Algèbre et arithmétique effectives

Bruno Grenet
Université Grenoble-Alpes

Version du 8 septembre 2023

1 Entiers et entiers modulaires

1.1 Propriétés de base des entiers

Notations. On note $\mathbb{Z}$ l'ensemble des entiers relatifs. On note respectivement $\mathbb{Z}_{<0}$, $\mathbb{Z}_{\leq 0}$, $\mathbb{Z}_{\geq 0}$ et $\mathbb{Z}_{>0}$ les ensembles d'entiers strictement négatifs, négatifs ou nuls, positifs ou nuls, et strictement positifs.

Théorème 1.1 Soit $a \in \mathbb{Z}_{\geq 0}$, $b \in \mathbb{Z}_{>0}$. Alors il existe un unique couple d'entiers (q, r) tel que $a = bq + r$ et $0 \leq r < b$.

Démonstration. L'existence du couple (q, r) est donnée par l'algorithme suivant.

Algorithme 1.2 – DivisionEuclidienne(a, b)

Entrées : deux entiers a et b tels que $a \geq 0$ et $b > 0$
Sortie : un couple (q, r) tel que $a = bq + r$ et $0 \leq r < b$

1. $(q, r) \leftarrow (0, a)$
2. Tant que $r \geq b$:
3. $\quad r \leftarrow r - b$
4. $\quad q \leftarrow q + 1$
5. Renvoyer (q, r)

Pour prouver la correction de l'algorithme, on commence par démontrer qu'il termine. En effet, la valeur de r diminue strictement à chaque itération, et r est bornée inférieurement par la condition d'arrêt. On démontre ensuite que l'égalité $a = bq + r$ est vérifiée tout au long de l'exécution, par induction. Pour cela, on peut définir les suites $(q_i)_{0 \leq i \leq n}$ et $(r_i)_{0 \leq i \leq n}$ où q_i et r_i sont les valeurs de q et r après i passages dans la boucle « Tant que », et on montre que $a = bq_i + r_i$ pour tout i. En particulier, $q_0 = 0$ et $r_0 = a$ sont les valeurs initiales de q et r et q_n et r_n les valeurs renvoyées par l'algorithme. On a évidemment $a = b \cdot q_0 + r_0 = b \cdot 0 + a$. Comme $r_{i+1} = r_i - b$ et $q_{i+1} = q_i + 1$, $bq_{i+1} + r_{i+1} = b(q_i + 1) + (r_i - b) = bq_i + r_i = a$ par hypothèse d'induction. Donc le résultat est démontré pour tout i.

Ainsi, en fin d'algorithme, $a = bq_n + r_n$ comme souhaité. D'autre part, la condition d'arrêt de la boucle montre que $r_n < b$. Pour montrer que $r_n \geq 0$, on remarque que $r_{n-1} \geq b$ (sinon l'algorithme se serait arrêté), donc $r_n = r_{n-1} - b \geq 0$.

Il reste à montrer l'unicité du couple (q, r), c'est-à-dire que s'il existe un autre couple (q', r') satisfaisant $a = bq' + r'$ et $0 \leq r' < b$, alors $q = q'$ et $r = r'$. Pour cela, on remarque que dans ce cas,

$a = bq + r = bq' + r'$, donc $b(q - q') = r' - r$. Donc $r' - r$ est un multiple de b. Or $-b < r' - r < b$ car $0 \leq r, r' < b$. Le seul multiple de b compris strictement entre $-b$ et b est 0. Donc $r = r'$. Donc $b(q - q') = 0$. Comme $b \neq 0$, $q - q' = 0$ et donc $q = q'$. ■

Notations. Dans le théorème précédent, q est le *quotient*, noté a quo b. L'entier r est le *reste*, noté a mod b.

R ! Le résultat reste vrai pour des entiers relatifs : pour tous entiers a et b, $b \neq 0$, il existe un unique couple (q, r) avec $0 \leq r < |b|$ tel que $a = bq + r$. On note toujours $q = a$ quo b et $r = a$ mod b.

Exercice 1.1.

1. Démontrer, simplement, les affirmations utilisées de manière implicite dans la preuve : si $xy = 0$ et $x \neq 0$, alors $y = 0$; si $x = yz$ et $-y < x < y$, alors $x = 0$.
2. Pourquoi doit-on supposer $b > 0$ dans l'énoncé du théorème ? Quelle partie de la preuve ne fonctionne pas si $b = 0$?
3. On peut définir une version *équilibrée* de la division euclidienne, qui fonctionne pour des entiers relatifs : si a et b sont deux entiers tels que $b \neq 0$, alors il existe un unique couple (q, r) tel que $a = bq + r$ et $-b/2 \leq r < b/2$. Adapter la démonstration (dont l'algorithme) pour démontrer ce résultat.

Théorème 1.3 Soit $a, b \in \mathbb{Z}$. Alors il existe un *unique* plus grand diviseur commun à a et b, noté $\text{PGCD}(a, b)$, c'est-à-dire un entier positif d qui divise a et b et tel que tout diviseur commun à a et b divise également d.

Démonstration. La démonstration est basée sur l'algorithme d'Euclide de calcul du PGCD. On le présente en deux versions, récursive et itérative, qui sont équivalentes.

Algorithme 1.4 – EUCLIDEREC(a, b)

Entrées : deux entiers a et b positifs
Sortie : le PGCD de a et b

1. Si $a < b$: Renvoyer EUCLIDEREC(b, a)
2. Si $b = 0$: Renvoyer a
3. Renvoyer EUCLIDEREC$(b, a \bmod b)$

Algorithme 1.5 – EUCLIDEIT(a, b)

Entrées : deux entiers a et b positifs
Sortie : le PGCD de a et b

1. Si $a < b$: $(a, b) \leftarrow (b, a)$
2. Tant que $b > 0$:
3. $\quad (a, b) \leftarrow (b, a \bmod b)$
4. Renvoyer a

L'existence d'un PGCD est assurée par la correction de ces algorithmes. On effectue la démonstration uniquement pour EUCLIDEREC. Celle pour EUCLIDEIT, quasiment identique, est laissée en exercice. On fait l'hypothèse qu'en entrée, $a \geq b$.

La terminaison est assurée par le fait que $a \bmod b < b$ par définition. Ainsi, la deuxième entrée décroît strictement dans les appels récursifs. La correction consiste à démontrer que EUCLIDEREC(a, b) renvoie effectivement PGCD(a, b), c'est-à-dire le plus grand entier qui divise à la fois a et b. Pour cela on utilise deux résultats élémentaires sur le PGCD.

Affirmation. Pour n'importe quel entier $a \geq 0$, PGCD$(a, 0) = a$.

► C'est évident : tout entier divise 0 et le plus grand entier qui divise a est a lui-même. ◄

Affirmation. L'ensemble des diviseurs communs à a et b est le même que l'ensemble des diviseurs communs à b et $a \bmod b$.

► On montre deux inclusions. On note $a = bq + r$ la division euclidienne de a par b, donc en particulier $r = a \bmod b$. Premièrement, si d est un diviseur commun de a et b, alors il divise aussi $a - bq = r$. Donc c'est un diviseur commun de b et $a \bmod b$. Réciproquement, si d est un diviseur commun de b et $r = a \bmod b$, il divise également $bq + r = a$. Donc c'est un diviseur commun à a et b. Ainsi, les ensembles sont égaux, et ils ont donc le même plus grand élément. ◄

À l'aide des deux affirmations, on déduit la correction de l'algorithme. Notons a_0 et b_0 les valeurs initiales de a et b et a_i, b_i les valeurs au $i^{\text{ème}}$ appel récursif. On a donc $a_{i+1} = b_i$ et $b_{i+1} = a_i \bmod b_i$. Alors PGCD(a_i, b_i) est *invariant* (PGCD(a_i, b_i) = PGCD(a_0, b_0) pour tout i) d'après la deuxième affirmation. S'il y a n appels récursifs, on a $b_n = 0$ et on renvoie a_n. L'algorithme est correct car PGCD$(a_n, b_n) = a_n$ d'après la première affirmation.

L'unicité du PGCD est évidente si on considère que c'est *le plus grand entier* qui divise a et b. On s'intéresse au fait que c'est le seul entier positif d tel que tout diviseur commun à a et b divise également d. En effet, en supposant qu'il en existe deux, d et d', alors par définition du PGCD, d divise d' et d' divise d. Comme ils sont positifs, cela implique en particulier que $d \leq d'$ et $d' \leq d$, d'où $d = d'$. ■

Proposition 1.6 L'algorithme EUCLIDEREC(a, b) effectue au plus $O(\log b)$ calculs de division euclidienne.

Démonstration. Le nombre de divisions euclidiennes effectuées est le nombre d'appels récursifs. On montre qu'à chaque étape de l'algorithme, la quantité $a + b$ diminue strictement. On remarque d'abord, avec les notations de la démonstration précédente, que $a_i \geq b_i$ pour tout i.

Ensuite, on pose $s_i = a_i + b_i$. On note $q_i = a_i$ quo b_i et $r_i = a_i \bmod b_i$ de telle sorte que $a_i = b_i q_i + r_i$. Alors $s_i = a_i + b_i = b_i(q_i + 1) + r_i = a_{i+1}(q_i + 1) + b_{i+1}$. Or $q_i \geq 1$ car $a_i \geq b_i$. Donc $s_i \geq 2a_{i+1} + b_{i+1}$. Comme $a_{i+1} \geq b_{i+1}$, on a $s_i \geq 2a_{i+1} + b_{i+1} - \frac{1}{2}(a_{i+1} - b_{i+1}) = \frac{3}{2}(a_{i+1} + b_{i+1}) = \frac{3}{2}s_{i+1}$. On en déduit par récurrence que $s_i \leq \frac{2}{3}^{i-1} s_1$. Comme $s_1 = a_1 + b_1 = b + (a \bmod b) < 2b$, s'il y a n appels récursifs, on a $s_n \leq 2 \cdot \frac{2}{3}^{n-1} b$ et donc $\frac{3}{2}^{n-1} s_n \leq 2b$. En utilisant le fait que $s_n \geq 1$ et en prenant le logarithme de chaque côté, $(n-1)\log\frac{3}{2} \leq \log(2b)$. Donc $n = O(\log b)$. ■

Exercice 1.2.

1. Montrer, avec les notations de la preuve, que $a_i \geq b_i$.
2. Écrire la preuve de terminaison, correction et complexité de EuclideIt. *On peut réutiliser les deux affirmations.*
3. Soit $\varphi = \frac{1}{2}(1 + \sqrt{5})$ le nombre d'or. En remplaçant s_i par la quantité $t_i = a_i + \frac{1}{\varphi} b_i$ dans la preuve, montrer que le nombre d'appels récursifs est exactement borné par $1 + \log b / \log \varphi$. *On utilisera le fait que* $\varphi^2 - \varphi - 1 = 0$.
4. Soit F_n le $n^{\text{ème}}$ nombre de Fibonacci, défini par $F_0 = 0$, $F_1 = 1$ et $F_{i+2} = F_i + F_{i+1}$ pour $i \geq 0$. Montrer que EuclideRec(F_{n+1}, F_n) effectue exactement n appels récursifs.

5. En utilisant le fait que $F_n \simeq \varphi^n/\sqrt{5}$, déduire que la borne de la question 3 est atteinte sur les entrées F_{n+1} et F_n.

Théorème 1.7 *(identité de Bézout)* Soit $a, b \in \mathbb{Z}$. Alors il existe un couple d'entiers (u, v) tels que $\text{PGCD}(a, b) = au + bv$.

Démonstration. L'existence de ces entiers est démontrée par l'algorithme d'Euclide étendu, dont on fournit une version récursive.

Algorithme 1.8 – EUCLIDEÉTENDU(a, b)

Entrées : deux entiers a et b positifs
Sortie : un triplet (d, u, v) tel que $\text{PGCD}(a, b) = d = au + bv$

1. Si $a < b$:
2. $\quad (d, u, v) \leftarrow$ EUCLIDEÉTENDU(b, a)
3. $\quad$ Renvoyer (d, v, u)
4. Si $b = 0$: Renvoyer $(a, 1, 0)$
5. $(q, r) \leftarrow (a \text{ quo } b, a \bmod b)$
6. $(d, u', v') \leftarrow$ EUCLIDEÉTENDU(b, r)
7. Renvoyer $(d, v', u' - qv')$

La terminaison et la complexité de cet algorithme se déduisent directement de celles de EUCLIDEREC. En effet, si on ignore les u et v de l'algorithme, on retrouve exactement EUCLIDEREC. En particulier, on a également que l'entier d renvoyé est bien le PGCD de a et b. Le fait que $d = au + bv$ se démontre par induction. Si $b = 0$ c'est clair car on a alors $d = a = a \cdot 1 + b \cdot 0$. Sinon, on écrit $a = bq + r$. Par hypothèse d'induction, (d, u', v') satisfait $d = bu' + rv'$. Donc $d = bu' + (a - bq)v' = av' + b(u' - qv')$. D'où le résultat.

Ainsi, on a démontré grâce à cet algorithme que pour tout couple d'entier (a, b), il existe un couple (u, v) tel que $\text{PGCD}(a, b) = au + bv$. ■

Vocabulaire. Les entiers u et v du théorème sont appelés les *coefficients de Bézout* associées à a et b.

R Pour tous entiers a, b, u et v, $\text{PGCD}(a, b)$ divise $au + bv$: en effet, le PGCD divise a donc également au, et il divise b donc bv, il divise donc leur somme $au + bv$.

Corollaire 1.9 S'il existe deux entiers u et v tels que $au + bv = 1$, alors $\text{PGCD}(a, b) = 1$.

Démonstration. C'est une conséquence immédiate de la remarque. Comme $\text{PGCD}(a, b)$ divise $au + bv = 1$, le PGCD ne peut valoir que 1. ■

Exercice 1.3.

1. Écrire une version itérative de l'algorithme d'Euclide étendu. *S'inspirer de* EuclideIt.
2. Montrer que le couple (u, v) tel que $au + bv = \text{pgcd}(a, b)$ n'est pas unique. *Ajouter $ab - ab$ à l'expression $au + bv$ et réorganiser les termes pour produire un nouveau couple (u', v').*

Théorème 1.10 *(lemme de Gauss)* Soit a, b et $c \in \mathbb{Z}$ tels que a divise bc, et $\text{PGCD}(a, b) = 1$. Alors a divise c.

Démonstration. Soit u et v tels que $au + bv = 1$. En multipliant par c, on obtient $auc + bvc = c$. Comme a divise bc, il divise aussi bvc. Donc il divise la somme $auc + bvc = c$. ■

Corollaire 1.11 Soit a, b et $c \in \mathbb{Z}$ tels que $\text{PGCD}(b, c) = 1$. Si a est divisible par b et c, il est divisible par leur produit bc.

Démonstration. Puisque a est divisible par b, il existe k tel que $a = bk$. Ensuite, c divise $a = bk$ et $\text{PGCD}(b, c) = 1$. Donc c divise k d'après le lemme de Gauss. Donc on peut écrire $k = c\ell$, donc $a = bc\ell$ est divisible par bc. ■

Définition 1.12 Un entier est *premier* s'il admet exactement deux diviseurs positifs, 1 et lui-même. Deux entiers sont *premiers entre eux* si leur PGCD vaut 1.

Théorème 1.13 *(théorème fondamental de l'arithmétique)* Tout entier non nul n peut s'écrire de manière unique sous la forme

$$n = \pm p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} = \prod_{i=1}^{k} p_i^{e_i}$$

où $p_1 < p_2 < \cdots < p_k$ sont premiers et $e_1, \ldots, e_k$ sont des entiers strictement positifs. *On utilise la convention qu'un produit vide (de zéro terme) est égal à* 1.

Démonstration. L'existence se prouve par récurrence. Si $n = 1$, le résultat est évident. Si $n > 1$, il y a deux cas. Soit n est premier, auquel cas le résultat est obtenu (avec $p_1 = n$, $e_1 = 1$ et $k = 1$). Sinon, n peut s'écrire $n = ab$, avec $a, b < n$. Par hypothèse de récurrence, a et b peuvent s'écrire chacun comme un produit de puissances de nombres premiers. Donc c'est également le cas de n.

