UNIVERSITÉ ABDELMALEK ESSAADI

FACULTÉ DES SCIENCES - TÉTOUAN

Licence Fondamentale Sciences de la Matière Chimie

Semestre 3 - M20 : Mathématiques pour la Chimie

SUPPORT DE COURS

Rédigé par : **Bouchaib FERRAHI**

Département de Mathématiques

2019-2020

Les documents relatifs à ce cours sont disponibles sur : www.ferrahi.cla.fr

---

Faculté des Sciences de Tétouan, BP. 2121 M'Hannech II, 93030 Tétouan Maroc.

Table des matières

Avant-propos

Ce polycopié, destiné aux étudiant du semestre trois de la Licence Fondamentale Sciences de la Matière Chimie, est conforme au nouveau programme appliqué depuis 2014. En particulier, la réforme 2014 a réintégrée des cours de Mathématiques dans la filière SMC visant le développement de l'esprit d'analyse et de synthèse et la favorisation de l'approche scientifique dans le traitement des problèmes théoriques et expérimentaux.

Le contenu proposé consiste en un recueil de thèmes allant de l'arithmétique et le calcul modulaire, à la théorie de groupe très utiles dans quelques branches et spécialités de cette filière, et enfin, un complément d'Analyse traitant les suites et les séries de fonctions, les séries entières et les séries de Fourier.

Ce polycopié est adapté à la filière sus-mentionnée et se limitera à la présentation des notions, définitions, propriétés et resultants fondamentaux avec des exemples d'application, les démonstrations et fondements théoriques ont été omit pour bien cibler les étudiants concernés.

Ce travail ne constitue pas une référence complète, le lecteur intéressé peut consulter d'autres références qui traitent ce même contenu d'une manière plus profonde.

BOUCHAIB FERRAHI

Chapitre 1

Notions d'Arithmétique et calcul modulaire

1.1 Notions d'Arithmétique

L'arithmétique étudie les propriétés des nombres entiers relatifs (ensemble $\mathbb{Z}$), il est parmi les plus anciens thèmes abordés en Mathématiques et toujours f'actualités vu ses nombreuses applications dans les sciences actuelles notamment en réseaux, cryptologie et codage.

1.1.1 Rappels

- $\mathbb{N} = \{0, 1, 2, ...\}$ l'ensemble de tous les entiers naturels ;
- $\mathbb{N}$ est menu des deux opérations habituelles : la somme $(5 + 7 = 12)$ et la multiplication $(5 \times 7 = 35)$;
- Tout élément de $\mathbb{N}$ admet un successeur : Pour tout $n \in \mathbb{N}$, il existe un entier $m > n$ tel qu'il n'existe aucun autre entier entre n et m, (5 et 6, 1001 et 1002,...) ;
- $\mathbb{N}$ est un ensemble ordonné (avec l'ordre naturel $\leq$ ou $\geq$) :
  1) Pour deux entiers naturels n et m nous avons ou bien $n \leq m$ (i.e. $m \geq n$) ou bien $m \leq n$ (i.e. $n \geq m$) ;
  2) Si $n \leq m$ et $m \leq n$ alors $n = m$;
- $\mathbb{N}$ admet l'élément 0 comme plus petit élément ;
- Toute partie de $\mathbb{N}$ admet un plus petit élément ;
- $\mathbb{Z} = \{..., -2, -1, 0, 1, 2, ...\}$ l'ensemble de tous les entiers relatifs ;
- $\mathbb{Z}$ est menu des deux opérations habituelles : la somme $(5+(-7) = -2)$ et la multiplication $(5\times(-7) = -35)$;
- Chaque élément non nul n admet un opposé noté $-n$, de cette manière on peut définir aussi la soustraction, sur $\mathbb{Z}$, par : $n - m = n + (-n)$, $(5 - 7 = 5 + (-7) = -2)$;
- Tout élément de $\mathbb{Z}$ admet un successeur et un prédécesseur : Pour tout $n \in \mathbb{Z}$, il existe deux entiers $m_1 < n$ et $m_2 > n$ tel que n est le seul entier entre m_1 et m_2, (-6, -5 et -4, 2999, 3000 et 3001,...) ;
- $\mathbb{Z}$ est un ensemble ordonné (avec l'ordre naturel $\leq$ ou $\geq$) :
  1) pour deux entiers relatifs n et m nous avons ou bien $n \leq m$ (i.e. $m \geq n$) ou bien $m \leq n$ (i.e. $n \geq m$) ;
  2) Si $n \leq m$ et $m \leq n$ alors $n = m$;

- Lorsque $n \leq m$ et $n \neq m$ on peut écrire $n < m$;
- $\mathbb{Z}$ n'admet pas de plus petit élément ;
- Une partie de $\mathbb{Z}$ admet un plus petit élément et un plus grand élément si et seulement s'elle est finie.

Remarques 1.1.1 *Raisonnement par récurrence :*
On Rappelle la méthode de raisonnement par récurrence :
Soit P_n une propriété qui dépend de l'entier naturel n, un raisonnement par récurrence ou par induction s'établit comme suit :
Si :

- *P_{n_0} est vraie pour un entier naturel n_0*
- *P_n vraie implique que P_{n+1} est vraie*

Alors : P_n est vraie pour tout entier naturel $n \geq n_0$.

1.1.2 Divisibilité

Soient a et b deux éléments de $\mathbb{Z}$, On dit que a est **divisible** par b, que b **divise** a ou encore que a est **multiple** de b, s'il existe un élément q dans $\mathbb{Z}$ tel que :

$$a = qb$$

Remarques 1.1.2 *Si $a \neq 0$ et b divise a alors b est non nul et q est unique. On dira que q est le* **quotient exact** *de a par b et on note $q = a \mid b$.*

Exemples 1.1.3

- 2 *divise* 16 *;*
- -3 *divise* 27 *;*
- -100 *est divisible par* -5 *;*
- -20 *est multiple de* -4 *;*
- 3 *ne divise pas* 31.

Proposition 1.1.4

- *Soient a et b deux entiers relatifs avec $b \neq 0$, b divise a si et seulement si $\frac{a}{b}$ est un entier relatif ;*
- *Tous les entiers relatifs divisent 0 et sont divisibles par 1 ;*
- *Tout entier a est toujours divisible par 1, -1, a et $-a$;*
- *Si b divise a et $a \neq 0$ alors $\mid b \mid \leq \mid a \mid$;*
- *Si b divise a et a divise b alors $a = \pm b$ ou encore $\mid b \mid = \mid a \mid$;*
- *a divise a ;*
- *0 divise a implique $a = 0$;*
- *c divise b et b divise a implique que c divise a ;*
- *bc divise ac et $c \neq 0$ implique que b divise a ;*
- *Si c divise a et b, il divise tout nombre de la forme $ua + vb$ en particulier la somme et la différence de a et b*
- *En géneral, si b divise a_1, a_2,...,a_n alors b divise $u_1a_1 + u_2a_2 + ... + u_na_n$ pour u_1, u_2,..., u_n des entiers quelconques ;*

1.1.3 Division Euclidienne

Définition 1.1.5 *Soit b un entier relatif non nul, tout entier relatif a s'écrit d'une facon unique $a = bq + r$ avec q entier relatif et r un entier naturel tel que $0 \leq r <\mid b \mid$.*

Remarques 1.1.6
- *Les entiers q et r sont appelés* **quotient** *et* **reste** *de la division euclidienne de a par b;*
- *Lorsque b divise a, q est le quotient exact de a par b et $r = 0$.*

Exemples 1.1.7
- *Division euclidienne de 18 par 5 : $18 = 3 \times 5 + 3$;*
- *Division euclidienne de -18 par 5 : $-18 = (-4) \times 5 + 2$;*
- *On ne peut pas écrire : $-18 = (-3) \times 5 - 3$ car -3 n'est pas positif;*

Remarques 1.1.8 *On note :*
- *$D_a = \{$l'ensemble de tous les entiers relatifs qui divisent $a\}$;*
- *$M_b = \{$l'ensemble de tous les entiers relatifs qui sont des multiples de $b\}$.*

Exemples 1.1.9
- *$D_{10} = \{-10, -5, -2, -1, 1, 2, 5, 10\}$;*
- *$D_{-8} = \{-8, -4, -2, -1, 1, 2, 4, 8\}$;*
- *$M_2 = \{..., -8, -6, -4, -2, 0, 2, 4, 6, 8, ...\}$;*
- *$M_{-3} = \{..., -9, -6, -3, 0, 3, 6, 9, ...\}$.*

Proposition 1.1.10
- *Si $a \neq 0$ alors D_a est un ensemble fini ;*
- *$D_0 = \mathbb{Z}^*$*
- *Si $b \in D_a$ (b divise a) alors : $D_b \subset D_a$ (tout diviseur de b divise a).*

1.1.4 PGCD et PPCM

Définition 1.1.11 *Soient a et b deux entiers relatifs, il existe un plus grand entier positif qui soit diviseur en commun à a et à b, cet entier est appelé* **le plus grand commun diviseur**. *On note :*

$$d = PGCD(a, b)$$

Remarques 1.1.12 *De la même manière le PGCD de n entiers est le plus grand de tous leurs diviseurs positifs en commun, et on note : $PGCD(a_1, a_2, ..., a_n)$*

Exemples 1.1.13
- $PGCD(2, 5) = 1$
- $PGCD(30, 12) = 6$
- $PGCD(-30, 42) = 6$

Proposition 1.1.14
- *Les diviseurs en commun à a et à b sont les diviseurs de $d = PGCD(a, b)$;*
- *$PGCD(a, b) = PGCD(b, a)$;*

- $PGCD(a,b,c) = PGCD(a, PGCD(b,d)) = PGCD(PGCD(a,b),c) = ...$;
- $PGCD(ca,cb) =\mid c \mid PGCD(a,b)$;
- $PGCD(a,1) = 1$;
- *Soient* $a' = \frac{a}{PGCD(a,b)}$ *et* $b' = \frac{b}{PGCD(a,b)}$ *alors* $PGCD(a',b') = 1$.

Theorem 1.1.15 *Si* $d = PGCD(a,b)$*, il existe deux entiers relatifs* u *et* v *tels que :*

$$d = ua + vb$$

Définition 1.1.16 *Soient* a *et* b *deux entiers relatifs, il existe un plus grand entier positif qui multiple de* a *et de* b*, cet entier est appelé* **le plus petit commun multiple**. *On note :*

$$m = PPCM(a,b)$$

Proposition 1.1.17

- *Si* $a = 0$ *ou* $b = 0$ *alors* $PPCM(a,b) = 0$;
- *Tout multiple commun de* a *et de* b *est un multiple du* $PPCM(a,b)$;
- *Si* $\mid ab \mid \neq 0$ *alors* $PPCM(a,b) = \frac{|ab|}{PGCD(a,b)}$;
- *Si* $\mid ab \mid \neq 0$ *alors :*

$$PPCM(a,b) =\mid ab \mid \Leftrightarrow PGCD(a,b) = 1$$

.

