Algèbre et Arithmétique (LU2MA220)
Sorbonne Université, 2019/2020

Jan Nekovář

1er décembre 2019

On va présenter dans ce polycopié des notions de base de l'arithmétique, des structures algébriques et de la théorie des corps finis.

Pour la plupart, ce texte correspond au cours LU2MA220 "Algèbre et Arithmétique" enseigné à Sorbonne Université en 2019/2020.

La partie arithmétique du cours correspond aux chapitres 1–4, qui sont consacrés aux propriétés de base des nombres premiers et de la divisibilité, l'unicité de décomposition en nombres premiers, l'algorithme d'Euclide, le théorème de Bézout, la théorie de congruences, le théorème d'Euler et quelques applications à la cryptographie.

La partie algébrique du cours correspond aux chapitres 6–8, où l'on introduit des groupes et des anneaux, et certains morceaux des chapitres 9–10, qui sont consacrés à l'étude des anneaux de polynômes et leurs quotients, ce qui permet de construire beaucoup de corps (notamment les corps finis).

Table des matières

1 Entiers, divisibilité, nombres premiers

1.1 Divisibilité, nombres premiers

On introduit dans ce paragraphe les objets principaux de la partie arithmétique du cours.

1.1.1 Notation On note

$$\mathbf{N} := \{0, 1, 2, 3, \ldots\}, \qquad \mathbf{N}_+ := \{1, 2, 3, \ldots\}, \qquad \mathbf{Z} := \{0, \pm 1, \pm 2, \pm 3, \ldots\}$$
$$\mathbf{Q} := \left\{ \tfrac{a}{b} \mid a, b \in \mathbf{Z},\, b \neq 0 \right\}$$

respectivement, l'ensemble des entiers, des entiers relatifs et des nombres rationnels.

Soient $a, b \in \mathbf{C}$ t $X, Y \in \mathbf{C}$; on note

$$X + Y := \{x + y \mid x \in X,\, y \in Y\}, \qquad aX = Xa := \{aX \mid x \in X\}.$$

En particulier, $aX + bY = \{ax + by \mid x \in X,\, y \in Y\}$.

1.1.2 Décomposition en facteurs premiers Une petite expérience numérique suggère que des entiers se décomposent d'une manière unique en termes de facteurs premiers :

$1 = 1$	$7 = \boxed{7}$	$13 = \boxed{13}$
$2 = \boxed{2}$	$8 = 2 \cdot 2 \cdot 2 = 2^3$	$14 = 2 \cdot 7$
$3 = \boxed{3}$	$9 = 3 \cdot 3 = 3^2$	$15 = 3 \cdot 5$
$4 = 2 \cdot 2 = 2^2$	$10 = 2 \cdot 5$	$16 = 2 \cdot 2 \cdot 2 \cdot 2 = 2^4$
$5 = \boxed{5}$	$11 = \boxed{11}$	$17 = \boxed{17}$
$6 = 2 \cdot 3$	$12 = 2 \cdot 2 \cdot 3 = 2^2 \cdot 3$	$18 = 2 \cdot 3 \cdot 3 = 2 \cdot 3^2$

Les entiers $2, 3, 5, 7, 11, 13, 17 \ldots$ sont des **nombres premiers** — on ne peut pas les décomposer.

1.1.3 Définition. Un entier $a > 1$ est un **nombre premier** si $a \neq bc$ avec $b, c \in \mathbf{N}$ tels que $b, c \neq 1$. On note $\mathcal{P} = \{2, 3, 5, 7, 11, 13, 17 \ldots\}$ l'ensemble de tous les nombres premiers.

1.1.4 Définition. Soient $a, b \in \mathbf{Z}$. On dit que b **divise** a ou que a **est un multiple de** b, ou encore que b **est un diviseur de** a s'il existe $c \in \mathbf{Z}$ tel que $a = bc$. **Notation :** $b \mid a$ (si b ne divise pas a, on écrit $b \nmid a$).

1.1.5 Propriétés de base de divisibilité Les propriétés suivantes sont des conséquences immédiates de la définition.

— $b \mid a \iff b\mathbf{Z} \supseteq a\mathbf{Z}$ ("b divise a si et seulement si tout multiple de a est un multiple de b")
— $\forall b \in \mathbf{Z} \quad b \mid 0 \quad (\text{car } b \cdot 0 = 0), \qquad \forall a \in \mathbf{Z} \quad 1 \mid a \quad (\text{car } 1 \cdot a = a)$
— $b \mid \pm 1 \iff b = \pm 1$
— $b \mid a \iff \pm b \mid \pm a$
— $b \mid a_1, a_2 \Longrightarrow b \mid (a_1 \pm a_2)$
— $c \mid b,\ b \mid a \Longrightarrow c \mid a$
— $b_1 \mid a_1,\ b_2 \mid a_2 \Longrightarrow b_1 b_2 \mid a_1 a_2 \qquad$ (en particulier, $b \mid a \Longrightarrow b^2 \mid a^2$)
— si $c \neq 0$, alors il est équivalent : $b \mid a \iff bc \mid ac \quad (\text{car } ac = bcd \iff a = bd)$.

De plus, on a

— si $a, b \in \mathbf{Z} \smallsetminus \{0\}$ satisfont à $b \mid a$ et $a \mid b$, alors $b = \pm a$.

En effet, on a $b = au$ et $a = bv$ avec $u, v \in \mathbf{Z}$, d'où $a = bv = auv$ et $a(1 - uv) = 0$, ce qui implique que $uv = 1$ (car $a \neq 0$). On a alors $u, v = \pm 1$.

1.1.6 Exercice. (1) Résoudre $x^2 - y^2 = n, \quad x, y \in \mathbf{N} \quad$ pour $n = 20, 21$ et 22.
(2) Si $x \in \mathbf{Z}$ est pair (resp. impair), alors on a $x^2 = 4k$ (resp. $x^2 = 4k + 1$), où $k \in \mathbf{Z}$.
(3) $\{x^2 - y^2 \mid x, y \in \mathbf{Z}\} \subseteq (2\mathbf{Z} + 1) \cup 4\mathbf{Z}$.
(4) $\{x^2 - y^2 \mid x, y \in \mathbf{Z}\} = (2\mathbf{Z} + 1) \cup 4\mathbf{Z}$.
(5) L'équation $x^2 + y^2 = 1000003$ admet-elle une solution $x, y \in \mathbf{Z}$?

1.1.7 Exercice. Soit a un entier impair. Montrer que l'on a $4 \mid (a - 1)$ ou $4 \mid (a + 1)$. En déduire que $a^2 - 1 = (a - 1)(a + 1)$ est divisible par 8, $a^4 - 1 = (a^2 - 1)(a^2 + 1)$ est divisible par 16,..., $a^{2^k} - 1$ est divisible par 2^{k+2} (pour tout $k \geq 1$).

1.1.8 Exercice. Si $p > 2$ est un nombre premier, alors on a $p = 4k \pm 1$ ($k \in \mathbf{N}$). Si $p > 3$ est un nombre premier, alors on a $p = 6l \pm 1$ ($l \in \mathbf{N}$). [Indication : écrire $p = 4k + a$ (resp. $p = 6k + a$).]

1.1.9 Proposition. *Un entier $a > 1$ est un nombre premier si et seulement si a n'a que deux diviseurs positifs (à savoir, 1 et a).*

Démonstration. En effet, l'existence d'un diviseur positif $b \mid a$ tel que $b \neq 1$, a équivaut à l'existence d'une factorisation $a = bc$ avec $b, c \in \mathbf{N}_+$ et $b, c \neq 1$. □

1.1.10 Proposition (Critère de primalité)**.** *Soit $a > 1$ un entier. Les propriétés suivantes sont équivalentes.*
(1) a n'est pas un nombre premier.
(2) Il existe un entier b tel que $1 < b \leq \sqrt{a}$ et $b \mid a$.
(3) Il existe un nombre premier p tel que $p \leq \sqrt{a}$ et $p \mid a$.