Pour prouver l'unicité de l'écriture, il suffit de montrer que si $n = p_1 \cdots p_s = q_1 \cdots q_t$ où les p_i et q_j sont des nombres premiers pas forcément distincts, alors $s = t$ et $(p_1, \ldots, p_s)$ est une permutation de $(q_1, \ldots, q_s)$. On le montre par récurrence sur s. Si $s = 0$, $n = 1$. Donc on a forcément $t = 0$ et le résultat est démontré. Supposons le résultat correct pour $s-1$. Comme p_s divise $p_1 \cdots p_s$, il doit diviser $q_1 \cdots q_t$. En appliquant le lemme de Gauss plusieurs fois si nécessaire, on déduit que p_1 divise l'un des q_j, et est donc égal à l'un des q_j. En divisant n par $p_1 = q_j$, on obtient à nouveau deux écritures égales, avec un terme de moins. Par hypothèse de récurrence, $(p_2, \ldots, p_s)$ est une permutation de $(q_1, \ldots, q_{j-1}, q_{j+1}, \ldots, q_t)$, donc on obtient le résultat. ■

Exercice 1.4.

1. Soit $a = \prod_i p_i^{e_i}$ et $b = \prod_i p_i^{f_i}$, où les p_i sont des premiers distincts et e_i, $f_i \geq 0$. Montrer que $\text{pgcd}(a, b) = \prod_i p_i^{\min(e_i, f_i)}$.
2. Montrer qu'il existe une infinité de nombres premiers. *Supposer à l'inverse que les seuls nombres premiers sont p_1, …, p_k et considérer $p_1 \cdots p_k + 1$.*

1.2 Entiers modulaires : $\mathbb{Z}/n\mathbb{Z}$

Vocabulaire. Deux entiers a et b sont dits *congruents modulo* n, noté $a \equiv_n b$ s'ils ont le même reste dans la division euclidienne par n, c'est-à-dire si $a \bmod n = b \bmod n$.

R De manière équivalente, $a \equiv_n b$ si n divise $a-b$, ou encore s'il existe $k \in \mathbb{Z}$ tel que $a = b + nk$. On rencontre de nombreuses notations pour la congruence. La notation utilisée ici n'est pas la plus courante. La relation « a est congru à b modulo n » est souvent écrite « $a \equiv b\ [n]$ » ou « $a \equiv b\ [\mathrm{mod} n]$ », ou encore en utilisant des variantes : en remplaçant les crochets par des parenthèses, ou en remplaçant le signe « $\equiv$ » par un signe « $=$ ». Dans ce texte, on garde « mod » pour le reste dans la division euclidienne, et on indique les congruences avec le symbole « $\equiv$ ».

Proposition 1.14 La relation de congruence modulo n est une relation d'équivalence : pour tout a, b et $c \in \mathbb{Z}$,

(i) $a \equiv_n a$ (*réflexivité*),
(ii) si $a \equiv_n b$, alors $b \equiv_n a$ (*symétrie*),
(iii) si $a \equiv_n b$ et $b \equiv_n c$ alors $a \equiv_n c$ (*transitivité*).

Exercice 1.5. Démontrer la proposition. *Indice : c'est immédiat.*

Théorème 1.15 La relation de congruence modulo n est *compatible* avec l'addition et la multiplication : pour tout a, a', b et $b' \in \mathbb{Z}$, si $a \equiv_n a'$ et $b \equiv_n b'$ alors $a+b \equiv_n a'+b'$ et $a \times b \equiv_n a' \times b'$.

Démonstration. En utilisant la remarque, $a \equiv_n a'$ et $b \equiv_n b'$ signifient qu'il existe k et ℓ tels que $a = a'+kn$ et $b = b'+\ell n$. Donc $a+b = (a'+kn)+(b'+\ell n) = (a'+b')+(k+\ell)n$, donc $a+b \equiv_n a'+b'$. De même, $a \times b = (a'+kn)(b'+\ell n) = a'b' + (a'\ell + b'k)n$ donc $ab \equiv_n a'b'$. ■

Définition 1.16 Soit $n \in \mathbb{Z}_{>0}$. La *classe d'équivalence modulo* n d'un entier $a \in \mathbb{Z}$ est l'ensemble des entiers congrus à a modulo n, c'est-à-dire l'ensemble $[a]_n = \{a+nk : k \in \mathbb{Z}\}$. Tout entier $b \in [a]_n$ est appelé un *représentant* de la classe d'équivalence.
L'ensemble $\mathbb{Z}/n\mathbb{Z}$ est l'ensemble des classes d'équivalences modulo n.

Proposition 1.17 Soit a, $b \in \mathbb{Z}$ et $n \in \mathbb{Z}_{>0}$. Alors

$$a \bmod n = b \bmod n \iff a \equiv_n b \iff [a]_n = [b]_n.$$

Théorème 1.18 Soit $n \in \mathbb{Z}_{>0}$. Alors $\mathbb{Z}/n\mathbb{Z}$ est l'ensemble des n classes d'équivalence $[0]_n$, $[1]_n$, …, $[n-1]_n$. Ainsi, toute classe d'équivalence possède un *représentant canonique* compris entre 0 et $n-1$.

Démonstration. La première partie consiste à montrer que n'importe quelle classe d'équivalence possède un représentant entre 0 et $n-1$. Soit $a \in \mathbb{Z}$. Par division euclidienne, on peut écrire $a = qn+r$ avec $0 \leq r < n$. Par définition, $[a]_n = [r]_n$, donc on a trouvé le représentant souhaité.

La seconde partie consiste à montrer que les n classes d'équivalences sont bien distinctes, ce qui revient à montrer que si $0 \leq a < b < n$, alors $[a]_n \neq [b]_n$. Puisque $0 < a < b < n$, $a \bmod n = a$ et $b \bmod n = b$. Donc $a \bmod n \neq b \bmod n$, donc les classes sont différentes. ■

Définition 1.19 Grâce au théorème 1.15, on définit les opérations d'addition et de multiplication sur $\mathbb{Z}/n\mathbb{Z}$ en posant $[a]_n + [b]_n = [a+b]_n$ et $[a]_n \times [b]_n = [a \times b]_n$.

R On peut définir $\mathbb{Z}/n\mathbb{Z}$ avec une vision informatique : c'est l'ensemble des entiers compris entre 0 et $n-1$, avec les opérations $a \oplus b = (a+b) \bmod n$ et $a \otimes b = (a \times b) \bmod n$. Cette vision est celle utilisée d'un point de vue pratique : les algorithmes que l'on utilise manipulent des entiers, et non des classes d'équivalence.

Notations. Lorsque le contexte est clair, on omet souvent l'indice pour les classes d'équivalences : on écrit simplement $[a]$ au lieu de $[a]_n$. De plus, par abus de notation, on oublie parfois les crochets : on écrit par exemple $3 \in \mathbb{Z}/7\mathbb{Z}$ à la place de $[3]_7 \in \mathbb{Z}/7\mathbb{Z}$. Cela rejoint la vision informatique : il y a l'entier 3 *vu comme un élément de* $\mathbb{Z}$ et l'entier 3 *vu comme un élément de* $\mathbb{Z}/7\mathbb{Z}$.
Pour parler d'un élément de $\mathbb{Z}/n\mathbb{Z}$ sans spécifier un représentant, on utilise une lettre grecque. Par exemple, si on écrit « soit $\alpha \in \mathbb{Z}/n\mathbb{Z}$ », α est une classe d'équivalence, c'est-à-dire qu'il existe un entier a tel que $\alpha = [a]$.

R Soit $\alpha \in \mathbb{Z}/n\mathbb{Z}$. Alors il existe $\beta \in \mathbb{Z}/n\mathbb{Z}$ tel que $\alpha + \beta = [0]$. En effet, si $\alpha = [a]$, il suffit de prendre $\beta = [-a]$. On appelle $[0]$ l'*élément nul* de $\mathbb{Z}/n\mathbb{Z}$.

Définition 1.20 Un élément $\alpha \in \mathbb{Z}/n\mathbb{Z}$ est dit *inversible* s'il existe $\beta \in \mathbb{Z}/n\mathbb{Z}$ tel que $\alpha\beta = [1]$. On note α^{-1} l'inverse de α.

Exercice 1.6. Montrer que si α est inversible, son inverse est unique. *Si β et γ sont deux inverses de α, écrire l'égalité $\alpha\beta = \alpha\gamma$ et multiplier par β pour conclure.*

Théorème 1.21 Un élément $\alpha \in \mathbb{Z}/n\mathbb{Z}$ est inversible si et seulement si ses représentants sont *premiers avec* n.

Démonstration. On remarque en premier lieu que tous les représentants d'une classe $\alpha \in \mathbb{Z}/n\mathbb{Z}$ ont le même PGCD avec n. En effet, en notant a le représentant canonique, tout représentant s'écrit $a + kn$ pour un certain k. Et $\text{PGCD}(a+kn, n) = \text{PGCD}(a, n)$ (pour s'en convaincre, il suffit de noter que la première étape de l'algorithme d'Euclide remplace le couple $(a+kn, n)$ par le couple (n, a)).

Soit a un représentant de α. Pour l'existence d'un inverse de α lorsque $\text{PGCD}(a, n) = 1$, on utilise l'algorithme d'inversion modulaire.

Algorithme 1.22 – InverseMod(a, n)

Entrée : Deux entiers a et $n \neq 0$
Sortie : Un entier b entre 0 et $n-1$ tel que $ab \equiv_n 1$ s'il en existe un, une erreur sinon

1. $(d, u, v) \leftarrow$ EuclideÉtendu(a, n)
2. Si $d \neq 1$: Renvoyer une erreur « a n'est pas inversible modulo n »
3. Renvoyer $u \bmod n$

L'algorithme EuclideÉtendu renvoie (d, u, v) où $d = \text{PGCD}(a, n)$ et $d = au + vn$. Si $d = 1$, on a $au = 1 + nv$. Autrement dit, $au \equiv_n 1$. Donc en prenant $\beta = [u]$, on a bien $\alpha\beta = [a][u] = [au] = [1]$.

Réciproquement, s'il existe β tel que $\alpha\beta = [1]$, on choisit des représentants a et b de α et β. Comme $[a][b] = [ab] = [1]$, $ab \equiv_n 1$. Donc il existe k tel que $ab = 1 + kn$, ou encore $ab - nk = 1$. D'après le corollaire 1.9, $\text{PGCD}(a, n) = 1$. ■

Notation. L'ensemble des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ est noté $(\mathbb{Z}/n\mathbb{Z})^\times$.

Définition 1.23 Un élément non nul $\alpha \in \mathbb{Z}/n\mathbb{Z}$ est appelé un *diviseur de zéro* s'il existe $\beta \in \mathbb{Z}/n\mathbb{Z}$ non nul tel que $\alpha\beta = [0]$.

Proposition 1.24 Tout élément non nul de $\mathbb{Z}/n\mathbb{Z}$ est soit inversible, soit un diviseur de zéro.

Démonstration. Soit $\alpha \in \mathbb{Z}/n\mathbb{Z}$, non nul, et a un représentant de α. Soit $d = \text{PGCD}(a, n)$. Si $d = 1$, α est inversible. Sinon, soit $b = n/d$ et $\beta = [b]$. Alors $\alpha\beta = [a][b] = [ab] = [n] = [0]$. Donc α est un diviseur de zéro. ■

Proposition 1.25 Soit p un nombre premier. Alors tous les éléments non nuls de $\mathbb{Z}/p\mathbb{Z}$ sont inversibles.

Démonstration. Soit $\alpha \in \mathbb{Z}/p\mathbb{Z}$, non nul, et a son représentant canonique. Alors $\text{PGCD}(a, p) = 1$ car $0 < a < p$ et que p est premier. Donc α est inversible. ■

Théorème 1.26 *(petit théorème de Fermat)* Soit p un nombre premier, et $0 < a < p$. Alors $a^{p-1} \equiv_p 1$.

R On peut définir l'exponentiation sur les éléments de $\mathbb{Z}/n\mathbb{Z}$ en notant $\alpha^k = \alpha \times \cdots \times \alpha$ avec k termes. Le petit théorème de Fermat s'écrit alors : pour tout $\alpha \in \mathbb{Z}/p\mathbb{Z}$, $\alpha^{p-1} = [1]$.

Démonstration. On effectue la preuve directement dans $\mathbb{Z}/p\mathbb{Z}$. Soit $\alpha \in \mathbb{Z}/p\mathbb{Z}$, non nul. Pour tout $\beta \in \mathbb{Z}/p\mathbb{Z}$ non nul, $\alpha\beta \neq [0]$ (car il n'existe pas de diviseur de zéro). De plus, $\alpha\beta = \alpha\gamma$ implique $\beta = \gamma$ en multipliant des deux côtés par l'inverse de α. Donc $\{\alpha\beta : \beta \in \mathbb{Z}/p\mathbb{Z}^x\} = \{[1], [2], \ldots, [p-1]\}$. En prenant le produit des deux ensembles, on obtient donc

$$\prod_{\beta \in \mathbb{Z}/p\mathbb{Z}^\times} \alpha\beta = \prod_{\beta \in \mathbb{Z}/p\mathbb{Z}^\times} \beta.$$

En factorisant les α et en multipliant par l'inverse de $\prod_{\beta \in \mathbb{Z}/p\mathbb{Z}^\times} \beta$, on trouve $\alpha^{p-1} = [1]$. ■

R Les opérations de $\mathbb{Z}/n\mathbb{Z}$ permettent de calculer *comme dans* $\mathbb{Z}$, en remplaçant simplement les additions, soustractions et multiplications par les mêmes opérations suivies d'une *réduction modulo* n.
Dans $\mathbb{Z}/p\mathbb{Z}$ où p est premier, on peut inverser tout élément non nul grâce à InverseMod, ce qui permet de diviser deux entiers. On peut donc calculer *comme dans* $\mathbb{Q}$ *ou dans* $\mathbb{R}$.
On verra dans la partie suivante des structures telles que $\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z}$ qui permettent l'addition, la soustraction et la multiplication sont appelées des *anneaux*, et des structures telles que $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{Z}/p\mathbb{Z}$ qui permettent en plus l'inversion ou la division sont appelées des *corps*.

Exercice 1.7. Montrer que le petit théorème de Fermat permet de décrire un nouvel algorithme d'inversion de a modulo p. Estimer sa complexité et la comparer à celle d'InverseMod. *Se rappeler de l'algorithme d'exponentiation rapide vu dans d'autres cours...*

1.3 Résolutions d'équations modulaires

Théorème 1.27 Si $\text{PGCD}(a,n)=1$, alors $az \equiv_n az'$ si et seulement si $z \equiv_n z'$.
Plus généralement, si $d=\text{PGCD}(a,n)$, $az \equiv_n az'$ si et seulement si $z \equiv_{n/d} z'$.

Démonstration. Pour le premier point, le plus simple est de le réécrire directement dans $\mathbb{Z}/n\mathbb{Z}$: si α est inversible, alors $\alpha\zeta=\alpha\zeta'$ si et seulement si $\zeta=\zeta'$. C'est évident, en multipliant par α^{-1}.

Si $d=\text{PGCD}(a,n)$, a/d et n/d sont des entiers et $\text{PGCD}(a/d,n/d)=1$. De plus $az \equiv_n az'$ signifie qu'il existe k tel que $az=az'+kn$. Donc $(a/d)z=(a/d)z'+k(n/d)$. Autrement dit, $(a/d)z \equiv_{n/d} (a/d)z'$. On peut donc appliquer le point précédent. ■

Théorème 1.28 Soit $a,\ b \in \mathbb{Z}$, $n \in \mathbb{Z}_{>0}$, et $d=\text{PGCD}(a,n)$. L'ensemble des solutions de l'équation $az \equiv_n b$ où z est l'inconnue est

- vide si d ne divise pas b ;
- une classe d'équivalence modulo n/d sinon.

Démonstration. On montre que si l'ensemble des solutions n'est pas vide, alors d divise b (c'est donc la contraposée du premier point). En effet, soit z_0 une solution. Alors il existe k tel que $az_0=b+kn$. Comme d divise a et n, il divise $az_0-kn=b$.

L'algorithme suivant calcule une solution à l'équation, si d divise b.