Exemples 1.1.18

- $PPCM(2,5) = 10$
- $PPCM(30,12) = 60$
- $PPCM(-30,42) = 210$

1.1.5 Nombres premiers entre eux

Définition 1.1.19 *Lorsque* $PGCD(a,b) = 1$ *nous dirons que* a *et* b *sont* **premiers entre eux**.

Theorem 1.1.20 *(de Bezout :) Deux entiers relatifs* a *et* b *sont premiers entre eux si et seulement si'il existe deux entiers relatifs* u *et* v *tels que :* $ua + vb = 1$.

Lemme 1.1.21 *(d'Euclide Gauss :)*
Si c *divise* ab *et si* c *est premier avec* b *alors* c *divise* a.

1.1.6 Nombres premiers et décomposition en facteurs premiers

Définition 1.1.22 *Un nombre premier dans* $\mathbb{Z}$ *est un entier* $n > 1$ *dont les seuls diviseurs positifs sont* 1 *et* n.

Exemples 1.1.23 *les nombres suivants sont premiers :*
2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, ...,
Le plus grand nombre premier connu à nos jours comporte 17425170 *de chiffres !*

Proposition 1.1.24
- *Le sous ensemble de $\mathbb{N}$ constitué par les nombres premiers est infini ;*
- *Tout entier $n > 1$ est soit un nombre premier soit un produit de nombres premiers ;*
- *Si un nombre premier 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.*

Theorem 1.1.25 *(Décomposition en produit de facteurs premiers)*
Tout entier $n > 1$ s'écrit de manière unique sous la forme :

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

où les α_i sont des entiers ≥ 1 et où les p_i sont des nombres premiers distincts tels que $p_i < p_{i+1}$.

Remarques 1.1.26 *Les entiers premiers p_i sont à considérer du plus petit au plus grand, il y a aucune confusion à écrire :*

$$n = \prod_{p\ Premier} p^{\alpha_p}$$

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

Theorem 1.1.27 *(diviseurs et décomposition en facteurs premiers) :*
Un entier $b > 1$ divise $a > 1$ si et seulement si chaque nombre premier qui figure dans la décomposition de b figure aussi dans la décomposition de a avec un exposant supérieur ou égal à celui qu'il a dans b. i.e : Si

$$a = \prod_{p\ Premier} p^{\alpha_p}$$

est la décomposition de a. Alors $b > 1$ divise a si et seulement si :

$$b = \prod_{p\ Premier} p^{\beta_p}$$

Où $\beta_p \leq \alpha_p$ pour tout entier premier p.

Exemples 1.1.28
- *[1.]* $6 = 2^1 \times 3^1$ *divise* $12 = 2^2 \times 3$ *et divise aussi* $60 = 2^2 \times 3 \times 5$ *;*
- *[2.]* $70 = 2^1 \times 5^1 \times 7^1$ *divise* $420 = 2^2 \times 3^1 \times 5^1 \times 7^1$.

Theorem 1.1.29 *(Caractérisation de nombres premiers entre eux en utilisant la décomposition) :*
Soient a et b deux entiers naturels non nuls et différents de 1. Alors a et b sont premiers entre eux si et seulement si l'ensemble des nombres premiers présents dans la décomposition de a et l'ensemble des nombres premiers présents dans la décomposition de b sont disjoints.

Exemples 1.1.30
- $15 = 3 \times 5$ *et* $16 = 2^4$ *sont premiers entre eux (aucun facteur en commun) ;*
- $15 = 3 \times 5$ *et* $30 = 2 \times 3 \times 5$ *ne sont pas premiers entre eux (deux facteurs en commun).*

Theorem 1.1.31 *(Détermination du PGCD et PPCM avec la décomposition en facteurs premiers) : Soient :*

$$a = \prod_{p\ Premier} p^{\alpha_p}$$

$$b = \prod_{p\ Premier} p^{\beta_p}$$

deux entiers naturels, non nuls et différents de 1*, décomposés en facteurs premiers. Alors :*

$$PGCD(a,b) = \prod_{p\ Premier} p^{min(\alpha_p,\beta_p)}$$

$$PPCM(a,b) = \prod_{p\ Premier} p^{max(\alpha_p,\beta_p)}$$

Exemples 1.1.32 *Soient :* $a = 532 = 2^2 \times 7 \times 19$ *et* $b = 246 = 2 \times 3 \times 41$ *alors :*

$$PGCD(532, 246) = 2^1 \times 3^0 \times 7^0 \times 19^0 \times 41^0 = 2$$

et

$$PPCM(532, 246) = 2^2 \times 3^1 \times 7^1 \times 19^1 \times 41^1 = 65436$$

1.1.7 Applications : Algorithmes

Proposition 1.1.33 *Algorithme d'Euclide (Division Euclidienne) L'algorithme d'Euclide permit la détermination du quotient* q *et du reste* r *de la division Euclidienne d'un entier relatif* a *par un entier relatif* b*.*

Proposition 1.1.34 *Algorithme d'Euclide (Cas où* $a \geq 0$ *et* $b > 0$*) :*
$B := b$
$R := a$
$Q := 0$
Tant que $R \geq B$*, faire :*
$R := R - B$
$Q := Q + 1$
Fin.
L'algorithme se termine lorsque $R < B$*, dans ce cas : la dernière de valeur de* Q *représente le quotient et la dernière valeur de* R *est le reste.*

Proposition 1.1.35 *Algorithme d'Euclide (cas général) :*
- On applique le 1^{er} *cas à* $\mid a \mid$ *et* $\mid b \mid$ *: on peut écrire*

$$\mid a \mid = q \mid b \mid + r$$

- La division Euclidienne de a *par* b *se déduit du tableau suivant :*

a	b	*Quotient*	*Reste*
$a \geq 0$	$b < 0$	$-q$	r
$a < 0$	$b > 0$	$-(q+1)$	$b - r$
$a < 0$	$b < 0$	$q + 1$	$-b - r$

Exemples 1.1.36 *1) Soient* $a = 46$ *et* $b = 15$*, l'application de l'algorithme d'Euclide :*
$R = 46$, $B = 15$
$R = 46 - 15 = 31$, $Q = 1$
$R = 31 - 15 = 16$, $Q = 2$
$R = 16 - 15 = 1$, $Q = 3$ *l'algorithme se termine car* $R = 1 < B = 15$*, donc :*

$$46 = 3 \times 15 + 1$$

2)Soient $a = -46$ *et* $b = -15$*, l'application de l'algorithme d'Euclide pour* $|a|$ *et* $|b|$ *donne* $|46| = 3 \times |15| + 1$ *et on en déduit :*

$$Q = q + 1 = 4 \text{ et } R = -b - r = 15 - 1 = 14 \text{ et } -46 = -15 \times 4 + 14$$

3)Soient $a = 325$, $b = 145$
$R_0 = 325$, $R_1 = 145$, $325 = 2 \times 145 + 35$
$R_0 = 145$, $R_1 = 35$, $145 = 4 \times 35 + 5$
$R_0 = 35$, $R_1 = 5$, $35 = 7 \times 5 + 0$
$R_0 = 5$, $R_1 = 0$, *donc :* $PGCD(325, 145) = 5$.

Proposition 1.1.37 *(Algorithme d'Euclide(Trouver* (u, v) *tel que* $PGCD(a, b) = ua + vb$*) :*
Initialisation :
$R_0 := a$
$R_1 := b$
$U_0 := 1$
$U_1 := 0$
$V_0 := 0$
$V_1 := 1$
Tant que $R_1 > 0$ *faire :*
$Q :=$ *quotient division de* R_0 *par* R_1
$R :=$ *reste division de* R_0 *par* R_1
$U := U_0 - Q \times U_1$
$V := V_0 - Q \times V_1$
$R_0 := R_1$
$R_1 := R$
$U_0 := U_1$
$U_1 := U$

$V_0 := V_1$
$V_1 := V$
Fin.
L'algorithme se termine lorsque $R_1 = 0$ *avec :*
$PGCD(a, b) = R_0$, $u = U_0$ *et* $v = V_0$.

Exemples 1.1.38 $a = 325$, $b = 145$
$R_0 = 325$, $R_1 = 145$, $U_0 = 1$, $U_1 = 0$, $V_0 = 0$ *et* $V_1 = 1$, *or :*

$$325 = 2 \times 145 + 35$$

$R_1 = 145 > 0$ *donc :*
$Q :=$ *quotient*$(325, 145) = 2$, $R :=$ *reste* $(325, 145) = 35$, $U = 1 - 2 \times 0 = 1$, $V = 0 - 2 \times 1 = -2$
$R_0 = 145$, $R_1 = 35$, $U_0 = 0$, $U_1 = 1$, $V_0 = 1$ *et* $V_1 = -2$, *or :*

$$145 = 4 \times 35 + 5$$

$R_1 = 35 > 0$ *donc :*
$Q :=$ *quotient*$(145, 35) = 4$, $R :=$ *reste* $(145, 35) = 5$, $U = 0 - 4 = -4$, $V = 1 + 8 = 9$
$R_0 = 35$, $R_1 = 5$, $U_0 = 1$, $U_1 = -4$, $V_0 = -2$ *et* $V_1 = 9$, *or :*

$$35 = 7 \times 5 + 0$$

$R_1 = 5 > 0$ *donc :*
$Q :=$ *quotient*$(35, 5) = 7$, $R :=$ *reste* $(35, 5) = 0$, $U = 1 + 28 = 29$, $V = 1 - 63 = -62$
$R_0 = 5$, $R_1 = 0$, $U_0 = -4$, $U_1 = 29$, $V_0 = 9$ *et* $V_1 = -62$,
Fin (car $R_0 = 0$*) avec :*
$PGCD(325, 145) = R_0 = 5$, $u = U_0 = -4$ *et* $v = V_0 = 9$

1.2 Écriture et représentation dans une base b

1.2.1 Définitions et propriétés

Remarques 1.2.1 $2132 =$ *"Deux" milles + "un" cent + "trois" dizaines + "deux" unités*
$2132 = 2 \times 1000 + 1 \times 100 + 3 \times 10 + 2 \times 1$
$2132 = 2 \times 10^3 + 1 \times 10^2 + 3 \times 10^1 + 2 \times 10^0$

Définition 1.2.2
- *On rappelle l'écriture habituelle suivant la base décimale (base 10)*
- *Tout entier* $a_n a_{n-1} ....a_1 a_2$ *s'écrit d'une manière naturelle :* $a_n \times 10^n + a_{n-1} \times 10^{n-1} + ... + a_1 \times 10^1 + a_0 \times 10^0$

D'une manière générale l'écriture suivant une base b est définie par :

