[\longrightarrow \mathbb{C}$ une fonction de classe C^∞. Alors :*
  f est développable en série entière si et seulement s'il existe $(\alpha, A, B) \in]0, a[\times \mathbb{R}^{+*} \times \mathbb{R}^{+*}$ tel que :

$$\left|f^{(n)}(x)\right| \leq BA^n n! \text{ pour tout } x \in]-\alpha, \alpha[.$$

Proposition 1.2.9 *(Formule de Taylor avec reste intégrale) :*

- *La formule de Taylor avec reste intégrale s'écrit :*

$$f(x) = \sum_{k=0}^{n} \frac{f^{(k)}(0)}{k!} x^k + \int_0^x \frac{(x-t)^n}{n!} f^{(n+1)}(t)dt;$$

- *f est développable en série entière si et seulement s'il existe $\beta \in]0, a[$ tel que*

$$r_n = \int_0^x \frac{(x-t)^n}{n!} f^{(n+1)}(t)dt \underset{n\to+\infty}{\longrightarrow} 0, \text{ simplement sur }]-\beta, \beta[.$$

Exemples 1.2.10

- $e^x = \sum_{k=0}^{+\infty} \frac{x^n}{n!}, R = +\infty$;
- $\frac{1}{1-x} = \sum_{k=0}^{+\infty} x^n, R = 1$;
- $\cos x = \sum_{k=0}^{+\infty} (-1)^n \frac{x^{2n}}{(2n)!}, R = +\infty$;
- $\sin x = \sum_{k=0}^{+\infty} (-1)^n \frac{x^{2n+1}}{(2n+1)!}, R = +\infty.$

1.2.2 Série de Fourier

Définition 1.2.11 *La série de fonctions f_n telle que : $f_n(x) = a_n \cos(nx) + b_n \sin(nx)$ est appelée Série de Fourier.*

Définition 1.2.12 *Soit f une fonction intégrable sur $[-\pi,\pi]$ et 2π-périodique. La série de Fourier associée à f est définie par $\sum f_n$ où : $f_n(x) = a_n\cos(nx) + b_n\sin(nx)$ avec :*

$$\begin{cases} a_0 = \dfrac{1}{2\pi}\displaystyle\int_{-\pi}^{\pi} f(t)dt; \\ a_n = \dfrac{1}{\pi}\displaystyle\int_{-\pi}^{\pi} f(t)\cos(nt)dt,\ n \geq 1; \\ b_n = \dfrac{1}{\pi}\displaystyle\int_{-\pi}^{\pi} f(t)\sin(nt)dt,\ n \geq 1. \end{cases}$$

Remarques 1.2.13

- *f paire* $\Longrightarrow b_n = 0$ *;*
- *f impaire* $\Longrightarrow a_n = 0$ *;*
- *Notation :* $f(x) \sim a_0 + \displaystyle\sum_{k=1}^{+\infty} \left(a_n\cos(nx) + b_n\sin(nx)\right)$.

Définition 1.2.14 *Soit f une fonction intégrable sur $[-L,L]$ et $2L$-périodique. La série de Fourier associée à f est définie par $\sum f_n$ où : $f_n(x) = a_n\cos\left(n\dfrac{\pi x}{L}\right) + b_n\sin\left(n\dfrac{\pi x}{L}\right)$ avec :*

$$\begin{cases} a_0 = \dfrac{1}{2\pi}\displaystyle\int_{-\pi}^{\pi} f\left(\frac{Lt}{\pi}\right)dt = \frac{1}{2L}\int_{-L}^{L} f(t)dt; \\ a_n = \dfrac{1}{\pi}\displaystyle\int_{-\pi}^{\pi} f\left(\frac{Lt}{\pi}\right)\cos(nt)dt = \frac{1}{L}\int_{-L}^{L} f(t)\cos\left(n\frac{\pi t}{L}\right)dt,\ n \geq 1; \\ b_n = \dfrac{1}{\pi}\displaystyle\int_{-\pi}^{\pi} f\left(\frac{Lt}{\pi}\right)\sin(nt)dt = \frac{1}{L}\int_{-L}^{L} f(t)\sin\left(n\frac{\pi t}{L}\right)dt,\ n \geq 1. \end{cases}$$

Exemple 1.2.15

- *$f(x) = x$ pour tout $x \in [-\pi,\pi]$ et 2π-périodique, f est impaire donc $a_n = 0$. Calculons b_n :*

$$\begin{aligned} b_n &= \frac{1}{\pi}\int_{-\pi}^{\pi} t\sin(nt)dt \\ &= \frac{1}{\pi}\left[-\frac{t\cos(nt)}{n} + \frac{\sin(nt)}{n^2}\right]_{-\pi}^{\pi} \\ &= \frac{2}{n}(-1)^{n+1}, \end{aligned}$$

d'où

$$f(x) \sim 2\left(\sin(x) - \frac{\sin(2x)}{2} + \frac{\sin(3x)}{3} + ...\right);$$

Ci-après les courbes de $S_n = \displaystyle\sum_{k=1}^{n} \frac{2}{n}(-1)^{n+1}\sin(nx)$.

FIGURE 1.2 – *n=1*

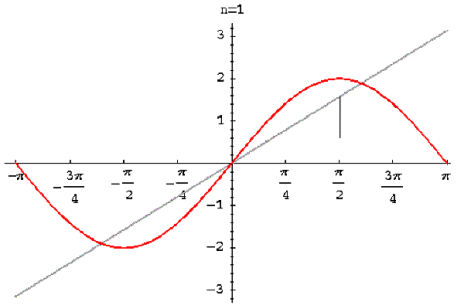


FIGURE 1.3 – *n=6*

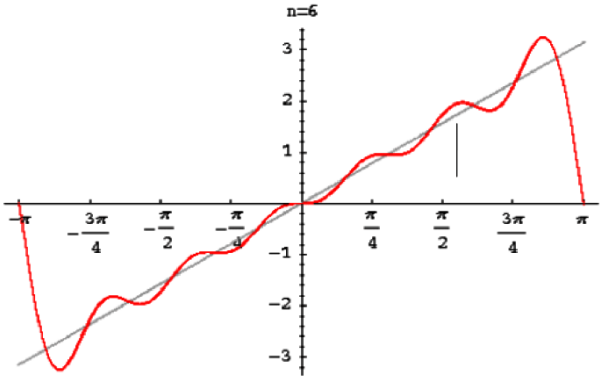
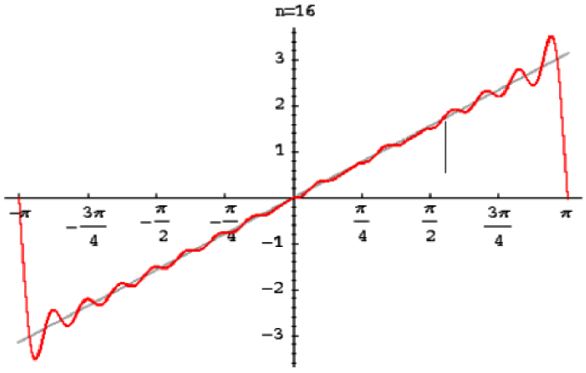


FIGURE 1.4 – *n=16*



L'approximation de f par les fonctions S_n est claire sur les graphiques. D'autant plus que n prend des grandes valeurs d'autant plus que les courbes de f et de S_n ont tendance à se rapprocher d'avantage.

Définition 1.2.16

La série de Fourier associée à une fonction f, T-périodique, peut être présentée avec des coefficients complexes (en utilisant la formule d'Euler) et elle prend la forme suivante :

$$f(x) = \sum_{n=-\infty}^{+\infty} c_n(f) e^{in\omega x} \qquad \text{avec } \omega = \frac{2\pi}{T}.$$

Cette notion peut se généraliser au cas quelconque (pas forcément périodique) de la manière suivante :

Définition 1.2.17

Soit $f : \mathbb{R} \longrightarrow \mathbb{R}$ une fonction continue par morceaux, on appelle transformée de Fourier de f ; la fonction $\mathcal{F}(f) : \mathbb{R} \longrightarrow \mathbb{C}$ telle que :

$$\mathcal{F}(f)(x) = \int_{-\infty}^{+\infty} f(t)e^{-2i\pi xt}dt.$$

Remarques 1.2.18

- *L'application $\mathcal{F} : f \longmapsto \mathcal{F}(f)$ est appelée : Transformation de Fourier ;*
- *la fonction $\mathcal{F}(f)$ est définie pour x réel, à valeurs complexes et elle est bornée et continue sur $\mathbb{R}$;*
- *la courbe d'équation : $y = |\mathcal{F}(f)|$ est appelé spectre de f et on montre que :*

$$\lim_{x\to+\infty} |\mathcal{F}(f)(x)| = 0;$$

- *si f est une fonction paire alors $\mathcal{F}(f)(x)$ est un nombre réel et :*

$$\mathcal{F}(f)(x) = 2\int_{0}^{+\infty} f(t)\cos(2\pi xt)dt;$$

- *si f est une fonction impaire alors $\mathcal{F}(f)(x)$ est un nombre imaginaire et :*

$$\mathcal{F}(f)(x) = -2i\int_{0}^{+\infty} f(t)\sin(2\pi xt)dt.$$

Exemple 1.2.19

- *Soit $\prod$ la fonction, qui représente un signal "porte", donnée par :*

$$\prod(t) = \begin{cases} 1 \quad \textit{si} \quad t \in [\frac{-1}{2}, \frac{1}{2}] ; \\ \\ 0 \quad \textit{sinon} . \end{cases}$$

Pour $x \neq 0$, on a :

$$\mathcal{F}(\prod)(x) = \frac{\sin(\pi x)}{\pi x}.$$

Pour $x = 0$, on a :

$$\mathcal{F}(\prod)(0) = 1.$$

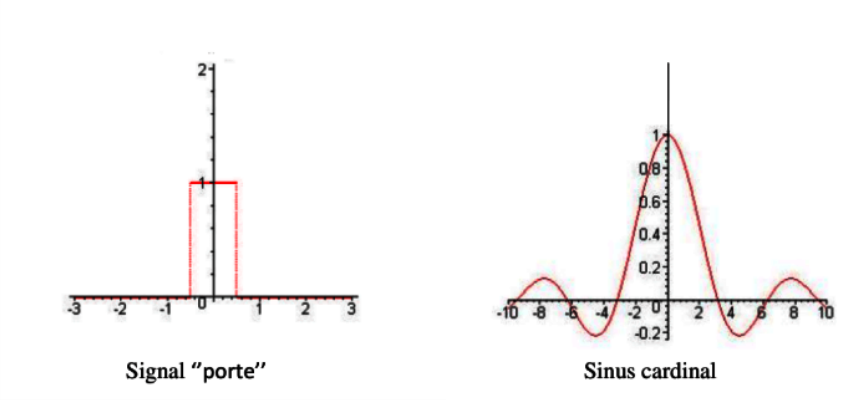
On remarque que la fonction $\mathcal{F}(\prod)$ est prolongeable par continuité en 0 et on en déduit que :

$$\mathcal{F}(\prod)(x) = \frac{\sin(\pi x)}{\pi x}.$$

Cette fonction est appelée sinus cardinal. Ci-après les courbes du signal "porte" et du sinus cardinal.

- *$\mathcal{F}$ est **linéaire :***

FIGURE 1.5 – *Courbes du signal "porte" et du sinus cardinal*



Pour deux fonctions f et g continues par morceaux et deux nombres complexes λ et μ on a :

$$\mathcal{F}(\lambda f + \mu g) = \lambda \mathcal{F}(f) + \mu \mathcal{F}(g).$$

- ***Transformée d'une dérivée :***
  Si la fonction f est continue et si $\frac{df}{dt}$ est continue par morceaux alors :

$$\mathcal{F}(\frac{df}{dt})(x) = 2i\pi x \mathcal{F}(f)(x).$$

- ***Règle de multiplication par t :***
  Si la fonction $\bullet f(\bullet) : t \longmapsto tf(t)$ est continue par morceaux, alors :

$$\frac{d\mathcal{F}(f)}{dt}(x) = -2i\pi \mathcal{F}(\bullet f(\bullet))(x).$$

- ***Image d'une translatée (formule du retard si a > 0) :***
  Soit a un réel. Pour tout $t \in \mathbb{R}$, on pose $g(t) = f(t-a)$ i.e. g est la translatée de f ou le signal f est "retardé" de a (si $a > 0$). Alors :

$$\mathcal{F}(g)(x) = e^{-2i\pi ax} \mathcal{F}(f)(x).$$

- ***Translation de l'image :***
  Soit la fonction $e^{2i\pi a\bullet} f(\bullet) : t \longmapsto e^{2i\pi at} f(t)$ où a est un réel. Alors :

$$\mathcal{F}(e^{2i\pi a\bullet} f(\bullet))(x) = \mathcal{F}(f)(x-a).$$

- ***Changement d'échelle :***
  Soit la fonction $\omega\bullet : t \longmapsto \omega t$ où $\omega \in \mathbb{R}^{+*}$. Alors :

$$\mathcal{F}(f(\omega\bullet))(x) = \frac{1}{\omega} \mathcal{F}(f) \frac{x}{\omega}.$$

1.2.3 Transformée de Laplace

Définition 1.2.20

*Soit f une fonction définie sur $\mathbb{R}$ telle que f est continue par morceaux sur $[0, +\infty[$ et nulle sur $]-\infty, 0[$ (qu'on appelle **fonction causale**). La transformée de Laplace de f est la fonction $\mathcal{L}(f)$ définie sur $\mathbb{R}$ à valeurs dans $\mathbb{C}$ telle que :*

$$\mathcal{L}(f)(p) = \int_0^{+\infty} e^{-pt} f(t) dt.$$

Notons que cette transformée n'est définie que pour les valeurs p telles que l'intégrale précédente converge. L'application qui associe à f sa transformée de Laplace $\mathcal{L}(f)$ est appelée la transformation de Laplace.

