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

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

$$\begin{array}{c|c}
\mathbb{N} & \mathbb{N}^* \\
\rotatebox{90}{$\in$} & \rotatebox{90}{$\in$} \\
a & b \\ \cline{2-2}
r & q \\
\uparrow & \uparrow \\
\text{reste} & \text{quotient}
\end{array}$$

Exercice 2:
1. On a

$$\begin{array}{cccc|l}
4 & 9 & 0 & & 133 \\ \cline{5-5}
3 & 9 & 9 & & 0{,}368421\ldots \\ \cline{1-3}
 & 9 & 1 & 0 & \\
 & \vdots & & &
\end{array}.$$

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 $49 \div 333$:

$$\begin{array}{ccccccc|c}
4 & 9 & 0 & & & & & 333 \\ \cline{8-8}
1 & 5 & 7 & 0 & & & & 0{,}\overline{147} \\
1 & 3 & 3 & 2 & & & & \\
 & 2 & 3 & 8 & 0 & & & \\
 & 2 & 3 & 3 & 1 & & & \\
 & & & 4 & 9 & 0 & &
\end{array}$$

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,

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

$$\begin{array}{r|l}
\mathbb{K}[X] \ni A & B \in \mathbb{K}[X] \setminus \{0\} \\ \cline{2-2}
R & Q
\end{array}$$

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

$$\begin{array}{r|c}
X^n & X^2 - (n-2)X - (n-1) \\ \cline{2-2}
R_n = ? & Q_n
\end{array}$$

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, $X^n = \left(X^2 - (n-2)X - (n-1)\right) Q_n(X) + R_n(X)$. 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, $X^n = \left(X - (n-1)\right)\left(X+1\right)Q_n(X) + \alpha_n X + \beta_n$. 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 :

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

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

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

- $(A, +, \times)$ 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.

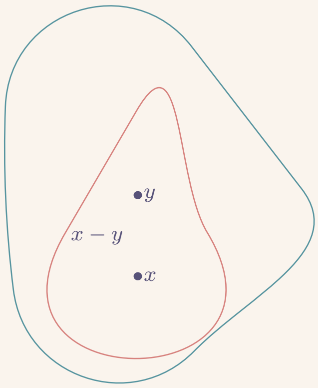

FIGURE 1 – Structure d'un sous-groupe $H \subset G$

DÉFINITION (Sous-groupe):
Soit H une partie de G $(H \subset G)$ et H est <u>stable</u> par $+$ $(\forall x, y \in H,\ x + y \in H)$ et avec la loi $+$ <u>induite</u> 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.

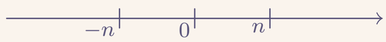

Figure 2 – Sous-groupe de $(\mathbb{Z}, +)$

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. À regarder.
2. I est un idéal de $\mathbb{Z}$ si et seulement s'il existe $n \in Z$ 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 $I = P(X) \cdot \mathbb{K}[X]$.

Preuve (2.): “ $\implies$ ” 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 $I = n\mathbb{Z}$.

“ $\impliedby$ ” 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 $\varphi(\varepsilon \times b) = \varphi(\varepsilon) \times \varphi(b) = 0$.