Définition 1.2.3 *Soit b un entier positif, tout entier naturel m admet une écriture unique suivant la base b donée par :*

$$m = a_n \times b^n + a_{n-1} \times b^{n-1} + ... + a_1 \times b^1 + a_0 \times b^0$$

avec : $a_n \neq 0$ et pout tout i on a : $a_i = 0, 1, 2,...,b-1$

Remarques 1.2.4

- *On note l'écriture dans une base b :*

$$m = (a_n a_{n-1}....a_1 a_0)_b$$

ou

$$m = \overline{a_n a_{n-1}.....a_1 a_0}^b$$

- *Si $b = 10$ on écrit habituellement, lorsque aucune confusion n'est possible, $a_n a_{n-1}....a_1 a_0$ au lieu de*

$$(a_n a_{n-1}....a_1 a_0)_{10}$$

ou

$$\overline{a_n a_{n-1}.....a_1 a_0}^{10}$$

Exemples 1.2.5

- *Base binaire : $b = 2$, tout entier naturel s'écrit $\overline{a_n a_{n-1}.....a_1 a_0}^2$ avec $a_i = 0$ ou $a_i = 1$, utilisée en Électronique et Informatique ;*
- *Base octale : $b = 8$, tout entier naturel s'écrit $\overline{a_n a_{n-1}.....a_1 a_0}^8$ avec $a_i = 0, 1,...,7$, utilisée en Informatique*
- *Base hexadécimal, $b = 16$, tout entier naturel s'écrit $\overline{a_n a_{n-1}.....a_1 a_0}^{16}$ avec $a_i = 0, 1,...,9$, $a = 10$, $b = 11,...f = 15$, utilisée en Informatique ;*
- $1830 = (1830)_{10} = \overline{1830}^{10} = 1 \times 10^3 + 8 \times 10^2 + 3 \times 10^1 + 0 \times 10^0$;
- $1830 = (11100100110)_2 = \overline{11100100110}^2 = 1 \times 2^{10} + 1 \times 2^9 + 1 \times 2^8 + 0 \times 2^7 + 0 \times 2^6 + 1 \times 2^5 + 0 \times 2^4 + 0 \times 2^3 + 1 \times 2^2 + 1 \times 2^1 + 0 \times 2^0$;
- $1830 = (726)_{16} = \overline{726}^{16} = 7 \times 16^2 + 2 \times 16^1 + 6 \times 16^0$.

- Écritures dans différentes bases des premiers entiers naturels :

Remarques 1.2.6 *Pour éviter les confusions, il est nécessaire de préciser la base utilisée, par exemple :*

- 1101 *en base* $b = 10$ *:* $(1101)_{10} = 1101$
- 1101 *en base* $b = 8$ *:* $(1101)_8 = 577$
- 1101 *en base* $b = 2$ *:* $(1101)_2 = 13$

Décimal (10)	Binaire (2)	Octal (8)	Hexadécimal (16)
0	00000	00	0
1	00001	01	1
2	00010	02	2
3	00011	03	3
4	00100	04	4
5	00101	05	5
6	00110	06	6
7	00111	07	7
8	01000	10	8
9	01001	11	9
10	01010	12	A
11	01011	13	B
12	01100	14	C
13	01101	15	D
14	01110	16	E
15	01111	17	F
16	10000	20	10

1.2.2 Conversion des écritures entre deux bases :

Définition 1.2.7 *base $b \to$ base décimale :*
La conversion d'une écriture $(a_n a_{n-1}...a_1 a_0)_b$ en base b quelque à une écriture en base décimale s'obtient en calculant la somme :

$$a_n \times b^n + a_{n-1} \times b^{n-1} + ... + a_1 \times b^1 + a_0 \times b^0$$

Exemples 1.2.8
- $(11001)_2 = 1 \times 2^4 + 1 \times 2^3 + 1 \times 2^0 = 16 + 8 + 1 = 25$;
- $(1201)_3 = 1 \times 3^3 + 2 \times 3^2 + 1 \times 3^0 = 27 + 18 + 1 = 46$;
- $(7A9E)_{16} = 7 \times 16^3 + 10 \times 16^2 + 9 \times 16^1 + 14 \times 16^0 = 7 \times 4096 + 10 \times 256 + 9 \times 16 + 14 = 28672 + 2560 + 144 + 14 = 31390$.

Définition 1.2.9 *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 :

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

Exemples 1.2.10
- $41 = 2 \times 20 + 1$, $20 = 2 \times 10 + 0$, $10 = 2 \times 5 + 0$, $5 = 2 \times 2 + 1$, $2 = 2 \times 1 + 0$ *et* $1 = 2 \times 0 + 1$ *donc :* $(41)_{10} = (101001)_2$
- $1830 = 16 \times 114 + 6$, $114 = 16 \times 7 + 2$, $7 = 16 \times 0 + 7$, *donc :* $(1830)_{10} = (726)_{16}$
- $479 = 7 \times 68 + 3$, $68 = 7 \times 9 + 5$, $9 = 7 \times 1 + 2$, $1 = 7 \times 0 + 1$, *donc :* $479_{10} = (1253)_7$

Définition 1.2.11 *base $b \to$ base b' :*
La conversion s'obtient en passant par la base décimale :
Base $b \to$ base $10 \to$ base b'.

Définition 1.2.12 *Base puissance de l'autre ($b \to b^k$)*
On découpe la représentation de m en base b en tranches de k chiffre, 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.

Exemples 1.2.13
- *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 :*

$$\underbrace{\overline{\mathbf{0}1}^3}_{=1}\underbrace{\overline{02}^3}_{=2}\underbrace{\overline{21}^3}_{=7}\underbrace{\overline{02}^3}_{=2} = (1272)_9$$

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

$$\underbrace{\overline{\mathbf{0}101^2}}_{=5}\underbrace{\overline{0110}^2}_{=6}\underbrace{\overline{1110}^2}_{=14=E} = (56E)_{16}$$

Définition 1.2.14 *Base puissance de l'autre ($b^k \to b$) 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.*

Exemples 1.2.15
- *Écriture de $1A2F_{16=2^4}$ en base $b = 2$:*

$$\overline{1}^{16}\overline{A}^{16}\overline{2}^{16}\overline{F}^{16} = \underbrace{\overline{\mathbf{000}1^2}}\underbrace{\overline{1010^2}}\underbrace{\overline{\mathbf{00}10^2}}\underbrace{\overline{1111^2}}$$

et

$$= (1A2F)_{16} = (1101000101111)_2$$

- *Écriture de $156_{8=2^3}$ en base $b = 2$:*

$$\overline{1}^8\overline{5}^8\overline{6}^8 = \underbrace{\overline{\mathbf{00}1}^2}\underbrace{\overline{101}^2}\underbrace{\overline{110}^2} = (001101110)_2 = (1101110)_2$$

1.3 Calcul Modulaire

1.3.1 Introduction et définitions

Le calcul modulaire est connaît depuis l'aube du temps avec les anciennes civilisations, Les Babylonians, par exemple, on utilisé le système classique d'une montre à aiguilles. A titre d'exemple, On a :

- $2 + 5 = 7$, $9 + 4 = 1$, $8 + 12 = 8$
- $.h45min + 25min = .h10min$, $16H = 04H$
- Le réveil sonne à $07H02$ et chaque $15min$: 02, 17, 32, 47, 02,...

Définition 1.3.1 *(Congruences) Soit $n > 1$ un entier. Deux entiers a et b sont dits* **congrus modulo** *n lorsque n divise $b - a$ (ou de facon équivalente $a - b$).*
Notation : $a \equiv b\ (mod\ n)$

Remarques 1.3.2 *$a \equiv b(mod\ n) \Leftrightarrow a - b$ (et $b - a$) est multiple de n*

Exemples 1.3.3
- $16 - 6 = 10 = 5 \times 2$ *donc* $16 \equiv 6(mod 2)$
- $17 - 107 = -90 = -9 \times 10$ *donc* $17 \equiv 107(mod 10)$
- $-15 + 30 = -15 = -3 \times 5$ *donc* $-15 \equiv -30(mod 5)$

Proposition 1.3.4
- *On a* $a \equiv 0 \ (mod\ n)$ *si et seulement si* n *divise* a*;*
- *Si* $a \equiv b \ (mod\ n)$ *et* $b \equiv c \ (mod\ n)$*, alors* $a \equiv c \ (mod\ n)$*;*
- *On a* $a \equiv b \ (mod\ n_1)$ *et* $a \equiv b \ (mod\ n_2)$ *si et seulement si* $a \equiv b \ (mod\ PPCM(n_1, n_2))$*;*
- *Tout entier est congru modulo* n *à un et un unique élément de l'ensemble* $\{0, ..., n-1\}$*. Il s'agit précisément du reste de la division euclidienne de cet entier par* n*. On dit parfois que l'ensemble* $\{0, ..., n-1\}$ *est un système complet de résidus modulo* n*. Un élément d'un système complet de résidu modulo* n *est parfois appelé un résidu;*
- *Les entiers congrus à* a *modulo* n *sont les entiers de la forme* $a + kn$*, avec* k *entier;*
- *Si* $a \equiv b \ (mod\ n)$ *et* $a' \equiv b' \ (mod\ n)$*, alors* $a + a' \equiv b + b' \ (mod\ n)$ *et* $aa' \equiv bb' \ (mod\ n)$*;*
- *Si* d *est un diviseur commun de* a*,* b *et* n*, alors* $a \equiv b \ (mod\ n)$ *implique* $\frac{a}{d} \equiv \frac{b}{d} \ (mod\ \frac{n}{d})$*;*
- *Si* d *divise* n*, alors* $a \equiv b \ (mod\ n)$ *implique* $a \equiv b \ (mod\ d)$.

Theorem 1.3.5 *Soit* $n > 1$ *un entier et* c *un entier premier avec* n*. Alors il existe un entier* c' *tel que* $cc' \equiv 1 \ (mod\ n)$*. Un tel entier* c' *est appelé un inverse de* c *modulo* n*.*

Exemples 1.3.6 $n = 5$*,* $c = 3$*, on a* $PGCD(5, 3) = 1$*,* c *et* n *premiers entre eux, il existe* $c' = 2$ *tel que :* $cc' = 2 \times 3 = 6 = 1 \times 5 + 1$*, c'est à dire :* $cc' \equiv 1 \ (mod\ 5)$.
2 *est un inverse de* 3 *modulo* 5.

Theorem 1.3.7 *Soient* $n > 1$ *un entier et* a*,* b *et* c *des entiers tels que* $ac \equiv bc \ (mod\ n)$*. Si* c *est premier avec* n*, alors on peut déduire que* $a \equiv b \ (mod\ n)$.

Exemples 1.3.8 $a = 2$*,* $b = 7$*,* $c = 3$ *et* $n = 5$*. On a :* $ac = 6 = 1 \times 5 + 1$ *et* $bc = 21 = 4 \times 5 + 1$ *donc* $ac \equiv 1 \ (mod\ 5)$ *et* $bc \equiv 1 \ (mod\ 5)$ *or,* 3 *et* 5 *sont premiers entre eux donc :*
$a \equiv b \ (mod 5)$ *vérification :* $b - a = 5$ *est multiple de* 5.