Exemple 1.2.21 *Soit la fonction **échelon-unité** $\mathcal{U}$ définie par :*

$$\mathcal{U}(x) = \begin{cases} 1 & \text{si} \quad x \in]0; +\infty[\, ; \\ \\ 0 & \text{sinon} \, . \end{cases}$$

Donc :

$$\mathcal{L}(\mathcal{U})(p) = \int_0^{+\infty} e^{-pt} dt = \frac{1}{p},$$

avec $p > 0$ (sinon l'intégrale généralisée diverge pour $p \leq 0$).

Proposition 1.2.22 *(Propriétés de la transformation de Laplace) :*

- *La transformée de Laplace est **linéaire** .*
- ***Effet de la translation :***
  Si $g(t) = f(t-a)$ pour $a > 0$ alors :

  $$\mathcal{L}(g)(p) = e^{-ap}(f)(p);$$

  à condition que les deux transformées soient bien définies.
- ***Effet de la multiplication par une exponentielle :***
  Si $g(t) = e^{at} f(t)$ pour $a \in \mathbb{R}$ alors :

  $$\mathcal{L}(g)(p) = e^{-ap}\mathcal{L}(f)(p-a);$$

  à condition que les deux transformées soient bien définies .
- ***Régularité d'une transformée de Laplace :***
  $\mathcal{L}(f)$ est de classe C^∞ et :

  $$\mathcal{L}(f)^{(n)}(p) = \mathcal{L}((-\bullet)^n f)(p);$$

  à condition que les deux transformées soient bien définies.
- ***Comportement à l'infini :***

  $$\lim_{p \to +\infty} \mathcal{L}(f)(p) = 0.$$

- *Si f est derivable, on a :*

$$\mathcal{L}(f')(p) = p\mathcal{L}(f)(p) - \lim_{o^+} f;$$

à condition que les transformées soient bien définies .

- *On pose :* $g(x) = \int_0^x f(t)dt$ *alors :*

$$\mathcal{L}(g)(p) = \frac{1}{p}\mathcal{L}(f)(p).$$

Chapitre 2

Notions d'Arithmétique et calcul modulaire

2.1 Notions d'Arithmétique

2.1.1 Rappels :

2.1.1.1 L'ensemble des entiers naturels

- $\mathbb{N} = \{0, 1, 2, ...\}$ *est l'ensemble de tous les entiers naturels, avec* 0 *est un élément particulier ;*
- *chaque entier naturel* m *possède un successeur que l'on note* $S(m) = m + 1$ *(où* S *est une application de* $\mathbb{N}$ *dans* $\mathbb{N}$ *) ;*
- 0 *n'est le successeur d'aucun entier naturel ;*
- *si deux entiers naturels* m *et* n *ont le même successeur, alors* $m = n$ *(c-à-d* S *est injective) ;*
- *si* A *est une partie de* $\mathbb{N}$ *contenant* 0 *et stable par* S *(c-à-d* $S(A) \subset A$*), alors* $A = \mathbb{N}$ *.*
- ***L'addition et la multiplication dans*** $\mathbb{N}$:
  On munit $\mathbb{N}$ *des deux opérations habituelles suivantes :*

  1. *Définition de l'addition :* $" + "$

$$\begin{cases} & m + 0 = m \\ \forall n \in \mathbb{N}, & m + S(n) = S(m + n); \end{cases}$$

  e.g. : $1 = S(0)$ *, et* $1, 2, 3, 4, 5, 6, 7, 8, 9$ *sont les* 9 *premiers itérés de* 0*, 11+7=(11+6)+1=18.*

  2. *Définition de la multiplication :* $" \times "$

$$\begin{cases} & m \times 0 = 0 \\ \forall n \in \mathbb{N}, & m \times S(n) = (m \times n) + m; \end{cases}$$

l'entier naturel (produit) $m \times n$ *est aussi noté* mn, $11 \times 7 = (11 \times 6) + 11 = 77$.

- ***Ordre sur*** $\mathbb{N}$:
  Par l'addition " $+$ " *, on définit l'ordre* " $\leq$ " *comme suivant :*

$$\forall m, n \in \mathbb{N} : \ (m \leq n \Leftrightarrow \exists! \ p \in \mathbb{N} : \ n = m + p);$$

  où p *est noté par* $n - m$ *.*
- ***Propriétés de l'ordre*** " $\leq$ " ***:***
  - *toute partie non vide de* $\mathbb{N}$ *admet un plus petit élément (*0 *est le plus petit élément de* $\mathbb{N}$ *);*
  - $\forall m \in \mathbb{N}$ *,* $S(m) = m + 1$ *est le plus petit majorant strict de* m *;*
  - *pour* $m, n \in \mathbb{N}$ *on a* $m \leq n$ *ou* $n \leq m$ *(i.e.* $n \geq m$ *ou* $m \geq n$*);*
  - *pour* $m, n \in \mathbb{N}$*, si* $m \leq n$ *et* $n \leq m$ *alors* $m = n$ *;*
  - " $\leq$ " *est compatible dans* $\mathbb{N}$ *avec* " $+$ " *et* " $\times$ "*, i.e. :*

$$\begin{aligned} \forall m, n, p \in \mathbb{N} \quad & m \leq n \Leftrightarrow m + p \leq n + p \\ & m \leq n \Rightarrow mp \leq np. \end{aligned}$$

2.1.1.2 L'ensemble des entiers relatifs

- $\mathbb{Z} = \{..., -m - 1, -m, ..., -2, -1, 0, 1, 2, ..., m, m + 1, ...\}$ *est l'ensemble des entiers relatifs, (*0 *est le seul nombre entier à la fois positif et négatif) ;*
- *dans un entier relatif, on distingue le signe (*$+$ *ou* $-$*) et la valeur absolue, e.g.* $-5 = -|5|$ *;*
- *chaque élément non nul* m *admet un opposé noté* $-m$ *;*
- *tout élément* m *de* $\mathbb{Z}$ *admet un successeur* $S(m) = m + 1$ *et un prédécesseur* $P(m) = m - 1$ *(*S *et* P *sont deux applications de* $\mathbb{Z}$ *dans* $\mathbb{Z}$ *) ;*
- *si deux entiers relatifs* m *et* n *ont le même successeur ou le même prédécesseur, alors* $m = n$ *(i.e.* P *et* S *sont injectives) ;*
- *si* A *est une partie de* $\mathbb{Z}$ *contenant* 0 *et stable par* S *et* P *, alors* $A = \mathbb{Z}$ *;*
- ***L'addition et la multiplication dans*** $\mathbb{Z}$
  $\mathbb{Z}$ *est menu des deux opérations habituelles :*
  1. *l'addition* " $+$ " *:*
     $(-2) + (-5) = -(2 + 5) = -7$ *;*
     $2 + (-5) = -(5 - 2) = -3$.
  2. *La multiplication* " $\times$ " *:*
     $(-2) \times (-5) = 2 \times 5 = 10$ *;*
     $2 \times (-5) = -(2 \times 5) = -10$.
  3. *On peut définir aussi la soustraction sur* $\mathbb{Z}$ *par :*
     $m - n = m + (-n), (2 - 5 = 2 + (-5) = -3$ *;*
- ***Ordre sur*** $\mathbb{Z}$ ***et ses propriétés***

- *$\mathbb{Z}$ est un ensemble ordonné, menu de l'ordre naturel " $\leq$ " tel que :*

$$\forall m, n \in \mathbb{Z} : \ (m \leq n \Leftrightarrow \exists! \ p \in \mathbb{Z} : \ n = m + p);$$

- *$\forall m \in \mathbb{Z}$, $P(m) = m - 1$ est le plus grand minorant (resp. $S(m) = m + 1$ est le plus petit majorant) strict de m ;*
- *pour $m, n \in \mathbb{Z}$ on a $m \leq n$ ou $n \leq m$ (i.e. $n \geq m$ ou $m \geq n$) ;*
- *pour $m, n \in \mathbb{Z}$, si $m \leq n$ et $n \leq m$ alors $m = n$;*
- *$\forall m, n, p \in \mathbb{Z}$ $m \leq n \Leftrightarrow m + p \leq n + p$ (i.e. " $\leq$ " est compatible dans $\mathbb{Z}$ avec " $+$ ") ;*
- *$\forall m, n, p \in \mathbb{Z}$ $m \leq n \Rightarrow mp \leq np$ si p est positif et $mp \geq np$ si p est négatif (i.e. " $\leq$ " est incompatible avec " $\times$ " dans $\mathbb{Z}$) ;*
- *$\mathbb{Z}$ n'admet ni plus petit élément, ni plus grand élément ;*
- *une partie A de $\mathbb{Z}$ est finie si et seulement si A admet un plus petit élément et un plus grand élément ;*
- *pour $m, n \in \mathbb{Z}$ tels que $m \leq n$, l'ensemble des entiers relatifs de m à n s'exprime sous la forme intervallaire $[\![m ; n]\!]$, ainsi :*
  $[\![-2; 3]\!] = \{-2, -1, 0, 1, 2, 3\}$;
  $]\!] - 2; 3[\![= [\![-1; 2]\!]$;
  $\mathbb{N}^* = [\![1; +\infty[\![= [\![1; \infty[\![$;
  $\mathbb{Z}^- =]\!] - \infty; 0]\!]$ ...

2.1.1.3 Raisonnement par récurrence

Soient $\mathcal{P}_n$ une propriété dépendant de l'entier naturel n et n_0 un entier naturel. Un raisonnement par récurrence ou par induction s'établit comme suit :

Si :

- *$\mathcal{P}_{n_0}$ est vraie (étape d'initialisation) ;*
- *pour $n \geq n_0$ tel que $\mathcal{P}_n$ est vraie, on a $\mathcal{P}_{n+1}$ vraie (étape d'hérédité) ;*

Alors, pour tout entier $n \geq n_0$, $\mathcal{P}_n$ est vraie.

-Exemple :

Montrons par récurrence que $\forall n \in \mathbb{N}^*$ on a $\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$.

. Initialisation :

Pour $n = 1$ on a d'une part $\sum_{i=1}^{1} i^2 = 1^2 = 1$ et d'autre part $\frac{1(1+1)(2\times 1+1)}{6} = \frac{6}{6} = 1$.

La propriété $\mathcal{P}_1$ est vraie.

. Hérédité :

Supposons que pour un entier $k \geqslant 1$, la propriété $\mathcal{P}_k$ soit vraie, c-à-d :

$$\sum_{i=1}^{k} i^2 = \frac{k(k+1)(2k+1)}{6}.$$

On souhaite démontrer qu'alors la proposition P_{k+1} est aussi vraie. Pour cela on a :

$$\sum_{i=1}^{k+1} i^2 = \sum_{i=1}^{k} i^2 + (k+1)^2;$$

or on a supposé que P_k est vraie. On remplace :

$$\begin{aligned}
\sum_{i=1}^{k+1} i^2 &= \frac{k(k+1)(2k+1)}{6} + (k+1)^2 \\
&= \frac{k(k+1)(2k+1) + 6(k+1)^2}{6} \\
&= \frac{(k+1)[k(2k+1) + 6(k+1)]}{6} \\
&= \frac{(k+1)[2k^2 + 7k + 6]}{6} \\
&= \frac{(k+1)(k+2)(2k+3)}{6}.
\end{aligned}$$

La propriété P_{k+1} est vraie.

. Conclusion :

d'après le principe de récurrence pour tout entier $n \in \mathbb{N}^*$ on a $\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$.

2.1.2 Divisibilité

Définition 2.1.1

Soient $m, n \in \mathbb{Z}$. On dit que m est divisible par n (i.e. n divise m ou encore que m est un multiple de n) et on note $n \mid m$, s'il existe un élément q dans $\mathbb{Z}$ tel que : $m = qn$.

Remarque 2.1.2

- *Si $m \neq 0$ et $n \mid m$, alors $n \neq 0$ et q est unique. On dira que q est le quotient exact de m par n et on note $q = \frac{m}{n}$.*
- *Tout entier $n \mid 0$;*
- *tout entier m est divisible par $\pm 1, \pm m$;*
- *si $0 \mid m$ alors $m = 0$;*

– *si* $n \mid m$ *et* $m \neq 0$ *alors* $|n| \leq |m|$, *(* $2 \mid -6$ *et* $2 > -6$ *)* .