Démonstration. Les implications (3) $\Longrightarrow$ (2) $\Longrightarrow$ (1) sont automatiques.
(1) $\Longrightarrow$ (2) : Si $a = bc$ avec des entiers $1 < b \leq c$, alors $b \mid a$ et $b^2 \leq bc = a$, d'où $b \leq \sqrt{a}$.
(2) $\Longrightarrow$ (3) : D'après la proposition 1.2.1 ci-dessous, l'entier b dans (2) est divisible par un nombre premier p ; on a alors $p \mid a$ et $p \leq \sqrt{a}$. □

1.1.11 Nombres premiers (exemples) (1) $a = 89$ est-il un nombre premier ? Oui : on a $89 < 10^2$ et $2, 3, 5, 7 \nmid 89$ (ici $\{2, 3, 5, 7\} = \{p \in \mathcal{P} \mid p < 10\}$).
(2) $a = 91$ est-il un nombre premier ? On a encore $91 < 10^2$ et $2, 3, 5 \nmid 91$, mais $7 \mid 91 = 7 \cdot 13$; par conséquent, 91 n'est pas un nombre premier.

1.1.12 Exercice. (1) Si $a_n, b_n \in \mathbf{C}$ $(n \geq 0)$ sont des nombres complexes tels que $a_n = b_n - b_{n-1}$ $(n \geq 1)$, alors on a

$$\forall n \geq 0 \quad \sum_{k=1}^{n} a_k = b_n - b_0.$$

(2) Déterminer $b_n - b_{n-1}$ lorsque $b_n = n$, $b_n = n(n+1)$, $b_n = n(n+1)(n+2)$ etc.
(3) Trouver une formule explicite pour les sommes suivantes :

$$\sum_{k=1}^{n} k, \qquad \sum_{k=1}^{n} k(k+1), \qquad \sum_{k=1}^{n} k(k+1)(k+2), \qquad \sum_{k=1}^{n} k^2, \qquad \sum_{k=1}^{n} k^3.$$

1.2 Existence de factorisation

1.2.1 Proposition (Existence de factorisation)**.** *Tout entier $n \geq 1$ s'écrit $n = p_1 \cdots p_r$, où $r \geq 0$ et $p_1, \ldots, p_r$ sont des nombres premiers (pas forcément distincts).*
[Ici $n = 1 \iff r = 0$. On applique la convention suivante : un produit vide $x_1 \cdots x_r$ pour $r = 0$ est égal à 1, de la même manière qu'une somme vide $x_1 + \cdots + x_r$ pour $r = 0$ est égale à 0.]

Démonstration. On va raisonner par récurence. Si $n = 1$, on prend $r = 0$. Soit $n > 1$. On suppose que l'énoncé est vrai pour tous les entiers positifs $m < n$. Il y a deux possibilités :

Cas 1. n est un nombre premier. Dans ce cas $n = p_1$.

Cas 2. n n'est pas un nombre premier. Dans ce cas $n = ab$ avec des entiers positifs $a, b > 1$ (ce qui implique que $a = n/b < n$ et $b = n/a < n$). Par l'hypothèse de récurrence on a $a = p_1 \cdots p_r$ et $b = q_1 \cdots q_s$, où p_i, q_j sont des nombres premiers. On en déduit que $n = p_1 \cdots p_r q_1 \cdots q_s$. □

1.2.2 Remarque sur le raisonnement par récurence La démonstration de la proposition 1.2.1 a procédé par récurrence. En général, on peut reformuler le raisonnement par récurence en utilisant le Principe de Minimalité suivant.

1.2.3 Théorème (Principe de Minimalité)**.** *Tout sous-ensemble non vide $S \subset \mathbf{N}$ contient un élément minimal (un élément $a \in S$ pour lequel il n'y a aucun $b \in S$ tel que $b < a$).*

1.2.4 Preuve en termes du Principe de Minimalité Voici une démonstration de la proposition 1.2.1 qui utilise le Principe de Minimalité 1.2.3. Soit $S \subset \mathbf{N}_+$ l'ensemble de tous les entiers positifs pour lesquels 1.2.1 est faux : $S := \{a \in \mathbf{N}_+ \mid a \neq p_1 \cdots p_r \ (r \geq 0)\}$. On veut montrer que $S = \emptyset$. On procède par contradiction, en supposant que l'ensemble S n'est pas vide. Dans ce cas il existe un élément minimal $a \in S$. On a $a > 1$ (car $1 \notin S$) et $a \notin \mathcal{P}$ (car $S \cap \mathcal{P} = \emptyset$), ce qui implique qu'il existe des entiers $b, c > 1$ tels que $a = bc$, d'après la proposition 1.1.9. En particulier, $b, c < a$; on déduit de la minimalité de $a \in S$ que $b, c \notin S$. Par définition de S, on a $a = p_1 \cdots p_r$ et $b = q_1 \cdots q_s$, où p_i, q_j sont des nombres premiers, ce qui implique que $a = p_1 \cdots p_r q_1 \cdots q_s \notin S$, contradiction.

1.2.5 Il y a une infinité de nombres premiers Une démonstration du résultat fondamental suivant se trouve déjà dans les Eléments d'Euclide.

1.2.6 Théorème. *Il y a une infinité de nombres premiers.*

Démonstration. Il suffit de montrer que pour n'importe quel ensemble fini de nombres premiers $A = \{p_1, \dots, p_r\}$ ($r \geq 0$) il existe un nombre premier $p \notin A$. On considère l'entier positif $N := 1 + p_1 \cdots p_r \geq 1 + 1 = 2$ (on a $N = 2 \iff r = 0$). D'après la proposition 1.2.1 il existe un nombre premier $p \mid N$. On affirme que $p \notin A$. En effet, si $p \in A$, alors il existe $i = 1, \dots, r$ tel que $p = p_i$, ce qui implique que $p \mid (N-1)$. On en déduit que $p \mid N-(N-1)$, ce qui est impossible. Cette contradiction montre que $p \notin A$. □

1.2.7 Nombres premiers modulo 10 On peut ranger des nombres premiers selon leur dernier chiffre. La table

$p = 10k + 1$	11	31	41	61	71	101	131	151
$p = 10k + 3$	3	13	23	43	53	73	83	103
$p = 10k + 7$	7	17	37	47	67	97	107	127
$p = 10k + 9$	19	29	59	79	89	109	139	149

suggère qu'il y a une infinité de nombres premiers dans chacune des progressions arithmétiques $10k + 1$, $10k+3$, $10k+7$ et $10k+9$. C'est bien le cas ; il s'agit d'un cas particulier d'un résultat général de Dirichlet (voir le théorème 5.2.12). On va montrer dans les propositions 5.2.2 et 5.2.4 qu'il y a une infinité de nombres premiers qui s'écrivent $p = 4k + 3$ et $p = 4k + 1$, respectivement.

Une étude plus attentive de la table ci-dessus suggère que les nombres premiers $p = 10k+3$ et $p = 10k+7$ apparaissent plus souvent que $p = 10k + 1$ et $p = 10k + 9$ dans un intervalle $p \leq X$. On étudie ce genre de phénomène, qui a été découvert par Čebyšev, sous la rubrique "Course de nombres premiers".

1.3 Factorisation de $a^n \pm 1$

On peut se demander s'il y a des règles naturelles derrière la factorisation des entiers spéciaux. Par exemple, on peut considérer les entiers $a^n \pm 1$, où l'on fixe $a > 1$ et fait varier n.

1.3.1 Formulaire utile Rappelons qu'on a

$$X^4 - 1 = (X - 1)(X^3 + X^2 + X + 1), \qquad Y^3 + 1 = (Y + 1)(Y^2 - Y + 1).$$

Plus généralement,

$$X^m - 1 = (X - 1)(X^{m-1} + X^{m-2} + \cdots + X + 1), \tag{1.3.1.1}$$

$$Y^{2k+1} + 1 = -((-Y)^{2k+1} - 1) = (Y + 1)(Y^{2k} - Y^{2k-1} + \cdots + Y^2 - Y + 1). \tag{1.3.1.2}$$

1.3.2 Factorisation des nombres de Mersenne $2^n - 1$ Voici la factorisation des **nombres de Mersenne** $M_n = 2^n - 1$ pour quelques petites valeurs de n.

n	M_n
1	1
2	$\boxed{3}$
3	$\boxed{7}$
4	$15 = 3 \cdot 5$
5	$\boxed{31}$
6	$63 = 3 \cdot 3 \cdot 7$
7	$\boxed{127}$
8	$255 = 3 \cdot 5 \cdot 17$
9	$511 = 7 \cdot 73$
10	$1023 = 3 \cdot 11 \cdot 31$

On voit que si $1 \leq n \leq 10$, alors M_n est un nombre premier si et seulement si $n = 2, 3, 5, 7$ l'est. Est-ce que ce comportement persiste pour $n > 10$?

