Annexe A

Structure division euclidienne

Hugo Salou MPI*

Dernière mise à jour le 22 mars 2023

1 Division euclidienne

Théorème 1 (divison euclidienne dans $\mathbb{N}$):
Soient deux entiers $a, b \in \mathbb{N}$. Si b est non-nul, alors

$$\exists!(q,r) \in \mathbb{N}^2, \qquad a = bq + r \quad \text{et} \quad 0 \leqslant r < b.$$

$\mathbb{N}$	$\mathbb{N}^\star$
$\cap$	$\cap$
a	b
r	q
$\uparrow$	$\uparrow$
reste	quotient

Exercice 2: 1. On a

4	9	0			133
3	9	9			0,368421 . . .
	9	1	0		.
	⋮				

2. On veut montrer que le réel x possède un développement limité implique qu'il est rationnel. On prend pour exemple $0,\overline{147} = 0,147147147\ldots$ On a

$$\begin{aligned} 0,\overline{147} &= 147 \times \left(10^{-3} + 10^{-6} + 10^{-9} + \cdots\right) \\ &= 147 \times 10^{-3}(1 + 10^{-3} + 10^{-6} + \cdots) \\ &= \frac{147}{100} \times \sum_{k=0}^{\infty} (10^{-3})^k = \frac{147}{100} \times \frac{1}{1 - 10^{-3}} \end{aligned}$$

D'où $0,\overline{147} = \frac{147}{999} = \frac{49}{333} \in \mathbb{Q}$.
On démontre maintenant montrer le "sens inverse." On prend pour exemple $49 \div 333$:

4	9	0				333
1	5	7	0			0,$\overline{147}$
1	3	3	2			
	2	3	8	0		
	2	3	3	1		
			4	9	0	

Il n'y a pas, par contre, unicité du développement décimal : $1 = 1,\overline{0} = 0,\overline{9}$.

Théorème 3:
Soient deux polynômes A et $B \in \mathbb{K}[X]$. Si B est non-nul,

$$\exists!(Q,R) \in \mathbb{K}[X]^2, \qquad A = BQ + R \quad \text{et} \quad \deg R < \deg B.$$

$\mathbb{K}[X] \ni A$	$B \in \mathbb{K}[X] \setminus \{0\}$
R	Q

Exercice 4:
Soit $n \in \mathbb{N}$. On va calculer $R_n(X)$ sans calculer $Q_n(X)$.

X^n	$X^2 - (n-2)X - (n-1)$
$R_n = ?$	Q_n

On sait, d'après le théorème de la division euclidienne, que $\deg R_n < 2$ d'où $R_n = \alpha_n X + \beta_n$. De plus, $X^n = \big(X^2 - (n-2)X - (n-1)\big)\, Q_n(X) + R_n(X)$. On sait que, pour un polynôme de la forme $X^2 - sX + p$, s est la somme des racines de ce polynôme et p est le produit des racines. On en déduit que les racines de $X^2 - (n-2)X - (n-1)$ sont $n-1$ et -1. D'où, $X^n = \big(X - (n-1)\big)\big(X+1\big)Q_n(X) + \alpha_n X + \beta_n$. On choisit des valeurs de X qui permettent

de calculer α_n et β_n. Par exemple, avec $X = n-1$, on a $(n-1)^n = \alpha_n(n-1) + \beta_n$; et, avec $X = -1$, on a $(-1)^n = -\alpha_n + \beta_n$. On résout ce système d'équations :

$$\left.\begin{array}{l}(n-1)^n = \alpha_n(n-1) + \beta_n \\ (-1)^n = \beta_n - \alpha_n\end{array}\right\} \underset{\substack{L_1 \leftarrow L_1 + (n-1)L_2 \\ L_2 \leftarrow L_2 - L_1}}{\iff} \begin{cases}(n-1)^n + (n-1)(-1)^n = \beta_n + (n-1)^n\beta_n \\ \dots\end{cases}$$

$$\iff \begin{cases}\alpha_n = \dots \\ \beta_n = \dots\end{cases}$$

2 Structures algébriques

Remarque: — Exemples de groupes : $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{Q}^\star, \times)$, $(S_n, \circ)$, $\big(\mathscr{M}_{n,m}(\mathbb{K}), +\big)$, $\big(\mathrm{GL}_n(\mathbb{K}), \times\big)$.