Exemple 2.1.3

– *L'ensemble des diviseurs de* 18 *est :*

$$D_{18} = \{\pm 1, \pm 2, \pm 3, \pm 6, \pm 9, \pm 18\}\,.$$

– *L'ensemble des diviseurs de* 27 *est :*

$$D_{27} = \{\pm 1, \pm 3, \pm 9, \pm 27\}\,.$$

– *5 ne divise pas 23 :* $5 \nmid 23$ *;*
– *soit* $m \in \mathbb{Z}$, $m^4 - 1 = (m-1)(m+1)(m^2+1)$ *donc* $m \pm 1$ *et* $m^2 + 1$ *divisent* $m^4 - 1$.

Proposition 2.1.4

– *Si* $n \mid m$ *et* $m \mid n$ *alors* $m = \pm n$ *c-à-d* $|m| = |n|$ *: eg.* $2 \mid -2$ *et* $-2 \mid 2$ *;*
– *si* $n \mid m$ *et* $m \mid p$ *alors* $n \mid p$ *: eg.* $7 \mid 21$ *et* $21 \mid 231$ $(231 = 21 \times 11)$ *donc* $7 \mid 231$ *;*
– *si* $np \mid mp$ *et* $p \neq 0$ *alors* $n \mid m$ *: eg. si* $3n \mid 21$ *donc* $n \mid 7$ *;*
– *si* $n \mid m$ *et* $n \mid p$, *alors* $n \mid um + vp$ *pour tous* $u, v \in \mathbb{Z}$ *, en particulier* $n \mid m \pm p$ *:*
  eg. si $n \mid 10$ *et* $n \mid 15$ *alors* $n \mid 15 - 10$ *c-à-d* $n \mid 5$ *donc* $n \in \{\pm 1, \pm 5\}$ *;*
– *en général, si* $n \mid m_i$ *pour tout* $i \in [\![0; k]\!]$ *, alors* $n \mid \sum_{i=0}^{k} u_i m_i$ *pour* u_i *des entiers quelconques ;*
– *si* $n_1 \mid m_1$ *et* $n_2 \mid m_2$, *alors* $n_1 n_2 \mid m_1 m_2$ *: eg.* $3/12$ *et* $2/10$ *donc* $6/120$ *;*
– *si* $n \mid m$ *alors* $n^k \mid m^k$ *pour tout* $k \in \mathbb{N}$ *: eg.* $2/10$ *donc* $8/1000$.

2.1.3 Division Euclidienne (D.E.) :

Théorème 2.1.5 *À tous couple* $(m; n) \in \mathbb{Z} \times \mathbb{Z}^*$, *on associe un unique couple* $(q; r) \in \mathbb{Z} \times \mathbb{N}$ *, pour lequel :*

$m = nq + r$ *;*

$r \in [\![0; |n-1|]\!]$.

Remarque 2.1.6

– *Les entiers* m, n, q *et* r *s'appellent resp. dividende, "diviseur", quotient et reste de la D.E. de* m *par* n *;*
– *lorsque* $n \mid m$, q *est le quotient exact de* m *par* n *et* $r = 0$.

Exemple 2.1.7

– $76 = 11 \times 6 + 10$ *est une D.E. où* $m = 76, n = 11, q = 6$ *et* $r = 10$.
– *D.E. de* 18 *par* 5 *:* $18 = 5 \times 3 + 3$ *où* $q = 3$ *et* $r = 3$.

- *D.E. de* -18 *par* 5 *:* $-18 = 5 \times (-4) + 2$ *où* $q = -4$ *et* $r = 2$.
- *D.E. de* -18 *par* -5 *:* $-18 = (-5) \times 4 + 2$ *où* $q = 4$ *et* $r = 2$.
- " $-18 = 4 \times (-4) - 2$" *n'est pas une D.E. car* -2 *est négatif .*

2.1.4 PGCD et PPCM :

2.1.4.1 PGCD :

Définition 2.1.8

Soient $m, n \in \mathbb{Z}$ *tels que* $(m, n) \neq (0, 0)$*. Le plus grand élément de l'ensemble des diviseurs communs à* m *et* n *s'appelle le plus grand commun diviseur de* m *et* n *. On le note* $PGCD(m, n)$ *ou encore* $m \wedge n$*.*

Remarque 2.1.9

De la même manière, $PGCD(m_1, m_2, ..., m_k)$ *ou encore* $m_1 \wedge m_2 \wedge ... \wedge m_k$ *est le plus grand commun diviseur de tous les entiers non tous nuls* m_i $(i \in [\![0; k]\!])$ *.*

Exemple 2.1.10

- $D_{18} \cap D_{27} = \{\pm 1, \pm 3, \pm 9\}$*, donc* $18 \wedge 27 = 9$ *;*
- $2 \wedge 5 = 1$ *;*
- $30 \wedge 12 = 6$ *;*
- $-36 \wedge 27 = 36 \wedge 27 = 9$ *;*
- $36 \wedge 27 \wedge 6 = (36 \wedge 27) \wedge 6 = 9 \wedge 6 = 3$ *.*

Proposition 2.1.11

- *Les diviseurs communs à* m *et* n *sont les diviseurs de* $m \wedge n$ *;*
- $m \wedge n = n \wedge m$ *;*
- $m \wedge n \wedge p = (m \wedge n) \wedge p = (m \wedge p) \wedge n = (n \wedge p) \wedge m$ *;*
- $mp \wedge np = |p|(m \wedge n)$ *;*
- $m \wedge 1 = 1$ *;*
- *soient* $m' = \dfrac{m}{m \wedge n}$ *et* $n' = \dfrac{n}{m \wedge n}$ *alors* $m' \wedge n' = 1$ *.*

Exemple 2.1.12

$18 \wedge 27 = 9$ *et* $D_{18} \cap D_{27} = D_{18 \wedge 27} = \{\pm 1, \pm 3, \pm 9\}$ *;*

$18 \wedge 30 \wedge 27 = (18 \wedge 27) \wedge 30 = 9 \wedge 30 = 3$ *;*

$42 \wedge 60 = 6(7 \wedge 10) = 6$ *;*

$\dfrac{42}{42 \wedge 60} = 7$ *et* $\dfrac{60}{42 \wedge 60} = 10$ *alors* $7 \wedge 10 = 1$ *.*

Proposition 2.1.13 *(Propriété de transmission du PGCD)*

Soient $m, n, q, r \in \mathbb{Z}^*$*. si* $m = nq + r$*, alors* $m \wedge n = n \wedge r$*.*

Exemple 2.1.14

$49 = 14 \times 3 + 7;$

$49 \wedge 14 = 14 \wedge 7 = 7.$

2.1.4.2 PPCM :

Définition 2.1.15

Soient $m, n \in \mathbb{Z}$. Le plus petit élément (pris non nul si $mn \neq 0$) de l'ensemble des multiples positifs communs à m et n s'appelle le plus petit commun multiple de m et n. On le note $PPCM(m, n)$ ou encore $m \vee n$.

Remarque 2.1.16

De la même manière, $PPCM(m_1, m_2, ..., m_k)$ ou encore $m_1 \vee m_2 \vee ... \vee m_k$ est le plus petit multiples positifs en commun de tous les entiers m_i $(i \in [\![0; k]\!])$.

Exemple 2.1.17

- *Les ensembles des multiples positifs de 4 et 5 sont respectivement $M_4^+ = \{0, 4, 8, 12, 16, 20, ...\}$ et $M_5^+ = \{0, 5, 10, 15, 20, 25, ...\}$, donc $4 \vee 5 = 20$;*
- *$-8 \vee 12 = 8 \vee 12 = 24$;*
- *$4 \vee 10 \vee 15 = (4 \vee 10) \vee 15 = 20 \vee 15 = 60$.*

Proposition 2.1.18

- *Si $mn = 0$ alors $m \vee n = 0$;*
- *tout multiple commun à m et n est un multiple du $m \vee n$;*
- *Si $mn \neq 0$, alors $m \vee n = \dfrac{|mn|}{m \wedge n}$, en particulier on a :*

$$m \vee n = |mn| \Leftrightarrow m \wedge n = 1.$$

Exemple 2.1.19

- *$4 \wedge 5 = 1$ donc $4 \vee 5 = 4 \times 5$;*
- *$4 \vee 5 = 20$ et $M_4 \cap M_5 = M_{4 \vee 5} = \{0, \pm 20, \pm 40, \pm 60, ..., \pm 20k, ...\}$;*
- *$18 \wedge 12 = 6$ et on a $18 \vee 12 = \dfrac{18 \times 12}{6} = 36$.*

2.1.4.3 Identité de Bézout pour deux entiers :

Théorème 2.1.20

Soient m et n deux entiers relatifs non tous deux nuls et $d = m \wedge n$, alors il existe deux entiers u et v tels que $mu + nv = d$. Une telle relation est appelée Identité de Bézout de m et n .

Exemple 2.1.21

- $2 \wedge 6 = 2, -2 \times 2 + 1 \times 6 = 4 \times 2 - 1 \times 6 = 10 \times 2 - 3 \times 6 = 2$, *donc le couple (u,v) n'est pas unique ;*
- $39 - 35 = 3 \times 13 - 5 \times 7 = 4$ *tandis que* $13 \wedge 7 = 1$ *donc la réciproque de l'identité de Bézout est fausse.*

Remarque 2.1.22

L'algorithme d'Euclide (cf. paragraphe suivant) nous permet de trouver le PGCD et de construire les entiers u *et* v *dans une Identité de Bézout.*

Théorème 2.1.23 *(Algorithme d'Euclide)*

L'algorithme suivant fournit un calcul du PGCD de m *et* n *:*
- $m = nq_1 + r_1$ *(D.E. de* m *par* n*) ;*
- $n = r_1q_2 + r_2$ *(D.E. de* n *par* r_1*) ;*
- $r_1 = r_2q_3 + r_3$ *(D.E. de* r_1 *par* r_2*) ;*
- *... ;*
- $r_{k-1} = r_kq_k + 1 + r_{k+1}$ *(D.E. de* r_{k-1} *par* r_k*) ;*
  l'algorithme s'arrête une fois que le reste $r_{k+1} = 0$ *, dans ce cas :* $m \wedge n = r_k$ *.*

Exemple 2.1.24

- $325 \wedge 145 = 5$.
  En effet, effectuons quelques divisions euclidiennes :
  - $325 = 145 \times 2 + 35$ *;*
  - $145 = 35 \times 4 + 5$ *;*
  - $35 = 5 \times 7 + 0$ *; (Fin du calcul du PGCD) , on a* $325 \wedge 145 = 5$.
  Trouvons maintenant u *et* v *:*
  $5 = 145 - 35 \times 4 = 145 - 4(325 - 145 \times 2) = -4 \times 325 + 9 \times 145$ *;* $325 \wedge 145 = 5$, *donc* $u = -4$ *et* $v = 9$ *.*

Exercice 2.1.25

Déterminer $702 \wedge 273$ *et chercher* u *et* v *correspondant à l'Algorithme d'Euclide.*

Algorithme d'Euclide étendu :(Présentation "pratique" du tableau sur Excel)

- *Par l'algorithme d'Euclide étendu on calcule* $m \wedge n$ *et un des couples de coefficients* $(u; v)$ *de Bézout.*

Solution de l'exercice précédent :$702 \wedge 273$

	A	B	C	D	E	F	*Commentaires :*
1	m	n	r	q	u	v	
2	-	-	*702*		*1*	*0*	$E_2 = F_3 = 1$, $F_2 = E_3 = 0$
3	-	-	*273*	-	*0*	*1*	$C_i = Mod(A_i; B_i)$, $(i > 4)$
4	*702*	*273*	*156*	*2*	*1*	*-2*	$D_i = Quotient(A_i; B_i)$, $(i > 4)$
5	*273*	*156*	*117*	*1*	*-1*	*3*	$E_i = E_{i-2} - (D_i * E_{i-1})$, $(i > 4)$
6	*156*	*117*	***39***	*1*	***2***	***-5***	$F_i = F_{i-2} - (D_i * F_{i-1})$, $(i > 4)$
7	*117*	*39*	***0***	*3*	*-7*	*18*	$702 \wedge 273 = 39$ *et* $(u, v) = (\mathbf{2}; \mathbf{-5})$

Manuellement on a :

$702 = 2 \times 273 + 156 \Rightarrow 156 = 702 - 2 \times 273$;

$273 = 1 \times 156 + 117 \Rightarrow 117 = -702 + 3 \times 273$;

$156 = 1 \times 117 + 39 \Rightarrow 39 = 2 \times 702 - 5 \times 273$;

$117 = 3 \times 39 + \mathbf{0} \Rightarrow 702 \wedge 273 = 39$ *et* $(u, v) = (\mathbf{2}; \mathbf{-5})$.

2.1.4.4 Nombres premiers entre eux :

Définition 2.1.26

Soient m et n deux entiers , si $m \wedge n = 1$, on dit que m et n sont premiers entre eux.

