

Annexe A Structures algébriques et division euclidienne

A.1 DIVISION EUCLIDIENNE

THÉORÈME 1 (division euclidienne dans $\mathbb{N}$)

Soient deux entiers $a \in \mathbb{N}$ et $b \in \mathbb{N}$. Si b n'est pas nul, alors

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

$$\begin{array}{c|c} a & b \\ \hline r & q \end{array}$$

EXERCICE 2 — Montrer que :

- (i) $\frac{49}{333} = 0, \overline{147}$;
- (ii) un réel est rationnel si, et seulement si, il possède un développement décimal périodique.

THÉORÈME 3 (division euclidienne dans $\mathbb{K}[X]$)

Soient deux polynômes $A \in \mathbb{K}[X]$ et $B \in \mathbb{K}[X]$. Si B n'est pas nul, alors

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

EXERCICE 4 — Pour tout $n \in \mathbb{N}$, déterminer le reste R_n de la division euclidienne du polynôme X^n par le polynôme $X^2 - (n-2)X - (n-1)$.

A.2 STRUCTURES ALGÈBRIQUES

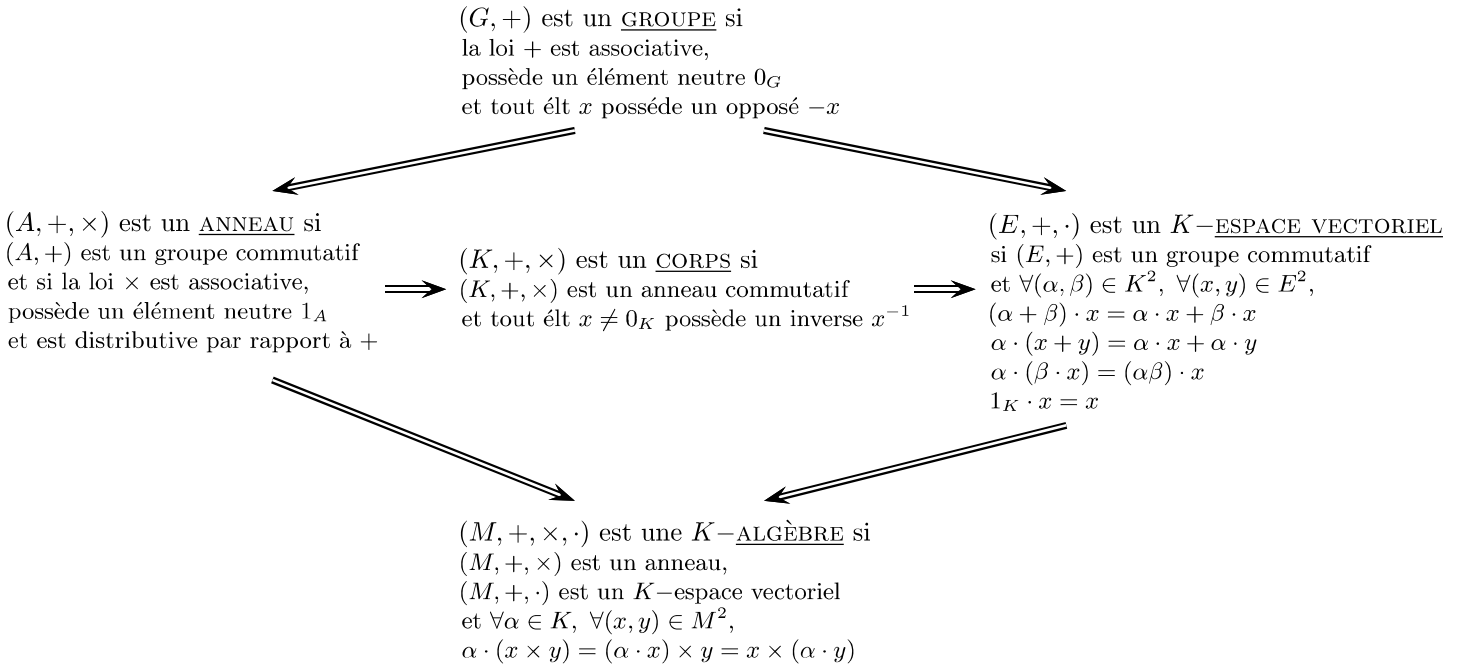


FIGURE A.1 – Structures algébriques

On dit qu'une partie H d'un groupe $(G, +)$ est un sous-groupe de G si H est stable par $+$ et si, muni de la loi induite, $(H, +)$ est encore un groupe. On définit de même un sous-anneau, un sous-corps, un sous-espace vectoriel et une sous-algèbre.