— $(A, +, \times)$ est un *anneau* si
  — $(A, +)$ est un groupe commutatif
  — $\times$ est associative
  — le neutre de $\times$ est 1_A
  — x est distributive par rapport à $+$ (dans les deux sens) :

$$(a+b) \times c = a \times c + b \times c \qquad \text{et} \qquad c \times (a+b) = c \times a + c \times b.$$

  Exemple d'anneau : $\big(\mathbb{K}[X], +, \times\big)$ est un anneau *commutatif* (car $\times$ est commutative) ; $\big(\mathscr{M}_n(\mathbb{K}), +, \times\big)$ est un anneau non-commutatif.

— $(K, +, \times)$ est un corps si $(A, +, \times)$ est un anneau commutatif et tout élément différent de 0_K est inversible.
  Exemple de corps : $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$ MAIS $\big(\mathrm{GL}_n(\mathbb{K}), +, \times\big)$ n'est pas un corps (et ce n'est pas un anneau non plus).

— La définition d'un espace vectoriel n'est pas *vraiment* à connaître... On utilisera, en général, plus la définition d'un sous-espace vectoriel.

— $(M, +, \times, \cdot)$ est une K-algèbre si
  — $(M, +, \times)$ est un anneau ;
  — $(M, +, \cdot)$ est un K-espace vectoriel ;
  — prop3

  Par exemple, $(\mathbb{R}^2, +, \cdot)$ est un espace vectoriel. $+$ est une opération interne (vecteur $+$ vecteur $=$ vecteur) mais $\cdot$ est une opération externe $(\mathscr{M}_n(\mathbb{K}, +, \cdot)$ est un espace vectoriel. $+$ est interne (matrice $+$ matrice $=$ matrice), $\cdot$ est externe (rel $\cdot$ matrice $=$ matrice), et $\times$ est interne (matrice $\times$ matrice $=$ matrice). On dit alors que $(\mathscr{M}_n(\mathbb{K}), +, \times, \cdot)$ est une K-algèbre.

Figure 1 – Structure d'un sous-groupe $H \subset G$

Définition (Sous-groupe):
Soit H une partie de G ($H \subset G$) et H est stable par $+$ ($\forall x, y \in H,\ x+y \in H$) et avec la loi $+$ induite sur H, $(H,+)$ est un groupe. Dans ce cas, H est un sous-groupe de $(G,+)$.

Dans la pratique, on montre

$$(H,+) \text{ est un sous-groupe} \iff \begin{cases} H \subset G \\ H \text{ stable par } + \\ 0_G \in H \\ \forall x \in H,\ -x \in H \end{cases} \iff \begin{cases} \varnothing \neq H \subset G \\ \forall x, y \in H,\ x - y \in H. \end{cases}$$

Exercice 5:
On va montrer que H est un sous-groupe de $(\mathbb{Z},+)$ si et seulement s'il existe un entier $n \in \mathbb{Z}$, tel que $H = n\mathbb{Z} = \{n \times k \mid k \in \mathbb{Z}\}$.

1. Soit $H = n\mathbb{Z}$. On veut montrer que H est un sous-groupe de $(\mathbb{Z},+)$. On a bien $H \subset G$ et, pour tout $x, y \in \mathbb{Z}$, on a
$$\underbrace{nx}_{\in H} + \underbrace{ny}_{\in H} = \underbrace{n(x+y)}_{\in H}.$$
On a aussi $0 \in H$ car $0 = 0 \times n$. Enfin, pour tout entier $x \in \mathbb{Z}$, on a $-(nx) = n \times (-x) \in H$.
On en conclut que $(H,+)$ est un sous groupe de $(\mathbb{Z},+)$.
2. Soit H un sous-groupe de $(\mathbb{Z},+)$. Si $H = \{0\}$ alors $H = 0\mathbb{Z}$. Si $H \neq \{0\}$, alors il existe $n \in \mathbb{Z}$, $n \in H$. D'où $-n \in H$, et d'où, il existe un élément positif dans H. On considère sans perte de généralité qu'il s'agit de n. On en déduit que $n\mathbb{Z} \subset H$.
On choisit, à présent, le plus petit n. On procède par l'absurde : on suppose qu'il existe $x \in H$ tel que $x \notin n\mathbb{Z}$. On fait la division euclidienne de x par n : $x = nq + r$ et $r < n$. D'où, $x - nq = r < n$. Or, x et nq sont deux éléments de H. On en conclut que $r \in H$. C'est absurde car $r < n$ et n est le plus petit.