Exemple 2.1.27

- *Pour tout $m \in \mathbb{Z}$, $m \wedge S(m) = 1$ $(ex.\ (-1) \wedge 0 = 0 \wedge 1 = 7 \wedge 8 = 20 \wedge 21 = 1)$;*
- $10 \wedge 33 = (2 \times 5) \wedge (3 \times 11) = 1$;
- $16 \wedge 25 = (4^2) \wedge (5^2) = 1$;
- $(2^2 \times 5^4) \wedge (3^2 \times 7^3) = 1$;

Théorème 2.1.28 *(Théorème de Bézout pour deux entiers)*

Deux entiers relatifs m et n sont premiers entre eux si et seulement s'il existe deux entiers relatifs u et v tels que : $u \times m + v \times n = 1$.

Remarque 2.1.29

S'il existe u et v tels que : $u \times m + v \times n = 1$, alors u et v sont aussi premiers entre eux .

Exemple 2.1.30

- *Pour $m \in \mathbb{Z}$, $(m + 1) - m = 1$ avec $u = 1$ et $v = -1$, donc $S(m) \wedge m = 1$;*
- $3 \times 17 - 5 \times 10 = 1$, *donc* $3 \wedge 5 = 3 \wedge 10 = 17 \wedge 5 = 17 \wedge 10 = 1$;
- $5 \wedge 7 = 1,\ 3 \times 5 - 2 \times 7 = 1,\ 10 \times 5 - 7 \times 7 = 1$ *... , c-à-d* (u, v) *n'est pas unique.*

Théorème 2.1.31 *(Théorème de Gauss)*

Soient $m, n, p \in \mathbb{Z}^*$. *Si* $p \wedge m = 1$ *et* $p \mid mn$, *alors* $p \mid n$.

Exemple 2.1.32

- $5 \mid 75$ *et* $5 \wedge 3 = 1$ *donc* $5 \mid 25$ $(75 = 25 \times 3)$;
- $30 \mid (2^3 \times 3 \times 5^2 \times 7^3)$ *et* $30 \wedge 7^3 = 1$ *d'où* $30 \mid (2^3 \times 3 \times 5^2)$.

Lemme 2.1.33 *(Lemme d'Euclide : cas particulier du Théorème de Gauss)*

Soient $m, n \in \mathbb{Z}^*$ *et* p *un nombre premier (voir déf. en paragraphe suivant), alors :*

$$p \mid mn \Rightarrow p \mid m \; ou \; p \mid n.$$

Exemple 2.1.34

- $7 \mid 42$ *et* $42 = 3 \times 14$ *donc* $7 \mid 14$;
- $3 \mid (33 \times 69)$, $3 \mid 33$ *et* $3 \mid 69$.

2.1.5 Nombres premiers et décomposition en facteurs premiers :

2.1.5.1 Nombres premiers :

Définition 2.1.35

Soit $p \in [\![2; \infty[\![$. *On dit que* p *est premier si les seuls diviseurs positifs de* p *sont* 1 *et* p *(i.e.* $D_p^+ = \{1; p\}$*). L'ensemble des nombres premiers est parfois noté* $\mathbb{P}$. *On dit que* p *est composé si* p *n'est pas premier.*

Exemple 2.1.36

- *les nombres suivants sont premiers :*
  $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97,$ *... ;*
- *Le nombre de Mersenne* $(2^{82589933} - 1)$ *est le plus grand nombre premier connu à nos jours qui comporte* $24\,862\,048$ *chiffres.*

Proposition 2.1.37

- *Le sous ensemble* $\mathbb{P}$ *de* $\mathbb{N}$ *est infini ;*
- *tout entier* $m \in [\![2; \infty[\![$ *est soit un nombre premier soit un produit de nombres premiers (ie. composé),*
- *si un nombre premier* p *ne divise pas un entier, il est premier avec lui ;*
- *si un nombre premier* p *divise un produit d'entiers, il divise au moins l'un d'entre eux .*

Exemple 2.1.38

- $7 \nmid 15$ *donc* $7 \wedge 15 = 1$;
- $9 \nmid 15$ *mais* $9 \wedge 15 = 3$ *(car* 9 *n'est pas premier) ;*
- $3 \mid 90$, $90 = 2 \times 5 \times 9$ *et* $3 \mid 9$.

Remarque 2.1.39 *(Test de primalité)*

- *Si un nombre m n'est pas premier alors l'un de ses diviseurs est $\leq \sqrt{m}$;*
- *pour tester si un nombre ≤ 100 est premier il suffit de tester les diviseurs ≤ 10 . Et comme il suffit de tester les diviseurs premiers, il suffit en fait de tester la divisibilité par $2, 3, 5$ et 7 ;*
- *Exemple : $(\sqrt{89} \approx 9.43)$ et 89 n'est pas divisible par $2, 3, 5$ et 7 donc 89 est un nombre premier.*

2.1.5.2 Décomposition en facteurs premiers :

Théorème 2.1.40

Tout entier $m \in [\![2; \infty[\![$ s'écrit de manière unique sous la forme :

$$m = \prod_{i=1}^{k} p_i^{\alpha_i} \ ;$$

appelée décomposition primaire (DP), où les $\alpha_i \in [\![1; \infty[\![$ et les $p_i \in \mathbb{P}$ tels que $p_i < p_{i+1}$.

Exemple 2.1.41 *(DP de 16758)*

16758	2
8379	3
2793	3
931	7
133	7
19	19
1	

$\Rightarrow 16758 = 2 \times 3^2 \times 7^2 \times 19.$

Théorème 2.1.42 *Diviseurs positifs*

Soit $\prod_{i=1}^{k} p_i^{\alpha_i}$ la DP de l'entier naturel m. Alors :

$$D_m^+ = \left\{ \prod_{i=1}^{k} p_i^{\beta_i}, \beta_i \in [\![0; \alpha_i]\!] \ et \ i \in [\![0; k]\!] \right\}.$$

Proposition 2.1.43 *(Nombre de diviseurs positifs d'un entier)*

Soit $\prod_{i=1}^{k} p_i^{\alpha_i}$ la DP. de l'entier naturel m. Alors, le nombre des diviseurs positifs de m est :

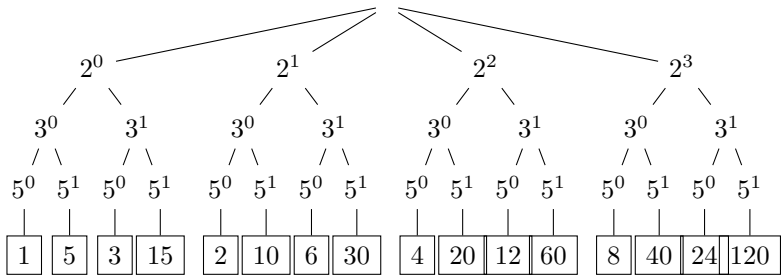
$$\left|D_m^+\right| = \prod_{i=1}^{k} (\alpha_i + 1);$$

Exemple 2.1.44

$16758 = 2^1 \times 3^2 \times 7^2 \times 19^1$ *et* $\left|D_{16758}^+\right| = 2 \times 3 \times 3 \times 2 = 36.$

Exemple 2.1.45

- $120 = 2^3 \times 3 \times 5$ *et* $\left|D_{120}^{+}\right| = 16$. *Pour obtenir tous les diviseurs de* 120, *on considère l'arbre suivant :*



$$D_{120}^{+} = \{1; 2; 3; 4; 5; 6; 8; 10; 12; 15; 20; 24; 30; 40; 60; 120\}.$$

Remarque 2.1.46

Les entiers premiers p_i *dans une DP sont à considérer du plus petit au plus grand, loin de toute confusion on peut écrire :*

$$m = \prod_{p \in \mathbb{P}} p^{\alpha_p} \ ;$$

où $\alpha_p = \alpha_i$ *si* $p = p_i$ *est un nombre premier présent dans la décomposition et* $\alpha_p = 0$ *sinon .*

Théorème 2.1.47 *(Caractérisation de nombres premiers entre eux)*

Soient $m, n \in [\![2; \infty[\![$ *. Alors* $m \wedge n = 1$ *si et seulement si les deux ensembles formés des nombres premiers présents dans la décomposition de* m *et* n *respectivement sont disjoints.*

Exemple 2.1.48

- $3^4 \times 5 \times 11^2$ *et* $2^3 \times 7^5$ *sont premiers entre eux ;*
- $(5^4 \times 7^3 \times 13) \wedge (3^2 \times 7 \times 13^2) \neq 1$ *(deux facteurs en commun).*

Théorème 2.1.49 *(Détermination du PGCD et PPCM)*

Si $\prod_{p \in \mathbb{P}} p^{\alpha_p}$ *et* $\prod_{p \in \mathbb{P}} p^{\beta_p}$ *sont resp. les DP des entiers* m *et* n *dans* $[\![2; \infty[\![$, *alors :*

$$m \wedge n = \prod_{p \in \mathbb{P}} p^{min(\alpha_p, \beta_p)} \ et \ m \vee n = \prod_{p \in \mathbb{P}} p^{max(\alpha_p, \beta_p)}.$$

Exemple 2.1.50

Puisque $532 = 2^2 \times 7^1 \times 19^1$ *et* $246 = 2^1 \times 3^1 \times 41^1$, *alors :*

- $532 \wedge 246 = 2^1 \times 3^0 \times 7^0 \times 19^0 \times 41^0 = 2$ *;*
- $532 \vee 246 = 2^2 \times 3^1 \times 7^1 \times 19^1 \times 41^1 = 65436$.

2.2 Écriture et représentation dans une base de numération b

À propos de notre système de numération usuel :

- *Dans la base décimale (habituelle) :* 2537 = 2 *milliers* $+5$ *centaines* $+3$ *dizaines* $+7$ *unités ;*
- $2537 = 2 \times 1000 + 5 \times 100 + 3 \times 10 + 7 \times 1 = 2 \times 10^3 + 5 \times 10^2 + 3 \times 10^1 + 7 \times 10^0$ *(écriture en base décimale) ;*
- *si* $m \in [\![10^n; 10^{n+1}[\![$ *pour* $n \in \mathbb{N}$*, alors* m *s'écrit avec* $n+1$ *chiffre .*

Définition 2.2.1 *(Écriture suivant la base décimale (base 10))*

Tout entier naturel $m = i_n i_{n-1} ... i_1 i_0$ *s'écrit d'une manière naturelle comme suit :*

$$m = \sum_{k=0}^{n} i_k 10^k.$$

Définition 2.2.2 *(Écriture suivant la base* b*)*

On peut aussi écrire un nombre entier naturel m *en n'importe quelle base* b *de* $[\![2; \infty[\![$ *comme suit :*

$$m = \sum_{k=0}^{n} i_k b^k,$$

où les entiers naturels $i_0, i_1, ..., i_n$ *sont strictement inférieurs à* b *(ce sont les chiffres permettant d'écrire le nombre* m *dans la base* b*).*

Remarque 2.2.3

- *si* $m \in [\![b^n; b^{n+1}[\![$ *pour* $n \in \mathbb{N}$*, alors* m *s'écrit avec* $n+1$ *chiffres en base* b *;*
- *On note l'écriture dans une base* b *:* $m = (i_n i_{n-1} ... i_1 i_0)_b$ *ou encore* $m = \overline{i_n i_{n-1} ... i_1 i_0}^b$*,*
- *Si* $b = 10$ *on écrit habituellement, lorsque aucune confusion n'est possible,* $i_n i_{n-1} ... i_1 i_0$ *au lieu de* $(i_n i_{n-1} ... i_1 i_0)_{10}$ *ou* $\overline{i_n i_{n-1} ... i_1 i_0}^{10}$*.*

Exemple 2.2.4 *(Quelques bases b)*

- *Base binaire :* $b = 2$*, pour* $m \in \mathbb{N}$*,* $m = \overline{i_n i_{n-1} ... i_1 i_0}^2$ *avec* $i_k = 0$ *ou* $i_k = 1$ *, utilisée en Électronique et Informatique ;*
- *base octale :* $b = 8$*, pour* $m \in \mathbb{N}$*,* $m = \overline{i_n i_{n-1} ... i_1 i_0}^8$ *avec* $i_k = 0, 1, ..., 7$*, utilisée en Informatique ;*
- *base hexadécimal,* $b = 16$*, pour* $m \in \mathbb{N}$*,* $m = \overline{i_n i_{n-1} ... i_1 i_0}^{16}$ *avec* $i_k = 0, 1, ..., 9, A, B, C, D, E, F$*, utilisée en Informatique ;*

Remarque 2.2.5

Pour éviter les confusions, il est nécessaire de préciser la base utilisée, par exemple :

- $1830 = (1830)_{10} = \overline{1830}^{10} = 1 \cdot 10^3 + 8 \cdot 10^2 + 3 \cdot 10^1 + 0 \cdot 10^0$ *;*
- $(11100100110)_2 = \overline{11100100110}^2 = 1 \cdot 2^{10} + 1 \cdot 2^9 + \ +1 \cdot 2^8 + 0 \cdot 2^7 + 0 \cdot 2^6 + 1 \cdot 2^5 + 0 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0 = 1830$ *;*

– $(726)_{16} = \overline{726}^{16} = 7 \cdot 16^2 + 2 \cdot 16^1 + 6 \cdot 16^0 = 1830$.