Algorithme 1.29 – RésolutionÉquationLinéaire(a,b,n)

Entrée : trois entiers a, b et n
Sortie : une solution de l'équation $az \equiv_n b$ si elle existe, une erreur sinon

1. $d \leftarrow \text{PGCD}(a,n)$
2. Si $b \bmod d \neq 0$: renvoyer une erreur « l'équation n'a pas de solution »
3. $(a',b',n') \leftarrow (a/d, b/d, n/d)$ *(divisions exactes)*
4. Renvoyer $b' \times \text{InverseMod}(a',n') \bmod n'$

On reprend les notations de l'algorithme. Par construction, a' et n' sont premiers entre eux, donc il existe un inverse de a' modulo n', que l'on note c'. L'entier renvoyé est $z_0=b'c' \bmod n'$. Il existe donc $k \in \mathbb{Z}$ tel que $z_0=b'c'+kn'$. Donc $az_0=ab'c'+akn'=a'bc'+a'kn$ car $a=a'd$, $b'=b/d$ et $n'=n/d$. Comme $a'c' \equiv_{n'} 1$, il existe aussi ℓ tel que $a'c'=1+\ell n'$. Donc, puisque $b=b'd$ et $n'=n/d$,

$$az_0=a'bc'+a'kn=b(1+\ell n')+a'kn=b+b'\ell n+a'kn$$

d'où $az_0 \equiv_n b$. Donc l'algorithme renvoie bien une solution de l'équation.

Il reste à montrer que toute solution z_1 est dans la classe d'équivalence de z_0 modulo n', c'est-à-dire $z_1 \equiv_{n'} z_0$. Si z_1 est une solution de l'équation, $az_1 \equiv_n b$, et comme précédemment $a'z_1 \equiv_{n'} b'$. En utilisant l'inverse c' de a' modulo n', on obtient $z_1 \equiv_{n'} c'b'$. Mais $z_0=b'c' \bmod n'$, donc $z_1 \equiv_{n'} z_0$. ■

Théorème 1.30 *(théorème chinois)* Soit $n_1, \ldots, n_k$ des entiers premiers entre eux deux à deux, c'est-à-dire $\text{PGCD}(n_i, n_j) = 1$ pour $i \neq j$, et $a_1, \ldots, a_k$ des entiers quelconques. Alors l'ensemble des solutions du système d'équation

$$\begin{cases} z & \equiv_{n_1} a_1 \\ & \vdots \\ z & \equiv_{n_k} a_k \end{cases}$$

est non vide, et c'est une classe d'équivalence modulo $N = \prod_{i=1}^{k} n_i$.

Démonstration. L'existence d'au moins une solution est donnée par l'algorithme suivant, qui renvoie le représentant canonique de la classe d'équivalence.

Algorithme 1.31 – RestesChinois$((a_1, \ldots, a_k), (n_1, \ldots, n_k))$

Entrée : deux k-uplets d'entiers $(a_1, \ldots, a_k)$ et $(n_1, \ldots, n_k)$ tels que les n_i sont premiers deux à deux

Sortie : le représentant canonique de la classe d'équivalence solution du système $z \equiv_{n_i} a_i$, $1 \leq i \leq k$

1. $N \leftarrow \prod_{i=1}^{k} n_i$
2. Pour $i = 1$ à k : $N_i \leftarrow N/n_i$ *(division exacte)*
3. Pour $i = 1$ à k : $U_i \leftarrow \text{InverseMod}(N_i, n_i)$
4. Renvoyer $\sum_{i=1}^{k} a_i U_i N_i \bmod N$

On démontre que la solution renvoyée vérifie bien le système d'équation. Tout d'abord, l'inversion modulaire est bien possible : puisque n_i est premier avec tous les autres n_j, $\text{PGCD}(n_i, N_i) = 1$. En particulier, $U_i N_i \equiv_{n_i} 1$ pour tout i. Donc $a_i U_i N_i \equiv_{n_i} a_i$. D'autre part, comme N_j est un multiple de n_i pour $j \neq i$, $N_j \equiv_{n_i} 0$ et $a_j U_j N_j \equiv_{n_i} 0$. Ainsi, $\sum_{i=1}^{k} a_i U_i N_i \equiv_{n_i} a_i$.

Soit z_0 la solution renvoyée (comprise entre 0 et $N-1$). Soit $z \equiv_N z_0$. Alors il existe k tel que $z = z_0 + kN = z_0 + kN_i \times n_i$, donc $z \equiv_{n_i} z_0 \equiv_{n_i} a_i$. Donc z est solution du système. Réciproquement, si z est une solution du système, alors $z \equiv_{n_i} a_i \equiv_{n_i} z_0$ pour tout i. Donc n_i divise $z - z_0$. Et puisque les n_i sont premiers entre eux, $N = \prod_i n_i$ divise $z - z_0$. Donc $z \equiv_N z_0$. ∎

Corollaire 1.32 Soit $n_1, \ldots, n_k$ des entiers premiers entre eux deux-à-deux, et $N = n_1 \cdots n_k$. Alors la fonction

$$\begin{aligned} \{0, \ldots, N-1\} &\to \{0, \ldots, n_1 - 1\} \times \cdots \times \{0, \ldots, n_k - 1\} \\ z &\mapsto (z \bmod n_1, \ldots, z \bmod n_k) \end{aligned}$$

est une bijection.

Démonstration. Pour montrer que la fonction est inversible, il suffit de montrer que tout k-uplet $(a_1, \ldots, a_k)$ avec $0 \leq a_i < n_i$ pour tout i admet un unique antécédent $z < N$: c'est l'énoncé du théorème chinois. ∎

2 Structures algébriques

2.1 Groupes, anneaux et corps

Définition 2.1 Un *groupe* est un couple $(G, \star)$ où G est un ensemble et $\star$ une opération binaire, tels que

(i) pour tout $a, b \in G$, $a \star b \in G$ (*opération interne*),
(ii) pour tout $a, b, c \in G$, $a \star (b \star c) = (a \star b) \star c$ (*associativité*),
(iii) il existe $e \in G$ tel que pour tout $a \in G$, $a \star e = e \star a = a$ (*élément neutre*),
(iv) pour tout $a \in G$, il existe $b \in G$ tel que $a \star b = b \star a = e$ (*inverse*).

Un groupe est *abélien* ou *commutatif* si de plus,

(iv) pour tout $a, b \in G$, $a \star b = b \star a$ (*commutativité*).

On parle de groupe *additif* si $\star = +$ et *multiplicatif* si $\star = \times$.

Exercice 2.1.

1. Montrer que $(\mathbb{Z}, +)$, $(\mathbb{R}, +)$, $(\mathbb{Q}, +)$, et $(\mathbb{Z}/n\mathbb{Z}, +)$ sont des groupes additifs.
2. Montrer que $(\mathbb{R}^*, \times)$ et $(\mathbb{Q}^*, \times)$ sont des groupes multiplicatifs.
3. Montrer que $(\mathbb{N}, +)$, $(\mathbb{Z}, \times)$ et $(\mathbb{R}, \times)$ *ne sont pas* des groupes.
4. Montrer que les couples suivants sont des groupes, et préciser s'ils sont abéliens :
   i. $(n\mathbb{Z}, +)$ où $n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$;
   ii. $(\{-1, 1\}, \times)$;
   iii. $(\{0,1\}^n, \otimes)$ (ensemble des mots binaires de longueur n fixée, avec l'opération « ou exclusif bit-à-bit ») ;
   iv. $(S_n, \circ)$ (ensemble des permutations de $\{1, \ldots, n\}$ avec l'opération de composition).
5. Le couple $(\{0,1\}^\star, \cdot)$ de l'ensemble des mots binaires avec l'opération de concaténation est-il un groupe ?

Vocabulaire. Par abus de langage, on dit souvent que « G est un groupe additif » pour dire que $(G, +)$ est un groupe. De même on dit « G est un groupe multiplicatif » pour dire que $(G, \times)$ est un groupe.

R Dans ce texte, on s'intéresse principalement aux groupes abéliens. En particulier, on fait l'hypothèse que le groupe est abélien dès que cela simplifie une notion ou une preuve.

Théorème 2.2 Soit $(G, \star)$ un groupe. Alors G possède un *unique* élément neutre et tout élément possède un *unique* inverse.

Démonstration. Soit e et e' des éléments neutres de G. Alors $e' = e \star e' = e$ car e et e' sont des éléments neutres.

Soit $a \in G$ et supposons que a possède deux inverses b et c. On note toujours e l'élément neutre de G. Alors $b = b \star e$. Or $e = a \star c$ car c est un inverse de a. Par associativité, on a donc $b = b \star (a \star c) = (b \star a) \star c$. Comme $b \star a = e$ et $e \star c = c$, on obtient $b = c$. ■

Notation. Grâce à l'associativité, on peut écrire $a \star b \star c$ sans parenthèse.
Dans un groupe multiplicatif G, l'élément neutre est (souvent) noté 1_G (ou 1 si ça ne cause pas de confusion), et l'inverse d'un élément $g \in G$ est noté g^{-1}. L'opération « $\times$ » est parfois omise ou remplacée par « $\cdot$ » : $a \times b = a \cdot b = ab$. Pour $n \in \mathbb{Z}_{>0}$, on note g^n l'élément $g \times g \times \cdots \times g$ (n

fois). On étend la notation en posant $g^0 = 1_G$ et $g^n = (g^{-1})^{-n}$ si $n < 0$. Enfin, on utilise la notation $\prod_{i=1}^{k} a_i = a_1 \times a_2 \times \cdots \times a_k$.
Dans un groupe additif G, l'élément neutre est (souvent) noté 0_G (ou 0) et l'inverse de $g \in G$ est noté $-g$. Pour $n \in \mathbb{Z}_{>0}$, on note $n \cdot g$ l'élément $g + g + \cdots + g$ (n fois). On étend la notation en posant $0 \cdot g = 0_G$ et $n \cdot g = (-n) \cdot (-g)$ si $n < 0$. Enfin, on utilise la notation $\sum_{i=1}^{k} a_i = a_1 + a_2 + \cdots + a_k$.

Théorème 2.3 Soit G un groupe. Alors pour tout $a, b, c \in G$,

(i) $a \star b = a \star c$ implique $b = c$,
(ii) l'équation $a \star x = b$ a une unique solution $x \in G$,
(iii) l'inverse de $a \star b$ est $b' \star a'$ où a' est l'inverse de a et b' l'inverse de b,
(iv) si a' est l'inverse de a, alors a est l'inverse de a'.

R Ce théorème devient intuitivement évident si on le réécrit dans le langage des groupes additifs, ou des groupes multiplicatifs.

Démonstration. (i) Puisque a est inversible, on peut mutliplier l'équation $a \star b = a \star c$ par l'inverse de a pour obtenir $a = b$.
(ii) L'unique solution est $x = a' \star b$ où a' est l'inverse de b : en multipliant l'équation par a', on obtient que x est solution si et seulement si $x = a' \star b$.
(iii) On a $(a \star b) \star (b' \star a') = a \star b \star b' \star a' = a \star a' = e$ (avec e l'élément neutre), et de même $(b' \star a') \star (a \star b) = e$.
(iv) Il suffit d'écrire la définition d'inverse. ■

Proposition 2.4 Soit G un groupe additif, $a, b \in G$ et $k, \ell \in \mathbb{Z}$. Alors $k \cdot (\ell \cdot a) = (k\ell) \cdot a = \ell \cdot (k \cdot a)$, $(k + \ell) \cdot a = k \cdot a + \ell \cdot a$ et $k \cdot (a + b) = k \cdot a + k \cdot b$.

R Dans l'énoncé précédent, certains « + » sont des opérations du groupe G, d'autres sont des additions dans $\mathbb{Z}$.

Démonstration. La notation $\ell \cdot a$ représente une somme de ℓ fois l'élément a : $\ell \cdot a = (a + \cdots + a)$. De même, la notation $k \cdot (\ell \cdot a)$ représente une somme de k fois l'élément $\ell \cdot a$, donc $k \cdot (\ell \cdot a) = (a + \cdots + a) + \cdots + (a + \cdots + a)$ où chaque parenthèse contient ℓ fois l'élément a et il y a k parenthèses. Par associativité, on peut supprimer les parenthèses et on obtient bien $k\ell$ fois l'élément a : donc $k \cdot (\ell \cdot a) = (k\ell) \cdot a$.
Les autres égalités se prouvent de la même manière : facile, mais pénible à écrire. ■

Exercice 2.2. Écrire l'énoncé analogue dans un groupe multiplicatif.

Définition 2.5 L'*ordre* d'un groupe est son nombre d'éléments, qui est soit un entier strictement positif, soit $+\infty$. Un groupe d'ordre fini est appelé un *groupe fini*.

Théorème 2.6 *(théorème de Lagrange, version 1)* Soit G un groupe abélien fini d'ordre n, noté multiplicativement. Alors pour tout $g \in G$, $g^n = 1_G$.

Démonstration. Soit $g \in G$. On considère les éléments de la forme gh avec $h \in G$. Si $gh_1 = gh_2$, alors $h_1 = h_2$. Donc tous les gh pour $h \in G$ sont deux-à-deux distincts. Autrement dit, l'ensemble $\{gh : h \in G\}$ est égal à l'ensemble G lui-même. On effectue le produit de chacun des deux ensembles, ce qui conduit à l'égalité

$$\prod_{h\in G} h = \prod_{h\in G} (gh).$$

En utilisant la commutativité, le membre de droite se réécrit $g^n \prod_{h\in G} h$. D'où $g^n = 1_G$. ■

R Le théorème Lagrange est très légèrement plus général, et valable pour un groupe non nécessairement abélien. Ce sera l'objet de la *version 2* présentée dans la partie 2.2.

Exercice 2.3. Comparer la preuve précédente à celle du petit théorème de Fermat.

Définition 2.7 Un *anneau* (commutatif) est un triplet $(A, +, \times)$ où A est un ensemble et $+$ et $\times$ sont deux opérations binaires, internes à A, tels que

(i) $(A, +)$ est un groupe abélien ;
(ii) l'opération $\times$ est associative, commutative, et A possède un neutre pour $\times$;
(iii) $\times$ est distributive sur $+$: pour tout $a, b, c \in A$, $a \times (b + c) = a \times b + a \times c$.

Un *corps* est un anneau $(K, +, \times)$ dont tout élément non nul est inversible pour $\times$.

R Un anneau $(A, +, \times)$ est donc un corps si et seulement si $(A^*, \times)$ est un groupe abélien. *Attention, on note ici $A^* = A \setminus \{0\}$, qu'on ne confondra pas avec $A^\times$ qui est l'ensemble des inversibles (pour $\times$) de A. Donc A est un corps si et seulement si $A^* = A^\times$.*

Notation. Dans un anneau, le neutre pour $+$ est noté 0 et le neutre pour $\times$ est noté 1. Le signe « $\times$ » est souvent omis ou remplacé par « $\cdot$ ».

Exercice 2.4.

1. Montrer que $(\mathbb{Z}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{Q}, +, \times)$ et $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ sont des anneaux.
2. Montrer que $(\mathbb{R}, +, \times)$ et $(\mathbb{Q}, +, \times)$ sont des corps, mais pas $(\mathbb{Z}, +, \times)$.
3. Montrer que $(n\mathbb{Z}, +, \times)$ n'est pas un anneau.
4. Montrer que $((\mathbb{Z}/n\mathbb{Z})^\times, +, \times)$ n'est pas un anneau.

Définition 2.8 Soit $(A, +, \times)$ un anneau. Un élément $a \in A$ non nul est un *diviseur de zéro* s'il existe $b \in A$ non nul tel que $ab = 0$.
Un anneau sans diviseur de zéro est appelé *anneau intègre*.

R Un corps est un anneau intègre. En effet, si a est inversible, alors $ab = 0$ implique $a^{-1}ab = 0$ donc $b = 0$.

Exercice 2.5.

1. Montrer que $\mathbb{Z}$, $\mathbb{Q}$ et $\mathbb{R}$ sont des anneaux intègres.
2. Montrer que $\mathbb{Z}/n\mathbb{Z}$ est intègre si et seulement si n est premier.