3 Idéaux

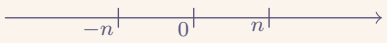

Figure 2 – Sous-groupe de $(\mathbb{Z},+)$

Définition 6:
Soit $(A,+,\times)$ un anneau commutatif. On appelle *idéal* de A tout sous-groupe I de $(A,+)$ tel que $\forall (i,a) \in I \times A,\ i \times a \in I$.

Figure 3 – Structure d'un idéal $I \subset A$

Remarque (⚠):
Un idéal n'est pas forcément un sous-anneau car on n'a pas forcément $1_A \in I$.

Exemple 7:
1. Soit $a \in \mathbb{K}$. On pose $I = \{P \in \mathbb{K}[X] \mid P(a) = 0\}$. On vérifie aisément que $(I, +)$ est bien un sous-groupe de $(\mathbb{K}[X], +)$:

   $0_{\mathbb{K}[X]}$ s'annule en a et si $P(a) = 0$ et $Q(a) = 0$ alors, $(P+Q)(a) = 0$ et $(P-Q)(a) = 0$.

   Pour tout polynôme $Q \in \mathbb{K}[X]$, on a, si $P(a) = 0$, alors $(P \times Q)(a) = 0$. On en conclut que I est un idéal de $(A, +, \times)$.
2. On considère l'ensemble des suites qui tendent vers 0, I. Ce n'est pas un idéal de l'ensemble des suites, $\mathbb{R}^{\mathbb{N}}$: on a bien que I est un sous-groupe de $(\mathbb{R}^{\mathbb{N}}, +)$ mais, par exemple la suite $\left(\frac{1}{n}\right) \in I$ multipliée par la suite $(n) \in \mathbb{R}^{\mathbb{N}}$ ne donne pas une suite tendant vers 0. En effet, $\frac{1}{n} \times n = 1 \not\to 0$. Mais, c'est bien un idéal de l'ensemble des suites bornées.

Proposition 8 (les idéaux de $\mathbb{Z}$ et $\mathbb{K}[X]$):
1. Dans l'anneau commutatif $(A, +, \times)$, pour tout $k \in A$, l'ensemble $k \times A$ des multiples de k est un idéal de A, appelé *idéal engendré* de A par k.
2. I est un idéal de $\mathbb{Z}$ si et seulement s'il existe $n \in \mathbb{Z}$ tel que $I = n\mathbb{Z}$.
3. I est un idéal de $\mathbb{K}[X]$ si et seulement s'il existe un polynôme $P(X) \in \mathbb{K}[X]$ tel que $I = P(X) \cdot \mathbb{K}[X]$.

Démonstration (2.): " $\Longrightarrow$ " Soit I un idéal de $\mathbb{Z}$. En particulier, $(I, +)$ est un sous-groupe de $(\mathbb{Z}, +)$ et donc, d'après l'exercice 5, il existe un entier n tel que $I = n\mathbb{Z}$.
" $\Longleftarrow$ " Réciproquement, si $I = n\mathbb{Z}$, alors c'est un idéal car :
- $(n\mathbb{Z}, +)$ est un sous-groupe de $(\mathbb{Z}, +)$ d'après l'exercice 5.
- $\underbrace{(nx)}_{\in I} \times \overbrace{y}^{\in \mathbb{Z}} = \underbrace{n(x \times y)}_{\in I}$.

Exercice 9:
Montrer que le noyau d'un morphisme d'anneaux commutatif est idéal.

Soient $(A, +, \times)$ et $(B, +, \times)$ deux anneaux. Soit $\varphi : A \to B$ un morphisme d'anneaux :

$$\varphi(a + b) = \varphi(a) + \varphi(b) \qquad \varphi(a \times b) = \varphi(a) \times \varphi(b) \qquad \varphi(1_A) = 1_B.$$

Montrons que $(\operatorname{Ker}\varphi, +)$ est un sous-groupe de $(A, +)$. On sait que $\varphi(0_A) = 0_B$ donc $0_A \in \operatorname{Ker}\varphi$ et donc $\operatorname{Ker}\varphi \neq \varnothing$. Soient $a, b \in \operatorname{Ker}\varphi$. On a $\varphi(a - b) = \varphi(a) - \varphi(b) = 0 - 0 = 0$ donc $(a - b) \in \operatorname{Ker}\varphi$.