EXERCICE 5 (les sous-groupes additifs de $\mathbb{Z}$) —

1. Soit $n \in \mathbb{Z}$. Montrer que l'ensemble $n\mathbb{Z} = \{nx, x \in \mathbb{Z}\} = \{y \in \mathbb{Z} \mid \exists x \in \mathbb{Z}, y = nx\}$ des multiples de n est un sous-groupe de $(\mathbb{Z}, +)$.
2. Réciproquement, montrer que : si H est un sous-groupe de $(\mathbb{Z}, +)$, alors il existe $n \in \mathbb{Z}$ tel que $H = n\mathbb{Z}$.

A.3 IDÉAUX

DÉFINITION 6

Soit $(A, +, \times)$ un anneau commutatif :

on appelle **idéal** de A tout sous-groupe I de $(A, +)$ tel que $\forall (i, a) \in I \times A, i \times a \in I$.

EXEMPLE 7 —

1. Pour tout $a \in \mathbb{K}$, l'ensemble des polynômes s'annulant en a est un idéal de l'anneau $\mathbb{K}[X]$.

Preuve — La somme de deux polynômes s'annulant en a s'annule en a , l'opposé d'un polynôme s'annulant en a s'annule en a et le polynôme nul aussi. L'ensemble I des polynômes s'annulant en a est donc un sous-groupe additif de $\mathbb{K}[X]$. De plus, le produit d'un polynôme s'annulant en a et d'un polynôme quelconque est un polynôme s'annulant en a . Donc I est un idéal de l'anneau $\mathbb{K}[X]$. $\square$

2. L'ensemble des suites tendant vers 0 n'est pas un idéal de l'anneau des suites mais est un idéal de l'anneau des suites bornées.

Preuve — L'ensemble des suites tendant vers 0 est un sous-groupe additif de l'ensemble des suites. Mais le produit de $(n+1)_{n \in \mathbb{N}}$ et de $(\frac{1}{n+1})_{n \in \mathbb{N}}$ ne tend pas vers 0. Par contre, toute suite tendant vers 0 est bornée et le produit d'une suite tendant vers 0 et d'une suite bornée est une suite tendant vers 0. $\square$

PROPOSITION 8 (les idéaux de $\mathbb{Z}$ et de $\mathbb{K}[X]$)

1. Dans tout anneau commutatif $(A, +, \times)$, pour tout $k \in A$, l'ensemble

$$k \times A = \{k \times x, x \in A\} = \{y \in A \mid \exists x \in A, y = k \times x\}$$

des multiples de k est un idéal de A (appelé l'idéal de A engendré par k).

2. I est un idéal de $\mathbb{Z}$ si, et seulement si, il existe $n \in \mathbb{Z}$ tel que $I = n\mathbb{Z}$.
3. I est un idéal de $\mathbb{K}[X]$ si, et seulement si, il existe $P \in \mathbb{K}[X]$ tel que $I = P\mathbb{K}[X]$.

Preuve —

1. Soit $k \in A$. L'ensemble $k \times A$ est un sous-groupe additif de A car, pour tout $(x_1, x_2) \in A^2$:
 - $0 \times x_1 = 0$, d'où 0 appartient à $k \times A$;
 - par distributivité, $k \times x_1 + k \times x_2$ est égal à $k \times (x_1 + x_2)$ et appartient donc à $k \times A$;
 - l'opposé $-(k \times x_1)$ est égal à $k \times (-x_1)$ et appartient donc à $k \times A$.

De plus, $(k \times x_1) \times x_2 = k \times (x_1 \times x_2)$ par associativité. Donc $k \times A$ est un idéal.