§ **Le cas $\mathbb{Z}/n\mathbb{Z}$**

Théorème 2.9 Soit $n > 0$. Alors

(i) $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe d'ordre n ;
(ii) $(\mathbb{Z}/n\mathbb{Z}^\times, \times)$ est un groupe multiplicatif ;
(iii) $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau ;
(iv) $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un corps si et seulement si n est premier.

Démonstration.

(i) Cela a été démontré, sans ce vocabulaire, dans la partie 1.2.
(ii) Presque tout a été démontré dans la partie 1.2. Le seul point à vérifier est la stabilité de $\mathbb{Z}/n\mathbb{Z}^\times$ par multiplication : si α et β sont inversibles, alors $\alpha\beta$ admet $\beta^{-1}\alpha^{-1}$ comme inverse, donc $\alpha\beta$ est inversible.
(iii) Cela se déduit de (i), et des propriétés des opérations + et × dans $\mathbb{Z}/n\mathbb{Z}$.
(iv) Cela revient à dire que tout élément non nul de $\mathbb{Z}/n\mathbb{Z}$ est inversible (pour ×) si et seulement si n est premier, ce qu'on a déjà démontré.

■

Définition 2.10 Soit $n > 0$. L'ordre de $(\mathbb{Z}/n\mathbb{Z})^\times$ est noté $\varphi(n)$. La fonction φ s'appelle l'*indicatrice d'Euler*.

Proposition 2.11 Soit $n = \prod_{i=1}^{k} p_i^{e_i}$ la décomposition de n en facteurs premiers. Alors

$$\varphi(n) = \prod_{i=1}^{k} (p_i - 1) p_i^{e_i - 1} = n \cdot \prod_{i=1}^{k} (1 - \frac{1}{p_i}).$$

Démonstration. On commence par les cas faciles. Premièrement, si $n = p$ est premier, tous les éléments non nuls de $\mathbb{Z}/p\mathbb{Z}$ sont inversibles donc $\varphi(p) = p-1$. Si $n = p^e$ où p est premier, les éléments inversibles de $\mathbb{Z}/p^e\mathbb{Z}$ sont ceux dont le représentant canonique a est premier avec p^e. Or être premier avec p^e équivaut à ne pas être divisible par p. Les multiples de p inférieurs à p^e sont les kp avec $0 \leq k < p^{e-1}$. Donc $\varphi(p^e) = p^e - p^{e-1}$.

On démontre maintenant que φ est *multiplicative* : si $\text{PGCD}(m, n) = 1$, alors $\varphi(mn) = \varphi(m)\varphi(n)$, ce qui suffit à conclure. Cela découle du théorème chinois. On considère la fonction $z \mapsto (z \bmod m, z \bmod n)$. On montre qu'elle fournit une bijection entre les éléments inversibles modulo mn et les couples (a, b) où a est inversible modulo m et b est inversible modulo n. Soit z inversible modulo mn, d'inverse z'. Alors $zz' = 1 + kmn$ pour un certain k. Donc en particulier $zz' \equiv_m 1$ et $z \bmod m$ est donc inversible (d'inverse $z' \bmod m$) modulo m. De même, $z \bmod n$ est inversible modulo n. Réciproquement, supposons que $a = z \bmod m$ est inversible modulo m, d'inverse a' et $b = z \bmod n$ est inversible modulo n, d'inverse b'. Par le théorème chinois, on construit $z' < mn$ tel que $z' \equiv_m a'$ et $z' \equiv_n b'$. Alors $zz' \equiv_m aa' \equiv_m 1$ et $zz' \equiv_n bb' \equiv_n 1$. Or il $y = 1$ est l'unique solution $< mn$ du système $y \equiv_m 1$ et $y \equiv_n 1$. Autrement dit, $zz' \equiv_{mn} 1$ donc z est inversible modulo mn. Comme la fonction $z \mapsto (z \bmod m, z \bmod n)$ est une bijection, les ensembles de départ et d'arrivée ont la même taille, ce qui démontre que $\varphi(mn) = \varphi(m)\varphi(n)$. ■

2.2 Sous-groupes et idéaux

Définition 2.12 Un *sous-groupe* d'un groupe $(G, \star)$ est un groupe $(H, \star)$ tel que $H \subset G$.

R Un groupe est toujours un sous-groupe de lui-même.
On peut définir de manière similaire des notions de *sous-anneau* et *sous-corps*, mais elles ne seront pas utiles dans ce texte. On définit après la notion d'*idéal* dans un anneau, qui est plus utile que celle de sous-anneau.

Exercice 2.6.

1. Montrer que $(n\mathbb{Z}, +)$ est un sous-groupe de $(\mathbb{Z}, +)$ pour tout $n > 0$. Trouver une condition pour que $(n\mathbb{Z}, +)$ soit un sous-groupe de $(m\mathbb{Z}, +)$, pour n, $m > 0$.
2. Montrer que $(\mathbb{Q}^*, \times)$ est un sous-groupe de $(\mathbb{R}^*, \times)$.

Proposition 2.13 Soit $(G, \times)$ un groupe, et $a \in G$. L'ensemble $\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$ est un sous-groupe de G, appelé *sous-groupe engendré par* a.

Démonstration. L'ensemble $\langle a \rangle$ contient le neutre ($n = 0$). Tout élément est inversible (en prenant a^{-n}). Et $a^m a^n = a^{m+n}$ donc l'ensemble est stable par $\times$. ∎

Définition 2.14 Un *groupe (multiplicatif) cyclique* est un groupe $(G, \times)$ tel qu'il existe $g \in G$ tel que $G = \langle g \rangle$. De même, un *groupe (additif) cyclique* est un groupe $(G, +)$ tel qu'il existe $g \in G$ tel que $G = \{n \cdot g : n \in \mathbb{Z}\}$. Dans les deux cas, l'élément g est un *générateur* de G.

Exercice 2.7. Montrer que $(\mathbb{Z}, +)$ est cyclique.

Définition 2.15 Soit G un groupe, et $a \in G$. L'*ordre de* a est l'ordre du sous-groupe cyclique $\langle a \rangle$.

Exercice 2.8.

1. Quel est l'ordre de $[1]_n$ dans le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$? Et son ordre dans $((\mathbb{Z}/n\mathbb{Z})^\times, \times)$?
2. Calculer l'ordre de $[2]_7$ et $[3]_7$ dans le groupe $(\mathbb{Z}/7\mathbb{Z}^\times, \times)$. Lequel des deux est générateur du groupe ?

R L'ordre d'un élément $a \in G$ (groupe multiplicatif) est le plus petit $k > 0$ tel que $a^k = 1$. En effet, si $a^k = 1$, alors $\langle a \rangle$ contient au plus k éléments. Et réciproquement, si $\langle a \rangle$ contient k éléments, alors a^0, a^1, …, a^{k-1} sont tous distincts.

Lemme 2.16 Soit $(G, \times)$ un groupe abélien (noté multiplicativement), H un sous-groupe de G et $\equiv_H$ la relation sur G définie par $x \equiv_H y$ si $xy^{-1} \in H$. Alors $\equiv_H$ est une relation d'équivalence. La classe d'équivalence d'un élément $x \in G$ est $[x]_H = \{xh : h \in H\}$. De plus, si $a \equiv_H a'$ et $b \equiv_H b'$, alors $ab \equiv_H a'b'$.

Démonstration. On montre d'abord que $\equiv_H$ est une relation d'équivalence : $x \equiv_H x$ car $xx^{-1} = 1$ et que H contient le neutre (réflexivité) ; si $x \equiv_H y$, alors $xy^{-1} \in H$, donc $yx^{-1} = (xy^{-1})^{-1} \in H$, donc $y \equiv_H x$ (symétrie) ; si $x \equiv_H y$ et $y \equiv_H z$, alors xy^{-1} et yz^{-1} sont dans H, donc $xz^{-1} = xy^{-1}yz^{-1} \in H$

et $x \equiv_H z$ (transitivité). On remarque ensuite que $x \equiv_H y$ si et seulement s'il existe $h \in H$ tel que $x = yh$. Donc la classe d'équivalence de x est bien $\{xh : h \in H\}$.

Enfin, écrivons $a = a'h$ et $b = b'k$ avec $h, k \in H$. Alors $ab = (a'h)(b'k) = (a'b')(hk)$. Comme H est un groupe, $hk \in H$ donc $ab \equiv_H a'b'$. ■

Définition 2.17 Soit $(G, \times)$ un groupe abélien (noté multiplicativement), et H un sous-groupe de G. Le *groupe quotient* de G par H est l'ensemble G/H des classes $[a]_H$ pour $a \in G$, avec la multiplication définie par $[a]_H \times [b]_H = [a \times b]_H$.

R On retrouve les notations et le vocabulaire pour $\mathbb{Z}/n\mathbb{Z}$, si on remplace la congruence modulo n « $\equiv_n$ » par « $\equiv_{n\mathbb{Z}}$ ».

Théorème 2.18 Soit $(G, \times)$ un groupe abélien et H un sous-groupe de G. Alors G/H est un groupe abélien d'ordre est $|G|/|H|$.

Démonstration. La définition affirme que G/H est un groupe, ce qu'on commence par démontrer. L'associativité de $\times$ vient directement de celle dans G. La classe $[1]_H$ est bien neutre pour $\times$ car $[a]_H \times [1]_H = [a \times 1]_H = [a]_H$. Et toute classe est inversible car l'inverse de $[a^{-1}]_H \times [a]_H = [a \times a^{-1}]_H = [1]_H$.

Pour l'ordre du groupe, on montre que chaque classe contient exactement $|H|$ éléments, ce qui revient à dire que si $ah = ah'$ pour $h, h' \in H$, alors $h = h'$. Et ce résultat vient simplement de l'inversibilité de a. Ainsi, chaque classe ayant exactement $|H|$ éléments, le nombre de classes est $|G|/|H|$. ■

Théorème 2.19 *(théorème de Lagrange, version 2)* Soit $(G, \times)$ un groupe et H un sous-groupe de G. Alors l'ordre de H divise l'ordre de G.

Démonstration. La preuve précédente suffit si G est abélien : G/H est un groupe avec $|G|/|H|$ éléments, donc $|G|/|H|$ est un entier ! La preuve dans le cas non abélien, quasiment identique, est omise. ■

Exercice 2.9.

1. Réécrire le lemme 2.16, la définition 2.17 et les deux théorèmes qui suivent, ainsi que les preuves, dans le langage des groupes additifs.
2. Soit $G = \mathbb{Z}/6\mathbb{Z}$ et $H = \{[0]_6, [3]_6\}$.
   i. Montrer que H est un sous-groupe de G.
   ii. Définir l'ensemble G/H.
   iii. Écrire la table d'addition de G/H.

Définition 2.20 Soit $(A, +, \times)$ un anneau. Un *idéal* de A est un sous-ensemble I de A tel que $(I, +)$ est un groupe et tel que pour tout $x \in I$ et $a \in A$, alors $ax \in I$.

Exercice 2.10. Montrer que pour tout $n > 0$, $n\mathbb{Z}$ est un idéal de $(\mathbb{Z}, +, \times)$.

Lemme 2.21 Soit $(A, +, \times)$ un anneau, I un idéal de A et $\equiv_I$ la relation définie sur A par $a \equiv_I b$ si $a - b \in I$. Alors $\equiv_I$ est une relation d'équivalence, dont les classes d'équivalence sont les

$[a]_I = \{a + x : x \in I\}$. De plus, si $a \equiv_I a'$ et $b \equiv_I b'$, $a + b \equiv_I a' + b'$ et $ab \equiv_I a'b'$.

Démonstration. Quasiment tout le lemme est une version additive du lemme 2.16, puisque I est en particulier un sous-groupe additif de A. Il ne reste qu'à démontrer que $a \equiv_I a'$ et $b \equiv_I b'$ impliquent $ab \equiv_I a'b'$. On écrit $a = a' + x$ et $b = b' + y$ avec $x, y \in I$. Alors $ab = (a' + x)(b' + y) = a'b' + a'y + b'x + xy$. Par définition d'un idéal, $a'y$, $b'x$ et xy sont tous dans I, et leur somme également. Donc $ab \equiv_I a'b'$. ■

Définition 2.22 Soit $(A, +, \times)$ un anneau et I un idéal de A. L'*anneau quotient* A/I est l'ensemble des classes modulo I, avec l'addition et la multiplication définies par $[a]_I + [b]_I = [a + b]_I$ et $[a]_I \times [b]_I = [ab]_I$.

R On vérifie que l'anneau quotient est effectivement un anneau : l'aspect groupe additif vient du fait que A est un groupe additif et I en est un sous-groupe ; les propriétés d'associativité, commutativité et distributivité de $\times$ héritent de celles provenant de A ; le neutre pour $\times$ est $[1]_I$.

§ Le cas $\mathbb{Z}/n\mathbb{Z}$

Théorème 2.23 Les sous-groupes additifs de $\mathbb{Z}$ et ses idéaux sont les $n\mathbb{Z}$ pour $n \geq 0$.

Démonstration. Le fait que les $n\mathbb{Z}$ soient des groupes additifs et des idéaux est laissé en exercice (facile).

Soit G un sous-groupe additif de $\mathbb{Z}$. Si $G = \{0\}$, il est bien de la forme $n\mathbb{Z}$ avec $n = 0$. On suppose que $G \neq \{0\}$ et on note n son plus petit élément strictement positif. Puisque G est un sous-groupe, il contient tous les multiples de n, donc $n\mathbb{Z} \subset G$. Réciproquement, soit $g \in G$. En effectuant une division euclidienne, on écrit $g = nq + r$ avec $0 \leq r < n$. Alors $nq = n + \cdots + n \in G$, et $r = g - nq \in G$. Or n a été choisi minimal dans G, donc $r = 0$ et n divise g. Autrement dit, $g \in n\mathbb{Z}$, et donc $G \subset n\mathbb{Z}$.

On a donc montré que tout sous-groupe additif est de la forme $n\mathbb{Z}$. Puisqu'un idéal est en particulier un sous-groupe additif, on obtient la deuxième partie de l'énoncé. ■

Théorème 2.24 Soit $n > 0$. Alors

(i) $\mathbb{Z}/n\mathbb{Z}$ est un groupe additif et un anneau ;
(ii) $(\mathbb{Z}/n\mathbb{Z}, +)$ est cyclique, et ses générateurs sont les $[m]_n$ tels que $\text{PGCD}(m, n) = 1$.

Démonstration. (i) Cela découle du fait que les $n\mathbb{Z}$ sont des sous-groupes additifs et des idéaux de $\mathbb{Z}$.

(ii) Pour $0 \leq m < n$, soit $\langle m \rangle = \{k \cdot [m]_n : k \in \mathbb{Z}\}$. L'égalité $k \cdot [m] = \ell \cdot [m]$ est équivalente à $km \equiv_n \ell m$. Si $d = \text{PGCD}(m, n)$, cette égalité est équivalente à $k \equiv_{n/d} \ell$. Donc $\langle m \rangle$ contient exactement n/d éléments. Ainsi, $[m]$ est générateur si et seulement si $d = 1$. Donc $\mathbb{Z}/n\mathbb{Z}$ est cyclique (car $\text{PGCD}(1, n) = 1$ pour tout n).

■

Théorème 2.25 Soit $n > 0$. Les sous-groupes additifs de $\mathbb{Z}/n\mathbb{Z}$ et ses idéaux les ensembles de la forme $m \cdot \mathbb{Z}/n\mathbb{Z} = \{m \cdot \alpha : \alpha \in \mathbb{Z}/n\mathbb{Z}\}$ où m divise n.

Démonstration. Le fait qu'on définisse ainsi des sous-groupes additifs et des idéaux est laissé en exercice. On va montrer qu'un sous-groupe additif est forcément de la forme $m \cdot \mathbb{Z}/n\mathbb{Z}$, ce qui impliquera le résultat pour les idéaux.