Soient $\varepsilon \in \operatorname{Ker}\varphi$ et $b \in A$. On a $\varphi(\varepsilon \times b) = \varphi(\varepsilon) \times \varphi(b) = 0$.

Proposition 10:
Dans l'anneau commutatif $(A, +, \times)$, la somme de deux idéaux et l'intersection de deux sont encore un idéal. En particulier, dans l'anneau $(\mathbb{Z}, +, \times)$ des entiers relatifs,

$$\forall (p, q) \in \mathbb{Z}^2, \quad p\mathbb{Z} + q\mathbb{Z} = \operatorname{pgcd}(p, q)\,\mathbb{Z} \qquad \text{et} \qquad p\mathbb{Z} \cap q\mathbb{N} = \operatorname{ppcm}(p, q)\,\mathbb{Z}$$

car $d \mid p \iff p\mathbb{Z} \subset d\mathbb{Z}$ (*i.e.* tout multiple de p est un multiple de d). [1]

Démonstration:
Soient I et J deux idéaux. L'intersection de deux sous-groupes est un sous-groupe. De plus, pour tout élément i de $I \cap J$, pour tout élément a de A, on a $a \times i \in I$ car I est un idéal, et $a \times i \in J$ car J est un idéal. D'où, $I \cap J$ est un idéal. De plus, pour tout élément $i + j$ de $I + J$, on a $(i + j) \times a = ia + ja \in I + J$.

Montrons $p\mathbb{Z} + q\mathbb{Z} = \operatorname{pgcd}(p, q)\,\mathbb{Z}$. On pourra montrer, d'une manière similaire, $p\mathbb{Z} \cap q\mathbb{Z} = \operatorname{ppcm}(p, q)\,\mathbb{Z}$. On sait que $p\mathbb{Z} + q\mathbb{Z}$ est un idéal de $\mathbb{Z}$, il existe $d \in \mathbb{Z}$ tel que $p\mathbb{Z} + q\mathbb{Z} = d\mathbb{Z}$ (♡). Montrons que $d = \operatorname{pgcd}(p, q) = p \wedge q$. D'après (♡), il en résulte que $p\mathbb{Z} \subset d\mathbb{Z}$, d'où $p \mid d$; et,

1. Rappel : $d \mid p$ si, et seulement si, d divise p si, et seulement si, p est un multiple de d si, et seulement si, il existe $k \in \mathbb{Z}$ tel que $p = k \times d$.

$q\mathbb{Z} \subset d\mathbb{Z}$, d'où $d \mid q$. Ainsi, d est un diviseur commun à p et q. Montrons que c'est le plus grand. On suppose que δ est un diviseur commun à p et q. On veut montrer que $\delta \mid d$. Ainsi, $\delta \mid p$ et $\delta \mid q$, alors δ est un diviseur de tout élément de $p\mathbb{Z} + q\mathbb{Z}$ et en particulier de d. D'où, $\delta \mid d$.

Corollaire 11:

Lemme de Bézout. Deux entiers relatifs a et b sont premiers entre eux si, et seulement si, il existe $(u, v) \in \mathbb{Z}^2$ tels que $a \times u + b \times v = 1$.

Lemme de Gauß. Si $a \mid bc$ et a est premier avec b, alors $a \mid c$.

Démonstration:

Lemme de Bézout. D'une part, si $a \wedge b = 1$, alors $a\mathbb{Z} + b\mathbb{Z} = 1\mathbb{Z}$ et en particulier $1 \in 1\mathbb{Z}$. D'autre part, si $au + bv = 1$, alors $a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$ d'où $a \wedge b = 1$.

Lemme de Gauß. On a $a \wedge b$ d'où, d'après le théorème de Bézout, il existe $(u, v) \in \mathbb{Z}^2$, tels que $au + bv = 1$. Ainsi, $acu + bcv = c$. Or, $a \mid bc$, et $a \mid ac$ d'où $a \mid c$.

Exercice 12:

Montrer que, si b et c sont premiers entre eux et divisent a, alors bc divise a.

Comme $b \mid a$, il existe $k \in \mathbb{Z}$ tel que $a = kb$. De plus, $b \wedge c = 1$, et $c \mid a = kb$, d'où $c \mid k$. Il existe donc $k' \in \mathbb{Z}$ tel que $k = k'\,c$. Ainsi, $a = kk'bc$, d'où $bc \mid\ a$.