Définition 1.3.9 *Classes d'équivalence : On appelle classe d'équivalence modulo* n *d'un élément* x *de* $\mathbb{N}$*; l'ensemble des* y *qui sont congrus à* x *modulo* n *:*
Notation : $\overline{x} = \{y \in \mathbb{N},\ y \equiv x \ (mod\ n)\}$.
x *est dit représentant de la classe* $\overline{x}$.

Remarques 1.3.10
- $x \equiv y \ (mod\ n)$ *Si et seulement s'ils ont le meme reste dans la division Euclidienne par* n*;*
- *les* n *restes possibles permettent de définir les* n *classes d'équivalence modulo* n*;*
- *Ces* n *classes se notent* $\mathbb{Z}/n\mathbb{Z}$*;*

Exemples 1.3.11
- $\mathbb{Z}/2\mathbb{Z} = \{\overline{0}, \overline{1}\}$
- $\mathbb{Z}/6\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$

1.3.2 Opérations modulaires

Définition 1.3.12 *Addition modulaire :*
$\overline{x} + \overline{y} = \overline{x+y}\ (mod\ n)$ *la somme est le reste de la division Euclidienne de* $x + y$ *par* n.

Proposition 1.3.13 *L'addition modulaire vérifie les propriétés suivantes :*

- *Commutativité* $\overline{x} + \overline{y} = \overline{y} + \overline{x}\ (mod\ n)$
- *Associativité* $\overline{x} + \overline{y} + \overline{z} = (\overline{x} + \overline{y}) + \overline{z} = \overline{x} + (\overline{y} + \overline{z})\ (mod\ n)$
- *Élément neutre* $\overline{x} + \overline{0} = \overline{0} + \overline{x} = \overline{x}\ (mod\ n)$
- *Existence d'un opposé* $\overline{x} + \overline{x'} = \overline{0}\ (mod\ n)$

Exemples 1.3.14 *Dans* $\mathbb{Z}/7\mathbb{Z}$ *:* $\overline{2} + \overline{4} = \overline{6}\ (mod\ 7)$, $\overline{4} + \overline{5} = \overline{9} = \overline{2}\ (mod\ 7)$, $\overline{3} + \overline{4} = \overline{0}\ (mod\ 7)$ *et généralement, on a la table suivante :*

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{6}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{6}$	$\overline{6}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$

Définition 1.3.15 *Soustraction modulaire :*
La soustraction modulaire est définie de la même manière :
$\overline{x} - \overline{y} = \overline{x-y}\ (mod\ n)$ *la différence est le reste de la division Euclidienne de* $x - y$ *par* n.

Exemples 1.3.16 *Dans* $\mathbb{Z}/7\mathbb{Z}$ *:* $\overline{4} - \overline{2} = \overline{2}\ (mod\ 7)$, $\overline{4} - \overline{5} = \overline{-1} = \overline{6}\ (mod\ 7)$, $\overline{4} - \overline{4} = \overline{0}\ (mod\ 7)$ *et généralement, on a la table suivante :*

$-$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{0}$	$\overline{0}$	$\overline{6}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$	$\overline{6}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$
$\overline{2}$	$\overline{2}$	$\overline{1}$	$\overline{0}$	$\overline{6}$	$\overline{5}$	$\overline{4}$	$\overline{3}$
$\overline{3}$	$\overline{3}$	$\overline{2}$	$\overline{1}$	$\overline{0}$	$\overline{6}$	$\overline{5}$	$\overline{4}$
$\overline{4}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$	$\overline{0}$	$\overline{6}$	$\overline{5}$
$\overline{5}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$	$\overline{0}$	$\overline{6}$
$\overline{6}$	$\overline{6}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$	$\overline{0}$

Définition 1.3.17 *Multiplication modulaire :*
La multiplication modulaire est définie par :
$\overline{x} \times \overline{y} = \overline{x \times y}\ (mod\ n)$ *le produit est le reste de la division Euclidienne de* $x \times y$ *par* n*.*

Proposition 1.3.18
- *Commutativité* $\overline{x} \times \overline{y} = \overline{y} \times \overline{x}\ (mod\ n)$
- *Associativité* $\overline{x} \times \overline{y} \times \overline{z} = (\overline{x} \times \overline{y}) \times \overline{z} = \overline{x} \times (\overline{y} \times \overline{z})\ (mod\ n)$
- *Élément neutre* $\overline{x} \times \overline{1} = \overline{1} \times \overline{x} = \overline{x}\ (mod\ n)$
- *Élément absorbant* $\overline{x} \times \overline{0} = \overline{0} \times \overline{x} = \overline{0}\ (mod\ n)$
- *La distributivité de la multiplication par rapport à l'addition :* $\overline{x} \times (\overline{y} + \overline{z}) = \overline{x} \times \overline{y} + \overline{x} \times \overline{z}\ (mod\ n)$
- **L'existence de l'inverse n'est pas automatique**

Exemples 1.3.19 *Dans* $\mathbb{Z}/7\mathbb{Z}$ *:* $\overline{3} \times \overline{2} = \overline{6}\ (mod\ 7)$, $\overline{4} \times \overline{5} = \overline{20} = \overline{6}\ (mod\ 7)$, $\overline{4} \times \overline{2} = \overline{1}\ (mod\ 7)$. *Plus généralement, la table de l'opération est donnée par :*

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{1}$	$\overline{3}$	$\overline{5}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{2}$	$\overline{5}$	$\overline{1}$	$\overline{4}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{1}$	$\overline{5}$	$\overline{2}$	$\overline{6}$	$\overline{3}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{3}$	$\overline{1}$	$\overline{6}$	$\overline{4}$	$\overline{2}$
$\overline{6}$	$\overline{0}$	$\overline{6}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Remarques 1.3.20 *Observons les tables de multiplication de* $\mathbb{Z}/7\mathbb{Z}$ *et* $\mathbb{Z}/8\mathbb{Z}$ *:*

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{1}$	$\overline{3}$	$\overline{5}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{2}$	$\overline{5}$	$\overline{1}$	$\overline{4}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{1}$	$\overline{5}$	$\overline{2}$	$\overline{6}$	$\overline{3}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{3}$	$\overline{1}$	$\overline{6}$	$\overline{4}$	$\overline{2}$
$\overline{6}$	$\overline{0}$	$\overline{6}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{\mathbf{0}}$	$\overline{2}$	$\overline{4}$	$\overline{6}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{1}$	$\overline{4}$	$\overline{7}$	$\overline{2}$	$\overline{5}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{\mathbf{0}}$	$\overline{4}$	$\overline{\mathbf{0}}$	$\overline{4}$	$\overline{\mathbf{0}}$	$\overline{4}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{2}$	$\overline{7}$	$\overline{4}$	$\overline{1}$	$\overline{6}$	$\overline{3}$
$\overline{6}$	$\overline{0}$	$\overline{6}$	$\overline{4}$	$\overline{2}$	$\overline{\mathbf{0}}$	$\overline{6}$	$\overline{4}$	$\overline{2}$
$\overline{7}$	$\overline{0}$	$\overline{7}$	$\overline{6}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

On a :
Pour $\mathbb{Z}/7\mathbb{Z}$*;*
- *Si* $\overline{x} \neq \overline{0}$ *et* $\overline{y} \neq \overline{0}$ *alors :* $\overline{x} \times \overline{y} \neq \overline{0}$*;*
- *pour tout* $\overline{x} \neq \overline{0}$*, il existe* $\overline{y} \neq \overline{0}$ *tel que :* $\overline{x} \times \overline{y} = \overline{1}$*;*

Alors que pour $\mathbb{Z}/8\mathbb{Z}$ *:*
- *Si* $\overline{x} = \overline{0}$ *ou* $\overline{y} = \overline{0}$ *alors :* $\overline{x} \times \overline{y} = \overline{0}$*;*

- $\overline{2} \times \overline{4} = \overline{4} \times \overline{2} = \overline{4} \times \overline{4} = \overline{4} \times \overline{6} = \overline{6} \times \overline{4} = \overline{0}$
- *Il existe* $\overline{x} \in \mathbb{Z}/8\mathbb{Z}$ *tel que* $\overline{x} \times \overline{y} \neq \overline{1}$ *pour tout* $\overline{y} \in \mathbb{Z}/8\mathbb{Z}$. *Exemples :* $\overline{x} = \overline{2}, \overline{4}, \overline{6}$

Définition 1.3.21 *(Inverse et diviseurs de* 0*)*

- *Lorsque* $\overline{x} \times \overline{y} = \overline{1}$ *alors la classe* $\overline{y}$ *est appelée :* **inverse de la classe** $\overline{x}$ *et on note :* $\overline{y} = \overline{x}^{-1}$ *(***on ne peut pas écrire** $\overline{\mathbf{y}} = \frac{\mathbf{1}}{\overline{\mathbf{x}}}$*);*
- *Si* $\overline{x} \neq \overline{0}$ *et* $\overline{y} \neq \overline{0}$ *sont tels que* $\overline{x} \times \overline{y} = \overline{0}$ *alors les classes* $\overline{x}$ *et* $\overline{y}$ *sont appelées :* **Diviseurs de zéro**.

Proposition 1.3.22

- *Pour que* $\overline{x}$ *possède une classe inverse, il faut et il suffit que* $PGCD(x, n) = 1$. *Dans ce cas, cet inverse est unique ;*
- *Si* $PGCD(x, n) \neq 1$ *alors* $\overline{x}$ *est un diviseur de zéro ;*
- *Si* n *est premier alors toute classe, sauf* $\overline{0}$*, posède un inverse (l'ensemble des diviseurs de zéro est vide) ;*
- *L'ensemble des classes qui possèdent un inverse (éléments inversible modulo* n*) est noté :* $\mathbb{Z}_n^*$ *;*

Exemples 1.3.23

- $\mathbb{Z}_7^* = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}$,$\mathbb{Z}_7^* = \mathbb{Z}/7\mathbb{Z}\backslash\{\overline{0}\}$
- $\mathbb{Z}_8^* = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$, $\mathbb{Z}_8^* \neq \mathbb{Z}/8\mathbb{Z}\backslash\{\overline{0}\}$
- *Si* n *est premier :* $\mathbb{Z}_n^* = \mathbb{Z}/n\mathbb{Z}\backslash\{\overline{0}\}$

Exemples 1.3.24 *Application :*

- *Etude de* $\overline{17}^{-1}\ (mod\ 50)$ *et de* $\overline{10}^{-1}\ (mod\ 50)$ *:*
- *Concernant* $\overline{17}^{-1}\ (mod\ 50)$ *:*
  on a 17 *et* 50 *sont premiers entre eux, d'après le théorème de Bezout, il existe deux entiers* u *et* v *tels que :* $50u + 17v = 1$ *et on a :*
  $\overline{50u + 17v} \equiv \overline{1}\ (mod\ 50)$
  $\overline{50}\overline{u} + \overline{17}\overline{v} \equiv \overline{1}\ (mod\ 50)$
  $\overline{17}\overline{v} \equiv \overline{1}\ (mod\ 50)$
  Donc $\overline{17}^{-1} \equiv \overline{v}\ (mod\ 50)$*, en utilisant l'algorithme d'Euclide on trouve* $u = -1$ *et* $v = 3$ *et on déduit que :*
  $\overline{17}^{-1} \equiv \overline{3}\ (mod\ 50)$.
- *Concernant* $\overline{10}^{-1}\ (mod\ 50)$ *: On a* $PGCD(10, 50) = 10 \neq 1$ *donc* $\overline{10}$ *est un diviseur de zéro et par conséquent* $\overline{10}^{-1}$ *n'existe pas.*

1.3.3 Équations utilisant les congruences et équations modulaires

Une équations modulaire est une équations dans $\mathbb{Z}/n\mathbb{Z}$ ce genre d'équations est très utile pour simplifier des problèmes Mathématiques difficile en utilisant les congruences.