En particulier, $n\mathbb{Z}$ et $P\mathbb{K}[X]$ sont des idéaux. Réciproquement :

2. Si I est un idéal de $\mathbb{Z}$, alors $(I, +)$ est un sous-groupe de $(\mathbb{Z}, +)$, donc I est de la forme $n\mathbb{Z}$ d'après l'exercice 5.
3. Si I contient seulement le polynôme nul, alors $I = 0\mathbb{K}[X]$. Sinon, l'ensemble des degrés des polynômes non nuls de I est une partie non vide de $\mathbb{N}$ et possède donc un minimum d . Soit alors $P \in I$ tel que $\deg P = d$. D'une part, $P\mathbb{K}[X] \subset I$ car I est un idéal. D'autre part, $I \subset P\mathbb{K}[X]$ car, après division euclidienne par P , tout polynôme de I s'écrit $PQ + R$, or $PQ \in I$, donc $R \in I$. Or $\deg R < d$, d'où R est nul.

$\square$

EXERCICE 9 — Montrer que le noyau d'un morphisme d'anneaux commutatifs est un idéal.

PROPOSITION 10

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

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

car $\forall (d, p) \in \mathbb{Z}^2, \quad d \mid p \iff p\mathbb{Z} \subset d\mathbb{Z}$ (i.e. tout multiple de p est un multiple de d .)

Preuve — On sait que l'intersection $I \cap J$ ou la somme $I + J$ de deux sous-groupes $(I, +)$ et $(J, +)$ d'un groupe $(A, +)$ est encore un sous-groupe. Si, de plus, I et J sont des idéaux, alors $\forall (a, i, j) \in A \times I \times J, \quad i \times a \in I$ et $j \times a \in J$. Par suite : si $x \in I \cap J$, alors $ax \in I \cap J$; si $x \in I + J$, alors $\exists (i, j) \in I \times J, \quad x = i + j$, d'où $a \times x = a \times i + a \times j \in I + J$.

En particulier, si $(p, q) \in \mathbb{Z}^2$, alors il existe $d \in \mathbb{Z}$ tel que $p\mathbb{Z} + q\mathbb{Z} = d\mathbb{Z}$ d'après la proposition 8. Or $d \mid p$ car $p\mathbb{Z} \subset d\mathbb{Z}$ et, de même, $d \mid q$, d'où d est un diviseur commun à p et q . Et c'est le plus grand car : si δ est un diviseur commun à p et q , alors δ divise tous les éléments de $p\mathbb{Z} + q\mathbb{Z}$, donc tous les éléments de $d\mathbb{Z}$, et en particulier d , qui est donc le *pgcd*. De même pour le *ppcm*. $\square$

COROLLAIRE 11

(Lemme de Bézout) Deux entiers relatifs a et b sont premiers entre eux ssi $\exists (u, v) \in \mathbb{Z}^2, \quad a \times u + b \times v = 1$.
(Lemme de Gauss) Si a divise bc et a est premier avec b , alors a divise c .

Preuve — (Bézout) $a\mathbb{Z} + b\mathbb{Z} = 1\mathbb{Z}$ si, et seulement si, $\exists (u, v) \in \mathbb{Z}^2, \quad a \times u + b \times v = 1$.

(Gauss) Si a est premier avec b , alors $\exists (u, v) \in \mathbb{Z}^2, \quad a \times u + b \times v = 1$. D'où $ac \times u + bc \times v = c$. Si, de plus, a divise bc , alors (comme a divise ac) il divise aussi $ac \times u + bc \times v$, c'est-à-dire c . $\square$

EXERCICE 12 — *Montrer que : si b et c sont premiers entre eux et divisent a , alors bc divise a .*

A.4 L'ALGORITHME D'EUCLIDE

LEMME 13

Pour tout couple d'entiers naturels $(a, b) \in \mathbb{N}^2$ tel que $b \neq 0$, $\text{pgcd}(a, b) = \text{pgcd}(b, a \bmod b)$.

Preuve — Soient q et $r = a \bmod b$ les quotient et reste de la division euclidienne de a par b . Si d divise a et b , alors d divise b et $r = a - q \cdot b$. Réciproquement : si d divise b et r , alors d divise $a = q \cdot b + r$ et b . Les entiers a et b d'une part, b et r d'autre part ayant les mêmes diviseurs, ils ont le même *pgcd*. $\square$

Algorithme 1: Algorithme d'Euclide

Entrée: Deux entiers naturels a et b et $a \geq b$

Sortie: Le *pgcd* de a et b

```

1  $A \leftarrow a; B \leftarrow b;$ 
2 tant que  $B \neq 0$  faire
3    $R \leftarrow A \bmod B;$                                 (*Le reste de la division euclidienne*)
4    $A \leftarrow B;$ 
5    $B \leftarrow R;$ 
6 retourner  $A$ 
```

PROPOSITION 14

L'algorithme d'Euclide s'arrête sur toutes ses entrées et calcule le *pgcd* de ses deux entrées.