Décimal (10)	*Binaire (2)*	*Ternaire (3)*	*Octal (8)*	*Duodécimal (12)*	*Hexadécimal (16)*
0	*0*	*0*	*0*	*0*	*0*
1	*1*	*1*	*1*	*1*	*1*
2	*10*	*2*	*2*	*2*	*2*
3	*11*	*10*	*3*	*3*	*3*
4	*100*	*11*	*4*	*4*	*4*
5	*101*	*12*	*5*	*5*	*5*
6	*110*	*20*	*6*	*6*	*6*
7	*111*	*21*	*7*	*7*	*7*
8	*1000*	*22*	*10*	*8*	*8*
9	*1001*	*100*	*11*	*9*	*9*
10	*1010*	*101*	*12*	*A*	*A*
11	*1011*	*102*	*13*	*B*	*B*
12	*1100*	*110*	*14*	*10*	*C*
13	*1101*	*111*	*15*	*11*	*D*
14	*1110*	*112*	*16*	*12*	*E*
15	*1111*	*120*	*17*	*13*	*F*
16	*10000*	*121*	*20*	*14*	*10*

Exemple : Écritures dans différentes bases des 17 ***premiers entiers naturels***

Définition 2.2.6 *(base $b \to$ base décimale)*

La conversion d'une écriture $(i_n i_{n-1} ... i_1 i_0)_b$ en base b à une écriture en base décimale s'obtient en calculant la somme :

$$m = \sum_{k=0}^{n} i_k b^k.$$

Exemple 2.2.7

– $(11001)_2 = 1 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^0 = 16 + 8 + 1 = 25$;
– $(1201)_3 = 1 \cdot 3^3 + 2 \cdot 3^2 + 1 \cdot 3^0 = 27 + 18 + 1 = 46$;
– $(7A9E)_{16} = 7{\cdot}16^3{+}10{\cdot}16^2{+}9{\cdot}16^1{+}14{\cdot}16^0 = 7{\cdot}4096{+}10{\cdot}256{+}9{\cdot}16{+}14 = 28672{+}2560{+}144{+}14 = 31390$.

Définition 2.2.8 *(base décimale $\to$ base b)*

La conversion s'obtient en effectuant des divisions successives du nombre, écrit en base décimale, par b et en classant les restes dans le sens inverse : $m = bq_0{+}r_0, q_0 = bq_1{+}r_1, ..., q_{n-2} = bq_{n-1}{+}r_{n-1}, q_{n-1} = b{\times}0{+}r_n$,

avec $q_{n-1} = r_n < b$ *et* $q_n = 0$*, alors :*

$$m = (r_n r_{n-1} ... r_1 r_0)_b.$$

Exemple 2.2.9

- $41 = 2 \cdot 20 + 1, 20 = 2 \cdot 10 + 0, 10 = 2 \cdot 5 + 0, 5 = 2 \cdot 2 + 1, 2 = 2 \cdot 1 + 0$ *et* $1 = 2 \cdot 0 + 1$ *donc :* $(41)_{10} = (101001)_2$ *;*
- $1830 = 16 \cdot 114 + 6, 114 = 16 \cdot 7 + 2, 7 = 16 \cdot 0 + 7$*, donc :* $(1830)_{10} = (726)_{16}$ *;*
- $479 = 7 \cdot 68 + 3, 68 = 7 \cdot 9 + 5, 9 = 7 \cdot 1 + 2, 1 = 7 \cdot 0 + 1$*, donc :* $(479)_{10} = (1253)_7$*.*

Définition 2.2.10 *(base* $b \to$ *base* b'*)*

La conversion s'obtient en passant par la base décimale, ainsi :

$$base\ b\ \to\ base\ dcimale\ \to\ base\ b'.$$

Exemple 2.2.11

- $(11001)_2 = (25)_{10}$ *(cf. e.g. 1.2.7) ;*
- $25 = 6 \cdot 4 + 1, 4 = 6 \cdot 0 + 4$*, donc :* $(25)_{10} = (41)_6$ *; et par conséquent :*

$$(11001)_2 = (41)_6$$

Définition 2.2.12 *(base* $b \to$ *base* b^k*)*

On découpe la représentation de m *en base* b *en tranches de* k *chiffres, en commençant par la droite et en rajoutant des* 0 *à gauche si le nombre de chiffres de* m *n'est pas un multiple de* k*. Chaque tranche de* k *chiffres est alors transformée en un chiffre en base* b^k*. Ces chiffres, écrits dans cet ordre, constituent l'écriture de* m *en base* b^k*.*

Exemple 2.2.13

- *Écriture de* $(1022102)_3$ *en base* $9 = 3^2$*, on coupe l'écriture à des tranches de* 2 *en commençant par la droite et en ajoutant* 0 *à gauche :*

$$\underbrace{(01)_3}_{=1}\underbrace{(02)_3}_{=2}\underbrace{(21)_3}_{=7}\underbrace{(02)_3}_{=2} = (1272)_9;$$

- *Écriture de* $(10101101110)_2$ *en base* $16 = 2^4$ *:*

$$\underbrace{(0101)_2}_{=5}\underbrace{(0110)_2}_{=6}\underbrace{(1110)_2}_{=14=E} = (56E)_{16}.$$

Définition 2.2.14 *(base* $b^k \to$ *base* b*)*

On exprime chaque chiffre en base b^k *comme un nombre écrit en base* b *sur* k *chiffres, en rajoutant des* 0 *(à gauche) si l'écriture du nombre obtenu comporte moins de* k *chiffres en base* b*.*

Exemple 2.2.15

- *Écriture de* $(1A2F)_{16=2^4}$ *en base* $b = 2$ *:*
  $(1A2F)_{16} = \overbrace{(0001)_2}^{\overline{1}^{16}=}\overbrace{(1010)_2}^{\overline{A}^{16}=}\overbrace{(0010)_2}^{\overline{2}^{16}=}\overbrace{(1111)_2}^{\overline{F}^{16}=} = (0001101000101111)_2 = (1101000101111)_2$;
- *Écriture de* $(156)_{8=2^3}$ *en base* $b = 2$ *:*

$$(156)_8 = \overbrace{(001)_2}^{\overline{1}^{8}=}\overbrace{(101)_2}^{\overline{5}^{8}=}\overbrace{(110)_2}^{\overline{6}^{8}=} = (1101110)_2.$$

2.3 Calcul Modulaire

2.3.1 Relation de congruence modulo un entier

Définition 2.3.1

Soit $p \in [\![1; \infty[\![$*. Deux entiers* m *et* n *sont dits congrus modulo* p *si :* $p \mid m - n$ *(ou de façon équivalente* $p \mid n - m$*), i.e. s'il existe* $k \in \mathbb{Z}$ *pour lequel :* $m = n + kp$*. Cette relation se note :*

$$m \equiv n \pmod{p} \text{ ou encore } m \equiv n\,[p]\,.$$

Notation dans laquelle les rôles de m *et* n *sont symétriques.*

Remarque 2.3.2

- *Les relations de congruence généralisent la relation de divisibilité et on a :*

$$n \mid m \Leftrightarrow m \equiv 0 \pmod{n};$$

  Cette équivalence relie les deux termes "Divisibilité" et "Congruence" , ainsi :
  - $5 \mid 75$, $3 \mid 75$, *..., on écrit alors :* $m \in D_{75} \Leftrightarrow 75 \equiv 0 \pmod{m}$;
  - $37 \nmid 75$ *mais* $37 \equiv 1 \pmod{75}$ *(ou encore* $1 \equiv 37 \pmod{75}$ *);*
- $m \equiv n \pmod{p} \Leftrightarrow m - n \in M_p$.

Exemple 2.3.3

- $16 = 5 \times 2 + 6$, *donc* $16 \equiv 6 \pmod{5}$ *et* $16 \equiv 6 \pmod{2}$ *;*
- $16 = 5 \times 3 + 1$, *donc* $16 \equiv 1 \pmod{5}$ *;*
- $16 = 8 \times 2 + 0$, *donc* $16 \equiv 0 \pmod{2}$ *;*
- $-25 + 13 = 13 - 25 = -12 \in M_4$, *donc* $13 \equiv 25 \pmod{4}$ *ou encore* $-13 \equiv -25 \pmod{4}$ *;*
- $22 + 14 = 36 \in M_6$, *donc* $22 \equiv -14 \pmod{6}$.

Proposition 2.3.4

Si $m \equiv n \pmod{q}$ *et* $n \equiv p \pmod{q}$, *alors* $m \equiv p \pmod{q}$.

Exemple 2.3.5

- $12 \equiv 2 \pmod{10}$, $22 \equiv 2 \pmod{10}$, *donc* $22 \equiv 12 \pmod{10}$;
- $13 \equiv 1 \pmod{4}$, $-11 \equiv 1 \pmod{4}$, *donc* $-11 \equiv 13 \pmod{4}$.

Proposition 2.3.6

$m \equiv n \pmod{p_1}, m \equiv n \pmod{p_2} \Leftrightarrow m \equiv n \pmod{(p_1 \vee p_2)}$.

Exemple 2.3.7

- $16 \equiv 1 \pmod{5}$, $16 \equiv 1 \pmod{3}$, *donc* $16 \equiv 1 \pmod{15}$;
- $10 \equiv 4 \pmod{6}$, *donc* $10 \equiv 4 \pmod{3}$ *et* $10 \equiv 4 \pmod{2}$.

Proposition 2.3.8

Les entiers congrus à m *modulo* n *sont les entiers de la forme* $m + kn$, *avec* $k \in \mathbb{Z}$.

Exemple 2.3.9

- $11 \equiv 3 \pmod{4}$ *donc* $11 + 10 \times 4 = 11 + 40 = 51 = 3 + 12 \times 4 \equiv 3 \pmod{4}$;
- $34 \equiv 22 \pmod{6}$ *et* $22 = 4 + 18$ *donc* $34 \equiv 4 \pmod{6}$;
- $20 \equiv -1 \pmod{7}$ *et* $-1 = 6 - 7$ *donc* $20 \equiv 6 \pmod{7}$.

Proposition 2.3.10

Si $m \equiv n \pmod{p}$, *alors* $m \equiv n \pmod{q}$ $\forall q \in D_p$.

Exemple 2.3.11

- $17 \equiv -1 \pmod{6}$ *donc* $17 \equiv -1 \pmod{2}$ *et* $17 \equiv -1 \pmod{3}$.

Proposition 2.3.12

Si $q \in D_m \cap D_n \cap D_p$, $m \equiv n \pmod{p}$, *alors* $\frac{m}{q} \equiv \frac{n}{q} \pmod{\frac{p}{q}}$.

Exemple 2.3.13

- $150 \equiv 90 \pmod{60}$ *et* $30 = 150 \wedge 90 \wedge 60$ *donc* $5 \equiv 3 \pmod{2}$.

Proposition 2.3.14

Si $m \equiv n \pmod{p}$, $m' \equiv n' \pmod{p}$, *alors*

$$m \cdot m' \equiv n \cdot n' \pmod{p} \; et \; m + m' \equiv n + n' \pmod{p}.$$

Exemple 2.3.15

- $10 \equiv 2 \pmod{4}$, $23 \equiv 3 \pmod{4}$, *donc* $230 \equiv 6 \pmod{4}$ *et* $33 \equiv 5 \pmod{4}$;
- $13 \equiv 1 \pmod{3}$, $14 \equiv -1 \pmod{3}$, *donc* $27 \equiv 0 \pmod{3}$.

Proposition 2.3.16

$\forall (m, n) \in \mathbb{Z} \times \mathbb{N}$, $\exists! r \in [\![0; n-1]\!]$ *tel que* $m \equiv r \pmod{n}$ *où* r *est le reste de la D.E. de* m *par* n. *L'intervalle entier* $[\![0; n-1]\!]$ *(resp. l'élément* r *) est appelé système complet de résidus (resp. résidu) modulo* n.

Exemple 2.3.17

- $13 \equiv -2 \pmod{5} \equiv 3 \pmod{5} \equiv 8 \pmod{5}$ *donc* $r = 3$.

Théorème 2.3.18 *(Inversibilité)*
Soit $(m,n) \in \mathbb{Z} \times \mathbb{N}^*$ *tel que* $m \wedge n = 1$. *Alors,* $\exists m' \in \mathbb{Z}$ *tel que* $mm' \equiv 1 \pmod{n}$. *L'entier* m' *s'appelle un inverse de* m *modulo* n .

Exemple 2.3.19

- $3 \wedge 5 = 1$ *et* $3 \cdot 2 = 6 \equiv 1 \pmod{5}$ *alors* 2 *est un inverse de* 3 *modulo* 5 ;
- $3 \equiv 1 \pmod{2}$ *donc* $3^2 \equiv 1 \pmod{2}$, *or* $3 \wedge 2 = 1$ *alors* 3 *est un inverse de lui même modulo* 2.

Théorème 2.3.20 *(Simplifiabilité)*
Soient $n \in \mathbb{N}^*$ *et* m, p *et* q *des entiers tels que* $mp \equiv mq \pmod{n}$. *Si* $m \wedge n = 1$, *alors on peut déduire que* $p \equiv q \pmod{n}$.