Le nombre premier suivant est $n = 11$. Pour tester la primalité de $M_{11} = 2047 < 46^2$, il faut vérifier si M_{11} est divisible ou pas par des nombres premiers $p < 46$. On a $2, 3, 5, 7, 11, 13, 17, 19 \nmid M_{11}$, mais $23 \mid M_{11} = 23 \cdot 89$. Alors M_{11} n'est pas premier !

Néanmoins, l'implication réciproque est vraie :

1.3.3 Proposition. *Si $M_n = 2^n - 1$ est un nombre premier, il en est de même de n.*

Démonstration. Il faut montrer que M_n n'est pas premier si n ne l'est pas. Dans ce cas on a soit $n = 1$ (où $M_n = 1$ n'est pas premier), soit $n = ab$ avec des entiers a, $b > 1$. La formule (1.3.1.1) pour $X = 2^a$ et $m = b$ montre alors que

$$M_n = 2^{ab} - 1 = (2^a - 1)(2^{a(b-1)} + 2^{a(b-2)} + \cdots + 2^a + 1)$$

est un produit non trivial (car $1 < 2^a - 1 < 2^{ab} - 1$), ce qui implique que M_n n'est pas premier. □

1.3.4 Nombres premiers de Mersenne Si p est un nombre premier pour lequel M_p est aussi un nombre premier, on dit que M_p est un **nombre premier de Mersenne**. On peut vérifier si c'est bien le cas en utilisant le critère de Lucas–Lehmer dans le théorème 1.3.5 ci-dessous. En utilisant ce critère, Lucas a vérifié en 1876 que M_{127} est un nombre premier. A l'heure actuelle (octobre 2019), le plus grand nombre premier explicite connu est M_p pour $p = 82589933$ (M_p a 24 862 048 chiffres décimaux). Voir `https://www.mersenne.org/`

1.3.5 Théorème (Lucas, Lehmer)**.** *On définit des entiers $(a_n)_{n\geq 0}$ par les règles suivantes : $a_0 = 2$, $a_1 = 1$ et $a_{n+2} = a_{n+1} + a_n$.*

n	*0*	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*	*15*	*16*
a_n	*2*	*1*	*3*	*4*	*7*	*11*	*18*	*29*	*47*	*76*	*123*	*199*	*322*	*521*	*843*	*1364*	*2207*

Si $p = 4k+3$ ($k \in \mathbf{Z}$) est un nombre premier, alors M_p est un nombre premier si et seulement si M_p divise $a_{2^{p-1}}$. [On peut reformuler cette propriété en utilisant les formules récursives $a_{2^{n+1}} = a_{2^n}^2 - 2$ ($n \geq 1$).] Un résultat analogue est valable pour les entiers $(b_n)_{n\geq 0}$ tels que $b_0 = 2$, $b_1 = 4$ et $b_{n+2} = 4b_{n+1} - b_n$ (on a $b_{2^{n+1}} = b_{2^n}^2 - 2$ ($n \geq 0$)), sans supposant que $p = 4k + 3$.

1.3.6 Factorisation de $2^n + 1$ On va maintenant étudier la factorisation des entiers $A_n = 2^n + 1$.

n	A_n
1	$\boxed{3}$
2	$\boxed{5}$
3	$9 = 3 \cdot 3$
4	$\boxed{17}$
5	$33 = 3 \cdot 11$
6	$65 = 5 \cdot 13$
7	$129 = 3 \cdot 43$
8	$\boxed{257}$
9	$513 = 3^3 \cdot 19$
10	$1025 = 5^2 \cdot 41$

On voit que si $1 \leq n \leq 10$, alors A_n est un nombre premier si et seulement si $n = 1, 2, 4, 8$ est une puissance de 2. Est-ce que ce comportement persiste pour $n > 10$?

On montre d'abord l'analogue suivant de la proposition 1.3.3.

1.3.7 Proposition. *Si A_n est un nombre premier, alors $n = 2^k$ ($k \in \mathbf{N}$).*

Démonstration. Si $n \in \mathbf{N}_+$ mais $n \neq 2^k$ ($k \in \mathbf{N}$), alors n s'écrit $n = ab$ avec des entiers a, $b > 1$ tels que $2 \nmid b$. La formule (1.3.1.2) pour $Y = 2^a$ et $m = b$ montre alors que

$$A_n = 2^{ab} + 1 = (2^a + 1)(2^{a(b-1)} - 2^{a(b-2)} + \cdots - 2^a + 1)$$

est un produit non trivial (car $1 < 2^a + 1 < 2^{ab} + 1$), ce qui implique que A_n n'est pas un nombre premier. □

1.3.8 Nombres de Fermat Il faut étudier maintenant les nombres de Fermat $F_k = A_{2^k} = 2^{2^k} + 1$. Si F_k est un nombre premier, on l'appelle un **nombre premier de Fermat**. Les nombres de Fermat F_0, F_1, F_2, F_3, F_4 dans la table ci-dessous sont tous des nombres premiers de Fermat.

k	0	1	2	3	4
F_k	3	5	17	257	65537

Euler a montré que le nombre de Fermat suivant $F_5 = 2^{32} + 1$ est divisible par 641, ce qui implique que F_5 n'est pas premier. A l'heure actuelle (octobre 2019) on ne connaît aucun nombre premier de Fermat plus grand que F_4. Par contre, on sait que parmi les nombres de Fermat F_k avec $5 \leq k \leq 32$ il n'y a aucun nombre premier.

1.3.9 Nombres premiers de Fermat en géometrie Un résultat célèbre de Gauss dit que si $p = F_k$ est un nombre premier de Fermat (par exemple, si $p = 17$), alors on peut construire un polygône régulier à p côtés à la règle et au compas.

En général, une telle construction existe pour un polygône régulier à n côtés si et seulement si $n = 2^a p_1 \cdots p_r$, où $p_j = 2^{2^{k_j}} + 1$ sont des nombres premiers de Fermat distincts.

1.3.10 Factorisation de $3^n \pm 1$ Que se passe-t-il si l'on remplace 2^n par 3^n ? Voici quelques exemples.

n	1	3	5	7
$(3^n-1)/2$	1	13	$121 = 11^2$	1093
$(3^n+1)/4$	1	7	61	547

n	2	4	6	8
$(3^n-1)/8$	1	$10 = 2 \cdot 5$	$91 = 7 \cdot 13$	$820 = 2^2 \cdot 5 \cdot 41$
$(3^n+1)/2$	5	41	$365 = 5 \cdot 73$	3281

1.3.11 Exercice. Soit $n \geq 1$ un entier.
(1) Si $2 \nmid n$, alors on a $2 \nmid (3^n-1)/2$.
(2) Si $2 \nmid n$ et si $(3^n-1)/2$ est un nombre premier, alors n est un nombre premier.
(3) Si $2 \mid n$, alors on a $2 \nmid (3^n+1)/2$.
(4) Si $2 \mid n$ et si $(3^n+1)/2$ est un nombre premier, alors $n = 2^k$.

1.4 Unicité de factorisation, lemme d'Euclide, valuations p-adiques

1.4.1 Théorème (Unicité de factorisation = Théorème Fondamental de l'Arithmétique)**.** *Tout entier non nul $a \in \mathbf{Z} \smallsetminus \{0\}$ s'écrit sous la forme $a = \pm p_1 \cdots p_r$, où $r \geq 0$ et $p_1, \ldots, p_r$ sont des nombres premiers (pas forcément distincts) et $\pm 1 = \mathrm{sgn}(a)$. Cette écriture est unique au sens suivant : si $a\,\mathrm{sgn}(a) = p_1 \cdots p_r = q_1 \cdots q_s$, où $s \geq 0$ et $q_1, \ldots, q_s$ sont des nombres premiers (pas forcément distincts), alors $r = s$ et, quitte à changer l'ordre des facteurs, on a $p_i = q_i$ pour chaque $i = 1, \ldots, r = s$.*

Démonstration. Il faut montrer l'unicité. Si $r = 0$, alors $a\,\mathrm{sgn}(a) = 1$, ce qui implique que $s = 0$. On suppose que $r > 0$ et que l'énoncé est vrai pour $r-1$. Le produit $q_1 \cdots q_s$ est divisible par p_r. D'après le lemme d'Euclide 1.4.3 ci-dessous il existe $1 \leq j \leq s$ tel que $p_r \mid q_j$. Après une renumérotation des facteurs on peut supposer que $p_r \mid q_s$. Les seuls diviseurs positifs de q_s sont 1 et q_s, ce qui implique que $p_r = q_s$. On divise l'égalité $p_1 \cdots p_r = q_1 \cdots q_s$ par p_r ; on obtient $p_1 \cdots p_{r-1} = q_1 \cdots q_{s-1}$. L'hypothèse de récurrence alors dit qu'on a (après une renumérotation des facteurs) $r-1 = s-1$ et $p_i = q_i$ pour chaque $i = 1, \ldots, r-1$. □