Exemples 1.3.25 *Soit l'équation suivante :*
Trouver x *tel que* $\overline{3x} \equiv \overline{5}\ (mod\ 7)$.
On a 7 **est un nombre premier** *: chaque classe, sauf* $\overline{0}$*, admet un inverse et on a :* $\overline{3}^{-1} = \overline{5}\ (mod\ 7)$ *(D'après*

la table de $\mathbb{Z}/n\mathbb{Z}$)
Donc : $\overline{x} \equiv \overline{3}^{-1} \times \overline{5} \equiv \overline{5} \times \overline{5} \equiv \overline{25} \equiv \overline{4}\ (mod\ 7)$ et la solutions dans $\mathbb{Z}$ est donnée par :

$$S = \{x = 4 + 7k \text{ avec } k \in \mathbb{Z}\}$$

Le cas général, n n'est pas un nombre premier, se déduit du théorème suivant :

Theorem 1.3.26 *Soient a, b et n trois entiers et $PGCD(a, n) = d$, alors :*

- *Si d ne divise pas b, alors l'équation $\overline{a}\overline{x} = \overline{b}\ (mod\ n)$ n'a pas de solution ;*
- *Sinon (d divise b) l'équation précedente à exactement d solutions qu'on peut déterminer en écrivant l'équation sous la forme :*

  $$(E') \qquad \overline{d}(\overline{a'}\overline{x} - \overline{b'}) = \overline{0} \qquad (\ mod\ n)$$

  et en utilisant les diviseurs de zéro dans $\mathbb{Z}/n\mathbb{Z}$. En effet, (E') veut dire que $\overline{d}$ et $(\overline{a'}\overline{x} - \overline{b'})$ sont des diviseurs de zéro.

Exemples 1.3.27 *Soit l'équation suivante :*
Trouver x tel que $(E)\ \overline{6x} \equiv \overline{9}\ (mod\ 15)$.
On a $a = 6$, $b = 9$, $n = 15$, $PGCD(a, n) = PGCD(6, 15) = 3$ et 3 divise b donc l'équation admet trois solutions :
On a $(E) \Rightarrow \overline{3}(\overline{2x} - \overline{3}) \equiv \overline{0}\ (mod\ 15)$
D'autre part, on sait que $\overline{3}$ est un diviseur de zéro ($PGCD(3, 15) \neq 1$) et $\overline{3} \times \overline{0} \equiv \overline{0}$, $\overline{3} \times \overline{5} \equiv \overline{0}$ et $\overline{3} \times \overline{10} \equiv \overline{0}$ $(mod\ 15)$, on en déduit :

- $\overline{2x} - \overline{3} \equiv \overline{0}\ (mod\ 15) \Rightarrow \overline{x} \equiv \overline{9}\ (mod\ 15)$
- $\overline{2x} - \overline{3} \equiv \overline{5}\ (mod\ 15) \Rightarrow \overline{x} \equiv \overline{4}\ (mod\ 15)$
- $\overline{2x} - \overline{3} \equiv \overline{10}\ (mod\ 15) \Rightarrow \overline{x} \equiv \overline{14}\ (mod\ 15)$

et :

$$S = \{4 + 15k, 9 + 15k, 14 + 15k \text{ avec } k \in \mathbb{Z}\}$$

Proposition 1.3.28 *(Equation de type $ax + by = C$ avec a, b, c, x, y des entiers)*
Soient a, b, c trois entiers. Nous cherchons tous les couples d'entiers $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ tels que (E) : $ax + by = c$

- *Si $a = b = c = 0$ alors tout couple (x, y) est solution de (E) ;*
- *Si $a = 0$, $b \neq 0$ alors : Si b divise c alors (E) admet au moins une solution, sinon (b ne divise pas c) elle n'a pas de solution ;*
- *Si $a \neq 0$, $b \neq 0$ alors :*
  - *Si a et b sont premiers entre eux, (E) admet au moins une solution ;*
  - *Si a et b ne sont pas premiers entre eux :*
    - *Si $PGCD(a, b)$ divise c alors (E) admet au moins une solution ;*
    - *Si $PGCD(a, b)$ ne divise pas c alors (E) n'admet pas de solution.*

Lorsque (E) admet au moins une solution, on peut la déterminer en utilisant l'une des deux méthodes suivantes :

- *Calcul direct utilisant le théorème de Bezout et l'algorithme d'Euclide (voir TD)*
- *Calcul utilisant les congruences : a et b sont premiers entre eux $(E) \Rightarrow \overline{ax} + \overline{by} = \overline{c}\ (mod\ b)$*
  $(E) \Rightarrow \overline{ax} = \overline{c}\ (mod\ b)$
  or a et b sont premiers entre eux, donc $\overline{a}$ admet un inverse $\overline{a}^{-1}$ et $\overline{x} = \overline{a}^{-1}c$.
  Soit x_0 un representant de la classe $\overline{a}^{-1}c$ alors les solutions de (E) sont données par :
  $x = x_0 + kb$ et $y = \frac{c-a(x_0+kb)}{b}$

Remarques 1.3.29 *Si a et b ne sont pas premiers entre eux et $PGCD(a,b)$ divise c alors :*
(E) $\Rightarrow \frac{a}{PGCD(a,b)}x + \frac{b}{PGCD(a,b)}y = \frac{c}{PGCD(a,b)}$ et on utilise la méthode précédente car $a' = \frac{a}{PGCD(a,b)}$ et $b' = \frac{b}{PGCD(a,b)}$ sont premiers entre eux.
On doit noter que a', b' et c' sont des entiers relatifs.

Chapitre 2

Théorie des Groupes

2.1 THÉORIE DES GROUPES

Introduction

La théorie des groupes est une théorie fondamentales dans les sciences Mathématiques, Elle connaît des développements permanents avec de nombreuses applications dans les autres disciplines scientifiques.
En chimie, la théorie des groupes à plusieurs applications notamment :
- Elle permet de simplifier l'écriture de l'Hamiltonien d'une molécule en exploitant ses symétries ;
- Elle permet de calculer les orbitales moléculaires comme somme d'orbitales atomiques ;
- En spectroscopie vibrationnelle, elle permet de prédire le type de déformation que peut subir une molécule et selon la symétrie de sa déformation elle permet de prévoir si une transition peut être visible dans les spectres.
Commençant par présenter les définitions et les propriétés fondamentales de la théorie des Groupes.

2.1.1 Définitions et propriétés

L'étude des ensembles $\mathbb{Z}/n\mathbb{Z}$ dans le chapitre precedent a montrée que certaines propriétés sont vérifiées suivant les opérations définies (par exemple, l'existence de l'inverse ou de l'opposée). L'étude de la structure algébrique d'un ensemble est faite en relation avec une loi (ou opération). La structure de Groupe est définie comme suit :

Définition 2.1.1 *Soit G un ensemble non vide, et $\star : G \times G \to G$ une application définie sur $G \times G$: $(a, b) \to a \star b$.*
$(G, \star)$ est un **Groupe** *si :*

- *La loi $\star$ est une loi de composition interne à G (i.e : $a \star b \in G$ si a et b sont dans G) ;*
- *$\star$ est associative : pour tout a, b et c dans G on a : $a \star (b \star c) = (a \star b) \star c$;*
- *G possède un élément neutre pour $\star$: il existe e dans G tel que : $e \star a = a \star e = a$ pour tout a dans G ;*
- *Tout a dans G admet un symétrique (par rapport à $\star$) : pour tout a dans G, il existe b dans G tel que : $a \star b = b \star a = e$;*

- *Si, de plus, la loi $\star$ est commutative (i.e. $a \star b = b \star a$ pour tout a et b dans G) alors on dit que G est un groupe Commutatif ou Abélien.*

Remarques 2.1.2

- *Il est important de vérifier que la loi est interne à G, par exemple la soustraction n'est pas interne à $\mathbb{Z}$ ($3 - 5 \notin \mathbb{N}$ même si 3 et 5 sont dans $\mathbb{N}$) et de la même manière la division n'est pas interne à $\mathbb{Z}$ ($\frac{1}{2} \notin \mathbb{Z}$ même si 1 et 2 sont dans $\mathbb{Z}$);*
- *Lorsque G à un nombre fini d'éléments, on dit que $(G, \star)$ est un Groupe fini et il est plus pratique de construire la table de la loi $\star$ (sur G) :*

$\star \vec{\Gamma}$	a_1	a_2	...	a_n
a_1	$a_1 \star a_1$	$a_1 \star a_2$	...	$a_1 \star a_n$
a_2	$a_2 \star a_1$	$a_2 \star a_2$	...	$a_2 \star a_n$
.	.	.	.	.
.	.	.	.	.
a_n	$a_n \star a_1$	$a_n \star a_2$	...	$a_n \star a_n$

- *Lorsque la loi $\star$ n'est pas commutative, il faut calculer $a_i \star a_j$ puis $a_j \star a_i$ qui peuvent prendre des valeurs différentes.*

Exemples 2.1.3 *Les exemples suivants sont faciles à vérifier en utilisant les propriétés des opérations habituelles :*

- *$(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$ et $(\mathbb{R}, +)$ sont des Groupes Abéliens;*
- *$(\mathbb{Q}^*, \times)$ et $(\mathbb{R}^*, \times)$ sont des Groupes Abéliens;*
- *$(\mathbb{Z}/n\mathbb{Z}, +)$ est un Groupe Abélien;*
- *$(\mathbb{Z}_n^*, \times)$ est un Groupe Abélien;*
- *Si E un ensemble, l'ensemble $\mathcal{S}(E)$ des bijections de E dans E, muni de la composition des applications est un Groupe, appelé : Groupe symétrique de E. Si E est un ensemble fini de n éléments on note le Groupe symétrique par $\mathcal{S}(E) = \mathcal{S}_n$ et ses éléments sont appelés permutations. En général, le Groupe $\mathcal{S}_n$ n'est pas commutatif;*
- *$E = \{a; b; c\}$, le Groupe des permutations $\mathcal{S}_3$ contient les 6 éléments suivants :*

$$Id = \begin{pmatrix} a & \to & a \\ b & \to & b \\ c & \to & c \end{pmatrix}; \ \sigma_1 = \begin{pmatrix} a & \to & b \\ b & \to & c \\ c & \to & a \end{pmatrix}; \ \sigma_2 = \begin{pmatrix} a & \to & c \\ b & \to & a \\ c & \to & b \end{pmatrix}; \ \tau_1 = \begin{pmatrix} a & \to & a \\ b & \to & c \\ c & \to & b \end{pmatrix};$$

$$\tau_2 = \begin{pmatrix} a & \to & c \\ b & \to & b \\ c & \to & a \end{pmatrix}; \ \tau_3 = \begin{pmatrix} a & \to & b \\ b & \to & a \\ c & \to & c \end{pmatrix}.$$