Exemple 2.3.21

- $21 \equiv 6 \pmod{5}$ *et* $3 \wedge 5 = 1$ *donc :* $\dfrac{21}{3} \equiv \dfrac{6}{3} \pmod{5}$, *i.e. :* $7 \equiv 2 \pmod{5}$;
- $28 \equiv 10 \pmod{9}$ *et* $2 \wedge 9 = 1$, *donc* $14 \equiv 5 \pmod{9}$.

2.3.2 Classes d'équivalence modulo n

Définition 2.3.22
La classe d'équivalence modulo n *d'un entier* m *est le sous-ensemble de* $\mathbb{Z}$ *formé des entiers de la forme* $kn + m$ *avec* $k \in \mathbb{Z}$. *Dans la suite, on représentera la classe d'équivalence de* m *modulo* n *par* $\overline{r}$ *où* r *est le reste de la D.E. de* m *par* n $(r \in [\![0; n-1]\!])$. *On note également* $\overline{m}$ *la classe d'équivalence de* m .

Remarque 2.3.23

- $m \equiv p \pmod{n}$ *si et seulement s'ils ont le même reste* r *dans la D.E. par* n, *ainsi* m, p *et* r *représentent la même classe d'équivalence modulo* n, *i.e.* $\overline{m} = \overline{p} = \overline{r} \pmod{n}$;
- *les* n *restes possibles permettent de définir toutes les* n *classes d'équivalence modulo* n ;
- *Ces* n *classes forment l'ensemble :*

$$\mathbb{Z}/n\mathbb{Z} = \left\{\overline{0}, \overline{1}, ..., \overline{n-1}\right\},$$

qu'on appelle ensemble-quotient de $\mathbb{Z}$ *par la relation d'équivalence :* " $\equiv \pmod{n}$ ".

Exemple 2.3.24

- $\mathbb{Z}/2\mathbb{Z} = \left\{\overline{0}, \overline{1}\right\}$;
- $\mathbb{Z}/6\mathbb{Z} = \left\{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\right\}$;
- $m \equiv 16 \pmod{6}$ *donc* $\overline{m} = \overline{4} = \overline{-2} \pmod{6}$;
- *dans* $\mathbb{Z}/3\mathbb{Z}$ *on :* $\overline{5} = \overline{2}$, $\overline{19} = \overline{1}$, $\overline{-1} = \overline{2}$, $\overline{3} = \overline{0}$.

2.3.3 Opérations modulaires

Définition 2.3.25 *(Addition / Soustraction modulaire)*

- *L'addition modulaire :* $\overline{m} + \overline{p} = \overline{m+p} \pmod{n}$,*i.e. la somme est le reste de la D.E. de* $m + p$ *par* n.
- *La soustraction modulaire :* $\overline{m} - \overline{p} = \overline{m-p} \pmod{n}$,*i.e. la différence est le reste de la D.E. de* $m - p$ *par* n.

Proposition 2.3.26

- *Commutativité :* $\overline{m}+\overline{p}=\overline{p}+\overline{m} \pmod{n}$;
- *associativité :* $\overline{m}+\overline{p}+\overline{q}=(\overline{m}+\overline{p})+\overline{q} \pmod{n}$;
- *élément neutre :* $\overline{m}+\overline{0}=\overline{m} \pmod{n}$;
- *existence d'un opposé :* $\overline{m}+\overline{m'}=\overline{0} \pmod{n}$.

Exemple 2.3.27

Dans $\mathbb{Z}/10\mathbb{Z}$ ***:***

- $\overline{5}+\overline{2}=\overline{7} \pmod{10}$;
- $\overline{7}+\overline{3}=\overline{10}=\overline{0}$;
- $\overline{9}+\overline{5}=\overline{14}=\overline{4}$;
- $\overline{7}-\overline{9}=\overline{-2}=\overline{8}$;
- $\overline{2}-\overline{8}=\overline{-6}=\overline{4}$
- $\overline{8}+\overline{5}+\overline{7}=\overline{20}=\overline{0}$;
- $\overline{7}+\overline{5}-\overline{1}=\overline{11}=\overline{1}$.

Dans $\mathbb{Z}/6\mathbb{Z}$ ***:***

- $\overline{5}+\overline{2}=\overline{7}=\overline{1} \pmod{6}$;
- $\overline{7}+\overline{3}=\overline{1}+\overline{3}=\overline{4}$;
- $\overline{9}+\overline{5}=\overline{3}+\overline{5}=\overline{8}=\overline{2}$;
- $\overline{7}-\overline{9}=\overline{-2}=\overline{4}$;
- $\overline{2}-\overline{8}=\overline{-6}=\overline{0}$;
- $\overline{8}+\overline{5}+\overline{7}=\overline{2}+\overline{5}+\overline{1}=\overline{2}$;
- $\overline{7}+\overline{5}-\overline{1}=\overline{1}+\overline{5}-\overline{1}=\overline{5}$.

Définition 2.3.28 *(Multiplication modulaire)*

$\overline{m}\times\overline{p}=\overline{m\times p} \pmod{n}$, *i.e. le produit est le reste de la D.E. de* $m\times p$ *par* n.

Proposition 2.3.29

- *Commutativité :* $\overline{m}\times\overline{p}=\overline{p}\times\overline{m} \pmod{n}$;
- *associativité :* $\overline{m}\times\overline{p}\times\overline{q}=(\overline{m}\times\overline{p})\times\overline{q} \pmod{n}$;
- *élément neutre :* $\overline{m}\times\overline{1}=\overline{m} \pmod{n}$;
- *élément absorbant :* $\overline{m}\times\overline{0}=\overline{0} \pmod{n}$;
- *La distributivité de la multiplication par rapport à l'addition :*

$$\overline{m}\times(\overline{p}+\overline{q})=\overline{m}\times\overline{p}+\overline{m}\times\overline{q} \pmod{n};$$

- *La distributivité de l'addition par rapport à la multiplication :*

$$(\overline{m}+\overline{p})\times\overline{q}=\overline{m}\times\overline{q}+\overline{p}\times\overline{q} \pmod{n};$$

- *L'existence de l'inverse n'est pas automatique :*
  - *Rappel :*

    Si $m\wedge n=1$, *alors (cf. th. de Bézout)* $\exists$ *m'* $\in\mathbb{Z}$ *tel que* $mm'\equiv 1 \pmod{n}$, *i.e.* $\overline{m}\times\overline{m'}=1$

$(\text{mod } n)$.

Exemple 2.3.30

Dans $\mathbb{Z}/10\mathbb{Z}$ ***:***

- $\overline{5} \times \overline{2} = \overline{10} = \overline{0} \ (\text{mod } 10)$;
- $\overline{7} \times \overline{3} = \overline{21} = \overline{1}$;
- $\overline{9} \times \overline{5} = \overline{45} = \overline{5}$;
- $\overline{7} \times \overline{-9} = \overline{7} \times \overline{1} = \overline{7}$;
- $\overline{2} \times \overline{-8} = \overline{2} \times \overline{2} = \overline{4}$;
- $\overline{8} \times \overline{5} \times \overline{7} = \overline{40} \times \overline{7} = \overline{0} \times \overline{7} = \overline{0}$;
- $\overline{7} \times \overline{5} \times \overline{-1} = \overline{-35} = \overline{5}$.

Dans $\mathbb{Z}/6\mathbb{Z}$ ***:***

- $\overline{5} \times \overline{2} = \overline{10} = \overline{4} \ (\text{mod } 6)$;
- $\overline{7} \times \overline{3} = \overline{1} \times \overline{3} = \overline{3}$;
- $\overline{9} \times \overline{5} = \overline{3} \times \overline{5} = \overline{15} = \overline{3}$;
- $\overline{7} \times \overline{-9} = \overline{1} \times \overline{3} = \overline{3}$;
- $\overline{2} \times \overline{-8} = \overline{2} \times \overline{4} = \overline{8} = \overline{2}$;
- $\overline{8} \times \overline{5} \times \overline{7} = \overline{2} \times \overline{5} \times \overline{1} = \overline{10} = \overline{4}$;
- $\overline{7} \times \overline{5} \times \overline{-1} = \overline{1} \times \overline{5} \times \overline{-1} = \overline{-5} = \overline{1}$.

Remarque 2.3.31

- *Dans* $\mathbb{Z}/n\mathbb{Z}$*, si* $m \wedge n = 1$*, alors il existe* $\overline{m'} \in \mathbb{Z}/n\mathbb{Z}$ *telle que* $\overline{m} \times \overline{m'} = \overline{1} \ (\text{mod } n)$ *:*
  - *Dans* $\mathbb{Z}/10\mathbb{Z}$:

    $\{\overline{1}, \overline{3}, \overline{7}, \overline{9}\}$ *est l'ensemble des classes* $(\text{mod } 10)$ *formé par les représentants premiers avec* 10 *et on a :*

    $$\overline{1} \times \overline{1} = \overline{3} \times \overline{7} = \overline{9} \times \overline{9} = \overline{1} \quad (\text{mod } 10);$$

    donc, $\forall \overline{m} \in \{\overline{2}, \overline{4}, \overline{6}, \overline{8}\}$ *et* $\forall \overline{p} \in \mathbb{Z}/10\mathbb{Z}$*, on a :*

    $$\overline{m} \times \overline{p} \neq \overline{1} \quad (\text{mod } 10);$$

- *si* n *est premier ;* $\forall r \in [\![1; n-1]\!]$*, il existe* $\overline{r'} \in \mathbb{Z}/n\mathbb{Z} - \{\overline{0}\}$ *tel que* $\overline{r} \times \overline{r'} = \overline{1} \ (\text{mod } n)$ *:*
  - *Dans* $\mathbb{Z}/5\mathbb{Z}$:

    $\mathbb{Z}/5\mathbb{Z} - \{\overline{0}\} = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}$ *est l'ensemble des classes* $(\text{mod } 5)$ *formé par les représentants premiers avec* 5 *et on a :*

    $$\overline{1} \times \overline{1} = \overline{2} \times \overline{3} = \overline{4} \times \overline{4} = \overline{1} \quad (\text{mod } 5).$$

Définition 2.3.32 *(Inverse modulaire et diviseurs de* 0*)*

- *Si* $\overline{m} \times \overline{p} = \overline{1}$*, la classe* $\overline{p}$ *est dite inverse modulaire de la classe* $\overline{m}$ *, on la note :* $\overline{p} = \overline{m}^{-1}$ (*l'écriture* $\overline{m}^{-1} = \dfrac{1}{\overline{m}}$ *est fausse* !) .
- *Si* $\overline{m} \times \overline{p} = \overline{0}$ *tel que* $\overline{m} \neq \overline{0}$ *et* $\overline{p} \neq \overline{0}$*, les classes* $\overline{m}$ *et* $\overline{p}$ *sont appelées : diviseurs de zéro.*

Notation : *L'ensemble des classes qui possèdent un inverse modulo* n *est noté :* $\mathbb{Z}_n^*$.

Proposition 2.3.33

- *Pour que $\overline{m}$ possède une classe inverse, il faut et il suffit que $m \wedge n = 1$. Dans ce cas, cet inverse est unique ;*
- *si $m \wedge n \neq 1$ alors $\overline{m}$ est un diviseur de zéro ;*
- *en générale, si n est premier alors toute classe (excepte $\overline{0}$) possède un inverse (l'ensemble des diviseurs de zéro est vide) .*

Exemple 2.3.34

- $\mathbb{Z}_5^* = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}$, *i.e.* $\mathbb{Z}_5^* = \mathbb{Z}/5 - \{\overline{0}\}$;
- $\mathbb{Z}_{10}^* = \{\overline{1}, \overline{3}, \overline{7}, \overline{9}\}$, *et* $\mathbb{Z}_{10}^* \neq \mathbb{Z}/10\mathbb{Z} - \{\overline{0}\}$;
- $\mathbb{Z}/12\mathbb{Z} = \{\overline{0}\} \cup \{\overline{1}, \overline{5}, \overline{7}, \overline{11}\} \cup \{\overline{2}, \overline{3}, \overline{4}, \overline{6}, \overline{8}, \overline{9}, \overline{10}\}$:
  - $\overline{1}^2 = \overline{5}^2 = \overline{7}^2 = \overline{11}^2 = \overline{1} \pmod{12}$, *et* $\mathbb{Z}_{12}^* = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}\}$;
  - $\overline{2} \times \overline{6} = \overline{3} \times \overline{4} = \overline{8} \times \overline{3} = \overline{9} \times \overline{4} = \overline{10} \times \overline{6} = \overline{0} \pmod{12}$, *et l'ensemble des diviseurs de zéro est* $\{\overline{2}, \overline{3}, \overline{4}, \overline{6}, \overline{8}, \overline{9}, \overline{10}\}$.

Application : (Etude de $\overline{17}^{-1} \pmod{50}$ ***et de*** $\overline{10}^{-1} \pmod{50}$***)***

Concernant $\overline{17}^{-1} \pmod{50}$ ***:***

- *On a* $17 \wedge 50 = 1$;
- *par le théorème de Bézout :* $\exists u, v \in \mathbb{N}$ *tels que :* $50u + 17v = 1$;
- $\overline{50u + 17v} = \overline{1}$, *i.e.* $\overline{50u} + \overline{17v} = \overline{0} + \overline{17v} = \overline{1}$;
- $\overline{17} \times \overline{v} = \overline{1}$ *donc* $\overline{v} = \overline{17}^{-1}$;
- *or, l'algorithme d'Euclide donne :* $u = -1$ *et* $v = 3$;
- *on déduit que :* $\overline{17}^{-1} = \overline{3}$.