1.4.2 Théorème (Unicité de factorisation (reformulation))**.** *Tout entier non nul $a \in \mathbf{Z} \smallsetminus \{0\}$ s'écrit de façon unique sous la forme $a = \pm p_1^{k_1} \cdots p_t^{k_t}$, où $p_1 < \cdots < p_t$ sont des nombres premiers, $t \geq 0$ et $k_1, \ldots k_t \geq 1$.*

Démonstration. On peut mettre les nombres premiers dans le produit qui apparaît dans le théorème 1.4.1 dans leur ordre naturel et puis regrouper les termes avec la même valeur de p, ce qui définit une numérotation canonique des facteurs. □

1.4.3 Lemme (Lemme d'Euclide)**.** *Soient $a, b \in \mathbf{Z} \smallsetminus \{0\}$, soit p un nombre premier. Si $p \mid ab$ et $p \nmid b$, alors $p \mid a$.*

Démonstration. On sait que p divise ab et ap ; on veut montrer que p divise aussi $a \cdot 1 = a$. Il est naturel d'étudier l'ensemble

$$X := \{x \in \mathbf{Z} \mid \ p \mid ax\}.$$

On remarque que $x \pm y \in X$ si $x, y \in X$. On a $p, b \in X$, ce qui implique que

$$X \supset p\mathbf{Z} + b\mathbf{Z} = \{pu + bv \mid u,\, v \in \mathbf{Z}\}.$$

D'après la forme faible du théorème de Bézout (voir les théorèmes 2.3.3 et 2.4.2 ci-dessous) il existe $d \in \mathbf{N}_+$ tel que $p\mathbf{Z} + b\mathbf{Z} = d\mathbf{Z}$. En particulier, les entiers $p, b \in p\mathbf{Z} + b\mathbf{Z} = d\mathbf{Z}$ sont des multiples de d. Les seuls diviseurs positifs de p étant 1 et p, on a $d = p$ ou $d = 1$. On ne peut pas avoir $d = p$, car b n'est pas un multiple de p. On en déduit que $d = 1$, ce qui implique que $1 = d \in X$ et $p \mid a \cdot 1$. □

1.5 Valuations p-adiques et leurs applications

1.5.1 Exposants dans la factorisation La factorisation d'un entier $a \in \mathbf{Z} \smallsetminus \{0\}$ dans le théorème 1.4.2 s'écrit sous la forme

$$a = \pm p_1^{k_1} \cdots p_t^{k_t} = \pm \prod_{p \in \mathcal{P}} p^{k(p)}, \qquad k(p) = \begin{cases} k_i & \text{if } p = p_i \\ 0 & \text{if } p \notin \{p_1, \ldots, p_t\}. \end{cases}$$

Les exposants $k(p) \in \mathbf{N}$ sont nuls pour tous sauf un nombre fini de $p \in \mathcal{P}$. Ils sont détérminés de façon unique par a, grâce au théorème 1.4.2. On va montrer que les relations de divisibilité entre des entiers non nuls s'expriment en termes de ces exposants. On va utiliser la terminologie suivante.

1.5.2 Définition. Soit $a \in \mathbf{Z} \smallsetminus \{0\}$. Pour tout nombre premier $p \in \mathcal{P}$ on appelle la **valuation p-adique** $v_p(a)$ de a l'exposant de p dans la décomposition (unique) de a en produit de puissances de nombres premiers :

$$a = \operatorname{sgn}(a) \prod_{p \in \mathcal{P}} p^{v_p(a)} \tag{1.5.2.1}$$

($v_p(a) \in \mathbf{N}$, et $v_p(a) = 0$ pour tous sauf un nombre fini de $p \in \mathcal{P}$). On définit $v_p(0) := +\infty$.
[Par exemple, $\pm 56 = \pm 2^3 \cdot 7$, $v_2(\pm 56) = 3$, $v_7(\pm 56) = 1$, $v_p(\pm 56) = 0$ si $p \neq 2, 7$.]

1.5.3 Attention Il faut remarquer que la définition de $v_p(a)$ ci-dessus utilise la validité du théorème 1.4.2, qui n'a pas encore été démontré dans ce texte. La preuve sera complétée quand on aura démontré le théorème de Bézout (dans la forme faible).

1.5.4 Proposition (Propriétés des valuations p-adiques)**.** *Soient $a, b, c \in \mathbf{Z} \smallsetminus \{0\}$.*
(1) $a = \pm b \iff \forall p \in \mathcal{P} \quad v_p(a) = v_p(b)$.
(2) $\forall p \in \mathcal{P} \quad v_p(bc) = v_p(b) + v_p(c)$.
(3) $b \mid a \iff \forall p \in \mathcal{P} \quad v_p(b) \leq v_p(a)$.
(4) Pour tous $p \in \mathcal{P}$ et $k \geq 0$, $\quad p^k \mid a \iff k \leq v_p(a)$.
(5) $\forall p \in \mathcal{P} \quad v_p(a + b) \geq \min(v_p(a), v_p(b))$.
(6) Si $v_p(a) \neq v_p(b)$, alors $\forall p \in \mathcal{P} \quad v_p(a + b) = \min(v_p(a), v_p(b))$.

Démonstration. Les points (1) et (2) sont des conséquences immédiates de la Définition (1.5.2.1). Si $b \mid a$ dans le point (3), alors $a = bc$ avec $c \in \mathbf{Z} \smallsetminus \{0\}$, ce qui implique que $v_p(a) = v_p(b) + v_p(c) \geq v_p(b)$ pour tout $p \in \mathcal{P}$, d'après (2). Réciproquement, si l'on a $\forall p \in \mathcal{P} \quad v_p(b) \leq v_p(a)$, on pose

$$c := \operatorname{sgn}(b)^{-1} \operatorname{sgn}(a) \prod_{p \in \mathcal{P}} p^{v_p(a) - v_p(b)}.$$

Tous les exposants $v_p(a) - v_p(b) \geq 0$ sauf un nombre fini sont nuls, ce qui implique que $c \in \mathbf{Z} \smallsetminus \{0\}$ est bien défini et que l'on a $bc = \operatorname{sgn}(a) \prod_{p \in \mathcal{P}} p^{v_p(a)} = a$, d'où $b \mid a$. Le point (4) est un cas prticulier $b = p^k$ de (3). Dans (5) et (6) on peut supposer que $k := \min(v_p(a), v_p(b)) = v_p(a) \leq v_p(b)$. On déduit de (4) que $p^k \mid a$ et $p^k \mid b$. Ceci implique que $p^k \mid (a+b)$, ce qui équivaut à $k \leq v_p(a+b)$. On vient de démontrer (5). Dans (6) on a aussi $k < v_p(b)$, ce qui implique que $p^{k+1} \mid b$. Si on avait $v_p(a+b) > k$, on obtiendrait $p^{k+1} \mid (a+b)$ et aussi $p^{k+1} \mid (a+b) - b = a$, ce qui est faux. Cette contradiction montre que $v_p(a+b) \leq k$, ce qui est le point (6). □

1.5.5 Proposition. *Pour tous $a, b \in \mathbf{Z} \smallsetminus \{0\}$ on a :* $\quad b \mid a \iff b^2 \mid a^2$.

Démonstration. L'implication '$\Longrightarrow$' est automatique : si $a = bc$ avec $c \in \mathbf{Z}$, alors $a^2 = b^2c^2$ et $c^2 \in \mathbf{Z}$, d'où $b^2 \mid a^2$. Pour montrer l'implication réciproque '$\Longleftarrow$' il faut utiliser l'unicité de factorisation sous la forme des corollaires démontrés dans la proposition 1.5.4 (voir la discussion autour de la proposition 1.5.20 ci-dessous) : si $b^2 \mid a^2$, alors

$$\forall p \in \mathcal{P} \quad \underbrace{v_p(b^2)}_{2v_p(b)} \leq \underbrace{v_p(a^2)}_{2v_p(a)}, \text{ ce qui implique que } \forall p \in \mathcal{P} \quad v_p(b) \leq v_p(a), \text{ d'où } b \mid a.$$

□

1.5.6 Diviseurs de n Si $n = p_1^{k_1} \cdots p_t^{k_t}$ et une factorisation d'un entier positif n en produit de puissances de nombres premiers, alors l'ensemble de tous les diviseurs positifs de n est égal à

$$\{p_1^{l_1} \cdots p_t^{l_t} \mid \forall i = 1, \ldots, t \quad 0 \leq l_i \leq k_i\}.$$

Il y a $k_i + 1$ valeurs possibles de l'exposant l_i, ce qui implique que le nombre de diviseurs positifs de n est égal à

$$(k_1 + 1) \cdots (k_t + 1) = \prod_{p \mid n} (v_p(n) + 1)$$

(dans le produit ci-dessus, p est un nombre premier).