La table de $\mathcal{S}_3$ est donnée par :

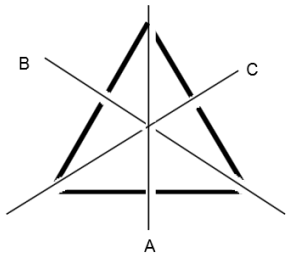
$f \circ g$	Id	σ_1	σ_2	τ_1	τ_2	τ_3
Id	Id	σ_1	σ_2	τ_1	τ_2	τ_3
σ_1	σ_1	σ_2	Id	τ_3	τ_1	τ_2
σ_2	σ_2	Id	σ_1	τ_2	τ_3	τ_1
τ_1	τ_1	τ_2	τ_3	Id	σ_1	σ_2
τ_2	τ_2	τ_3	τ_1	σ_2	Id	σ_1
τ_3	τ_3	τ_1	τ_2	σ_1	σ_2	Id

- *L'ensemble $\mathcal{M}_n$ des matrices carrées inversibles de rang n muni de la multiplication matricielle est un Groupe non-Abélien ;*
- *On montre que l'ensemble des opérations de transformations géométriques (rotation, réflexion, inversion), faisant coïncider un objet symétrique, est un Groupe fini.*
- *Soit $G = \{A, B, C, D, E, F\}$, on considère la loi T définie sur G par la table suivante :*

T ↱	A	B	C	D	E	F
A	E	D	F	B	A	C
B	F	E	D	C	B	A
C	D	F	E	A	C	B
D	C	A	B	F	D	S
E	A	B	C	D	E	F
F	B	C	A	E	F	D

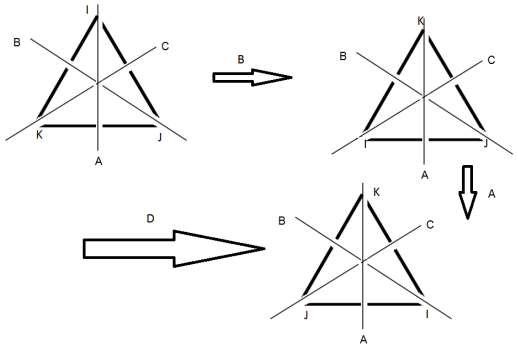
On vérifie que (G, T) est un Groupe fini.

Exactement la même table de Groupe peut être obtenue en considérant que les éléments de G représentent les opérations de symétrie faisant coïncider un triangle équilatéral comme indiqué dans la figure ci-après : Les éléments A, B, ..., F représentent les transformations géométriques suivantes :



- *A : Rotation de π autour de l'axe A ;*
- *B : Rotation de π autour de l'axe B ;*
- *C : Rotation de π autour de l'axe C ;*
- *D : Rotation de $\frac{2\pi}{3}$ dans le sens des aiguilles d'une montre et dans le plan du triangle ;*
- *E : l'identité, rotation de 2π dans le plan du triangle ;*
- *F : Rotation de $\frac{2\pi}{3}$ dans le sens contraire aux aiguilles d'une montre et dans le plan du triangle.*

Exemple de vérification des calculs : $A \star B$, on commence par effectuer B puis A car il s'agit de composition de transformations. La transformation $A \star B$ est identique à la transformation D.



Proposition 2.1.4 • *L'élément neutre e est unique : $e' = e' \star e = e \star e' = e$;*

- *Le symétrique est unique : $b = (b' \star a) \star b = b' \star (a \star b) = b'$;*
- *L'équation $ax = b$ admet une solution unique : $x = a^{-1}b$ ou a^{-1} est le symétrique de a.*

Définition 2.1.5 *(Sous-Groupe) :*
Soit $(G, \star)$ un Groupe. Une partie $H \subset G$ est un **Sous-Groupe** *de G si :*

- *$e \in H$;*
- *$x \star y \in H$, pour tout x et y dans H ;*
- *le symétrique de x appartient à H, pour tout x dans H.*

Remarques 2.1.6 • *Tout sous-Groupe H est aussi un Groupe $(H, \star)$ avec la loi induite par celle de G ;*

- *H est sous-Groupe Si et seulement s'il est non vide et vérifie : $x \star y^{-1} \in H$, pour tout x et y dans H (y^{-1} est le symétrique de y).*

Exemples 2.1.7 • *$(\mathbb{Z}, +)$ est un sous-Groupe de $(\mathbb{R}, +)$;*

- *$(\mathbb{R}^{*+}, \times)$ est un sous-Groupe de $(\mathbb{R}^*, \times)$;*
- *L'ensemble des matrices carrées diagonales est un sous-Groupe de $\mathcal{M}_n$;*
- *$\mathcal{S}_3$ possède 6 sous-Groupes : $\{Id\}$, $\{Id, \tau_1\}$, $\{Id, \tau_2\}$, $\{Id, \tau_3\}$, $\{Id, \sigma_1, \sigma_2\}$, $\mathcal{S}_3$,*

Exemples 2.1.8 *(sous-Groupes de $\mathbb{Z}$) :*
Les sous-Groupes de $(\mathbb{Z}, +)$ sont les ensembles $n\mathbb{Z}$, $n \in \mathbb{Z}$. $n\mathbb{Z} = \{k.n, k \in \mathbb{Z}\}$ est l'ensemble des multiples de n. Autrement dit, chaque sous groupe de $(\mathbb{Z}, +)$ est l'ensemble des multiples d'un entier relatif n_0.

Définition 2.1.9 *(ordre d'un Groupe) :*
L'ordre d'un Groupe $(G, \star)$ est, par définition, le Cardinal de G.
L'ordre d'un sous-Groupe $H \subset G$ est le cardinal de H.

Proposition 2.1.10 *(ordre d'un Groupe :*
Si l'ordre de $G, \star)$ est fini, alors l'ordre de tout sous-Groupe $H \subset G$ divise l'ordre du Groupe G.

Définition 2.1.11 *sous-Groupe engendré) : Soit $(G, \star)$ un Groupe et $H \subset G$. Le sous-Groupe, de $(G, \star)$, engendré par H est e plus petit sous-Groupe contenant H.*

Exemples 2.1.12
- *[] Dans $(\mathbb{R}^*, \times)$, le sous-groupe engendré par $E = \{2\}$ est $H = \{2^n, n \in \mathbb{Z}\}$;*
- *[] Dans $(\mathbb{Z}, +)$, le sous-groupe engendré par $E = \{2\}$ est $H = 2\mathbb{Z}$;*
- *[] Dans $(\mathbb{Z}, +)$, le sous-groupe engendré par $E = \{2, 8\}$ est $H = 2\mathbb{Z}$;*
- *[] Dans $(\mathbb{Z}, +)$, le sous-groupe engendré par $E = \{a, b\}$ est $H = d\mathbb{Z}$ avec $d = PGCD(a, b)$.*

Définition 2.1.13 *(Groupe engendré par un élément) :*
Soit $(G, \star)$ un Groupe et $a \in G$. Le sous-Groupe engendré par a est le sous-Groupe engendré par l'ensemble $\{a\}$.
L'ordre d'un élément $a \in G$ est l'ordre du sous-Groupe engendré par a.
On démontre que l'ordre de a est égal au plus petit entier n tel que $\underbrace{a \star a \star a \star ... \star a}_{n \quad fois} = e$

Définition 2.1.14 *(Morphisme de Groupes) : Soient $(G, \star)$ et $(G', \diamond)$ deux groupes. Une application $f : (G, \star) \to (G', \diamond)$ est un morphisme de Groupes si, pour tout x et y dans G :*

$$f(x \star y) = f(x) \diamond f(y)$$

Exemples 2.1.15
- *L'application $f : (\mathbb{Z}, +) \to (\mathbb{R}, +)$ telle que $f(n) = \frac{1}{2}.n$ est un morphisme de Groupes;*
- *L'application $f : (\mathbb{R}, +) \to (\mathbb{R}^{+*}, \times)$ telle que $f(x) = e^x$ est un morphisme de Groupes.*

Proposition 2.1.16 *Soit $f : (G, \star) \to (G', \diamond)$ un morphisme de Groupes alors :*
- *$f(e_G) = e_{G'}$;*
- *Pour tout x dans G, $f(x^{-1}) = (f(x))^{-1}$ où : x^{-1} est le symétrique de x dans G et $(f(x))^{-1}$ est le symétrique de $f(x)$ dans G'.*

Exemples 2.1.17
- *$f(0_{\mathbb{Z}}) = \frac{1}{2}.0_{\mathbb{Z}} = 0_{\mathbb{Z}} = 0_{\mathbb{R}}$ et $f(-x) = \frac{1}{2}.(-x) = -\frac{1}{2}.X = -(\frac{1}{2}.x)$*
- *$f(0) = e^0 = 1$ et $f(-x) = e^{-x} = \frac{1}{e^x}$*

Proposition 2.1.18
- *Soient deux morphismes de Groupes $f : G \to G'$ et $g : G' \to G''$. Alors $gof : G \to G''$ est un morphisme de Groupes;*
- *Soit $f : G \to G'$ un morphisme de Groupe bijectif. Alors $f^{-1} : G' \to G$ est un morphisme de Groupes.*

Définition 2.1.19 *Un morphisme bijectif est appelé un* **isomorphisme**. *Deux Groupes sont isomorphes s'il existe un ismorphisme de Groupes $f : G \to G'$.*

Définition 2.1.20 *(Noyau et Image) :*

- *Le noyau de f est :*
$$Kerf = \{x \in G | f(x) = e_{G'}\}$$
- *L'image de f est :*
$$Imf = \{f(x) | x \in G\}$$

Proposition 2.1.21 *Soit $f : G \to G'$ un morphisme de Groupes :*

- *$Kerf$ est un sous-Groupe de G ;*
- *Imf est un sous-Groupe de G' ;*
- *f est injectif si et seulement si $Kerf = \{e_G\}$;*
- *f est surjectif si et seulement si $Imf = G'$.*