Soit G un sous-groupe additif de $\mathbb{Z}/n\mathbb{Z}$. Si $G = \{[0]\}$ le résultat est trivial. Sinon, soit $H = \{z \in \mathbb{Z} : [z] \in G\}$. On vérifie que H est un sous-groupe de $\mathbb{Z}$: il contient le neutre et si a, $b \in H$, alors $[a]$, $[b] \in G$ donc $[a]+[b] = [a+b] \in G$ et $-[a] = [-a] \in G$, donc $a+b$ et $-a \in H$. Donc $H = m\mathbb{Z}$ pour un certain m. Or $G = \{[z] : z \in H\}$, donc $G = \{[mk] : k \in \mathbb{Z}\} = \{m \cdot [k] : k \in \mathbb{Z}\} = m \cdot \mathbb{Z}/n\mathbb{Z}$. De plus, $n \in H = m\mathbb{Z}$ donc m divise n. ■

2.3 Morphismes

§ Morphismes de groupes

Définition 2.26 Soit $(G, \star)$ et $(H, *)$ deux groupes. Un *morphisme* de G dans H est une fonction $\rho : G \to H$ *compatible* avec les opérations de groupe : pour tout a, $b \in G$, $\rho(a \star b) = \rho(a) * \rho(b)$. L'*image* du morphisme ρ est le sous-ensemble $\rho(G) = \{\rho(a) : a \in G\} \subset H$ des images d'éléments de G par f. Le *noyau* du morphisme est le sous-ensemble $\ker \rho = \{a : a \in G, \rho(a) = e_H\} \subset G$ des éléments de G dont l'image est le neutre de H.

Exercice 2.11.

1. Montrer que si H est un sous-groupe de G, alors l'application identité $id : H \to G$ est un morphisme de groupe. Déterminer son image et son noyau.
2. Soit H un sous-groupe d'un groupe abélien G. Montrer que la fonction $\rho : G \to G/H$ définie par $\rho(a) = [a]_H$ est un morphisme de groupe dont le noyau est $\ker \rho = H$.
3. Soit $m \in \mathbb{Z}$. Montrer que la fonction $n \mapsto mn$ est un morphisme de $\mathbb{Z}$ dans $m\mathbb{Z}$. Déterminer son noyau.

Proposition 2.27 Soit $\rho : G \to H$ un morphisme de groupe. Alors l'image par ρ du neutre de G est le neutre de H, et l'image par ρ de l'inverse d'un élément $g \in G$ est l'inverse de $\rho(g)$.

Démonstration. Pour simplifier, on note les deux groupes additivement. On calcule de deux manières $\rho(0_G + 0_G)$. Puisque ρ est un morphisme, c'est égal à $\rho(0_G) + \rho(0_G)$. Mais comme 0_G est le neutre de G, c'est aussi égal à $\rho(0_G)$. Donc $\rho(0_G) = \rho(0_G) + \rho(0_G)$. D'où, en simplifiant par $\rho(0_G)$, $\rho(0_G) = 0_H$.

De même, $\rho(a-a)$ est égal à $\rho(a) + \rho(-a)$ car ρ est un morphisme, et à $\rho(0_G)$ car $a - a = 0_G$. Comme $\rho(0_G) = 0_H$, $\rho(a) + \rho(-a) = 0_H$, donc $\rho(-a) = -\rho(a)$. ■

Théorème 2.28 Soit $\rho : G \to G'$ et $\rho' : G' \to G''$ deux morphismes de groupes. Alors leur composition $\rho' \circ \rho : G \to G''$ est un morphisme de groupes.

Démonstration. Pour simplifier, notons tous les groupes multiplicativement. Alors pour a, $b \in G$, $\rho' \circ \rho(ab) = \rho'(\rho(ab)) = \rho'(\rho(a)\rho(b)) = \rho'(\rho(a)) \cdot \rho'(\rho(b)) = \rho' \circ \rho(a) \cdot \rho' \circ \rho(b)$. ■

Définition 2.29 Un morphisme de groupe $\rho : G \to H$ est un *isomorphisme* si c'est une fonction bijective, c'est-à-dire s'il existe une fonction $\rho^{-1} : H \to G$ telle que $\rho \circ \rho^{-1}$ est l'identité. Dans ce cas, les deux groupes G et H sont dits *isomorphes*, ce qu'on note $G \simeq H$.
Si $G = H$, alors ρ est un *automorphisme*.

Proposition 2.30 Si $\rho : G \to H$ est un isomorphisme, alors ρ^{-1} également.

Démonstration. Il faut montrer que ρ^{-1} est bien un morphisme. On note G et H multiplicativement. Pour $a, b \in H$, on a $\rho(\rho^{-1}(a)\rho^{-1}(b)) = \rho(\rho^{-1}(a))\rho(\rho^{-1}(b)) = ab$. Donc $\rho^{-1}(a)\rho^{-1}(b) = \rho^{-1}(ab)$. ■

Exercice 2.12.

1. Soit m et n deux entiers premiers entre eux, et $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ l'application définie par $f([a]_n) = [ma]_n$ pour tout a. Montrer que f est un automorphisme de $\mathbb{Z}/n\mathbb{Z}$.
2. Soit $G = \mathbb{Z}/6\mathbb{Z}$ et $H = \{[0]_6, [3]_6\}$.
   i. Montrer que H est un sous-groupe de G.
   ii. Montrer que G/H est isomorphe à $\mathbb{Z}/3\mathbb{Z}$.

Théorème 2.31 Soit $\rho : G \to G'$ un morphisme de groupe. Alors

(i) si H est un sous-groupe de G, $\rho(H)$ est un sous-groupe de G' ;
(ii) si H' est un sous-groupe de G', $\rho^{-1}(H')$ est un sous-groupe de G ;
(iii) $\ker\rho$ est un sous-groupe de G et $\rho(G)$ un sous-groupe de G' ;
(iv) ρ est injectif si et seulement si $\ker\rho = \{e_G\}$.

Démonstration. On note les groupes additivement.

(i) On sait que $\rho(H)$ contient le neutre et l'inverse de chacun de ses éléments, et puisque $\rho(a) + \rho(b) = \rho(a+b) \in \rho(H)$, c'est un sous-groupe de G'.
(ii) La démonstration est quasiment identique : puisque $\rho(0_G) = 0_{G'}$, $\rho^{-1}(H')$ contient le neutre ; puisque $-\rho(a) = \rho(-a)$, $\rho^{-1}(H)$ contient l'inverse de chaque élément ; et de même $\rho^{-1}(H)$ est stable par addition.
(iii) C'est une conséquence de $\ker\rho = \rho^{-1}(\{0'_G\})$ et des points (i) et (ii).
(iv) Si ρ est injectif, alors $\rho^{-1}(\{0_{G'}\})$ contient (au plus) un élément et on sait que 0_G en fait partie, donc $\ker\rho = \{0_G\}$. Si ρ n'est pas injectif, il existe $a \neq b$ tels que $\rho(a) = \rho(b)$, d'où $\rho(a-b) = 0_{G'}$. Donc $a - b \in \ker\rho$.

■

Théorème 2.32 Soit $\rho : G \to G'$ un morphisme de groupes, de noyau K et d'image H'. Alors $G/K \simeq H'$, *via* l'isomorphisme

$$\begin{aligned} \bar{\rho} : G/K &\to H' \\ [a]_K &\to \rho(a). \end{aligned}$$

Démonstration. Il faut déjà démontrer que $\bar{\rho}$ est bien définie, c'est-à-dire que si $[a]_K = [b]_K$, alors $\rho(a) = \rho(b)$. Pour cela, notons les deux groupes multiplicativement. On sait que $[a]_K = [b]_K$ équivaut à l'existence de $k \in K$ tel que $a = bk$, et donc $\rho(a) = \rho(b)\rho(k)$. Comme $k \in K = \ker\rho$, $\rho(k) = 1_{G'}$ donc $\rho(a) = \rho(b)$.

On note ensuite que $\bar{\rho}$ est injective : en effet, si $\rho(a) = \rho(b)$, $\rho(a)\rho(b)^{-1} = \rho(ab^{-1}) = 1_{G'}$ donc $ab^{-1} \in K$ et $[a]_K = [b]_K$. Puisque par définition, H' est l'image de G par ρ, $\bar{\rho}$ est aussi surjective, donc c'est isomorphisme. ■

§ Morphismes d'anneaux

Définition 2.33 Soit A et B deux anneaux. Un *morphisme d'anneau* de A dans B est nune fonction $\rho : A \to B$ *compatible* avec les opérations d'anneaux :

(i) pour $a, b \in A$, $\rho(a+b) = \rho(a) + \rho(b)$;
(ii) pour $a, b \in A$, $\rho(a \times b) = \rho(a) \times \rho(b)$;
(iii) $\rho(0_A) = 0_B$ et $\rho(1_A) = \rho(1_B)$.

L'*image* de ρ est $\rho(A) = \{\rho(a) : a \in A\}$ et son *noyau* est $\ker \rho = \{a \in A : \rho(a) = 0_B\}$.
Un *isomorphisme* d'anneau est un morphisme bijectif $\rho : A \to B$. Les anneaux A et B sont alors *isomorphes*, ce qu'on note $A \simeq B$.

R Un morphisme d'anneaux de A dans B est en particulier un morphisme de groupes additifs.

Proposition 2.34 La composition de deux morphismes d'anneaux est un morphismes d'anneaux. Si ρ est un isomorphisme d'anneaux, sa réciproque ρ^{-1} également.

Théorème 2.35 Soit $\rho : A \to B$ un morphisme d'anneaux. Alors

(i) si I est un idéal de A, alors $\rho(I)$ est un idéal de $\rho(A)$;
(ii) si J est un idéal de $\rho(A)$, alors $\rho^{-1}(J)$ est un idéal de A (en particulier, $\ker \rho$ est un idéal de A).

Démonstration. Pour la partie *additive*, cela découle du résultat sur les morphismes de groupes. Il reste à vérifier la partie *multiplicative* : le produit d'un élément de l'anneau et d'un élément de l'idéal appartient à l'idéal.

(i) Soit $\rho(x) \in \rho(I)$ et $\rho(a) \in \rho(A)$. Alors $\rho(a)\rho(x) = \rho(ax)$. Comme $ax \in I$, $\rho(a)\rho(x) \in \rho(I)$.
(ii) Soit $x \in \rho^{-1}(J)$ et $a \in A$. Alors comme $\rho(ax) = \rho(a)\rho(x)$ et $\rho(x) \in J$, $\rho(a)\rho(x) \in J$. Donc $ax \in \rho^{-1}(J)$.

■

Proposition 2.36 Soit $\rho : A \to B$ un isomorphisme d'anneau. Alors

(i) $a \in A$ est un diviseur de zéro ssi $\rho(a)$ est un diviseur de zéro ;
(ii) $a \in A$ est inversible ssi $\rho(a)$ est inversible ;
(iii) ρ induit un isomorphisme $A^\times \to B^\times$ entre les groupes des inversibles de A et B.

Démonstration. On démontre uniquement (iii). D'après (ii), ρ envoie des inversibles vers des inversibles, et sa réciproque également. ■

Proposition 2.37 Soit $A, B_1, \ldots, B_k$ des anneaux, et $\rho_i : A \to B_i$ un morphisme d'anneaux pour tout i. Alors $B_1 \times \cdots \times B_k$ est un anneau (avec les opérations composante par composante), et $\rho : A \to B_1 \times \cdots \times B_k$ défini par $\rho(a) = (\rho_1(a), \ldots, \rho_k(a))$ est un morphisme d'anneaux.

Démonstration. Laissée en exercice. ■

Théorème 2.38 Soit $\rho : A \to B$ un morphisme d'anneaux, de noyau K et d'image L. Alors $A/K \simeq L$, *via* l'isomorphisme

$$\begin{aligned}\bar{\rho} : A/K &\to L \\ [a]_K &\to \rho(a).\end{aligned}$$

Démonstration. Laissée en exercice : elle est quasiment identique au cas des groupes. ■

§ **Le cas $\mathbb{Z}/n\mathbb{Z}$**

Théorème 2.39 Soit $(G, \star)$ un groupe abélien cyclique. Alors $(G, \star)$ est isomorphe à

(i) $(\mathbb{Z}, +)$ s'il est d'ordre infini ;
(ii) $(\mathbb{Z}/n\mathbb{Z}, +)$ s'il est d'ordre n.

Démonstration. Soit a un générateur de G, que l'on note multiplicativement. On considère la fonction $\rho : \mathbb{Z} \to G$ définie par $\rho(z) = a^z$. Comme $\rho(z + z') = a^{z+z'} = a^z \cdot a^{z'}$, c'est un morphisme de groupes. Comme a est générateur, ρ est surjective. Il y a alors deux cas possibles.

(i) Si $\ker \rho = \{0\}$, ρ est injective, donc est un isomorphime et $G \simeq \mathbb{Z}$.
(ii) Sinon, $\ker \rho$ est un sous-groupe de $\mathbb{Z}$, donc de la forme $n\mathbb{Z}$ pour un $n > 1$. Donc $\bar{\rho} : \mathbb{Z}/n\mathbb{Z} \to G$ définie par $\bar{\rho}([z]_n) = \rho(z) = a^z$ est un isomorphisme.

■

Théorème 2.40 *(théorème chinois, nouvelle version)* Soit $n_1, \ldots, n_k$ des entiers premiers deux-à-deux, et $N = \prod_{i=1}^{k} n_i$. La fonction

$$\begin{aligned}\rho : \mathbb{Z}/N\mathbb{Z} &\to \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z} \\ [a]_N &\to ([a]_{n_1}, [a]_{n_2}, \ldots, [a]_{n_k})\end{aligned}$$

est un isomorphisme d'anneaux.
De plus, ρ induit un isomorphisme de groupes (multiplicatifs) $\mathbb{Z}/N\mathbb{Z}^\times \simeq \mathbb{Z}/n_1\mathbb{Z}^\times \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}^\times$.

Démonstration. Pour la première partie, il suffit de vérifier que l'énoncé précédent du (corollaire du) théorème chinois est exactement équivalent au fait que ρ soit un isomorphisme d'anneaux. Pour la seconde, on l'a déjà démontrée pour le calcul de l'indicatrice d'Euler. ■

Théorème 2.41 Soit p un nombre premier. Alors le groupe $\mathbb{Z}/p\mathbb{Z}^\times$ est cyclique, d'ordre $p - 1$.

Démonstration. L'ordre de $\mathbb{Z}/p\mathbb{Z}^\times$ est par définition $\varphi(p)$, qui vaut $p - 1$ comme on l'a déjà vu. Pour démontrer que $\mathbb{Z}/p\mathbb{Z}^\times$ est cyclique, on doit montrer qu'il existe un générateur. La démonstration est assez longue. On la découpe en trois affirmations.

Affirmation. Pour tout $d \geq 0$, un *polynôme de degré d a au plus d racines dans $\mathbb{Z}/p\mathbb{Z}$*, c'est-à-dire que toute équation du type $\lambda_d \zeta^d + \cdots + \lambda_0 = 0$ a au plus d solutions.

► On remarque d'abord que si α est solution, $\lambda_d\alpha^d + \cdots + \lambda_0 = 0$. En soustrayant cette égalité à l'équation d'origine, on obtient

$$\lambda_d(\zeta^d - \alpha^d) + \cdots + \lambda_1(\zeta - \alpha) = 0$$

(en particulier les λ_0 s'annulent). Dans cette équation, on peut alors *factoriser* $(\zeta-\alpha)$: en effet, on vérifie en développant le produit que pour tout t, $\zeta^t - \alpha^t = (\zeta-\alpha)(\zeta^{t-1}+\zeta^{t-2}\alpha+\cdots+\zeta\alpha^{t-2}+\alpha^{t-1})$. Autrement dit, on a montré que si α est solution, alors l'équation peut s'écrire $(\zeta-\alpha)(\mu_{d-1}\zeta^{d-1}+\cdots+\mu_0) = 0$, où les μ_i sont calculés à partir des λ_i et de α. On en déduit une preuve par récurrence. Si $d = 0$, le résultat est évident. Si on le suppose au rang $d-1$, il y a deux cas : soit il n'y a aucune solution et c'est gagné. Soit il existe une solution α et on peut réécrire l'équation sous la forme $(\zeta-\alpha)(\mu_{d-1}\zeta^{d-1}+\cdots+\mu_0) = 0$. Une solution de cette équation est soit α, soit une solution de l'équation $\mu_{d-1}\zeta^{d-1} + \cdots + \mu_0 = 0$ car $\mathbb{Z}/p\mathbb{Z}$ n'a pas de diviseur de zéro. Par hypothèse de récurrence, cette équation a au plus $d-1$ solutions, d'où le résultat. ◄

Affirmation. Soit $N_d(p)$ le nombre d'éléments d'ordre exactement d dans $\mathbb{Z}/p\mathbb{Z}^\times$. Si $N_d(p) > 0$, alors $N_d(p) = \varphi(d)$.