Preuve — On établit que la grandeur $\mathcal{V}(A, B) = B$ est un variant de la boucle **tant que** et que cette boucle admet la propriété invariante suivante, $\mathcal{I} : \text{pgcd}(a, b) = \text{pgcd}(A, B)$ et $A \in \mathbb{N}$ et $B \in \mathbb{N}$.

- Montrons que la propriété $\mathcal{I}$ est bien une propriété invariante.
 - Initialement $A = a$ et $B = b$ avec $a \in \mathbb{N}$ et $b \in \mathbb{N}$, $\mathcal{I}$ découle de telles hypothèses.

- Nommons $\underline{A}, \underline{B}$ les valeurs de A et B au début d'une itération de boucle et $\overline{A}, \overline{B}$ les valeurs de A et B à la fin de cette même itération de boucle. Supposons que $\underline{A}, \underline{B}$ satisfont $\mathcal{I}$ et la *condition de boucle* et montrons que $\overline{A}, \overline{B}$ satisfont $\mathcal{I}$. Par lecture de l'algorithme : $\overline{A} = \underline{B}$ et $\overline{B} = \underline{A} \bmod \underline{B} \neq 0$. Du lemme 13 : $\text{pgcd}(\overline{A}, \overline{B}) = \text{pgcd}(\underline{A}, \underline{B})$. De plus $\overline{A} = \underline{B} \in \mathbb{N}$ et $\overline{B} = \underline{A} \bmod \underline{B}$ d'où par propriété de la division euclidienne $\overline{B} \in \mathbb{N}$.
 - Montrons que la grandeur $\mathcal{V}$ est bien un variant de boucle.
 - $\mathcal{V}$ est à valeurs dans l'espace bien fondé $(\mathbb{N}, \leq)$, par propriété $\mathcal{I}$.
 - Nommons $\underline{A}, \underline{B}$ les valeurs de A et B au début d'une itération de boucle et $\overline{A}, \overline{B}$ les valeurs de A et B à la fin de cette même itération de boucle. Par lecture de l'algorithme : $\mathcal{V}(\overline{A}, \overline{B}) = \overline{B} = \underline{A} \bmod \underline{B} < \underline{B} = \mathcal{V}(\underline{A}, \underline{B})$.
- $\mathcal{V}$ est donc bien un variant de l'algorithme d'Euclide.

On conclut donc que la boucle **tant que** de l'algorithme d'Euclide termine, et ce sur toutes entrées, et produit un état des variables vérifiant $\mathcal{I}$ ainsi que la négation de la condition de boucle. En particulier $\text{pgcd}(A, B) = \text{pgcd}(a, b)$ et $B = 0$. Or $\text{pgcd}(A, 0) = A = \text{pgcd}(a, b)$. On en déduit la correction de l'algorithme. $\square$

PROPOSITION 15

En notant $(C_n)_{n \in \mathbb{N}}$ la suite donnant la complexité pire cas, en nombre de tours de boucle, de l'algorithme d'Euclide, sur des entrées inférieures à n , $C_n = \Theta(\log n)$.

Preuve —

- On montre dans un premier temps que si l'algorithme d'Euclide effectue $p \in \mathbb{N}$ itérations de boucle sur des entrées a et b alors $a \geq F_{p+1}$ où $(F_p)_{p \in \mathbb{N}}$ est la suite de Fibonacci. En effet, considérons la suite finie des valeurs des variables $(A_i)_{i \in \llbracket 0, p \rrbracket}$ et $(B_i)_{i \in \llbracket 0, p \rrbracket}$ en tête des p tours de boucle, numérotées dans l'ordre inverse de leur exécution : $a = A_p$. Notons $(Q_i)_{i \in \llbracket 1, p \rrbracket}$ la suite des quotients des divisions euclidiennes de A par B .