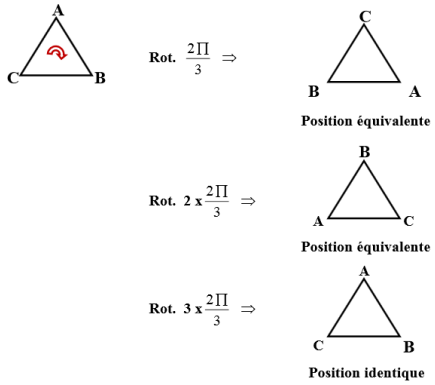
2.1.2 Exemples d'applications en Chimie

Proposition 2.1.22 *(fondamentale) : On montre que l'ensemble de tous les éleéments de symétrie d'un molécule menu de la composition est un Groupe (généralement non-Abélien).*

Remarques 2.1.23 *Utilisation de la théorie des Groupes :*

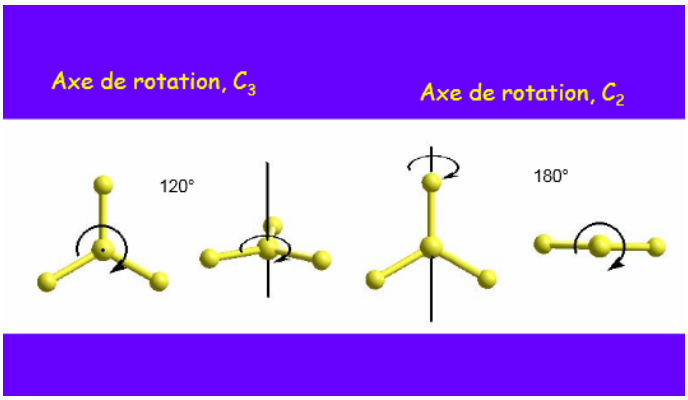
- *Détermination de tous les éléments de symétrie de la molécule ;*
- *Construction de la table du Groupe ;*
- *Détermination des Sous-Groupe et leurs ordres.*

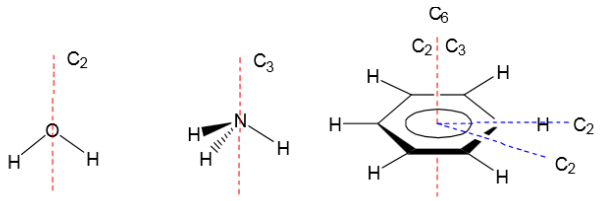
Définition 2.1.24 *Opérations de symétrie : Une opération de symétrie est le mouvement de déplacement d'un objet le conduisant soit à une position équivalente soit à une position identique :*



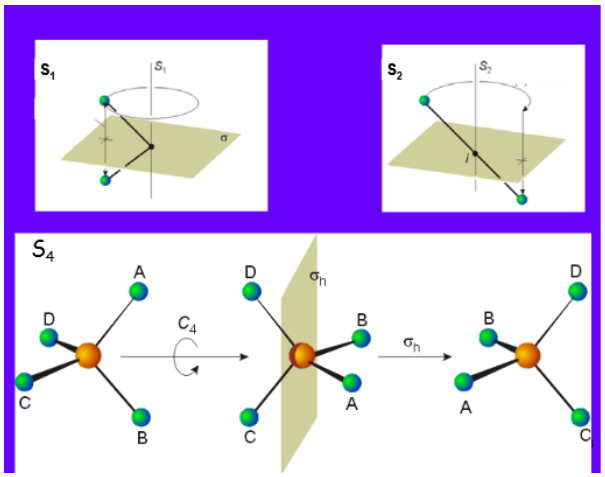
Définition 2.1.25 *Éléments de symétrie : Un élément de symétrie est un objet géométrique qui sert à définir l'opération de symétrie : un point, une droite, un plan.*

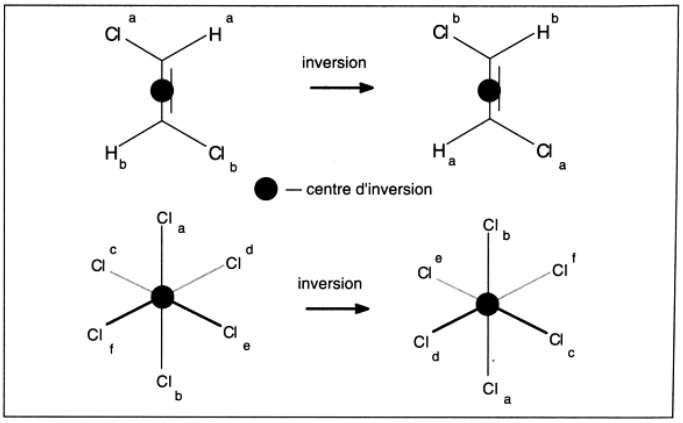
Élément de symétrie	*Symbole*	*Opération*
Axe de rotation	C_n	*Rotation d'un angle de* $\frac{2\pi}{n}$ *par rapport à l'axe de rotation*
Axe de rotation impropre	S_n	*Rotation de* $\frac{2\pi}{n}$ *puis réflexion par rapport au plan perpendiculaire à l'axe* C_n
Plan vertical	σ_v	*Réflexion par rapport au plan*
Plan horizontal	σ_h	*Réflexion par rapport au plan*
Centre d'inversion	i	*Inversion*
Aucun	E	*Ne rien faire à la molécule*





Exemples 2.1.26


S1
S2
S4
A
D
C
B
C4
σh
σh


inversion
centre d'inversion
inversion

Chapitre 3

Complément d'Analyse

3.1 Compléments d'Analyse

Introduction

Ce chapitre constitue un complément des cours d'analyse étudiés en S1 et S2. les notions étudiées précédemment (Suites, fonctions, séries numérique) utilisées et complétées par l'étude des suites et series de fonctions avec des exemples d'applications tels que les séries entière et les series de Fourier.

3.1.1 Suites et séries de fonctions

Définition 3.1.1 *Suite de fonctions : Une suite de fonctions définie sur* $[a, b]$ *est la donnée, pour tout entier* $n \in \mathbb{N}$*, d'une fonction* f_n *définie sur* $[a, b]$ *à valeurs dans* $\mathbb{R}$ *:*
- Pour toute valeur n *fixée,* f_n *est une fonction* $x \mapsto f_n(x)$
- Pour toute valeur x *fixée,* $(f_n(x))_n$ *est une suite numérique.*

Exemples 3.1.2 $f_n(x) = \sqrt{nx+1}$, $f_n(x) = \frac{1}{nx+1}$, $f_n(x) = \ln(1 + \frac{x}{n})$

Définition 3.1.3 *Convergence d'une suite de fonctions :*

- *La suite* $(f_n)_n$ *converge simplement sur* $[a, b]$ *vers une fonction* f *si, pour tout* $x_0 \in [a, b]$*, la suite* $(f_n(x_0))_n$ *converge vers* $f(x_0)$*. Dans ce cas, on peut que dire qu'on a une convergence point par point dans* $[a, b]$ *;*
- *La suite* $(f_n)_n$ *converge uniformément vers une fonction* f *sur* $[a, b]$ *si :*

$$Sup_{x\in[a,b]}|f_n(x) - f(x)| \to 0$$

  Dans ce cas, la convergence est globale pour tout l'intervalle $[a, b]$ *;*
- $(f_n)_n$ *converge uniformément* $\Longrightarrow$ $(f_n)_n$ *converge simplement.*
  La réciproque est fausse !

Exemples 3.1.4 *1) Soit* $f_n(x) = \frac{nx^3}{1+nx^2}$*, on a :*

- *Pour $x = 0$, on a : $f_n(0) = 0$ et $\lim_{n\to+\infty} f_n(0) = 0$.*
  Pour $x \neq 0$, on a : $\lim_{n\to+\infty} f_n(x) = x$. Donc :
  La suite de fonction $(f_n)_n$ converge simplement vers f définie par : $f(x) = x$.
- *D'autre part :*

$$|f_n(x) - f(x)| = |\frac{nx^3}{1+nx^2} - x| = \frac{|-x|}{1+nx^2} = \frac{|x|}{1+nx^2} \leq |x|$$

Distinguons deux cas :

- *1er cas : Si $|x| \leq \frac{1}{\sqrt{n}}$ alors $|f_n(x) - f(x)| \leq \frac{1}{\sqrt{n}}$*
- *2ème cas : Si $|x| \geq \frac{1}{\sqrt{n}}$. Remarquons d'abord que $\frac{nx^2}{1+nx^2} \leq 1$ et par conséquent : $\frac{|x|}{1+nx^2} \leq \frac{1}{n|x|}$. En déduit que $|f_n(x) - f(x)| = \frac{|x|}{1+nx^2} \leq \frac{1}{n|x|} \leq \frac{1}{\sqrt{n}}$*

En conclusion :

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

et

$$Sup_{x\in\mathbb{R}}|f_n(x) - f(x)| \leq \frac{1}{\sqrt{n}} \to 0$$

Donc $(f_n)_n$ converge uniformément vers f définie par $f(x) = x$.

2) Soit la suite de fonction définie par : $f_n(x) = \ln(1 + \frac{x}{n})$

- *Convergence simple : $f_n(0) = 0$ et pour tout $x \in D_{f_n}\backslash\{0\}$ on a : $\lim_{n\to+\infty} f_n(x) = 0$ donc :*

$$f_n \text{ converge simplement vers } f \text{ avec } f(x) = 0$$

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

$$Sup_{x\in\mathbb{R}^+}|f_n(x) - f(x)| = |\ln(1 + \frac{x}{n})| = +\infty \text{ étude de la fonction)}$$

Donc, f_n ne converge pas uniformément sur $[0, +\infty]$.

D'autre part, on a pour n fixé :

$$Sup_{x\in[0,a]}|f_n(x) - f(x)| < |\ln(1 + \frac{a}{n})| \to 0$$

Donc, f_n converge uniformément sur tout intervalle fermé borné de type $[0, a]$.

Proposition 3.1.5 *(Fondamentale) :*
Soit $(f_n)_n$ une suite de fonctions telle que $f_n : I \to \mathbb{R}$ avec $I = [a, b]$. Si $(f_n)_n$ converge uniformément sur I vers une fonction f alors, on a les propriétés suivantes :

- *Si les fonctions f_n sont continues sur I alors I est aussi continue sur I ;*
- *Si les fonctions f_n sont intégrables sur I alors f est aussi intégrable sur I, et :*

$$\lim_{n\to+\infty} \int_a^b f_n(x)dx = \int_a^b \lim_{n\to+\infty} f_n(x)dx.$$

- *On pose : $F_n(x) = \int_a^x f_n(t)dt$ la primitive de f_n qui s'annule en a et $F(x) = \int_a^x f(t)dt$ la primitive de f qui s'annule en a. Alors F_n converge uniformément sur I vers F.*

Remarques 3.1.6 *La propriété n'est vraie que sur un intervalle fermé borné $[a, b]$. Soit $(f_n)_n$ la suite de fonction telle que :*

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

On a bien $(f_n)_n$ converge unformément vers $f(x) = 0$ mais $\int_0^{+\infty} f_n(t)dt = 1 \neq 0 = \int_0^{+\infty} f(t)dt$.