► Soit α un élément d'ordre d (donc on suppose $N_d(p) > 0$). Puisque $(\alpha^i)^d = (\alpha^d)^i = 1$ pour tout i, on en déduit que α^0, α^1, α^2, …, α^{d-1} sont des racines de $\zeta^d - 1 = 0$. Par le fait précédent, et puisque les α^i sont distincts, ce sont toutes les racines de ce polynômes. Donc tout élément d'ordre d est de la forme α^i. De plus, l'ordre de α^i est le plus petit entier k tel que $\alpha^{ki} = 1$, donc c'est le plus petit entier tel que ki est multiple de d : c'est donc $d/\text{PGCD}(d,i)$. Ainsi, α^i est d'ordre d ssi $\text{PGCD}(d,i) = 1$. Donc le nombre de i tels que α^i est d'ordre d est égal au nombre de $i < d$ premiers avec d : c'est donc $\varphi(d)$. ◄

Affirmation. Pour tout n, $\sum_{d|n}\varphi(d) = n$.

► On considère les n fractions $\frac{1}{n}$, $\frac{2}{n}$, …, $\frac{n}{n}$. Si on écrit $\frac{k}{n}$ sous forme irréductible, on obtient $\frac{k}{n} = \frac{i}{d}$ avec $\text{PGCD}(i,d) = 1$ et $d|n$. Réciproquement, chaque fraction $\frac{i}{d}$ avec $\text{PGCD}(i,d) = 1$ et $d|n$ est bien irréductible, et égale à une fraction $\frac{k}{n}$ (en multipliant i et d par n/d). Ainsi, chaque dénominateur d (qui divise n) apparaît exactement $\varphi(d)$ fois (une fois pour chaque i tel que $\text{PGCD}(i,d) = 1$), et le nombre total de fraction est $\sum_{d|n}\varphi(d) = n$. ◄

On en déduit enfin le résultat. Premièrement, comme tout élément de $\mathbb{Z}/p\mathbb{Z}^\times$ est d'un ordre qui divise $p-1$, $\sum_{d|p-1}N_d(p) = p-1$. Deuxièmement, $N_d(p) = \varphi(d)$ si $N_d(p) > 0$ donc $\sum_{d|p-1}N_d(p) \leq \sum_{d|p-1}\varphi(d)$. Finalement, $\sum_{d|p-1}\varphi(d) = p-1$. On en déduit que $N_d(p) = \varphi(d)$ pour tout d qui divise $p-1$, donc en particulier que $N_{p-1}(p) > 0$: il existe donc un élément γ d'ordre $p-1$ dans $\mathbb{Z}/p\mathbb{Z}^\times$. Par définition, γ^0, γ^1, …, γ^{p-2} sont des éléments distincts, et il y en a $p-1$: tout élément de $\mathbb{Z}/p\mathbb{Z}^\times$ est donc une puissance de γ, ce qui revient à dire que γ est générateur. ■

3 Algèbre linéaire

Définition 3.1 Soit $A \in \mathbb{K}^{m\times n}$ et $B \in \mathbb{K}^{n,p}$ deux matrices, et $v \in \mathbb{K}^n$ un vecteur. Alors

- $A \cdot v \in \mathbb{K}^m$ est le vecteur défini par $(A\cdot v)_i = \sum_{j=1}^n A_{i,j}v_j$ pour $1 \leq i \leq m$;
- $v \cdot B \in \mathbb{K}^p$ est le vecteur défini par $(v\cdot B)_k = \sum_{j=1}^n v_j B_{j,k}$ pour $1 \leq k \leq p$;
- $(A\cdot B) \in \mathbb{K}^{m\times p}$ est la matrice définie par $(A\cdot B)_{i,k} = \sum_{j=1}^n A_{i,j}B_{j,k}$ pour $1 \leq i \leq m$ et $1 \leq k \leq p$.

R Un vecteur, dans notre formalisme, n'a pas d'orientation. Cependant, on peut toujours voir un vecteur $v \in \mathbb{K}^n$ comme une matrice de $\mathbb{K}^{1\times n}$ (« vecteur ligne ») ou de $\mathbb{K}^{n\times 1}$ (« vecteur colonne »). On vérifie que les définitions précédentes de $A \cdot v$ et $v \cdot B$ sont cohérentes avec la définition de multiplication de matrices, en voyant v comme un vecteur colonne ou ligne, respectivement.

Proposition 3.2 Le produit de matrices est associatif, mais pas commutatif.

Définition 3.3 Une matrice *carrée* $P \in \mathbb{K}^{n\times n}$ est *inversible* s'il existe $Q \in \mathbb{K}^{n\times n}$ telle que $P \cdot Q = I_n$, où $(I_n)_{i,i} = 1$ pour tout i, et $(I_n)_{i,j} = 0$ si $i \neq j$. On note $Q = P^{-1}$.

Proposition 3.4 Si $Q = P^{-1}$, alors $P = Q^{-1}$. Si P et Q sont deux matrices inversibles de mêmes dimensions, alors $P \cdot Q$ est une matrice inversible, d'inverse $Q^{-1} \cdot P^{-1}$.

3.1 Résolution de systèmes linéaires

Définition 3.5 Un *système linéaire* de m équations à n inconnues sur un corps $\mathbb{K}$ est défini par un couple (A, b) où $A \in \mathbb{K}^{m\times n}$ est une matrice et $b \in \mathbb{K}^m$ un vecteur, qui représentent les équations

$$(\mathscr{S}) = \begin{cases} A_{11}x_1 + A_{12}x_2 + \cdots + A_{1n}x_n = b_1 \\ A_{21}x_1 + A_{22}x_2 + \cdots + A_{2n}x_n = b_2 \\ \vdots \\ A_{m1}x_1 + A_{m2}x_2 + \cdots + A_{mn}x_n = b_m \end{cases}$$

où $x_1, \ldots, x_n$ sont les inconnues. Une *solution* du système $(\mathscr{S})$ est un vecteur $s = (s_1, \ldots, s_n)$ tel que chaque équation soit satisfaite, c'est-à-dire tel que $A \cdot s = b$.
Deux systèmes sont *équivalents* s'ils ont le même ensemble de solutions.

Vocabulaire. Une équation est dite *vide* si tous les coefficients des variables valent 0. Autrement dit, une équation est vide si la ligne correspondant dans la matrice ne contient que des 0. Le *pivot* d'une équation non vide (ou d'une ligne non vide de la matrice) est le coefficient non nul d'indice minimal (*i.e.* $A_{i,j} \neq 0$ tel que $A_{i,\ell} = 0$ pour $\ell < j$).

Notation. On note souvent $A \cdot x = b$ un système (A, b).

Lemme 3.6 Soit (A, b) un système linéaire sur un corps $\mathbb{K}$. Alors pour tout $k \neq i$ et $\lambda \neq 0$, le système (A', b') obtenu en ajoutant λ fois la ligne i à la ligne k est équivalent à (A, b).
Formellement, $A'_{\ell,j}$ est défini pour tout j par $A'_{k,j} = A_{k,j} + \lambda A_{i,j}$ et $A'_{\ell,j} = A_{\ell,j}$ pour $\ell \neq k$, et b'_ℓ est défini par $b'_k = b_k + \lambda b_i$ et $b'_\ell = b_\ell$ pour $\ell \neq k$.

Démonstration. Soit $s = (s_1, \ldots, s_n)$ une solution du système (A, b). Alors par définition s satisfait les équations i et k du système. Donc $A'_{k,1}s_1 + \cdots + A'_{k,n}s_n = (A_{k,1} + \lambda A_{i,1})s_1 + \cdots + (A_{k,n} + \lambda A_{i,n})s_n = (A_{k_1}s_1 + \cdots + A_{k,n}s_n) + (A_{i,1}s_1 + \cdots + A_{i,n}s_n) = b_k + \lambda b_i = b'_k$. Donc s est solution du système (A', b'). De même, si s est solution de (A', b'), il est solution de (A, b), d'où l'équivalence. ■

Théorème 3.7 (*algorithme de Gauss*) Soit (A, b) un système linéaire à m équations et n inconnues sur un corps $\mathbb{K}$. On peut calculer en temps $O(mn\min(m,n))$ un système équivalent (A', b') dont la matrice A' est sous *forme échelonnée par lignes* : les lignes vides sont toutes en dessous des lignes non vides, et le *pivot* de chaque ligne non vide se trouve strictement à droite du pivot de la ligne précédente.

Démonstration. L'algorithme de Gauss permet de calculer la forme échelonnée d'un système (A, b).

Algorithme 3.8 – GAUSS(A, b) :

Entrée : un système (A, b) à m équations et n inconnues
Sortie : un système (A', b') équivalent à (A, b), sous forme échelonnée

```
1  (i, j) ← (1, 1)
2  Tant i ≤ m et j ≤ n :
3      i' ← min{k ≥ i : A_{k,j} ≠ 0} ou +∞ si A_{k,j} = 0 pour tout k
4      Si i' = +∞ : j ← j + 1
5      Sinon :
6          Échanger les lignes i et i' de A et de b
7          Pour k = i + 1 à m :
8              λ = A_{k,j} / A_{i,j}
9              Pour ℓ = j à n : A_{k,ℓ} ← A_{k,ℓ} − λ A_{i,ℓ}
10             b_k ← b_k − λ b_i
11         (i, j) ← (i + 1, j + 1)
12 Renvoyer (A, b)
```

Il est clair que cet algorithme termine (puisque i ou j augmente à chaque itération. De plus, la troisième branche du test (le « Sinon ») ne peut être effectué que $\min(m,n)$ fois. Donc le nombre total d'opérations est $O(mn\min(m,n))$.

On veut montrer que le système (A', b') renvoyé est sous forme échelonnée. Pour cela, on démontre qu'à chaque entrée dans la boucle « Tant que », les propriétés suivantes sont respectées : (i) la matrice constituée des lignes 1 à $i-1$ de A' est sous forme échelonnée ; (ii) $A_{k,\ell} = 0$ pour $k \geq i$ et $\ell < j$. Initialement, c'est évident car les conditions n'imposent rien. Supposons donc que les deux conditions sont vérifiées à l'entrée de la boucle. Si la colonne *sous* $A_{i,j}$ est vide, on incrémente j et les propriétés restent vraies : remarquons qu'en particulier, $A_{k,j} = 0$ pour tout $k \geq i$ donc (ii) reste vraie. Sinon, on échange les équations i et i', donc la nouvelle équation i contient son pivot en case j. Puisqu'*in fine* on incrémente i et j, cela démontre que la condition (i) est respectée. De plus, la double boucle a pour effet d'annuler tous les $A_{k,j}$ pour $k > i$ puisqu'on remplace $A_{k,j}$ par $A_{k,j} - A_{k,j}A_{i,j}/A_{i,j} = 0$. Donc (ii) reste vraie après avoir incrémenté i et j.

À la fin de l'algorithme, soit $i > m$ soit $j > n$. Dans le premier cas, la condition (i) montre que la matrice est échelonnée. Dans le second cas, la condition (ii) implique que toutes les dernières lignes sont nulles, et la condition (i) que la matrice est bien échelonnée.

Il reste à montrer que le système représenté est équivalent au système d'origine. En effet, les seules opérations effectuées sur le système sont l'échange de lignes (qui ne change pas les solutions), et la mise à jour de la ligne k en y ajoutant un multiple de la ligne i, ce qui ne change pas non plus les solutions d'après le lemme précédent. ∎

R On peut voir l'algorithme de Gauss directement sur une matrice. À partir d'un système $(A, b) \in \mathbb{K}^{m\times n} \times \mathbb{K}^n$, on crée la *matrice augmentée* $(A|b) \in \mathbb{K}^{m\times(n+1)}$ dont les n premières colonnes sont celles de A et la $(n+1)^{\text{ème}}$ est b. On remarque que dans l'algorithme de Gauss, les opérations effectuées sur le vecteur b sont les mêmes que celles effectuées sur les colonnes de A. On applique donc simplement l'algorithme sur la matric augmentée, en ignorant les instructions concernant le vecteur b. La seule chose à laquelle faire attention est de ne jamais chercher de pivot dans la dernière colonne : autrement dit, il faut sortir de la boucle principale dès que $j = n$, même si la matrice augmentée possède $n+1$ colonnes.

Théorème 3.9 (*algorithme de Gauss-Jordan*) Soit (A, b) un système linéaire à m équations et n inconnues sur un corps $\mathbb{K}$. On peut calculer en temps $O(mn\min(m, n))$ un système équivalent (A', b') dont la matrice A' est sous *forme échelonnée réduite par lignes* : le système est échelonné, et chaque pivot vaut 1 et est le seul élément non nul dans sa colonne.

Démonstration. L'algorithme de Gauss-Jordan applique d'abord l'algorithme de Gauss pour transformer le système de départ en système échelonné. La deuxième partie de l'algorithme consiste à remplacer les pivots par des 1, puis à effacer les éléments non nuls au dessus de chaque pivot.

Algorithme 3.10 – GaussJordan(A, b) :

Entrée : un système (A, b) à m équations et n inconnues
Sortie : un système (A', b') équivalent à (A, b), sous forme échelonnée réduite

```
1  (A', b') ← Gauss(A, b)
2  Pour i = 1 à m :
3     j ← indice du pivot de la ligne i de A'
4     Pour ℓ = j + 1 à n : A'_{i,ℓ} ← A'_{i,ℓ} / A'_{i,j}
5     b'_ℓ ← b'_ℓ / A'_{i,j}
6     A'_{i,j} ← 1
7     Pour k = 1 à i − 1 :
8        λ = A'_{k,j}
9        Pour ℓ = j à n : A'_{k,ℓ} ← A'_{k,ℓ} − λ A'_{i,ℓ}
10       b'_k ← b'_k − λ b'_i
11 Renvoyer (A', b')
```

On remarque que l'algorithme s'arrête dans la même complexité que l'algorithme de Gauss. En particulier, chaque pivot « coûte » $O(mn)$ à traiter et il y en a au plus $\min(m, n)$. Le fait que le système renvoyé soit équivalent à l'ancien vient encore du même lemme, puisqu'on ne fait qu'ajouter des multiples d'une ligne à une autre, et du fait que multiplier une ligne par une constante *non nulle* ne change pas les solutions. Enfin, le caractère échelonné réduit est assez évident : chaque pivot est remplacé par 1, et on l'utilise ensuite pour supprimer les éléments non nuls *au dessus* de lui. On remarque que par définition de forme échelonnée, les éléments sous un pivot sont déjà nuls. ■

R Comme pour l'algorithme de Gauss, on peut voir l'algorithme de Gauss-Jordan directement sur la matrice augmentée $(A|b)$.

Théorème 3.11 (*résolution de système linéaire*) L'ensemble des solutions d'un système linéaire (A, b) de m équations à n inconnues dans $\mathbb{K}$ peut être calculé en temps $O(mn\min(m,n))$. Il est soit vide, soit de la forme $\{s + \sum_{k=1}^{t} \lambda_i v_i : \lambda_1, \ldots, \lambda_t \in \mathbb{K}\}$ où s, v_1, …, $v_t \in \mathbb{K}^n$. En particulier, le nombre de solutions est soit 0, soit 1, soit $|\mathbb{K}|^t$ (infini si $|\mathbb{K}|$ est infini).

Démonstration. À nouveau, on utilise un algorithme.