4 L'anneau $\mathbb{Z}/n\mathbb{Z}$

Définition 13:

Soit $n \in \mathbb{N}^\star$. La relation $x \equiv a\ [n]$ (« x est congru à a modulo n ») définie par $n \mid (x-a)$ est une relation d'équivalence sur $\mathbb{Z}$. L'ensemble $\bar{a} = \{x \in \mathbb{Z} \mid x \equiv a\ [n]\}$ est la *classe d'équivalence* de a. L'ensemble $\{\bar{1}, \bar{2}, \ldots, \bar{n}\}$ des classes d'équivalences est noté $\mathbb{Z}/n\mathbb{Z}$.

Ainsi, $\bar{x} = \bar{y} \iff x \equiv y\ [n]$. De plus, si $x \equiv a\ [n]$ et $y \equiv b\ [n]$, on a $(x + y) \equiv (a + b)\ [n]$, on note donc $\bar{x} + \bar{y} = \overline{x + y}$. De même pour le produit.

Proposition 14:

Un entier $x \in \mathbb{Z}$ est premier avec $n \in \mathbb{N}^\star$ si, et seulement si, $\bar{x} \in \mathbb{Z}/n\mathbb{Z}$ est inversible. Par suite, l'ensemble $\mathbb{Z}/n\mathbb{Z}$ est un corps (aussi noté $\mathbb{F}_n$) si, et seulement si, $n \in \mathbb{N}^\star$ est un nombre premier.

Contre-exemple : avec le corps nul $0 = \{\bar{0}\}$, ce théorème est faux.

Démonstration:

$$\begin{aligned}
\bar{x} \in \mathbb{Z}/n\mathbb{Z} \text{ est inversible} &\iff \exists u \in \mathbb{Z},\ \bar{u} \times \bar{x} = \bar{1} \\
&\iff \exists u \in \mathbb{Z},\ \overline{u \times x} = \bar{1} \\
&\iff \exists u \in \mathbb{Z},\ u \times x \equiv 1\ [n] \\
&\iff \exists u \in \mathbb{Z},\ \exists k \in \mathbb{Z},\ u \times x = 1 + k \times n \\
&\iff \exists (u, k) \in \mathbb{Z}^2,\ u \times x - k \times n = 1 \\
&\iff x \wedge n = 1
\end{aligned}$$

En particulier, tous les éléments non nuls de $\mathbb{Z}/n\mathbb{Z}$ sont inversibles.

Théorème 15 (Théorème chinois):

Si a et b sont premiers entre eux, alors deux congruences modulo a et modulo b équivalent à une congruence modulo ab car les anneaux $\mathbb{Z}/ab\,\mathbb{Z}$ et $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ sont isomorphes.

Démonstration:

Pour tout $x \in \mathbb{Z}$, on note $\pi_a(x) \in \mathbb{Z}/a\mathbb{Z}$ la classe d'équivalence de x dans $\mathbb{Z}/a\mathbb{Z}$; de même, on note $\pi_b(x) \in \mathbb{Z}/b\mathbb{Z}$ et $\pi_{ab}(x) \in \mathbb{Z}/(ab)\mathbb{Z}$. On construit la fonction

$$\begin{aligned}
f : \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} &\longrightarrow \mathbb{Z}/(ab)\mathbb{Z} \\
(\pi_a(x), \pi_b(x)) &\longmapsto \pi_{ab}(x).
\end{aligned}$$

Elle est bien définie car : si $\pi_a(y) = \pi_a(x)$ et $\pi_b(y) = \pi_b(x)$, alors $y \equiv x\ [a]$ et $y \equiv x\ [b]$, d'où il existe $k \in \mathbb{Z}$ tel que $y = x + ka$ et il existe $\ell \in \mathbb{Z}$ tel que $y = x + \ell b$, donc $ka = \ell a$ et donc $b \mid ka$; et, $a \wedge b$, par le théorème de Gauss, on a $b \mid k$, il existe donc $m \in \mathbb{Z}$ tel que $k = mb$ donc $y = x + m \cdot ab$, d'où $\pi_{ab}(y) = \pi_{ab}(x)$. L'application f est un morphisme d'anneaux par les propriétés des classes d'équivalences vues précédemment ($\bar{x} + \bar{y} = \overline{x+y}$ et $\bar{x} \times \bar{y} = \overline{x \times y}$), et par construction. De plus, f est injective car $\operatorname{Ker} f = \{(0,0)\}$ ($x \equiv 0\ [ab]$ implique $x \equiv 0\ [a]$ et $x \equiv 0\ [b]$). De plus, $\operatorname{Card}(\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}) = a \times b = \operatorname{Card}(\mathbb{Z}/(ab)\mathbb{Z})$. D'où, f est bijective.