Exemple : $n = 12 = 2^2 \cdot 3^1$. L'ensemble de tous les diviseurs positifs de 12 est égal à

$$\{2^i \cdot 3^j \mid 0 \leq i \leq 2,\, 0 \leq j \leq 1\} = \{1, 2, 2^2, 3, 2 \cdot 3, 2^2 \cdot 3\} = \{1, 2, 4, 3, 6, 12\}.$$

La somme de tous les diviseurs positifs de 12 est égale à

$$1 + 2 + 2^2 + 3 + 2 \cdot 3 + 2^2 \cdot 3 = (1 + 2 + 2^2)(1 + 3) = 7 \cdot 4 = 28.$$

1.5.7 Exercice. Pour $n = p_1^{k_1} \cdots p_t^{k_t}$ comme ci-dessus, la somme de tous les diviseurs positifs de n est égale à

$$\sigma_1(n) := \sum_{d \mid n} d = \sigma_1(p_1^{k_1}) \cdots \sigma_1(p_t^{k_t}) = (1 + p_1 + \cdots + p_1^{k_1}) \cdots (1 + p_t + \cdots + p_t^{k_t}) =$$

$$= \prod_{i=1}^{t} \left(\frac{p_i^{k_i+1} - 1}{p_i - 1} \right) = \prod_{p \mid n} \left(\frac{p^{v_p(n)+1} - 1}{p - 1} \right).$$

Plus généralement, pour tout $s \in \mathbf{C}$ la somme des puissances s-ièmes de tous les diviseurs positifs de n est égale à

$$\sigma_s(n) := \sum_{d|n} d^s = \prod_{i=1}^{t} \sigma_s(p_i^{k_i}), \qquad \sigma_s(p^k) = 1 + p^s + \cdots + p^{ks} = \frac{p^{(k+1)s} - 1}{p - 1}.$$

Déterminer le nombre et la somme de tous les diviseurs positifs de $n = 2160$.

1.5.8 Nombres parfaits La somme de tous les diviseurs positifs **propres** (ceux qui sont strictement inférieurs à n) de $n = 6$ est égale à $1+2+3 = 6 = n$. De même, pour $n = 28$ on a $1+2+4+7+14 = 28 = n$.

On appelle un entier positif qui satisfait à la propriété

$$\sum_{\substack{d|n \\ d \neq n}} d = n$$

(ce qui équivaut à $\sigma_1(n) = 2n$) un **nombre parfait**. On conjecture qu'il n'y a aucun nombre parfait impair. Les nombres parfaits pairs sont classifiés de la façon suivante.

1.5.9 Exercice. Si $M_p = 2^p - 1$ est un nombre premier de Mersenne, alors $n = 2^{p-1}(2^p - 1)$ est un nombre parfait. Réciproquement, tout nombre parfait pair s'écrit sous cette forme.

1.5.10 Irrationalité de $\sqrt[n]{a}$ (1) Le nombre $\sqrt{3}$ n'est pas rationnel : si $\sqrt{3} \in \mathbf{Q}$, alors $\sqrt{3} = \frac{a}{b}$ avec $a, b \in \mathbf{N}_+$, ce qui implique que $3b^2 = a^2$. On en déduit qu'on a

$$v_p(3b^2) = v_p(a^2) \implies v_p(3) + 2v_p(b) = 2v_p(a)$$

(pour tout $p \in \mathcal{P}$). En particulier, pour $p = 3$ on obtient $1 + 2v_3(b) = 2v_3(a)$ et $1 = 2(v_3(a) - v_3(b))$, ce qui est impossible, car $2 \nmid 1$.
(2) Le nombre $\alpha = \frac{5+\sqrt[3]{20}}{7}$ n'est pas rationnel : Si $\alpha \in \mathbf{Q}$, alors $\sqrt[3]{20} = 7\alpha - 5 \in \mathbf{Q}$. En écrivant $\sqrt[3]{20} = \frac{a}{b}$ avec $a, b \in \mathbf{N}_+$, on obtient $20b^3 = a^3$ et

$$\forall p \in \mathcal{P} \quad v_p(20b^3) = v_p(a^3),$$

ce qui implique, comme ci-dessus, que $v_p(20) = 3(v_p(a) - v_p(b))$ est divisible par 3. On obtient une contradiction si l'on prend $p = 2$ ou $p = 5$, car $20 = 2^2 \cdot 5$: on a $v_2(20) = 2$ et $v_5(20) = 1$.

Voici le résultat général.

1.5.11 Théorème (Irrationalité de $\sqrt[n]{a}$)**.** *Soient $a, n \in \mathbf{N}_+$. Les propriétés suivantes sont équivalentes :*
(1) $\sqrt[n]{a} \in \mathbf{Q}$.
(2) $\forall p \in \mathcal{P} \quad n \mid v_p(a)$.
(3) Il existe $b \in \mathbf{N}_+$ tel que $a = b^n$.
(4) $\sqrt[n]{a} \in \mathbf{Z}$.

Démonstration. Les implications (3) $\iff$ (4) $\implies$ (1) sont automatiques, tandis que (3) $\implies$ (2) est une conséquence de l'égalité $v_p(a) = v_p(b^n) = nv_p(b)$. Réciproquement, (2) implique que que l'on a $a = b^n$, où $b := \prod_{p \in \mathcal{P}} p^{v_p(a)/n} \in \mathbf{N}_+$, d'où (3). Pour montrer que (1) implique (2), l'hypothèse (1) nous dit que $\sqrt[n]{a} = \frac{b}{c}$ avec $b, c \in \mathbf{N}_+$, d'où $ac^n = b^n$. On en déduit, pour tout $p \in \mathcal{P}$, que $v_p(ac^n) = v_p(a) + nv_p(c)$ est égal à $v_p(b^n) = nv_p(b)$, ce qui implique que $v_p(a) = n(v_p(b) - v_p(c))$ est bien divisible par n. □

1.5.12 Corollaire. *Si $a, n \in \mathbf{N}_+$ et s'il existe $k \in \mathbf{N}_+$ tel que $k^n < a < (k+1)^n$, alors $\sqrt[n]{a} \notin \mathbf{Z}$, ce qui implique que $\sqrt[n]{a} \notin \mathbf{Q}$.*

1.5.13 Théorème (Unicité de factorisation dans $\mathbf{Q}$). *Tout nombre rationnel non nul $a \in \mathbf{Q} \smallsetminus \{0\}$ s'écrit de façon unique sous la forme*

$$a = \operatorname{sgn}(a) \prod_{p \in \mathcal{P}} p^{k(p)},$$

où les exposants $k(p) \in \mathbf{Z}$ sont nuls pour tous sauf un nombre fini de $p \in \mathcal{P}$. On appelle l'exposant $k(p)$ la ***valuation p-adique de*** *a (notation : $v_p(a) := k(p) \in \mathbf{Z}$). [Par exemple, $a = \frac{15}{100} = \frac{3^1 \cdot 5^1}{2^2 \cdot 5^2} = \frac{3}{20} = \frac{3}{2^2 \cdot 5^1} = 2^{-2} \cdot 3^1 \cdot 5^{-1}$ et $v_2(a) = -2$, $v_3(a) = 1$, $v_5(a) = -1$ et $v_p(a) = 0$ si $p \neq 2, 3, 5$.]*

Démonstration. **Existence :** soient $b, c \in \mathbf{Z} \smallsetminus \{0\}$ tels que $a = b/c$; on a

$$a = \operatorname{sgn}(b) \prod_{p \in \mathcal{P}} p^{v_p(b)} / \operatorname{sgn}(c) \prod_{p \in \mathcal{P}} p^{v_p(c)} = \operatorname{sgn}(a) \prod_{p \in \mathcal{P}} p^{v_p(b) - v_p(c)}.$$

Unicité : on suppose que l'on a

$$\prod_{p \in \mathcal{P}} p^{k(p)} = \prod_{p \in \mathcal{P}} p^{l(p)}, \tag{1.5.13.1}$$

où les entiers $k(p), l(p) \in \mathbf{Z}$ sont nuls pour $p \notin S$, où $S \subset \mathcal{P}$ est un ensemble fini de nombres premiers. On multiplie (1.5.13.1) par $\prod_{p \in S} p^n$, où $n \geq \max_{p \in S}(|k(p)| + |l(p)|)$; on obtient

$$\prod_{p \in \mathcal{P}} p^{k(p)+n} = \prod_{p \in \mathcal{P}} p^{l(p)+n},$$

où $k(p)+n, l(p)+n \geq 0$ pour tout $p \in S$. L'unicité dans le théorème 1.4.2 implique que $k(p)+n = l(p)+n$ (d'où $k(p) = l(p)$) pour tout $p \in S$. □

1.5.14 Exercice. Les énoncés (1), (2), (5) et (6) dans la proposition 1.5.4 sont valables pour $a, b \in \mathbf{Q} \smallsetminus \{0\}$.