Concernant $\overline{10}^{-1} \pmod{50}$ ***:***

- *On a* $10 \wedge 50 = 10 \neq 1$, *donc* $\overline{10}$ *est un diviseur de zéro et par conséquent* $\overline{10}^{-1}$ *n'existe pas. En plus on a*

$$\overline{10} \times \overline{5} = \overline{0} \pmod{50}.$$

2.3.4 Équations modulaires

Définition 2.3.35

Une équation modulaire est une équation (ayant au moins une variable inconnue) valide selon une congruence linéaire $\pmod{n}$.

Exemple 2.3.36 *Trouver* u *dans* $\mathbb{Z}$ *tel que* $\overline{7u} = \overline{4} \pmod{n}$.

- *Si* $n = 5, \overline{7} \in \mathbb{Z}_5^*, \overline{7}^{-1} = \overline{2}^{-1} = \overline{3} \pmod{5}$, *donc* $\overline{u} = \overline{7}^{-1} \times \overline{4} = \overline{2} \pmod{5}$. *Ainsi,*

$$S_{\mathbb{Z}} = \{u = 2 + 5k, k \in \mathbb{Z}\}$$

- *Si* $n = 12, \overline{7} \in \mathbb{Z}_{12}^*, \overline{7}^{-1} = \overline{7} \pmod{12}$, *donc* $\overline{u} = \overline{7}^{-1} \times \overline{4} = \overline{4} \pmod{12}$. *Ainsi,*

$$S_{\mathbb{Z}} = \{u = 4 + 12k, k \in \mathbb{Z}\}.$$

Théorème 2.3.37

Soient $(m, n, p) \in \mathbb{N}^* \times \mathbb{Z} \times \mathbb{Z}$ *et* $m \wedge n = d$, *alors :*

- *Si $d \nmid p$, alors l'équation (E) : $\overline{mu} = \overline{p} \pmod{n}$ n'a pas de solution ;*
- *sinon ($d \mid p$) l'équation précédente a exactement d formes de solutions qu'on peut déterminer en utilisant les diviseurs de zéro dans $\mathbb{Z}/n\mathbb{Z}$ dans l'équation obtenue sous la forme :*

$$(E') : \quad \overline{d} \times (\overline{m'u} - \overline{p'}) = \overline{0} \pmod{n},$$

où d et $(\overline{m'u} - \overline{q'})$ sont des diviseurs de zéro.

Exemple 2.3.38

Trouver u dans $\mathbb{Z}$ tel que (E) : $\overline{6u} = \overline{9} \pmod{15}$.

On a $6 \wedge 15 = 3$, et $3 \mid 9$ donc l'équation (E) a trois formes de solutions :

$(E') : \quad \overline{3} \times (\overline{2u} - \overline{3}) = \overline{0} \pmod{15}$ *. Or on sait que 3 est un diviseur de zéro (car $3 \wedge 15 = 3 \neq 1$), et $\overline{3} \times \overline{0} = \overline{3} \times \overline{5} = \overline{3} \times \overline{10} = \overline{0} \pmod{15}$, donc :*

- $\overline{2u} - \overline{3} = \overline{0} \pmod{15} \Rightarrow \overline{u} = \overline{9} \pmod{15}$;
- $\overline{2u} - \overline{3} = \overline{5} \pmod{15} \Rightarrow \overline{u} = \overline{4} \pmod{15}$;
- $\overline{2u} - \overline{3} = \overline{10} \pmod{15} \Rightarrow \overline{u} = \overline{14} \pmod{15}$,

ainsi,

$$S_{\mathbb{Z}} = \{4 + 15k, 9 + 15k, 14 + 15k \; avec \; k \in \mathbb{Z}\}.$$

Définition 2.3.39

Soit m, n et p trois nombres entiers fixes. L'équation $mu + nv = p$ est une équation diophantienne si les solutions cherchées u et v sont des nombres entiers.

Proposition 2.3.40 *(Résultat d'existence d'une solution)*

Soit m et n deux entiers fixes. On a l'équivalence :

L'équation (E) : $mu + nv = p$ admet (au moins) une solution entière si et seulement si $m \wedge n \mid p$.

Proposition 2.3.41 *(Recherche d'une solution particulière)*

Si l'équation (E) : $mu + nv = p$ a au moins une solution, alors :

- *Grâce au théorème de Bézout combiné avec l'algorithme d'Euclide on trouve une solution particulière $(u_0 ; v_0)$ de l'équation (E_0) : $mu + nv = m \wedge n$;*
- *Pour avoir une solution particulière $(u_1 ; v_1)$ de l'équation (E), on multiplie u_0 et v_0 par $\dfrac{p}{m \wedge n}$. Ainsi*

$$(u_1; v_1) = (u_0 \cdot \frac{p}{m \wedge n}; v_0 \cdot \frac{p}{m \wedge n}).$$

Exemple 2.3.42

Trouver une solution $(u; v)$ de l'équation (E) : $22u + 18v = 14$.

- *Cherchons $22 \wedge 18$:*
  - $22 = 18 \cdot 1 + 4$;
  - $18 = 4 \cdot 4 + 2$;
  - $4 = 2 \cdot 2 + 0$, *d'où $22 \wedge 18 = 2$, or $2 \mid 14$, donc l'équation (E) possède au moins une solution, et* $(E_0) : 22u + 18v = 2$.
- *Trouvons une solution particulière $(u_0 ; v_0)$ de (E_0) :*
  - $2 = 18 - 4 \cdot 4 = 18 - (22 - 18 \cdot 1) \cdot 4 = 18 - (22 \cdot 4) + (18 \cdot 4) = -4 \cdot 22 + 5 \cdot 18$, *d'où*

$(u_0 ; v_0)$=$(-4 ; 5)$;

- *ainsi,* $(u_1; v_1) = (-4 \cdot \frac{14}{2}; 5 \cdot \frac{14}{2}) = (-28; 35)$ *est une solution particulière de* (E) *.*

Théorème 2.3.43 *(Résolution d'une équation diophantienne)*

Soit l'équation diophantienne $(E) : \ mu + nv = p$ *et* $(u_1; v_1)$ *une solution particulière.*

Soit aussi l'équation homogène associée $(EH) : \ mu + nv = 0$*. On a :*

- *Si* $(u_H ; v_H)$ *est une solution de* (EH)*, alors* $(u_H + u_1 ; v_H + v_1)$ *est une solution de* (E)*.*
- *Si* $(u ; v)$ *est une solution de* (E)*, alors* $(u - u_1 ; v - v_1)$ *est une solution de* (EH)*.*

Remarque 2.3.44

Autrement dit, à travers la solution particulière $(u_1; v_1)$ *, à chaque solution de* (E) *correspond une unique solution de* (EH) *et réciproquement.*

Exemple 2.3.45

Considérons l'équation $(E) : 22u + 18v = 14$ *(cf. e.g. précédent).*

- $(u_1; v_1) = (-28; 35)$ *est une solution particulière de* (E)*;*
- $(EH) : 22u + 18v = 0 \Leftrightarrow 11u + 9v = 0$ *;*
- $\overline{11u} = \overline{0} \pmod 9$*, i.e.* $\overline{2} \times \overline{u} = \overline{0} \pmod 9$ *;*
- *or,* $\overline{2} \in \mathbb{Z}_9^*$ *(car* $2 \wedge 9 = 1$*), donc* $\overline{u} = \overline{0} \pmod 9$ *;*
- *pour* $k \in \mathbb{Z}$*,* $(u_H; v_H) = (9k, -11k)$ *est une solution de* (EH)*;*
- *ainsi, l'ensemble des solutions de l'équation* (E) *est :*

$$S_{\mathbb{Z}^2} = \{(-28 + 9k; 35 - 11k) \ avec \ k \in \mathbb{Z}\} .$$

Proposition 2.3.46 *(Détermination des solutions par les congruences)*

Si l'équation $(E) : \ mu + nv = p$ *admet au moins une solution* $(m \wedge n \mid p)$ *, on peut la déterminer en utilisant les congruences :*

- *si* $m \wedge n = 1$*, alors* $\overline{m}^{-1} \pmod n$ *existe, d'autre part* $(E) \Rightarrow \overline{mu} = \overline{p} \pmod n$*, donc* $\overline{u} = \overline{m}^{-1} \times \overline{p} = \overline{u_0} \pmod n$*.*

  Ainsi,

$$S_{\mathbb{Z}^2} = \left\{ (u_0 + kn, \frac{p - m(u_0 + kn)}{n}) \ avec \ k \in \mathbb{Z} \right\} ;$$

- *si* $m \wedge n \neq 1$*, on se ramène au cas précédent via l'implication* $(E) \Rightarrow \overline{m'u} = \overline{p'} \pmod{n'}$ *où* $m' = \frac{m}{m \wedge n}, n' = \frac{n}{m \wedge n}$ *et* $p' = \frac{p}{m \wedge n}$*, dans ce cas* $m' \wedge n' = 1$*.*

Exemple 2.3.47

Considérons l'équation $(E) : 22u + 18v = 14$ *(cf. e.g. précédent).*

- $(E) \Leftrightarrow 11u + 9v = 7$ *;*
- $\overline{11u} = \overline{2} \times \overline{u} = \overline{7} \pmod 9$ *et* $2 \wedge 9 = 1$*,* $\overline{2}^{-1} \pmod 9$ *existe ;*
- $\overline{u} = \overline{2}^{-1} \times \overline{7} = \overline{5} \times \overline{7} = \overline{8} \pmod 9$ *;*

Ainsi,

$$S_{\mathbb{Z}^2} = \left\{ (8 + 9k, \frac{7 - 11(8 + 9k)}{9}) = (8 + 9k, -9 - 11k), k \in \mathbb{Z} \right\} .$$

Remarque 2.3.48

– *Par deux méthodes différentes on obtient la solution de l'équation* $(E) : 22u + 18v = 14$ *:*

$$(-28 + 9k; 35 - 11k) = (8 + 9(\underbrace{k - 4}_{=k'}); -9 - 11(\underbrace{k - 4}_{=k'})).$$

Chapitre 3

Introduction à la Théorie des Groupes

3.1 Définitions et propriétés

3.1.1 Loi de composition interne : l.c.i.

Définition 3.1.1

On appelle loi de composition interne (l.c.i.) sur un ensemble E toute application $* : E \times E \to E$. Au lieu d'utiliser une notation fonctionnelle $*(x, y)$ on utilise une notation en loi : $x * y$.

Exemples 3.1.2

- *l'addition ou la multiplication sont des l.c.i. sur $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$;*
- *la soustraction définit une l.c.i. sur $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$ mais pas sur $\mathbb{N}$ (e.g. 2-7=-5 $\notin \mathbb{N}$) ;*
- *la division est une l.c.i. sur $\mathbb{Q}$ mais pas sur $\mathbb{Z}$ (e.g. $\frac{1}{2} \notin \mathbb{Z}$ même si 1 et 2 sont dans $\mathbb{Z}$) ;*
- *l'application de $\mathcal{F}(E; E) \times \mathcal{F}(E; E)$ dans $\mathcal{F}(E; E)$ définie par $(f; g) \longmapsto f \circ g$ est aussi une l.c.i. sur $\mathcal{F}(E; E)$.*

Remarque 3.1.3

En générale, $a * b$ et $b * a$ peuvent prendre des valeurs différentes, e.g. $3 - 5 \neq 5 - 3$, $3 \div 5 \neq 5 \div 3$.

3.1.2 Notion de groupe et sous-groupe

3.1.2.1 Groupe

Définition 3.1.4

La "collection" d'objets $\{a; b; c; ...\}$ forme un groupe G pour une l.c.i. $*$ dés que les propriétés suivantes sont assurées :

- *Existence d'un élément neutre noté e :*

$$\exists e \in G, \forall a \in G : a * e = e * a = a;$$

- *existence d'un symétrique pour chaque élément de G :*

tout élément $a \in G$ possède un symétrique $a' \in G$ (inverse a^{-1} si $* = \times$, opposé $-a$ si $* = +$) par rapport à $*$ tel que :

$$a * a' = a' * a = e;$$

- *propriété d'associativité : $\forall (a, b, c) \in G^3$ on a :*

$$(a * b) * c = a * (b * c).$$

Le groupe G muni de sa loi $*$ est souvent noté $(G, *)$.

Définition 3.1.5

Soit $(G; *)$ un groupe. Si, la loi $*$ est commutative (i.e. $a * b = b * a$ pour tout $(a, b) \in G^2$), alors on dit que $(G; *)$ est un groupe commutatif ou abélien (du non de Niels Henrik Abel : mathématicien norvégien).