Exercice 16:
Déterminer tous les entiers relatifs tels que $x \equiv 2\ [4]$ et $x \equiv 3\ [5]$.

On note (S) le système $x \equiv 2\ [4]$ et $x \equiv 3\ [5]$, (S_1) et (S_2) les deux équations. Comme $4 \wedge 5 = 1$, d'après le théorème chinois, le système (S) est équivalent à $x \equiv ?\ [4 \times 5]$.

1ère méthode. (On devine « ? ».) Avec 18 est une solution car $18 \equiv 2\ [4]$ (car $4 \mid (18-2)$) et $18 \equiv 3\ [5]$ (car $5 \mid (18-3)$).

2nde méthode. Analyse. L'équation (S_1) est équivalente à $\exists t \in \mathbb{Z}$, $x = 2 + 4t$. On choisit ce t. D'où, d'après l'équation (S_2), on a $2 + 4t \equiv 3\ [5]$, d'où $4t \equiv 1\ [5]$. Or, $\bar{4}$ est inversible dans $\mathbb{Z}/5\mathbb{Z}$, car $4 \wedge 5 = 1$. On trouve cet inverse : 4. Ainsi, $t \equiv 4\ [5]$. Synthèse : *c.f.* 1ère méthode.

Définition 17:
Le nombre d'éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ (*i.e.* le nombre d'entiers de $[\![1, n]\!]$ premiers avec n) est noté $\varphi(n)$. L'application $\varphi : n \mapsto \varphi(n)$ est appelée l'*indicatrice d'Euler*.

Exemple:
On a $\varphi(8)$ car les entiers de $[\![1, 7]\!]$ premiers avec 8 sont 1, 3, 5, 7.

Méthode 18 (Comment calculer l'indicatrice d'Euler):

(*i*) Si p est premier, alors $\varphi(p) = p - 1$ car tous les éléments de $[\![1, p-1]\!]$ sont premiers avec p. Et, $\forall k \in \mathbb{N}^\star$, on a $\varphi(p^k) = p^k \cdot (1 - 1/p)$.

(*ii*) Si a et b sont premiers entre eux, alors $\varphi(ab) = \varphi(a) \cdot \varphi(b)$. En effet, d'après le théorème chinois, il y a autant d'éléments inversibles dans $\mathbb{Z}/(ab)\mathbb{Z}$ et dans $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ par isomorphisme.

(*iii*) Si $p_1, \ldots, p_k$ sont les diviseurs premiers de n, alors

$$\varphi(n) = n \times \left(1 - \frac{1}{p_1}\right) \times \cdots \times \left(1 - \frac{1}{p_k}\right).$$

En effet, on a $n = p_1^{\alpha_1} \times \cdots \times p_k^{\alpha_k}$, d'où $\varphi(n) = \varphi(p_1^{\alpha_1}) \cdot \ldots \cdot \varphi(p_k^{\alpha_k})$. Calculons $\varphi(p_1^{\alpha_1})$: on cherche tous les entiers de $[\![1, p_1^{\alpha_1}]\!]$ premiers avec $p_1^{\alpha_1}$. On cherche donc tous les entiers $[\![1, p_1^{\alpha_1}]\!]$. Les multiples de p_1 dans $[\![1, p_1^{\alpha_1}]\!]$ sont $p_1, 2p_1, \ldots, p_1^{\alpha_1 - 1} \times p_1$: il y en a $p_1^{\alpha_1 - 1}$. Il y a donc $p_1^{\alpha_1} - p_1^{\alpha_1 - 1}$ non multiples de p_1. D'où, $\varphi(p_1^{\alpha_1}) = p_1^{\alpha_1} \cdot (1 - 1/p_1)$. Ainsi, on en déduit la formule de $\varphi(n)$ précédente.

5 L'ordre d'un élément

Si a est un élément d'un groupe $(G, \cdot)$ d'élément neutre 1, alors l'ensemble $\{\ldots, a^{-2}, a^{-1}, 1, a^1, a^2, \ldots\} = \{a^k \mid k \in \mathbb{Z}\}$ est un sous-groupe de G, appelé le sous-groupe engendré par a, et il est noté $\langle a \rangle$. C'est le plus petit sous-groupe de G contenant a.