1.5.15 Exercice. Le nombre $(4/7)^{4/7}$ n'est pas rationnel.

1.5.16 Exercice. Soient $a \in \mathbf{Q}$, $a > 0$ et $n \in \mathbf{N}_+$. Les propriétés suivantes sont équivalentes : $\sqrt[n]{a} \in \mathbf{Q} \iff \forall p \in \mathcal{P} \quad n \mid v_p(a)$.

1.5.17 Digression : sous-anneaux de C Peut-on démontrer l'implication $b^2 \mid a^2 \Longrightarrow b \mid a$ dans la proposition 1.5.5 sans utilisant l'unicité de factorisation ? La réponse est "NON". On va voir qu'on peut définir la notion de divisibilité dans un cadre plus général, et que l'implication ci-dessus n'est pas forcément valable dans ce cas-là.

1.5.18 Définition. Un **sous-anneau** de $\mathbf{C}$ est un sous-ensemble $A \subset \mathbf{C}$ tel que

$$0, 1 \in A; \qquad a, b \in A \Longrightarrow a \pm b,\ ab \in A.$$

Si $a, b \in A$, on dit que b divise a (notation : $b \mid a$) s'il existe $c \in A$ tel que $a = bc$.
Un **sous-corps** de $\mathbf{C}$ est un sous-anneau $A \subset \mathbf{C}$ tel que

$$a \in A \smallsetminus \{0\} \Longrightarrow a^{-1} \in A.$$

Un **sous-groupe additif** de $\mathbf{C}$ est un sous-ensemble $X \subset \mathbf{C}$ tel que

$$0 \in X; \qquad x, y \in X \Longrightarrow x \pm y \in X.$$

En particulier, tout sous-anneau de $\mathbf{C}$ est un sous-groupe additif de $\mathbf{C}$.

1.5.19 Sous-anneaux et sous-groupes additifs de C (exemples) (1) $X = \frac{1}{2}\mathbf{Z}$ est un sous-groupe additif de $\mathbf{C}$ qui n'est pas un sous-anneau de $\mathbf{C}$ (car $\frac{1}{2} \cdot \frac{1}{2} \notin \frac{1}{2}\mathbf{Z}$).
(2) $A = \mathbf{Z}$ est un sous-anneau de $\mathbf{C}$.
(3) $A = \mathbf{Z} + i\mathbf{Z} = \{u + iv \mid u, v \in \mathbf{Z}\}$ est un sous-anneau de $\mathbf{C}$.
(4) $A = \mathbf{Z} + 2i\mathbf{Z} = \{u + 2iv \mid u, v \in \mathbf{Z}\}$ est un sous-anneau de $\mathbf{C}$.
(5) $A = \mathbf{Q} + i\mathbf{Q} = \{u + iv \mid u, v \in \mathbf{Q}\}$ est un sous-corps de $\mathbf{C}$ (car $(u + iv)^{-1} = (u - iv)/(u^2 + v^2)$).

1.5.20 Proposition. *(1) Si $A \subset \mathbf{C}$ est un sous-anneau, $a, b \in A$ et $b \mid a$, alors $b^2 \mid a^2$.*
(2) On considère les éléments $b = 2$ et $a = 2i$ du sous-anneau $A = \mathbf{Z} + 2i\mathbf{Z}$ de $\mathbf{C}$. Dans ce cas on a $b^2 \mid a^2$ mais $b \nmid a$ dans A.

Démonstration. (1) Voir la preuve de la proposition 1.5.5. En ce qui concerne le point (2), on a bien que $2^2 = 4$ divise $(2i)^2 = -4$ (car $-1 \in A$) mais 2 ne divise pas $2i$ (car $i \notin A$). □

1.5.21 Meta-remarque En général, toutes les implications "faciles" qui ne concernent que la divisibilité (exemple : $b \mid a \Longrightarrow b^2 \mid a^2$) sont valables dans tous les sous-anneaux de $\mathbf{C}$.

Par contre, supposons qu'on a trouvé un sous-anneau de $\mathbf{C}$ dans lequel une implication qui s'exprime en termes de la divisibilité (telle que $b^2 \mid a^2 \Longrightarrow b \mid a$) n'est pas valable, comme dans la proposition 1.5.20(2) ci-dessus. On en déduit que même si cette implication était valable dans $\mathbf{Z}$, on ne pourrait pas le démontrer en n'utilisant que les propriétés de base de divisibilité, telles que celles dans 1.1.5.

1.5.22 Exercice. Soient $a, b \geq 1$ des entiers. Les affirmations suivantes sont-elles vraies ou fausses (et pourquoi) ?
(1) si $b^2 \mid a^3$, alors $b \mid a$.
(2) si $b^3 \mid a^2$, alors $b \mid a$.
(3) si $b^3 \mid a^3$, alors $b \mid a$.

1.5.23 Exercice. (1) Déterminer le plus petit sous-groupe additif de $\mathbf{C}$ qui contient $\frac{1}{2}$ (resp. $\frac{i}{2}$).
(2) Déterminer le plus petit sous-anneau de $\mathbf{C}$ qui contient $\frac{1}{2}$ (resp. $\frac{i}{2}$).

1.5.24 Coefficients binomiaux On va étudier la divisibilité de coefficients binomiaux par des nombres premiers dans l'exercise 2.6.6. Voici le cas le plus simple.

1.5.25 Proposition. *Si p est un nombre premier, alors $\binom{p}{j}$ est divisible par p pour chaque entier $0 < j < p$.*

Démonstration. La formule

$$\binom{p}{j} = \frac{p(p-1)\cdots(p-j+1)}{1 \cdot 2 \cdots j}$$

implique que

$$v_p(\binom{p}{j}) = v_p(p) + \sum_{i=1}^{j-1} v_p(p-i) - \sum_{i=1}^{j} v_p(i) = 1 + 0 - 0 = 1.$$

□

1.5.26 Théorème (Petit théorème de Fermat)**.** *Si $p \in \mathcal{P}$ et $a \in \mathbf{Z}$, alors $p \mid (a^p - a)$.*

Démonstration. On a

$$(a+1)^p - (a+1) = (a^p - a) + R, \qquad R = \sum_{0<j<p} \binom{p}{j} a^j.$$

D'après la proposition 1.5.25, l'entier R est divisible par p. Il en résulte que l'énoncé du théorème est valable pour $a+1$ si et seulement si il est valable pour a. Le cas $a = 0$ étant trivial, on en déduit le théorème par récurrence. □

1.5.27 Exercice. Démontrer directement le petit théorème de Fermat pour $p = 2$ et $p = 3$ en utilisant les formules $a^2 - a = a(a-1)$ et $a^3 - a = (a-1)a(a+1)$. Que se passe-t-il pour $p = 5$ où l'on a $a^5 - a = (a-1)a(a+1)(a^2+1)$?