$$\begin{array}{ll}
 A_p = Q_p B_p (= A_{p-1}) + R_p (= A_{p-2}) & A_p = Q_p A_{p-1} + A_{p-2} \\
 A_{p-1} = Q_{p-1} B_{p-1} (= A_{p-2}) + R_{p-1} (= A_{p-3}) & A_{p-1} = Q_{p-1} A_{p-2} + A_{p-3} \\
 \dots = \dots & \dots = \dots \\
 A_i = Q_i B_i (= A_{i-1}) + R_{i-1} (= A_{i-2}) & A_i = Q_i A_{i-1} + A_{i-2} \\
 \dots = \dots & \dots = \dots \\
 A_1 = Q_1 A_0 + 0 & A_1 = Q_1 A_0 + 0
 \end{array}$$

Remarquons que par divisions euclidiennes : $\forall i \in \llbracket 1, p-1 \rrbracket, A_{i-1} < A_i$, de plus par hypothèse sur l'algorithme d'Euclide $a (= A_p) \geq b (= A_{p-1})$. Ainsi les $(A_i)_{i \in \llbracket 0, p \rrbracket}$ forment une suite croissante. On en déduit que $\forall i \in \llbracket 1, p \rrbracket, Q_i \geq 1$, et donc $\forall i \in \llbracket 1, p \rrbracket, A_i \geq A_{i-1} + A_{i-2}$ (en prolongeant $A_{-1} = 0$). De plus $A_0 > 0$. Finalement, une récurrence nous donne : $\forall i \in \llbracket -1, p \rrbracket, A_i \geq F_{i+1}$.

- Dans un second temps, on se rappelle que la suite de Fibonacci a une croissance exponentielle, à savoir :

$$\forall p \geq 2, \phi^{p-2} \leq F_p \leq \phi^{p-1}$$

en notant $\phi = \frac{1+\sqrt{5}}{2}$ le nombre d'or, qui est une solution de l'équation $x^2 - x - 1 = 0$.

- Finalement, on encadre C_n . Soit $n \in \mathbb{N}$ avec $n \geq 2$, on rappelle que la suite de Fibonacci est strictement croissante, soit donc $p \in \mathbb{N}$ tel que $F_p \leq n < F_{p+1}$. On remarque que $n \geq 2$ donc $p \geq 2$ car $F_2 = 1$ et donc on peut utiliser l'encadrement obtenu ci-avant : $\phi^{p-2} \leq n < \phi^p$, soit donc $\log_\phi(n) < p \leq \log_\phi(n) + 2$ par croissance de $\log_\phi$. L'exécution de l'algorithme d'Euclide sur les entrées (F_p, F_{p-1}) conduit à la séquence de p tours de boucles $(F_p, F_{p-1}, F_{p-2}, \dots, F_0)$ pour les valeurs de A . Finalement C_n étant une complexité pire cas : $C_n \geq p > \log_\phi(n)$.

Il nous reste donc à majorer C_n . Supposons qu'il existe deux entrées $(a, b) \in \mathbb{N}^2$ telles que $a \leq n$ et $b \leq n$ conduisant à un nombre de tours de boucle $q > \lceil \log_\phi(n) \rceil + 1$. On déduit des remarques précédentes que $A_q = a \geq F_{q+1}$. En utilisant la croissance de la suite de Fibonacci : $a > F_{\lceil \log_\phi(n) \rceil + 2} = \phi^{\lceil \log_\phi(n) \rceil} \geq \phi^{\log_\phi(n)} = n$ ce qui est absurde car $a \leq n$. On en conclut donc que toutes entrées $(a, b) \in \mathbb{N}^2$ telles que $a \leq n$ et $b \leq n$ conduisent à un nombre de tours de boucle $\leq \lceil \log_\phi(n) \rceil + 1$. Soit $C_n \leq \lceil \log_\phi(n) \rceil + 1 \leq \log_\phi(n) + 2$.

$\square$

REMARQUE 16 — L'algorithme 1 d'Euclide modifie les entiers A et B en préservant l'invariant suivant : A et B sont une combinaison entière affine des valeurs de a et b initiales. En effet à chaque tour de boucle on effectue l'opération : $(A, B) \leftarrow (B, A - QB)$ où $Q = A/B$. Ce résultat nous intéresse particulièrement puisque le lemme de Bézout nous donne l'existence d'une combinaison linéaire entière de a et b valant $\text{pgcd}(a, b)$. En reprenant les notations $(A_i)_{i \in \llbracket 0, n \rrbracket}$ introduites ci-dessus, et en notant u_i et v_i de sorte que $A_i = u_i a + v_i b$, en remarquant que $A_i = Q_i A_{i-1} + A_{i-2}$ on déduit $A_{i-2} = (u_i - Q_i u_{i-1})a + (v_i - Q_i v_{i-1})b$.