Si ce sous-groupe est un ensemble fini, alors son cardinal est appelé l'*ordre* de a. L'ordre de a est le plus petit entier k strictement positif tel que $a^k = 1$. Et, les entiers k tels que $a^k = 1$ sont les multiples de l'ordre de a. On dit que le groupe G est *monogène* s'il est, lui-même, engendré par un élément et qu'il est *cyclique* s'il est monogène et fini.

Exercice 19:
Décomposer en cycle disjoints la permutation σ du groupe symétrique $\mathfrak{S}_7$ et en déduire l'ordre de σ, où

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 4 & 7 & 2 & 6 & 1 & 3 \end{pmatrix}.$$

Les images successives de 1 sont 1, 5 et 6 ; celles de 2 sont 2 et 4 ; celles de 3 sont 3 et 7. D'où, $\sigma = \begin{pmatrix} 1 & 5 & 6 \end{pmatrix} \cdot \begin{pmatrix} 2 & 4 \end{pmatrix} \cdot \begin{pmatrix} 3 & 7 \end{pmatrix}$. L'ordre de σ est 6, ce qui correspond au plus petit commun multiple des ordres des cycles (donc $\text{ppcm}(2,2,3)$).

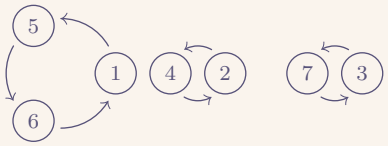

FIGURE 4 – Décomposition en cycles de la permutation σ

EXEMPLE:
Le groupe $(\mathbb{Z}, +)$ est monogène car $\mathbb{Z} = \langle 1 \rangle$. Mais, $(\mathfrak{S}_n, \cdot)$ n'est pas monogène.

PROPOSITION 20:
Si G est un groupe fini, alors $\forall a \in G$, $o(a) \mid \operatorname{Card} G$, où $o(a)$ est l'ordre de a. □

COROLLAIRE 21:**Théorème d'Euler.** Si $a \in \mathbb{Z}$ est premier avec $n \in \mathbb{N}^\star$, alors $a^{\varphi(n)} \equiv 1 \ [n]$.

Petit théorème de Fermat. Si p est un nombre premier, alors $\forall a \in \mathbb{Z}$, on a $a^p \equiv a \ [p]$.

EXERCICE 22:
Calculer $\varphi(10)$ et en déduire que le dernier chiffre de l'écriture décimale de 3^{345} est 3. Calculer $\varphi(100)$ et en déduire que les deux derniers chiffres de l'écriture décimale de 3^{345} sont 4 et 3.

On trouve $\varphi(10) = 4$ car les entiers de $[\![1, 10]\!]$ premiers avec 10 sont 1, 3, 7 et 9. On trouve aussi $\varphi(100) = 40$ car $100 = 4 \times 25 = 2^2 \times 5^2$, d'où les diviseurs premiers de 100 sont 2 et 5, et donc $\varphi(100) = 100 \times \left(1 - \frac{1}{2}\right) \times \left(1 - \frac{1}{5}\right) = 50 \times 4/5 = 40$.

On cherche $r \in [\![0, 9]\!]$ tel que $3^{385} \equiv 1 \ [10]$. On a $3 \wedge 10 = 1$, d'où, d'après le théorème d'Euler, $3^{\varphi(10)} \equiv 1 \ [1]\, 0$ et donc $3^4 \equiv 1 \ [1]\, 0$. Or,

$$3^{345} = 3^{344} \times 3 = (3^4)^{86} \times 3 \equiv 1^{86} \times 3 \equiv 3 \ [10]\,.$$

Donc $r = 3$.

On cherche $r \in [\![0, 99]\!]$ tel que $3^{345} \equiv r \ [100]$. De même, d'après le théorème d'Euler, $3^{\varphi(100)} \equiv 1 \ [100]$, d'où $3^{40} \equiv 1 \ [100]$. Or, $3^{345} = (3^{40})^8 \times 3^{25} \equiv 3^{25} \ [100]$. Et, $3^{25} = 3^5 \times (3^5)^4 = 3 \cdot 81 \cdot (3^5)^4 \equiv 43 \times (3^4)^5 \equiv 43 \ [100]$. D'où, $3^{345} \equiv 43 \ [100]$.