1.6 Plus grand commun diviseur, plus petit commun multiple

1.6.1 Diviseurs communs (exemple) Soient $a = 44 = 2^2 \cdot 11$ et $b = 16 = 2^4$. On a

$$\{\text{diviseurs de } 44\} = \{\pm1, \pm2, \pm4, \pm11, \pm22, \pm44\}, \quad \{\text{diviseurs de } 16\} = \{\pm1, \pm2, \pm4, \pm8, \pm16\}$$
$$\{\text{diviseurs communs à 44 et 16}\} := \{\text{diviseurs de } 44\} \cap \{\text{diviseurs de } 16\} =$$
$$= \{\pm1, \pm2, \pm4\} = \{\text{diviseurs de } 4\}.$$

On voit que 4 est le **plus grand commun diviseur** de 44 et 16 **par rapport à la divisibilité** : c'est un diviseur commun à 44 et 16, et chaque diviseur commun à 44 et 16 le divise. On le note

$$\operatorname{pgcd}(44, 16) = 4.$$

1.6.2 Théorème (Existence et unicité du pgcd)**.** *Soient $a, b \in \mathbf{Z} \smallsetminus \{0\}$.*
(1) Il existe un unique entier positif $d \in \mathbf{N}_+$ tel que
(a) $d \mid a$ et $d \mid b$;
(b) si $c \in \mathbf{Z} \smallsetminus \{0\}$, $c \mid a$ et $c \mid b$, alors $c \mid d$.
On le note $\operatorname{pgcd}(a, b)$ *(le plus grand commun diviseur de a et b).*
(2) Si $a = \pm \prod_{p\in\mathcal{P}} p^{v_p(a)}$ et $b = \pm \prod_{p\in\mathcal{P}} p^{v_p(b)}$, alors $d = \operatorname{pgcd}(a, b) = \prod_{p\in\mathcal{P}} p^{\min(v_p(a), v_p(b))}$.
(3) Si $\operatorname{pgcd}(a, b) = 1$*, on dit que les entiers relatifs a et b sont* ***premiers entre eux****.*

Démonstration. (1) L'unicité est facile : si $d, d' \in \mathbf{N}_+$ vérifient (a) et (b), alors $d \mid d'$ et $d' \mid d$, ce qui implique que $d' = \pm d$. On a supposé que $d, d' > 0$, d'où $d' = d$.

On va montrer ici que l'existence du $\operatorname{pgcd}(a, b)$ est une conséquence de la formule (2). Cette formule dépend de l'unicité de factorisation dans le théorème 1.4.2, qui n'a pas encore été démontré dans les paragraphes précédents. Voir le paragraphe 2.3 ci-dessous pour une autre démonstration de l'existence du $\operatorname{pgcd}(a, b)$ qui n'utilise qu'une forme faible du théorème de Bézout $a\mathbf{Z} + b\mathbf{Z} = d\mathbf{Z}$ (mais qui n'utilise pas l'unicité de factorisation).
(2) D'après la proposition 1.5.4(3), on a

$$\{\text{diviseurs de } a\} = \Big\{\pm \prod_{p\in\mathcal{P}} p^{c_p} \mid \forall p \in \mathcal{P} \quad 0 \le c_p \le v_p(a)\Big\}$$
$$\{\text{diviseurs de } b\} = \Big\{\pm \prod_{p\in\mathcal{P}} p^{c_p} \mid \forall p \in \mathcal{P} \quad 0 \le c_p \le v_p(b)\Big\},$$

ce qui implique que

$$\{\text{diviseurs de } a\} \cap \{\text{diviseurs de } b\} = \Big\{ \pm \prod_{p \in \mathcal{P}} p^{c_p} \mid \forall p \in \mathcal{P} \quad 0 \leq c_p \leq \min(v_p(a), v_p(b)) \Big\} = \\ = \{\text{diviseurs de } d\},$$

où $d = \prod_{p \in \mathcal{P}} p^{\min(v_p(a), v_p(b))}$. □

1.6.3 Théorème (Existence et unicité du ppcm)**.** *Soient $a, b \in \mathbf{Z} \smallsetminus \{0\}$.*
(1) Il existe un unique entier positif $m \in \mathbf{N}_+$ tel que
(a) $a \mid m$ et $b \mid m$;
(b) si $c \in \mathbf{Z} \smallsetminus \{0\}$, $a \mid c$ et $b \mid c$, alors $m \mid c$.
On le note $\mathrm{ppcm}(a, b)$ *(le plus petit common multiple de a et b).*
(2) Si $a = \pm \prod_{p \in \mathcal{P}} p^{v_p(a)}$ et $b = \pm \prod_{p \in \mathcal{P}} p^{v_p(b)}$, alors $m = \mathrm{ppcm}(a, b) = \prod_{p \in \mathcal{P}} p^{\max(v_p(a), v_p(b))}$.

Démonstration. (1) Si $m' \in \mathbf{N}_+$ vérifie aussi (a) et (b), alors on a $m \mid m'$ et $m' \mid m$, d'où $m' = \pm m$ et $m' = m$, grâce à la positivité. L'existence est une conséquence de la formule (2), dont la preuve (qui utilise l'unicité de factorisation) suit la même démarche que celle du théorème 1.6.2, sauf que toutes les inéqualités vont dans l'autre sens :

$$\{\text{multiples de } a\} \cap \{\text{multiples de } b\} = \Big\{ \pm \prod_{p \in \mathcal{P}} p^{c_p} \mid \forall p \in \mathcal{P} \quad c_p \geq \max(v_p(a), v_p(b)) \Big\} = \\ = \{\text{multiples de } m\}.$$

□

1.6.4 Caractérisation du pgcd et ppcm En résumé, les entiers positifs $d = \mathrm{pgcd}(a, b), m = \mathrm{ppcm}(a, b) \in \mathbf{N}_+$ sont caractérisés par les propriétés suivantes :

$$\{\text{diviseurs de } a\} \cap \{\text{diviseurs de } b\} = \{\text{diviseurs de } d\},$$
$$\{\text{multiples de } a\} \cap \{\text{multiples de } b\} = \{\text{multiples de } m\}.$$

1.6.5 Exercice. (1) $\forall x, y \in \mathbf{R} \quad \min(x, y) + \max(x, y) = x + y$.
(2) $\forall a, b \in \mathbf{Z} \smallsetminus \{0\} \quad \mathrm{pgcd}(a, b)\mathrm{ppcm}(a, b) = |ab|$.

1.6.6 Exemple du $\mathrm{pgcd}(a, b)$ **et** $\mathrm{ppcm}(a, b)$ Soient $a = 50 = 2^1 \cdot 5^2$ et $b = 15 = 3^1 \cdot 5^1$. On a $\mathrm{pgcd}(a, b) = 5^1 = 5$ et $\mathrm{ppcm}(a, b) = 2^1 \cdot 3^1 \cdot 5^2 = 150$.

1.6.7 Exercice. Si $a_1, \ldots, a_r \in \mathbf{Z} \smallsetminus \{0\}$ $(r \geq 2)$, alors

$$\{\text{diviseurs communs à } a_1, \ldots, a_r\} = \{\text{diviseurs de } d = \mathrm{pgcd}(a_1, \ldots, a_r)\},$$
$$\{\text{multiples communs à } a_1, \ldots, a_r\} = \{\text{multiples de } m = \mathrm{ppcm}(a_1, \ldots, a_r)\},$$

où

$$d = \prod_{p \in \mathcal{P}} p^{\min(v_p(a_1), \ldots, v_p(a_r))}, \qquad m = \prod_{p \in \mathcal{P}} p^{\max(v_p(a_1), \ldots, v_p(a_r))}.$$

Attention : si $r > 2$ alors il n'y a aucune relation générale entre d et m.

1.6.8 Exemple du $\mathrm{pgcd}(a,b,c)$ **et** $\mathrm{ppcm}(a,b,c)$ Le plus grand commun diviseur $\mathrm{pgcd}(6,10,15)$ est égal à $\mathrm{pgcd}(\mathrm{pgcd}(6,10),15) = \mathrm{pgcd}(2,15) = 1$ (et aussi à $\mathrm{pgcd}(6,\mathrm{pgcd}(10,15)) = \mathrm{pgcd}(6,5) = 1$). En termes des factorisations $6 = 2^1 \cdot 3^1$, $10 = 2^1 \cdot 5^1$ et $15 = 3^1 \cdot 5^1$ on a $\mathrm{pgcd}(6,10,15) = 1$ et $\mathrm{ppcm}(6,10,15) = 2^1 \cdot 3^1 \cdot 5^1 = 30$.

1.6.9 Exercice. Soient a et b deux entiers strictement positifs et posons $m = \mathrm{ppcm}(a,b)$. Montrer qu'il existe un diviseur a' de a, un diviseur b' de b, tels que $\mathrm{pgcd}(a',b') = 1$ et $m = a'b'$.
[Par exemple, si $a = 15$ et $b = 20$, alors on peut prendre soit $a' = 15$ et $b' = 4$, soit $a' = 3$ et $b' = 20$.]