Algorithme 2: Algorithme d'Euclide étendu**Entrée:** Deux entiers naturels a et b et $a \geq b$ **Sortie:** Le pgcd de a et b , les coefficients de Bézout1 $A \leftarrow a; B \leftarrow b; U \leftarrow 1; V \leftarrow 0; U' \leftarrow 0; V' \leftarrow 1;$ 2 **tant que** $B \neq 0$ **faire**

3	$Q \leftarrow A/B;$	(*Le quotient de la division euclidienne*)
4	$(A, B) \leftarrow (B, A - QB);$	
5	$(U, V, U', V') \leftarrow (U', V', U - QU', V - QV')$	

6 **retourner** A, U, V **PROPOSITION 17**

L'algorithme d'Euclide étendu s'arrête sur toutes ses entrées (a, b) et calcule un triplet (d, u, v) tel que $d = \text{pgcd}(a, b)$ et $d = au + bv$

A.5 L'ANNEAU $\mathbb{Z}/n\mathbb{Z}$ **DÉFINITION 18**

Soit $n \in \mathbb{N}^*$. 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 $\{\bar{1}; \bar{2}; \dots; \bar{n}\}$ des classes d'équivalence est noté $\mathbb{Z}/n\mathbb{Z}$.

Ainsi, pour tout $(x, a) \in \mathbb{Z}^2$, $\bar{x} = \bar{a} \iff x \equiv a[n]$. Et, parce que $(x \equiv a[n] \text{ et } y \equiv b[n]) \implies (x + y \equiv (a + b)[n] \text{ et } x \times y \equiv (a \times b)[n])$, on peut définir $\bar{x} + \bar{y} = \overline{x + y}$ et $\bar{x} \times \bar{y} = \overline{x \times y}$, ce qui fait de $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ un anneau commutatif.

PROPOSITION 19

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

Preuve — Soit x un entier relatif : $\bar{x}$ est inversible ssi il existe $u \in \mathbb{Z}$ tel que $\bar{x} \times \bar{u} = \bar{1}$, ssi il existe $u \in \mathbb{Z}$ tel que $xu \equiv 1[n]$, ssi il existe $(u, v) \in \mathbb{Z}^2$ tel que $xu + nv = 1$. D'après le lemme de Bézout, c'est le cas ssi x est premier avec n . Par suite l'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps ssi tous les éléments autres que l'élément nul $\bar{n}$ sont inversibles, ssi n est premier avec tous les éléments de $\llbracket 1, n - 1 \rrbracket$, ssi n est premier. $\square$

MÉTHODE 20 (calculer un inverse ou le retour de Bézout) — *Insistons sur la caractère calculable de l'inverse d'un élément x dans $\mathbb{Z}/n\mathbb{Z}$ lorsque n est premier. En effet, étant donné un entier $x \in \mathbb{Z}/n\mathbb{Z}$ et $n \in \mathbb{Z}$ premier, l'exécution de l'algorithme d'Euclide étendu sur les entrées (n, x) conduit au calcul d'un triplet (d, u, v) de sorte que $d = \text{pgcd}(n, x) = 1$, et $1 = nu + vx$. Soit finalement $vx \equiv 1[n]$ et donc $\bar{v}\bar{x} = 1$ soit $\bar{v}$ est l'inverse de $\bar{x}$.*

PROPOSITION 21 (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.

Preuve — Notons $\pi_a : \mathbb{Z} \rightarrow \mathbb{Z}/a\mathbb{Z}$, $x \mapsto \bar{x}$ et de même π_b et π_{ab} . L'application $f : \mathbb{Z}/(ab)\mathbb{Z} \rightarrow \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$, $\pi_{ab}(x) \mapsto (\pi_a(x), \pi_b(x))$ est un isomorphisme d'anneaux. D'une part elle est bien définie et c'est un morphisme d'anneaux.