Proposition 3.1.7 *(Fondamentale) :*
Soit $(f_n)_n$ une suite de fonctions telle que : $f_n : I \to \mathbb{R}$ avec $I = [a, b]$. si

- *Chaque fonction f_n est dérivable sur I ;*
- *La suite de fonctions $(f'_n)_n$ converge uniformément sur tout intervalle fermé borné contenu dans I. On note g la limite de la suite $(f'_n)_n$ sur I ;*
- *Il existe $x_0 \in I$ tel que la suite $(f_n(x_0))_n$ converge.*
  Alors :
- *La suite $(f_n)_n$ converge uniformément sur tout intervalle fermé borné contenu dans I vers une fonction f.*
- *la fonction f est dérivable et vérifie : $f' = g$ sur I.*

Définition 3.1.8 *(Série de fonctions) :*
Soit $(f_n)_n$ une suite de fonction. On appelle série de fonction de terme général $(f_n)_n$, la suite de fonctions $(S_n)_n$ définie par :

$$S_n(x) = \sum_{k=0}^{n} f_k(x)$$

On note $\sum f_n$ la série de terme général $(f_n)_n$.

Définition 3.1.9 *(Convergence d'une série de fonctions) :*

- *La série $\sum f_n$ converge simplement sur I si la suite de fonction S_n converge simplement vers une fonction S. i.e. : pour tout $x \in I$ la suite numérique $(f_n(x))_n$ converge simplement vers $S(x)$. La fonction $\mapsto \sum_{k=n+1}^{+\infty} f_k(x)$ est appelée reste de la série $\sum f_n$.*

  Lorsqu'elle existe, la limite de $\sum f_n$ est notée $\sum_{n=0}^{+\infty} f_n$ i.e. la fonction définie par :

$$(\sum_{n=0}^{+\infty} f_n)(x) = \sum_{n=0}^{+\infty} f_n(x)$$

- *La série $\sum f_n$ converge uniformément sur I si la suite de fonction $(S_n)_n$ converge uniformément sur I. C'est à dire : il existe une fonction S telle que :*

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

- *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 $\sum Sup_{x\in I}|f_n|$;*

Définition 3.1.10 *(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 :*

$$|f_n(x)| \leq u_n \text{ pour tout } x \in I \text{ et pour tout entier } n$$

Exemples 3.1.11 *Soit $f_n(x) = \frac{sin(nx)}{n!}$, on a :*

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

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

Proposition 3.1.12 *(Fondamentale) :*
Soit $\sum f_n$ une série de fonctions définies sur $I = [a, b]$. On suppose $\sum f_n$ converge uniformément sur I et que les f_n sont continues. Alors :

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

$$\int_a^b (\sum f_n(x))dx = \sum(\int_a^b f_n(x)dx).$$

Proposition 3.1.13 *Soit $\sum f_n$ une série de fonctions de classe C^1 vérifiant :*

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

Alors :

- *$\sum f_n$ converge uniformément ;*
- *$f = \sum_{k=0}^{+\infty} f_n$ est classe C^1 ;*
- *$f' = (\sum_{k=0}^{+\infty} f_n)' = \sum_{k=0}^{+\infty} f'_n$.*

3.1.2 Séries entières et séries de Fourier

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

Définition 3.1.14 *(Séries entières) :*
Une série entière est une série de fonctions de terme général $f_n(z) = a_n z^n$. Une série entière est notée :

$$\sum a_n z^n \text{ avec } a_n \in \mathbb{C}$$

Lemme 3.1.15 *(d'Abel) :*
Soit $\sum a_n z^n$ une série entière. S'il existe z_0 tel que $\sum |a_n z_0^n|$ converge, alors pour tout $z \in \mathbb{C}$ tel que $|z| \leq |z_0|$, la série est absolument convergente.

Définition 3.1.16 *(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 appellé : Rayon de convergence de a série entière $\sum a_n z^n$.

Exemples 3.1.17 -

- *la série entière $\sum z^n$ à pour rayon de convergence $R = 1$ et elle diverge lorsque $|z| = 1$;*
- *la série entière $\sum \frac{z^n}{n^2}$ à pour rayon de convergence $R = 1$ et elle converge lorsque $|z| = 1$.*

Proposition 3.1.18 *(Règle d'Alembert) : Soit $\sum a_n z^n$ une série entière.*

$$\lim_{n \to +\infty} |\frac{a_{n+1}}{a_n}| = l \Longrightarrow R = \frac{1}{l} \text{ avec } \frac{1}{0^+} = +\infty \text{ et } \frac{1}{+\infty} = 0$$

Proposition 3.1.19 *Soit $\sum a_n x^n$ une série entière.*

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

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

$S^{(k)}$ est la dérivée d'ordre k de S.

Définition 3.1.20 *(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 :

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

f est de classe C^∞ sur $]-R, R[$ et :

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

Proposition 3.1.21 **1)** *Si f est développable en série entière avec $f(x) = \sum a_n x^n$, alors :*
f pair $\Longrightarrow a_{2p+1} = 0$
f impair $\Longrightarrow a_{2p} = 0$

2) *Soit $f :]-a, a[\to \mathbb{C}$ une fonction de classe $C^{+\infty}$. Alors :*
f est développable en série entière $\Longleftrightarrow$ il existe $0 < \alpha < a$, $A > 0$ et $B > 0$ tels que :

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

Proposition 3.1.22 • *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 développable en série entière $\Longleftrightarrow$ il existe $0 < \beta < a$ tel que :

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

$$\text{pour tout } -\beta < x < \beta$$

Exemples 3.1.23 • $e^x = \sum_{n=0}^{+\infty} \frac{x^n}{n!}$, $R = +\infty$

- $\frac{1}{1-x} = \sum_{n=0}^{+\infty} x^n$, $R = 1$
- $cosx = \sum_{n=0}^{+\infty} (-1)^n \frac{x^{2n}}{(2n)!}$, $R = +\infty$
- $sinx = \sum_{n=0}^{+\infty} (-1)^n \frac{x^{2n+1}}{(2n+1)!}$, $R = +\infty$

Définition 3.1.24 *(série de Fourier) :*

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 3.1.25 • *Soit f une fonction intégrable sur $[-\pi, \pi]$ et périodique de période 2π. 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 :*

$$\begin{cases} A_0 = \frac{1}{2\pi} \int_{-\pi}^{\pi} f(t)dt, \\ A_n = \frac{1}{\pi} \int_{-\pi}^{\pi} f(t)cos(nt)dt, \quad n \geq 1; \\ B_n = \frac{1}{\pi} \int_{-\pi}^{\pi} f(t)sin(nt)dt, \quad n \geq 1. \end{cases}$$

Remarques 3.1.26 • *f paire $\Longrightarrow b_n = 0$;*

- *f impaire $\Longrightarrow a_n = 0$;*
- *Notation :* $f(x) \sim A_0 + \sum_{n=1}^{+\infty} (A_n cos(nx) + B_n sin(nx))$.

Définition 3.1.27 • *SI f une fonction intégrable sur $[-T, T]$ et périodique de période $2T$. La série de Fourier associée à f est définie par $\sum f_n$ où : $f_n(x) = A_n cos(n\frac{\pi x}{T}) + B_n sin(n\frac{\pi x}{T})$ avec :*

$$\begin{cases} A_0 = \frac{1}{2\pi} \int_{-\pi}^{\pi} f(\frac{Lt}{\pi})dt = \frac{1}{2L} \int_{-L}^{L} f(t)dt, \\ A_n = \frac{1}{\pi} \int_{-\pi}^{\pi} f(\frac{Lt}{\pi})cos(nt)dt = \frac{1}{L} \int_{-L}^{L} f(t)cos(n\frac{\pi t}{L})dt, \\ B_n = \frac{1}{\pi} \int_{-\pi}^{\pi} f(\frac{Lt}{\pi})sin(nt)dt = \frac{1}{L} \int_{-L}^{L} f(t)sin(n\frac{\pi t}{L})dt, \end{cases}$$

$$\text{pour } n \geq 1.$$

Exemples 3.1.28 • $f(x) = x$ *pour tout* $x \in [-\pi, \pi]$.

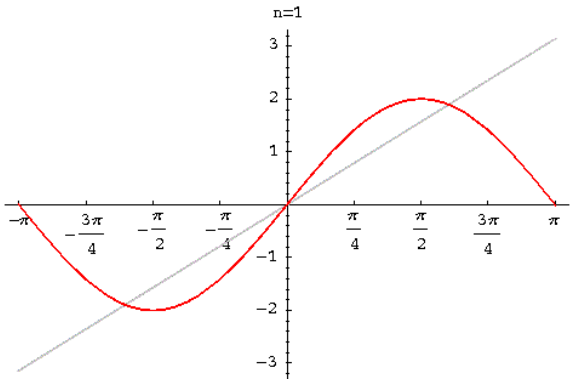
f *impaire* $\Longrightarrow a_n = 0$, *calculons* b_n *:*

$$b_n = \frac{1}{\pi}\int_{-\pi}^{\pi} xsin(nx)dx = \frac{1}{\pi}\left[-\frac{xcos(nx)}{n} + \frac{sin(nx)}{n^2}\right]_{-\pi}^{\pi}$$

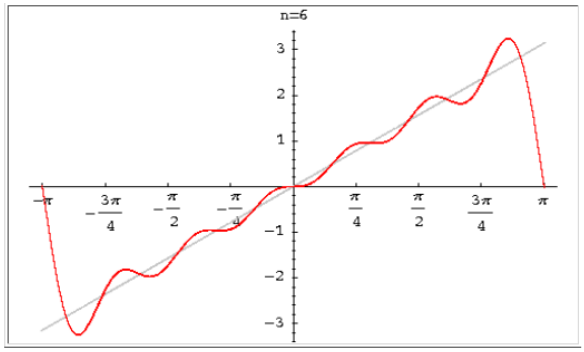
$$= \frac{2}{n}(-1)^{(n+1)}$$

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

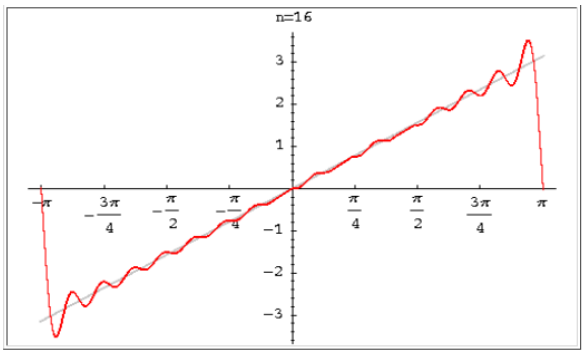
Exemples 3.1.29 $n = 1$



$n = 6$



$n = 12$



L'approximation de f par les fonctions f_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 f_n ont tendance à se rapprocher d'avantage.