Algorithme 3.12 – RésolutionSystèmeLinéaire(A, b) :

Entrée : un système (A, b) de m équations à n inconnues
Sortie : une description de son ensemble de solutions

$(A', b') \leftarrow$ GaussJordan(A, b)
Avec une boucle de $i = 1$ à m, remplir les trois variables suivantes :
  $n_p \leftarrow$ nombre de pivots dans A'
  $pos \leftarrow$ tableau de m entiers : $pos[i]$ est la position du pivot en ligne i ($+\infty$ si inexistant)
  $piv \leftarrow$ tableau de n entiers : $piv[j] = i$ si x_j est pivot en ligne i ($+\infty$ si non pivot)
S'il existe une ligne vide ($pos[i] = +\infty$) telle que $b'_i \neq 0$: renvoyer $\emptyset$

$s \leftarrow$ vecteur de dimension n initialisé à 0 *(solution particulière)*
$V \leftarrow$ matrice de dimension $n \times (n - n_p)$ initialisée à 0 *(variables libres)*
$k \leftarrow 0$ *(compteur des variables libres)*
Pour $j = 1$ à n :
  Si $piv[j] \neq +\infty$: $s_j \leftarrow b'_{piv[j]}$
  Sinon :
    Pour $i = 1$ à m tel que $A'_{i,j} \neq 0$: $V_{pos[i],k} \leftarrow -A'_{i,j}$
    $V_{j,k} \leftarrow 1$
    $k \leftarrow k + 1$
Renvoyer s, V

La terminaison de l'algorithme est claire. On considère le système (A', b') sous forme échelonnée réduite. S'il existe une ligne de 0 dans A' et que le coefficient correspondant de b' est non nul, le système contient une équation $0 = b'_i$: il n'y a aucune solution possible. Sinon, si la ligne i contient son pivot en colonne ℓ, elle représente l'équation $x_\ell + A'_{i,\ell+1} x_{\ell+1} + \cdots + A'_{i,n} x_n = b'_i$, où l'on sait que les $A'_{i,j}$ non nuls correspondent à des variables qui ne sont pas pivot. Cela signifie en particulier que le vecteur s défini par $s_\ell = b'_i$ si le pivot de la $i^{\text{ème}}$ ligne est en colonne ℓ, et $s_\ell = 0$ si aucun pivot n'est en colonne ℓ, est bien solution du système. Ensuite, si x_ℓ n'est pas pivot, on définit v par $v_j = -A'_{i,\ell}$ si le pivot en ligne i est x_j, $v_\ell = 1$ et $v_j = 0$ pour les autres j. Alors $(A \cdot v)_t = \sum_{j=1}^{n} A'_{t,j} v_j$. Si on fixe un terme $A'_{t,j} v_j$ de cette somme, il y a plusieurs cas :

— soit $j = \ell$, auquel cas $A'_{t,j} v_j = A'_{t,\ell}$ car $v_\ell = 1$;
— soit x_j n'est pas pivot (et $j \neq \ell$), et $v_j = 0$ donc le terme est nul ;
— soit x_j est pivot, donc le terme vaut $-A'_{t,j} A_{i,\ell}$: puisque x_j est pivot en ligne i, $A'_{t,j} = 0$ si $t \neq i$ et $A'_{i,j} = 1$, donc le terme vaut soit 0 soit $-A_{t,\ell}$.

En faisant la somme, il ne reste donc deux termes non nul : si $j = \ell$, on obtient $A'_{t,\ell}$ et si $j = t$, on obtient $-A'_{t,\ell}$. La somme est donc nulle.

Autrement dit, si on définit un vecteur $s' = s + \lambda v$ pour λ quelconque, on a $A' \cdot s' = A' \cdot s + \lambda A' \cdot v = b$ donc s' est toujours solution. On a donc démontré que les vecteurs de la forme $s + \sum_k \lambda_k v_k$ où les v_k sont les colonnes de V sont solutions du système.

Il y a donc trois cas :

(i) soit il existe une ligne vide de A *en face* d'un élément non nul de b et il n'y aucune solution ;
(ii) soit la matrice M ne contient aucune colonne (toutes les variables sont pivot) et s est l'unique solution ;
(iii) soit l'ensemble des solutions est infini (si $\mathbb{K}$ est infini).

■

Corollaire 3.13

— Si $m < n$ (*système sous-déterminé*), l'ensemble des solutions est soit vide, soit contient $|\mathbb{K}|^t$ éléments pour $t \geq 1$.
— Si $b = \vec{0}$ (*système homogène*), l'ensemble des solutions est non vide.
— Si $m < n$ et $b = \vec{0}$, l'ensemble des solutions contient $|\mathbb{K}|^t$ éléments.

3.2 Vision matricielle

Définition 3.14 Deux matrices $A, B \in \mathbb{K}^{m \times n}$ sont dites *équivalentes par lignes* s'il existe une matrice inversible $M \in \mathbb{K}^{m \times m}$ telle que $B = M \cdot A$.

Lemme 3.15 Soit $A \in \mathbb{K}^{m \times n}$. On peut calculer en temps $O(mn \min(m, n))$ une matrice échelonnée par lignes, équivalente par lignes à A, ainsi qu'une matrice échelonnée réduite par lignes, équivalente par lignes à A.

Démonstration. Il suffit de montrer que les algorithmes de Gauss et Gauss-Jordan produisent des matrices équivalentes par lignes à A. Pour cela, on note en premier lieu qu'on effectue trois types de transformation sur A dans ces algorithmes :

(I) permuter deux lignes ;
(II) ajouter un multiple d'une ligne à une autre ;
(III) multiplier une ligne par un scalaire.

Chaque transformation revient à multiplier A par une matrice *élémentaire* inversible.

(I) Pour $k \neq \ell$, soit $P^{k,\ell}$ la matrice $m \times m$ définie par

$$P^{k,\ell}_{i,j} = \begin{cases} 1 & \text{si } (i,j) = (k,\ell) \text{ ou } (i,j) = (\ell,k), \\ 1 & \text{si } i = j \notin \{k,\ell\}, \text{ et} \\ 0 & \text{sinon.} \end{cases}$$

Alors pour tout i, j, $(P^{k,\ell} \cdot A)_{i,j} = \sum_{t=1}^{m} P^{k,\ell}_{i,t} A_{t,j}$. Si $i \notin \{k,\ell\}$, $P^{k,\ell}_{i,t} = 1$ uniquement si $i = t$, donc $(P^{k,\ell} \cdot A)_{i,j} = A_{i,j}$. Pour $i = k$, $P^{k,\ell}_{k,t} = 1$ uniquement pour $t = \ell$, donc $(P^{k,\ell} \cdot A)_{k,j} = A_{\ell,j}$. De même, $(P^{k,\ell} \cdot A)_{\ell,j} = A_{k,j}$. Ainsi $P^{k,\ell} \cdot A$ est la matrice A dont on a permuté les lignes k et ℓ.

(II) Pour $k \neq \ell$, soit $M_\lambda^{k,\ell}$ la matrice $m \times m$ définie par

$$(M_\lambda^{k,\ell})_{i,j} = \begin{cases} \lambda & \text{si } (i,j) = (k,\ell), \\ 1 & \text{si } i = j, \\ 0 & \text{sinon.} \end{cases}$$

Donc $M_\lambda^{k,\ell}$ est une matrice identité avec une entrée λ en case (k,ℓ). Donc $M_\lambda^{k,\ell} \cdot A$ est la matrice A dans laquelle on a ajouté λ fois la $\ell^{\text{ème}}$ ligne à la $k^{\text{ème}}$.

(III) Soit S_λ^k la matrice identité dont le coefficient (k,k) est remplacé par λ. Alors $S_\lambda^k \cdot A$ est la matrice A dont la $k^{\text{ème}}$ ligne est multipliée par λ.

Ainsi, toutes les transformations des algorithmes de Gauss et Gauss-Jordan correspondent à multiplier A à gauche par une matrice $P^{k,\ell}$, $M_\lambda^{k,\ell}$ ou S_λ^k. Les algorithmes dans leur entièreté reviennent à multiplier A par un produit de ces matrices. Il reste à montrer que chacune de ces matrices est inversible, ce qui impliquera que leur produit l'est également (car l'inverse de $P \cdot Q$ est $Q^{-1}P^{-1}$). D'après l'action de $P^{k,\ell}$ sur une matrice, on voit aisément qu'elle est sa propre inverse. L'action de $M_\lambda^{k,\ell}$ est d'ajouter λ fois la $\ell^{\text{ème}}$ ligne à la $k^{\text{ème}}$: son inverse est donc $M_{-\lambda}^{k,\ell}$. Enfin, l'inverse de S_λ^k est $S_{1/\lambda}^k$ (quand λ est non nul). ■

Théorème 3.16 Soit $A \in \mathbb{K}^{m\times n}$. Alors il existe une unique matrice E échelonnée réduite par lignes, équivalente par lignes à A.

Démonstration. L'existence de E est assurée par l'algorithme de Gauss-Jordan. Montrons alors l'unicité par récurrence sur n. Si $n = 1$, le résultat est évident. Supposons maintenant $n > 1$.

Supposons qu'il existe deux matrices E et E', toutes deux équivalentes par lignes à A et sous forme échelonnée réduite. Soit $A_\star$, $E_\star$ et $E'_\star$ les matrices obtenues en supprimant leur dernière colonne respective. Il est clair que $E_\star$ et $E'_\star$ sont également échelonnée réduites, et équivalentes par lignes à $A_\star$. Par hypothèse de récurrence, elles sont donc égales. Autrement dit, E et E' ne peuvent différer que par leur dernière colonne. Si $E \neq E'$, il existe une ligne i telle que $E_{i,n} \neq E'_{i,n}$. Soit s un vecteur tel que $A \cdot s = 0$. Comme $E = P \cdot A$ pour une certaine matrice inversible P et $E' = Q \cdot A$ pour une matrice inversible Q, cela implique que $E \cdot s = (P \cdot A) \cdot s = 0$ et $E' \cdot s = (Q \cdot A) \cdot s = 0$. Donc $(E - E') \cdot s = 0$. Or $E_\star - E'_\star = 0$, donc en particulier $(E_{i,n} - E'_{i,n})s_n = 0$. On en déduit que $s_n = 0$ dans toute solution de $A \cdot x = 0$. En particulier, les colonnes n de E et E' doivent comporter un pivot, donc n'avoir chacune qu'un coefficient non nul. Puisque seules les dernières lignes d'une forme échelonnée sont nulles, le pivot est dans la même ligne dans les deux matrices. Donc $E = E'$. ■

Théorème 3.17 Soit $A \in \mathbb{K}^{m\times n}$. Alors il existe trois matrices P, L et E telles que $A = P \cdot L \cdot E$ où

— $P \in \mathbb{K}^{m\times m}$ est une matrice de permutation ;
— $L \in \mathbb{K}^{m\times m}$ est une matrice *triangulaire inférieure* avec des 1 sur la diagonale ;
— $E \in \mathbb{K}^{m\times n}$ est une matrice sous forme échelon.

Démonstration. Cette factorisation s'obtient via l'algorithme de Gauss. Cet algorithme effectue deux types d'opérations : permuter deux lignes et ajouter un multiple d'une ligne à une autre. De plus, une fois les lignes permutées, l'ajout d'un multiple d'une ligne se fait toujours sur une ligne plus basse. Autrement dit, matriciellement, on multiplie par une matrice $M_\lambda^{k,\ell}$ avec $k > \ell$. Cette matrice est triangulaire supérieure avec des 1 sur la diagonale car sa seule entrée non nulle hors diagonale est

la case (k,ℓ). Ainsi, en notant E la forme échelonnée de A obtenue avec l'algorithme de Gauss, on obtient E en multipliant A à gauche par des $P^{k,\ell}$ (permutations) et des $M_\lambda^{k,\ell}$ (triangulaires inférieures).

On peut réordonner les $P^{k,\ell}$ et $M_\lambda^{k,\ell}$ pour multiplier d'abord par des matrices de permutations, puis des matrices $M_\lambda^{k,\ell}$. Cela revient, algorithmiquement, à faire toutes les permutations de ligne en premier. En effet, si on applique une matrice $M_\lambda^{k,\ell}$ puis une permutation $P^{u,v}$, on peut commencer par permuter les lignes puis appliquer la matrice $M_\lambda^{k',\ell'}$ où k' et ℓ' sont calculés à partir de k, ℓ, u et v.

De cette manière, on montre que U peut être calculée en multipliant A par des matrices de permutations $(P^{k,\ell})$, puis des matrices triangulaires inférieures $(M_\lambda^{k,\ell})$:

$$E = \left(M_{\lambda_s}^{k_s,\ell_s} \cdots M_{\lambda_1}^{k_1,\ell_1}\right) \cdot \left(P^{k'_t,\ell'_t} \cdots P^{k'_1,\ell'_1}\right) \cdot A.$$

Chacune de ces matrices est inversibles. En particulier, $P^{k,\ell}$ est sa propre inverse, et l'inverse de $M_\lambda^{k,\ell}$ est $M_{-\lambda}^{k,\ell}$ est encore triangulaire inférieure. Donc en multipliant l'égalité précédente par les inverses (dans le bon sens), on obtient

$$\left(P^{k'_1,\ell'_1} \cdots P^{k'_t,\ell'_t}\right) \cdot \left(M_{-\lambda_1}^{k_1,\ell_1} \cdots M_{-\lambda_s}^{k_s,\ell_s}\right) \cdot E = A.$$

Le produit des $P^{k,\ell}$ est une matrice de permutation, qu'on note P. Le produit des $M_\lambda^{k,\ell}$ est encore une matrice triangulaire inférieure avec des 1 sur la diagonale, notée L. On a donc démontré que $A = P \cdot L \cdot E$. ■

R Dans la factorisation $A = P \cdot L \cdot E$, la matrice E est échelonnée par lignes, mais pas (nécessairement) réduite. Pour la réduire, il faut encore diviser par les pivots (ce qui ne pose pas de problème), mais ensuite réduire à 0 les entrées au dessus des pivots. Ceci se fait en multipliant par des matrices de la forme $M_\lambda^{k,\ell}$ où $k < \ell$, qui sont donc des matrices triangulaires *supérieures*. On pourrait définir une autre factorisation, faisant intervenir une matrice triangulaire supérieure et la matrice échelonnée réduite, mais elle serait assez peu utile.

3.3 Espaces ligne et colonne, noyau et rang

Définition 3.18 Soit $A \in \mathbb{K}^{m\times n}$. L'*espace ligne* de A est le sous-espace vectoriel de $\mathbb{K}^n$ engendré par les lignes de A. L'*espace colonne* de A est le sous-espace vectoriel de $\mathbb{K}^m$ engendré par les colonnes de A. Le *noyau (à droite)* de A est l'ensemble $\ker A$ des vecteurs $v \in \mathbb{K}^n$ tels que $A \cdot v = 0$.

R Le noyau de A est un espace vectoriel. En effet, si $v, w \in \ker A$ et $\lambda \in \mathbb{K}$, il est clair que $A\cdot(v+\lambda w) = 0$, donc que $v + \lambda w \in \ker A$. L'espace colonne de A est également l'image de l'application linéaire de $\mathbb{K}^n$ dans $\mathbb{K}^m$ définie par $v \mapsto A \cdot v$.

Définition 3.19 Le *rang* d'une matrice $A \in \mathbb{K}^{m\times n}$ est la dimension de son espace colonne.

Lemme 3.20 Le rang de A est égal au nombre de pivots dans une forme échelonnée de A.

Démonstration. On remarque en premier lieu que le nombre de pivot ne dépend pas de la forme échelonnée : de n'importe quelle forme échelonnée, on peut obtenir l'unique forme échelonnée réduite et le nombre de pivots ne change pas dans cette transformation.

On considère la forme échelonnée réduite E de A et M inversible telle que $A = M \cdot E$. Dans la matrice E, seules les p premières lignes sont non nulles, où p est le nombre de pivots. Pour calculer le rang de A, on commence par celui de E. D'après la remarque qui précède, un vecteur de l'espace colonne de E ne peut contenir des coordonnées non nulles que dans ses p premières coordonnées. Autrement dit, cet espace est de dimension au plus p. D'autre part, la sous-matrice de E constituée des colonnes contenant un pivot est une matrice identité sur les p premières lignes et nulle en dessous. Ces p colonnes sont indépendantes et l'espace colonne est de dimension au moins p, donc égale à p.

Finalement, l'action de M ne change pas la dimension car M est inversible. En effet, soit $v_1, \ldots, v_p$ une base de l'espace colonne de E. Alors $M \cdot v_1, \ldots, M \cdot v_p$ est une famille libre de l'espace colonne de A : si la famille était liée, il y aurait une relation de dépendance linéaire $\sum_i \lambda_i M \cdot v_i = 0$, qui se traduirait par la même relation sur les v_i en multipliant par M^{-1}. Donc la dimension de l'espace colonne de A est au moins p. Le même raisonnement appliqué symétriquement montre l'égalité. ■

Théorème 3.21 Soit $A \in \mathbb{K}^{m\times n}$. Le rang de A est l'entier r minimal tel qu'il existe $C \in \mathbb{K}^{m\times r}$ et $R \in \mathbb{K}^{r\times n}$ telles que $A = C \cdot R$.