D'autre part ses ensembles de départ et d'arrivée ont le même cardinal ab , elle est donc bijective ssi elle est injective. Ce qu'elle est car : si $\pi_a(x)$ et $\pi_b(x)$ sont nuls, alors a et b divisent x , d'où (exercice 12) ab divise x car a et b sont premiers entre eux, donc $\pi_{ab}(x)$ est nul. $\square$

MÉTHODE 22 (Résoudre un système de congruences avec l'algorithme d'Euclide étendu) — *Soit donc une famille $(p_1, p_2, \dots, p_n)$ d'entiers deux à deux premiers entre eux. On souhaite construire un isomorphisme*

de $(\mathbb{Z}/p_1\mathbb{Z} \times \mathbb{Z}/p_2\mathbb{Z} \times \cdots \times \mathbb{Z}/p_n\mathbb{Z}) \rightarrow \mathbb{Z}/p_1p_2 \dots p_n\mathbb{Z}$. Ainsi étant donné un élément x dont on connaît uniquement les valeurs $x_1 = x \bmod p_1$, $x_2 = x \bmod p_2$, ..., $x_n = x \bmod p_n$ on cherche à calculer la valeur de $x \bmod p_1p_2 \dots p_n$. Pour ce faire on construit une famille d'entiers $(l_i)_{i \in \llbracket 1, n \rrbracket}$ tels que $l_i \bmod p_j = \delta_{i,j}$. Armé d'une telle famille on pourra alors construire l'entier $x = x_1l_1 + x_2l_2 + \cdots + x_nl_n$ qui sera bien tel que $\forall j \in \llbracket 1, n \rrbracket$, $x \bmod p_j = x_j$. Pour tout $i \in \llbracket 1, n \rrbracket$ et tout $j \neq i$, l_i doit donc être multiple de p_j , soit donc $K_i = p_1p_2 \dots p_{i-1}p_{i+1} \dots p_n$ qui convient. Mais il faut de plus que $l_i \bmod p_i = 1$, or $K_i \bmod p_i$ n'est pas nécessairement 1. On peut toutefois calculer l'inverse de K_i dans $\mathbb{Z}/p_i\mathbb{Z}$ grâce à l'algorithme d'Euclide étendu, notons J_i cette inverse. Finalement K_iJ_i est tel que pour tout $j \neq i$ $K_iJ_i \bmod p_j = 0$ car K_i est multiple de p_j et $K_iJ_i \bmod p_i = 1$. On conclut donc que le choix $l_i = K_iJ_i$ convient.

EXEMPLE 23 — On cherche les entiers relatifs x tels que $x \equiv 2[3]$, $x \equiv 4[5]$, $y \equiv 2[8]$. On note que $p_1 = 3$, $p_2 = 5$ et $p_3 = 8$ sont premiers entre eux deux à deux. On calcule $K_1 = 5 \times 8 = 40$, $K_2 = 3 \times 8 = 24$ et $K_3 = 3 \times 5 = 15$. On calcule les inverses des K_i module p_i au moyen de l'algorithme d'Euclide étendu :

- $3 \times (-13) + 40 \times 1 = 1$ donc $J_1 = \overline{40}^{-1} = \overline{1}$ dans $\mathbb{Z}/3\mathbb{Z}$;
- $5 \times 5 + 24 \times (-1) = 1$ donc $J_2 = \overline{24}^{-1} = \overline{-1}$ dans $\mathbb{Z}/5\mathbb{Z}$;
- $8 \times 2 + 15 \times (-1) = 1$ donc $J_3 = \overline{15}^{-1} = \overline{-1}$ dans $\mathbb{Z}/8\mathbb{Z}$.

On fabrique alors les entiers $l_1 = K_1J_1 = 40$, $l_2 = -24$ et $l_3 = -15$. Donc

$$\begin{cases} x \equiv 2[3] \\ x \equiv 4[5] \\ y \equiv 2[8] \end{cases} \Leftrightarrow x \equiv 2l_1 + 4l_2 + 2l_3[120] \Leftrightarrow x \equiv -46[120]$$

DÉFINITION 24

Le nombre d'éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ (i.e. le nombre d'entiers de $\llbracket 1, n \rrbracket$ premiers avec n) est noté $\varphi(n)$. L'application $\varphi : \mathbb{N}^* \rightarrow \mathbb{N}$, $n \mapsto \varphi(n)$ est appelée l'**indicatrice d'Euler**.