Exemples 3.1.6

- *$(\mathbb{Z}; +); (\mathbb{Q}; +); (\mathbb{R}; +)$ et $(\mathbb{C}; +)$ sont des groupes abéliens, il en est de même pour $(\mathbb{Q}^*; \times); (\mathbb{R}^*; \times)$ et $(\mathbb{C}^*; \times)$;*
- *$(\mathcal{V}_3; +)$ l'ensemble des vecteurs de l'espace muni de l'addition des vecteurs est un groupe abélien ;*
- *$(\mathbb{Q}; \times)$ n'est pas un groupe car 0 est inversible ;*
- *$(\mathbb{N}; +)$ n'est pas un groupe : un entier n non nul n'admet pas d'opposé dans $\mathbb{N}$.*

Remarques 3.1.7

- *En combinant deux éléments d'un groupe G, on génère automatiquement un élément appartenant à ce groupe ;*
- *l'ordre d'un groupe fini G est, par définition, le cardinal de G. On le notera $|G|$ (ou encore card(G)) ;*
- *une convention fréquente veut que l'on note $+$ la loi d'un groupe commutatif ;*
- *loin de toute ambigüité possible, $a * b$ peut être allégée en écrivant tout simplement ab.*

Théorème 3.1.8

Soit $(G; *)$ un groupe :

- *Les éléments du groupe G sont réguliers :*

$$a * b = a * c \Rightarrow b = c;$$

- *l'élément neutre de G est nécessairement unique ;*
- *tout élément $a \in G$, admet un symétrique a^{-1} qui est unique ;*
- *l'inverse du produit de 2 ou plusieurs éléments du groupe G est égal au produit des éléments inverses dans l'ordre inverse :*

$$(a * b * c)^{-1} = c^{-1} * b^{-1} * a^{-1}.$$

Remarque 3.1.9

Si a et b ne commutent pas, il est faux d'écrire $(a * b)^{-1} = a^{-1} * b^{-1}$.

3.1.2.2 Sous-groupe

Définition 3.1.10

Soit $(G;*)$ un groupe . Une partie $H \subset G$ est un sous-groupe de G si H lui-même possède la structure de groupe pour la loi $*$.

Exemples 3.1.11

- *Pour tout groupe G, G lui même et $\{e\}$ sont deux sous-groupes de G ;*
- *$(\mathbb{R}^{+*};\times)$ est un sous-groupe abélien de $(\mathbb{C}^*;\times)$;*
- *$(\mathbb{Q}^*;\times)$ est un sous-groupe abélien de $(\mathbb{R}^*;\times)$ qui est lui-même sous-groupe abélien de $(\mathbb{C}^*;\times)$;*
- *$(\mathbb{Z};+)$ est un sous-groupe abélien de $(\mathbb{Q};+)$ qui est lui-même sous-groupe abélien de $(\mathbb{R};+)$, qui est encore sous-groupe de $(\mathbb{C};+)$.*

Théorème 3.1.12 *Théorème de Lagrange sur les groupes*

Soit $(G;*)$ un groupe : Pour tout groupe fini G et tout sous-groupe H de G,on a :

$$|H| \ divise \ |G| .$$

Théorème 3.1.13 *(Caractérisation des sous-groupes)*

Soient $(G;*)$ un groupe et H une partie de G. H est un sous-groupe de G si et seulement si :

- *$H \neq \emptyset$;*
- *$\forall a, b \in H, a * b^{-1} \in H$.*

3.1.3 Morphisme de groupes

Définition 3.1.14

Une application $f : (G;*) \to (G';\bullet)$ est un morphisme (=homomorphisme) de groupes si :

$$\forall a, b \in G, f(a * b) = f(a) \bullet f(b).$$

Si de plus f est une bijection, on dit que f est un isomorphisme de groupes et que G et G' sont isomorphes.

Exemples 3.1.15

- *L'application $f : (\mathbb{Z};+) \to (\mathbb{R};+)$ telle que $f(n) = 3n$ est un morphisme de groupes :*

$$3(n+m) = 3n + 3m;$$

- *l'application $g : (\mathbb{R};+) \to (\mathbb{R}^{+*};\times)$ telle que $g(x) = e^x$ est un isomorphisme de groupes :*

$$e^{x+y} = e^x \times e^y; e^x \text{ est strictement croissante et continue donc bijective};$$

- *l'application $h : x \longmapsto x^n$ (pour $n \in \mathbb{Z}$), est un morphisme de $(\mathbb{Q}^*;\times)$ dans $(\mathbb{Q}^*;\times)$ (resp.$(\mathbb{R}^*;\times)$, resp.$(\mathbb{C}^*;\times)$). Cette application donne un isomorphisme du groupe $(\mathbb{R}^{+*};\times)$ dans $(\mathbb{R}^{+*};\times)$;*
- *soient $(G;\circ)$ un groupe et $a \in G$, posons par récurrence $a^0 = e$, $a^{n+1} = a \circ a^n$ et $a^{-n} = (a^n)^{-1}$ (pour $n \in \mathbb{N}$). L'application $k : n \longmapsto a^n$ de $(\mathbb{Z};+)$ dans $(G;\circ)$ est un morphisme de groupe.*

Proposition 3.1.16

Soit $f : (G; *) \to (G'; \bullet)$ un morphisme de groupes, on a :

- $f(e_G) = e_{G'}$;
- $\forall a \in G, f(a^{-1}) = (f(a))^{-1}$ *où :* a^{-1} *est le symétrique de* a *dans* G *et* $(f(a))^{-1}$ *est le symétrique de* $f(a)$ *dans* G'.

Exemples 3.1.17 *(Exemples précédents)*

- $f(n) = 3n$ *:* $f(0) = 0$, $f(-n) = -3n = -f(n)$;
- $g(x) = e^x$ *:* $g(0) = 1$, $g(-x) = e^{-x} = (e^x)^{-1} = (g(x))^{-1}$;
- $h(x) = x^n$ *:* $h(1) = 1$, $h(x^{-1}) = (x^{-1})^n = (x^n)^{-1} = (h(x))^{-1}$;
- $k(n) = a^n$ *:* $k(0) = a^0 = e$, $k(-n) = a^{-n} = (k(n))^{-1}$.

Proposition 3.1.18

- *Soient deux morphismes de groupes $f : G \to G'$ et $g : G' \to G$". Alors $g \circ f : G \to G$" est un morphisme de groupes ;*
- *Soit $f : G \to G'$ un isomorphisme de groupe. Alors $f^{-1} : G' \to G$ est un isomorphisme de groupes.*

Définition 3.1.19 *(Noyau et image d'un homomorphisme de groupes)*

soit $f : (G; *) \to (G'; \bullet)$ un morphisme de groupes, alors :

- *Le noyau de f est le sous-groupe de G suivant :*

$$Ker\ f = f^{-1}(\{e_{G'}\}) = \{a \in G \mid f(a) = e_{G'}\}.$$

- *L'image de f est le sous-groupe de G' suivant :*

$$Im\ f = f(G) = \{f(a) \mid a \in G\}.$$

Proposition 3.1.20

Soit $f : (G; *) \to (G'; \bullet)$ un morphisme de groupes, alors :

- $Ker\ f$ *est un sous-groupe de G ;*
- $Im\ f$ *est un sous-groupe de G' ;*
- f *est injectif si et seulement si* $Ker\ f = \{e_G\}$;
- f *est surjectif si et seulement si* $Im\ f = G'$.

Exemples 3.1.21 *(Exemples précédents)*

- $f : (\mathbb{Z}; +) \to (\mathbb{R}; +)$, $n \mapsto 3n$ *:* $Ker\ f = \{0\}$ *d'où f est injectif.* $Im\ f = 3\mathbb{Z} \neq \mathbb{R}$ *d'où f est non surjectif ;*
- $g : (\mathbb{R}; +) \to (\mathbb{R}^{+*}; \times)$, $x \mapsto e^x$ *:* $Ker\ g = \{0\}$ *et* $Im\ g = \mathbb{R}^{+*}$ *donc g est un isomorphisme ;*
- $h_1 : (\mathbb{R}^*; \times) \to (\mathbb{R}^*; \times)$, $x \mapsto x^n$, $n \in \mathbb{N}^*$ *:*
  - *si* $n = 2k$ *:* $Ker\ h_1 = \{\pm 1\}$ *et* $Im\ h_1 = \mathbb{R}^{+*} \neq \mathbb{R}^*$, *donc h_1 n'est ni injectif ni surjectif ;*
  - *si* $n = 2k + 1$ *:* $Ker\ h_1 = \{1\}$ *et* $Im\ h_1 = \mathbb{R}^*$, *donc h_1 est un isomorphisme ;*
  - $h_2 : (\mathbb{C}^*; \times) \to (\mathbb{C}^*; \times)$, $x \mapsto x^n$, $n \in \mathbb{N}^*$ *:* $Ker\ h_2 = \left\{e^{\frac{2k\pi i}{n}}, k \in [\![0; n-1]\!]\right\}$ *d'où h_2 n'est pas injectif.* $Im\ h_2 = \mathbb{C}^*$, *donc h_2 est surjectif ;*
  - $h_3 : (\mathbb{R}^{+*}; \times) \to (\mathbb{R}^{+*}; \times)$, $x \mapsto x^n$, $n \in \mathbb{N}^*$ *:* $Ker\ h_3 = \{1\}$ *et* $Im\ h_3 = \mathbb{R}^{+*}$, *donc h_3 est un*

isomorphisme .

3.1.4 Le groupe symétrique

Définition 3.1.22

Les bijections d'un ensemble E sur lui-même sont appelées permutations ou substitutions de E, elles forment le groupe symétrique de E noté $\mathcal{S}(E)$.

Remarques 3.1.23

- *Pour $E_n = \{1, 2, ..., n\}$ on note $\mathcal{S}_n = \mathcal{S}(E)$. Si $E = \{a_1, a_2, ..., a_n\}$, on écrit un élément σ de $\mathcal{S}(E)$ sous la forme suivante :*

$$\sigma = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ \sigma(a_1) & \sigma(a_2) & \cdots & \sigma(a_n) \end{pmatrix};$$

- *on a $|\mathcal{S}_n| = n!$;*
- *en général, le groupe $\mathcal{S}_n$ n'est pas commutatif.*

Exemples 3.1.24

- *Si $\sigma_1 = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 5 & 6 & 3 & 1 \end{smallmatrix}\right)$ et $\sigma_2 = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 5 & 2 & 6 & 3 \end{smallmatrix}\right)$, on a $\sigma_1, \sigma_2 \in \mathcal{S}_6$;*
- *$\mathcal{S}_2 = \{id, \tau\}$ où $id = \left(\begin{smallmatrix} 1 & 2 \\ 1 & 2 \end{smallmatrix}\right)$ et $\tau = \left(\begin{smallmatrix} 1 & 2 \\ 2 & 1 \end{smallmatrix}\right)$;*
- *$\mathcal{S}_3 = \{id, \tau_{12}, \tau_{13}, \tau_{23}, \rho_1, \rho_2\}$ où $id = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{smallmatrix}\right)$, $\tau_{12} = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{smallmatrix}\right)$, $\tau_{13} = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{smallmatrix}\right)$, $\tau_{23} = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{smallmatrix}\right)$, $\rho_1 = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix}\right)$ et $\rho_2 = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{smallmatrix}\right)$.*

TABLE 3.1 – *Loi du groupe S_3*

$f \circ g$	id	τ_{12}	τ_{13}	τ_{23}	ρ_1	ρ_2
id	id	τ_{12}	τ_{13}	τ_{23}	ρ_1	ρ_2
τ_{12}	τ_{12}	id	ρ_2	ρ_1	τ_{23}	τ_{13}
τ_{13}	τ_{13}	ρ_1	id	ρ_2	τ_{12}	τ_{23}
τ_{23}	τ_{23}	ρ_2	ρ_1	id	τ_{13}	τ_{12}
ρ_1	ρ_1	τ_{13}	τ_{23}	τ_{12}	ρ_2	id
ρ_2	ρ_2	τ_{23}	τ_{12}	τ_{13}	id	ρ_1

On voit en particulier que S_3 n'est pas commutatif car le tableau n'est pas symétrique par rapport à sa diagonale .

Bibliographie

[1] J. FARAUT et E. KHALILI , Arithmétique.

[2] P. CAHEN et C. TOUIBI, Arithmétique et algèbre.

[3] G. A. SEDOGBO , *Mathématiques - Algèbre* .

[4] D. ALIBERT , Arithmétique et algèbre commutative .

[5] Elie AZOULAY , Mathématiques .

[6] Elie AZOULAY et Jean AVIGNANT , Mathématiques .

[7] Daniel PERRIN , Cours d'algèbre .

[8] Jean de BIASI , Mathématiques pour CAPES .

[9] Murray R. SPIEGEL , Théorie et applications de l'Analyse .

[10] L. Chambadal , Exercices et problèmes résolus d'Analyse .

[11] S. DESREUX et All , Analyse2 .

[12] Josette Calais , Éléments de la Théorie des groupes .

[13] Jean Marie Monier , Analyse 4 .

[14] Duward Shriver, Mark Weller, Tina Overton, Jonathan Rourke, Fraser Armstrong , Inorganic Chemistry .

[15] W. H. Freeman and Company , 2014 .

[16] Serge Lang , Algebra, éditions Addison-Welsey .

[17] P. Samuel , Théorie des nombres, Collection Méthodes, éditions Hermann .

[18] J. P. Serre , Cours d'arithmétique, éditions PUF .