Démonstration. On commence par montrer que si $A = C \cdot R$, alors le rang de A est au plus r. En effet, soit $v_1, \ldots, v_n$ les colonnes de A, et $w = \sum_{j=1}^{n} \lambda_j v_j$ un élément de son espace colonne. Alors puisque $A = C \cdot R$, chaque colonne de A est une combinaison linéaire des colonnes de C : $A_{i,j} = \sum_k C_{i,k} R_{k,j}$ donc $v_j = \sum_k c_k R_{k,j}$ où c_k est la $k^{\text{ème}}$ colonne de C. Donc $w = \sum_{j,k} \lambda_j R_{k,j} c_k$. Ainsi, tout élément de l'espace colonne est engendré par les colonnes de C. Comme C n'a que r colonnes, le rang de A est au plus R.

On montre maintenant que si r est le rang de A, on peut effectivement trouver C et R comme dans l'énoncé. Soit E la forme échelonnée réduite de A, et M une matrice inversible telle que $A = M \cdot E$. On sélectionne pour R les r premières lignes de E (les seules non nulles) et pour C les r premières colonnes de M. Alors $A = C \cdot R$. On peut préciser aussi comment construire C. En effet, si la $i^{\text{ème}}$ colonne de R contient un pivot en ligne j, on a $R_{i,j} = 1$ et $R_{k,j} = 0$ pour $k \neq i$. Ainsi, puisque $A = C \cdot R$, pour tout k on obtient $A_{k,j} = \sum_\ell C_{k,\ell} R_{\ell,j} = C_{k,i}$. Donc la $i^{\text{ème}}$ colonne de C est la $j^{\text{ème}}$ colonne de A. Avec les r pivots, on obtient les r colonnes de C : ce sont les colonnes de A qui ont un pivot dans la forme échelonnée réduite. ■

Corollaire 3.22 Soit $A \in \mathbb{K}^{m\times n}$ de rang r. Alors il existe trois matrices P, L et E telles que $A = P \cdot L \cdot E$ où

- $P \in \mathbb{K}^{m\times m}$ est une matrice de permutation ;
- $L \in \mathbb{K}^{m\times r}$ est une matrice triangulaire supérieure ;
- $E \in \mathbb{K}^{r\times n}$ est une matrice sous forme échelon.

Démonstration. On considère la factorisation $A = P \cdot L \cdot E$ de la partie précédente. Comme E est constituée de r lignes non nulles puis des lignes nulles, on peut supprimer ses lignes nulles et les colonnes correspondantes dans L. On obtient $A = P \cdot L^\star \cdot E^\star$ avec les bonnes dimensions. ■

Corollaire 3.23 Le rang d'une matrice est également la dimension de son espace ligne.

Démonstration. Soit $A \in \mathbb{K}^{m\times n}$. On remarque que si $w = A \cdot v$, alors $w = v \cdot A^\top$ où $A^\top \in \mathbb{K}^{n\times m}$ est la transposée de A, définie par $A^\top_{j,i} = A_{i,j}$. En effet, $w_i = \sum_j A_{i,j} v_j = \sum_j A^\top_{j,i} v_j = v \cdot A^\top$. Donc l'espace ligne de A est l'espace colonne de $A^\top$.

Or $A = C \cdot F$ si et seulement si $A^\top = F^\top \cdot C^\top$. Ainsi, les rangs de A et $A^\top$ sont les mêmes, ce qui revient à dire que le rang de A est la dimension de son espace colonne. ■

Théorème 3.24 *(théorème du rang)* Soit $A \in \mathbb{K}^{m\times n}$. Alors $\operatorname{rg} A + \dim \ker A = n$.

Démonstration. On considère le système $A \cdot x = 0$. En observant le fonctionnement de l'algorithme de résolution de système linéaire, on remarque que ce système a pour ensemble de solution un espace vectoriel engendré par k vecteurs où k est le nombre de variables libres du système. De plus, ces k vecteurs forment une famille libre puisque seul le vecteur correspondant à la variable x_j a une entrée non nulle en ligne j. Ainsi, on a montré que la dimension du noyau correspond au nombre de variables libres dans le système. D'autre part, le rang de A est son nombre de pivots, donc son nombre de variables liées. Puisque chaque variable est soit libre soit liée, on obtient le résultat. ■

Corollaire 3.25 Soit $A \cdot x = b$ un système. L'ensemble des solutions du système est

(i) vide si b n'appartient pas à l'espace colonne de A ;
(ii) de la forme $s + \ker A$ sinon, où s est un vecteur.

Démonstration. Par définition, si $A \cdot v = b$, b appartient à l'espace colonne de A. Donc pour que le système ait une solution, b doit appartenir à cet espace colonne.

Si c'est le cas, on sait que l'ensemble des solutions est de la forme $\{s + \sum_i \lambda_i v_i : \lambda_i \in \mathbb{K}\}$ où les v_i sont des vecteurs. Il reste donc à montrer qu'ils engendrent exactement $\ker A$. Or puisque $A \cdot s = b$ et $A \cdot (s + v_i) = b$ pour n'importe quel v_i, $A \cdot v_i = 0$: les v_i appartiennent au noyau de A. Mais on a vu précédemment qu'ils sont indépendants et que leur nombre est égal à la dimension du noyau. ■

R On en déduit que si le rang de A est égal à n, il y a au plus une solution. Par contre, si le rang est $< n$, il y a soit aucune solution, soit $|\mathbb{K}|^t$ solutions où $t = n - \operatorname{rg} A$.

3.4 Matrices carrées, déterminant

Définition 3.26 Soit $A \in \mathbb{K}^{n\times n}$. Le *déterminant* de A est défini par $\det A = A_{1,1}$ si $n = 1$, et

$$\det A = \sum_{i=1}^{n} (-1)^{1+i} A_{i,1} \det A^{(i,1)}$$

si $n > 1$, où $A^{(i,j)} \in \mathbb{K}^{(n-1)\times(n-1)}$ est la matrice obtenue en supprimant la ligne i et la colonne j de A.

Proposition 3.27 *On admet* la multiplicativité du déterminant : pour tout A, $B \in \mathbb{K}^{n\times n}$, $\det(A \cdot B) = \det(A)\det(B)$.

Corollaire 3.28 Soit $A \in \mathbb{K}^{n\times n}$ et $A = P \cdot L \cdot E$ avec P une matrice de permutation, L une matrice triangulaire inférieure avec des 1 sur la diagonale et E une forme échelonnée. Alors $\det A = \pm \prod_{i=1}^{n} E_{i,i}$.

Démonstration. D'une part, $\det(A) = \det(P)\det(L)\det(E)$. Ensuite, P possédant exactement un 1 par ligne et colonne, on montre aisément par récurrence que $\det(P) = \pm 1$. On peut ensuite calculer $\det(L) = \sum_i (-1)^{1+i} L_{i,1} \det(L^{(i,1)})$. Comme la matrice $L^{(i,1)}$ pour $i > 1$ possède une ligne de 0, $\det(L^{(i,1)}) = 0$ pour $i > 1$ (à nouveau par une récurrence facile). Donc $\det(L) = L_{1,1}\det(L^{(1,1)}) = \det(L^{(1,1)})$ car $L_{1,1} = 1$. On en déduit par une nouvelle récurrence immédiate que $\det(L) = 1$. Enfin, puisque E est sous forme échelon, elle est en particulier triangulaire supérieure, et le même raisonnement (en plus simple !) montre que $\det(E) = \prod_i E_{i,i}$. ■

Théorème 3.29 Soit $A \in \mathbb{K}^{n\times n}$. Alors les propositions suivantes sont équivalentes :

(a) A est inversible ;
(b) le rang de A est n ;
(c) $\det(A) \neq 0$;
(d) une forme échelonnée de A est triangulaire supérieure avec des éléments non nuls sur la diagonale ;
(e) la forme échelonnée réduite de A est la matrice identité I_n ;
(f) A est un produit de matrices élémentaires $P^{i,j}$, $M_\lambda^{i,j}$, S_λ^i.
(g) $\ker(A) = \{0\}$;
(h) $A \cdot x = 0$ n'a que la solution triviale $x = 0$;
(i) $A \cdot x = b$ a une unique solution pour tout b ;
(j) l'espace colonne de A est $\mathbb{K}^n$;
(k) l'espace ligne de A est $\mathbb{K}^n$.

Démonstration. On est principalement intéressé par l'équivalence (a) $\iff$ (b) $\iff$ (c).

D'une part, (a) $\Rightarrow$ (h) car si A est inversible, $A \cdot x = 0$ implique $A^{-1} \cdot A \cdot x = x = 0$. Par définition, ceci est équivalent à $\ker(A) = \{0\}$, d'où $\mathrm{rg}(A) = n$ par le théorème du rang. Donc (a) $\Rightarrow$ (b).

D'autre part, (b) $\Rightarrow$ (d) car une forme échelonnée doit posséder n pivots. D'après le corollaire précédent, cela implique que $\det(A) \neq 0$ donc (b) $\Rightarrow$ (c).

Enfin, supposons $\det(A) \neq 0$. En écrivant $A = P \cdot L \cdot E$ en utilisant le fait que $\det(A) = \pm \prod_i E_{i,i}$, on en déduit que E est triangulaire supérieure avec des éléments non nuls sur la diagonale. Or une telle matrice est inversible, ainsi que P et L, donc A est inversible. Ainsi (c) $\Rightarrow$ (a).

Les autres équivalences ont déjà été démontrées. ■

Théorème 3.30 *(Borne de Hadamard simplifiée)* Soit $A \in \mathbb{Z}^{n\times n}$. Alors $\det(A) \in \mathbb{Z}$ et $|\det A| \leq n! \cdot M^n$ où $M = \max_{i,j} |A_{i,j}|$.

Démonstration. L'appartenance à $\mathbb{Z}$ est immédiate d'après la définition. On prouve le résultat par récurrence. C'est évident pour $n = 1$. Pour $n > 1$, on a $\det(A) = \sum_i (-1)^{1+i} A_{i,1} \det(A^{(i,1)})$. Donc $|\det A| \leq \sum_i |A_{i,1}||\det(A^{(i,1)})|$. Par récurrence, on obtient $|\det A| \leq nM(n-1)!M^{n-1}$ d'où le résultat. ■

R La *vraie* borne de Hadamard est $\det(A)^2 \leq \prod_j \sum_i |a_{i,j}|^2$, d'où $|\det A| \leq n^{n/2} M^n$. La borne simplifiée implique $|\det A| \leq n^n M^n$. Dans les deux cas, on en déduit que $\det A$ est un entier de $O(n(\log M + \log n))$ bits.

Théorème 3.31 Soit $A \in \mathbb{Z}^{n\times n}$. On peut calculer son déterminant en temps $O(n^4(\log^2 n + \log M(\log n + \log\log M))$.

Démonstration. L'idée est d'utiliser le théorème chinois : si on connaît $\det(A) \bmod p_i$ pour suffisamment de nombres premiers p_i, on peut retrouver $\det(A)$. Il faut adapter un peu le théorème pour travailler avec des nombres négatifs. Cela revient simplement à *représenter* un anneau $\mathbb{Z}/N\mathbb{Z}$ par des entiers positifs et négatifs. Le théorème chinois dit que le système d'équations $z \equiv_{p_i} a_i$ admet comme solution une classe d'équivalence $[a]_N$ où $N = \prod_i p_i$. Ainsi, il existe un unique a entre $-(N-1)/2$ et $(N-1)/2$ qui vérifie le système. Autrement dit, si $\det(A)$ est compris entre $-(N-1)/2$ et $(N-1)/2$, la connaissance de $d_i = \det(A) \bmod p_i$ permet de calculer $\det(A)$.

On en déduit l'algorithme suivant.

Algorithme 3.32 – DéterminantModulaire(A) :

Entrée : Une matrice $A \in \mathbb{Z}^{n\times n}$
Sortie : $\det(A)$

1 $M \leftarrow \max_{i,j} |A_{i,j}|$
2 $B \leftarrow M^n \times n!$
3 $p_1, \ldots, p_k \leftarrow$ nombres premiers tels que $\prod_i p_i > 2B$
4 Pour $i = 1$ à k :
5 $d_i \leftarrow$ Déterminant($A \bmod p_i$)
6 Renvoyer RestesChinois($(d_1, \ldots, d_k), (p_1, \ldots, p_k)$)

Dans cet algorithme, le calcul du déterminant de A modulo p_i est effectué de la manière suivante : on commence par réduire tous les éléments de A modulo p_i, on effectue une élimination de Gauss dans $\mathbb{Z}/p_i\mathbb{Z}$, puis on calcule le produit des éléments diagonaux de la matrice échelon obtenue. La correction de l'algorithme est alors assurée par celles de l'algorithme de Gauss et de RestesChinois.

Pour la complexité, il faut connaître la valeur de k, et la taille des p_i pour savoir le coût des opérations dans $\mathbb{Z}/p_i\mathbb{Z}$. En réalité, on a le choix pour les p_i (l'algorithme n'est pas entièrement spécifié puisque la façon de les choisir ne l'est pas). La seule contrainte est $\prod_i p_i > 2B$. Il y a deux stratégies possibles : soit prendre un unique nombre premier $> 2B$, soit en prendre plusieurs des petits.

Si on prend un unique nombre premier $> 2B$, on effectue un calcul de déterminant dans $\mathbb{Z}/p\mathbb{Z}$. Cela nécessite $O(n^3)$ opérations dans $\mathbb{Z}/p\mathbb{Z}$, et chacune coûte [1] $O(\log^2 p) = O(n^2(\log n + \log M)^2)$. Ainsi, on obtient un algorithme de complexité $O(n^5(\log n + \log M)^2)$.

Une deuxième solution consiste à sélectionner tous les plus petits nombres premiers jusqu'à ce que leur produit dépasse $2B$. Cette solution n'est pas difficile à mettre en pratique, mais plus compliquée à analyser. De plus, ce n'est en pratique pas toujours la meilleure.

La troisième solution est de fixer une taille en bits pour les premiers, et de ne prendre que des nombres de cette taille. Pour que leur produit dépasse $2B$, il suffit d'en prendre k tel que $(2^b)^k > 2B$, c'est-à-dire $k \simeq \log(2B)/b$. Dans ce cas, le coût du calcul est celui de k déterminants dans $\mathbb{Z}/p\mathbb{Z}$ où p possède b bits, donc $O(kn^3b^2) = O(n^4b(\log n + \log M))$. L'idéal est d'avoir b aussi petit que possible. Cependant, il faut qu'il existe suffisamment de nombres premiers de b bits. Or une version explicite du *théorème des nombres premiers* permet d'affirmer qu'il en existe au moins $2^b/b$ (pour $b \geq 4$). Donc il faut que $(2^b)^{2^b/b} > 2B$, c'est-à-dire $2^{2^b} > 2B$ ou encore $b > \log\log B$. Comme $\log B = O(n(\log n + \log M)) = O(n\log(n)\log(M))$, $\log\log B = O(\log n + \log\log M)$. On en déduit la complexité $O(n^4(\log n + \log M)(\log n + \log\log M)) = O(n^4(\log^2 n + \log n \log M + \log M \log\log M))$.

Enfin, il faut être capable de produire des nombres premiers : on admet que le coût est là encore négligeable.Pour conclure, il faut vérifier que les autres étapes ne prennent pas plus de temps. Il faut d'abord calculer $A \bmod p_i$ pour chaque p_i. Le calcul de $a_{i,j} \bmod p$ où p est premier coûte $O(\log a_{i,j} \log p) = O(\log M(\log n + \log\log M))$. Donc le calcul complet est n^2 fois ce coût. Il faut

1. On pourrait faire mieux, en $O(\log p \log\log p)$.

également appliquer l'algorithme RestesChinois qui a aussi un coût plus faible que les calculs de déterminant. Enfin, il faut être capable de produire des nombres premiers : on admet que le coût est là encore négligeable. ■