MÉTHODE 25 (Comment calculer l'indicatrice d'Euler) —

- (i) Si p est premier, alors $\varphi(p) = p - 1$ et $\forall k \in \mathbb{N}^*$, $\varphi(p^k) = p^k \left(1 - \frac{1}{p}\right)$.
- (ii) Si a et b sont premiers entre eux, alors $\varphi(ab) = \varphi(a)\varphi(b)$.
- (iii) Si $p_1, \dots, p_k$ sont les diviseurs premiers de n , alors $\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right)$.

Preuve — (i) Si p est premier, alors : les éléments de $\llbracket 1, p \rrbracket$ premiers avec p sont $1, \dots, p - 1$, donc $\varphi(p) = p - 1$. Et un élément de $\llbracket 1, p^k \rrbracket$ est premier avec p^k ssi il est premier avec p ssi il n'est pas un multiple de p . Or $\llbracket 1, p^k \rrbracket$ contient p^{k-1} multiples de p . Donc $\varphi(p^k) = p^k - p^{k-1} = p^k \left(1 - \frac{1}{p}\right)$.

(ii) Il y a $\varphi(a)$ inversibles dans $\mathbb{Z}/a\mathbb{Z}$ et il y en a $\varphi(b)$ dans $\mathbb{Z}/b\mathbb{Z}$. Il y en a donc $\varphi(a)\varphi(b)$ dans $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ et autant dans $\mathbb{Z}/(ab)\mathbb{Z}$ par l'isomorphisme du théorème chinois si a et b sont premiers entre eux.

(iii) n est de la forme $p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, d'où $\varphi(n) = \varphi(p_1^{\alpha_1}) \cdots \varphi(p_k^{\alpha_k}) = n \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right)$. □

A.6 L'ORDRE D'UN ÉLÉMENT

Si a est un élément d'un groupe $(G, \cdot)$ d'élément neutre 1, alors l'ensemble $\{\dots; a^{-2}; a^{-1}; 1; a^1; a^2; \dots\} = \{a^k, k \in \mathbb{Z}\}$ est un sous-groupe de G , appelé le sous-groupe engendré par a ; 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 alors 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 .

Preuve — Soit b l'ordre de a . Si k est un multiple bq de l'ordre, alors $a^{bq} = (a^b)^q = 1^q = 1$. Réciproquement, supposons que $a^k = 1$. Après division euclidienne, $\exists!(q, r) \in \mathbb{N}^2$, $k = bq + r$ et $r < b$. D'où $a^k = a^{bq} \cdot a^r$, d'où $1 = 1 \cdot a^r$ d'où $a^r = 1$. Or $r < b$, donc $r = 0$ par définition de l'ordre de a . $\square$

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 26 — Décomposer en cycles disjoints la permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 4 & 7 & 2 & 6 & 1 & 3 \end{pmatrix}$ du groupe symétrique S_7 et en déduire l'ordre de σ .

PROPOSITION 27 (Théorème de Lagrange)

Si a est un élément d'un groupe G fini, alors l'ordre de a divise le cardinal de G .

Preuve — (La preuve qui suit est valable seulement si G est commutatif.) L'application $G \rightarrow G, x \mapsto ax$ est bijective. D'où le produit $\prod_{x \in G} x$ de tous les éléments du groupe est aussi égal à $\prod_{x \in G} (ax) = a^n \prod_{x \in G} x$, en notant n le cardinal de G . Donc $a^n = 1$. $\square$

COROLLAIRE 28

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

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

Preuve — (Euler) Si a est premier avec n , alors $\bar{a}$ est un élément inversible de $\mathbb{Z}/n\mathbb{Z}$. Le groupe des inversibles de $\mathbb{Z}/n\mathbb{Z}$ a pour cardinal $\varphi(n)$. L'ordre de $\bar{a}$ divise donc $\varphi(n)$. Par suite $\bar{a}^{\varphi(n)} = \bar{1}$. Autrement dit $a^{\varphi(n)} \equiv 1[n]$.

(Fermat) Parce que p est premier : ou bien a est divisible par p , d'où a^p l'est aussi, donc $a^p \equiv a \equiv 0[p]$. Ou bien a est premier avec p et alors, d'après le théorème d'Euler, $a^{p-1} \equiv 1[p]$, d'où $a^p \equiv a[p]$. $\square$

EXERCICE 29 — 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 les deux derniers chiffres de l'écriture décimale de 3^{345} sont 4 et 3.