2 Algorithme d'Euclide, théorème de Bézout

2.1 Introduction

2.1.1 Description générale L'algorithme d'Euclide est un outil fondamental en arithmétique. On va le rencontrer aussi dans la partie algébrique du cours (voir le paragraphe 10). Cet algorithme n'est rien d'autre qu'une version itérée de la division euclidienne.

L'entrée de l'algorithme est un couple $a, b \in \mathbf{Z} \smallsetminus \{0\}$. La sortie est, d'une part, un entier $d \neq 0$ tel que

$$a\mathbf{Z} + b\mathbf{Z} = d\mathbf{Z} = |d|\mathbf{Z} \tag{2.1.1.1}$$

(une **forme faible du théorème de Bézout**), et d'autre part deux entiers relatifs $u, v \in \mathbf{Z}$ tels que

$$au + bv = d \tag{2.1.1.2}$$

(une **relation de Bézout**). Il est facile de déduire de (2.1.1.1) que l'on a

$$|d| = \mathrm{pgcd}(a, b).$$

Plus précisement, $|d| \in \mathbf{N}_+$ est un diviseur positif commun à a et b qui est divisible par tous les diviseurs communs à a et b.

2.1.2 Théorème de Bézout En particulier, on obtient d'ici une démonstration directe de l'existence du $\mathrm{pgcd}(a, b)$, ainsi qu'une version plus précise de (2.1.1.1) :

$$a\mathbf{Z} + b\mathbf{Z} = \mathrm{pgcd}(a, b)\mathbf{Z} \tag{2.1.2.1}$$

(**le théorème de Bézout**, qu'il ne faut pas confondre avec le théorème de Bézout concernant l'intersection de deux courbes algébriques planes).

En résumé, l'algorithme d'Euclide nous permet, d'une part, d'obtenir des résultats théoriques très importants (on a déjà vu dans la preuve du lemme 1.4.3 que l'égalité (2.1.1.1) implique le lemme Euclide), et d'autre part de calculer explicitement le $\mathrm{pgcd}(a, b)$ et u, v dans (2.1.1.2).

2.1.3 Sous-groupes de Z L'égalité (2.1.2.1) implique par récurrence que l'on a

$$a_1\mathbf{Z} + \cdots + a_r\mathbf{Z} = \mathrm{pgcd}(a_1, \ldots, a_r)\mathbf{Z}, \tag{2.1.3.1}$$

où $r \geq 2$ et $a_i \in \mathbf{Z} \smallsetminus \{0\}$.

Le terme à gauche dans (2.1.3.1) est un sous-groupe additif de $\mathbf{Z}$ (il contient 0 et, s'il contient x et y, il contient aussi $x \pm y$).

Il s'avère qu'une version plus abstraite de (2.1.3.1) est valable : **tout sous-groupe additif** X de $\mathbf{Z}$ s'écrit sous la forme $X = d\mathbf{Z}$, où $d \in \mathbf{N}$ ("tous les sous-groupes de $\mathbf{Z}$ sont cycliques", en utilisant le language abstrait de la Définition 7.2.7 ci-dessous). Ce résultat abstrait sera déduit directement de la division euclidienne dans le théorème 2.3.2.

2.2 Division euclidienne, algorithme d'Euclide (exemple)

2.2.1 Exemple : division de 44 **par** 16 L'entier 16 ne divise pas 44, mais on peut écrire

$$44 = 2 \cdot 16 + 12, \qquad 0 \leq 12 < 16. \tag{2.2.1.1}$$

On dit que 2 est le **quotient** et 12 est le **reste** de la division de 44 par 16. La formule (2.2.1.1) équivaut à

$$\frac{44}{16} = 2 + \frac{12}{16}. \tag{2.2.1.2}$$

Voici le cas général.

2.2.2 Proposition (Division euclidienne)**.** *Soient $a, b \in \mathbf{Z} \smallsetminus \{0\}$. Il existe un unique couple $q, r \in \mathbf{Z}$ tel que*

$$a = qb + r, \qquad 0 \leq r < |b|$$

*(q est le **quotient** et r est le **reste** de la division de a par b). On a, comme dans* (2.2.1.2)*,*

$$\frac{a}{b} = q + \frac{r}{b}.$$

Démonstration. **Unicité :** si l'on a $a = bq + r = bq' + r'$ et $0 \leq r, r' < |b|$, alors $r' - r = b(q - q')$ et

$$-|b| = 0 - |b| \leq r' - |b| < r' - r = b(q - q') < |b| - r \leq |b| - 0 = |b|.$$

On peut diviser ces inégalités par $|b| > 0$; on obtient $-1 < q - q' < 1$. Le seul entier qui vérifie cette inéquality est $q - q' = 0$, ce qui implique que $q = q'$ et $r = r'$.
Existence : on applique le Principe de Minimalité 1.2.3 à l'ensemble

$$S := \mathbf{N} \cap \{a - qb \mid q \in \mathbf{Z}\} = \mathbf{N} \cap (a + b\mathbf{Z}) \subset \mathbf{N}$$

(S est non vide, car $0 \leq a + |a| \leq a + |a||b| \in S$). Soit $r = a - qb \in S$ un élément minimal de S ; on a $r \geq 0$. Si $r \geq |b|$, alors $0 \leq r - |b| = a - (q + \operatorname{sgn}(b))b \in S$, ce qui contredit la minimalité de r. Il en résulte que $0 \leq r < |b|$ et $a = qb + r$, ce qu'il fallait démontrer. □

2.2.3 Algorithme d'Euclide (exemple) L'algorithme d'Euclide fonctionne de la façon suivante. Etant donné un couple d'entiers non nuls (a, b) on calcule d'abord le quotient q et le reste r de la division euclidienne de a par b, et puis on remplace le couple (a, b) par (b, r). On répète la même procédure jusqu'au moment où on obtient un couple $(d, 0)$.

Par exemple, si $a = 44$ et $b = 16$, alors on obtient

$$\begin{aligned} 44 &= 2 \cdot 16 + 12 \\ 16 &= 1 \cdot 12 + 4 \\ 12 &= 3 \cdot 4 + 0 \\ 4 &= d \end{aligned}$$

Ces égalités impliquent par récurrence, d'une part, que le dernier entier $d = 4$ divise tous les entiers qui apparaîssent à gauche, à savoir

$$12 = 3 \cdot 4, \qquad 16 = 1 \cdot 12 + 4, \qquad 44 = 2 \cdot 16 + 12.$$

En particulier, 4 est un diviseur commun à 44 et 16. D'autre part, on peut exprimer ces entiers comme des combinaisons linéaires entières de 44 et 16 :

$$44 = 1 \cdot 44 + 0 \cdot 16 \tag{2.2.3.1}$$
$$16 = 0 \cdot 44 + 1 \cdot 16 \tag{2.2.3.2}$$
$$12 = 1 \cdot 44 + (-2) \cdot 16 \tag{2.2.3.3}$$
$$4 = 16 - 1 \cdot 12 = 16 - (44 - 2 \cdot 16) = (-1) \cdot 44 + 3 \cdot 16 \tag{2.2.3.4}$$

Autrement dit, on a

$$4 \mid 44, \quad 4 \mid 16 \tag{2.2.3.5}$$
$$4 \in 44\mathbf{Z} + 16\mathbf{Z} \tag{2.2.3.6}$$

On peut reformuler les deux énoncés (2.2.3.5) et (2.2.3.6) en disant que

$$44\mathbf{Z} + 16\mathbf{Z} = 4\mathbf{Z} \tag{2.2.3.7}$$

En effect, (2.2.3.5) équivaut à

$$44\mathbf{Z} \subseteq 4\mathbf{Z}, \quad 16\mathbf{Z} \subseteq 4\mathbf{Z},$$

ce qui implique que $44\mathbf{Z} + 16\mathbf{Z} \subseteq 4\mathbf{Z}$, tandis que (2.2.3.6) implique l'inclusion réciproque $4\mathbf{Z} \subseteq 44\mathbf{Z} + 16\mathbf{Z}$.

Réciproquemnt, la relation de Bézout (2.2.3.7) implique, d'une part, (2.2.3.6), et d'autre part que

$$4\mathbf{Z} = 44\mathbf{Z} + 16\mathbf{Z} \supseteq 44\mathbf{Z}, \quad 4\mathbf{Z} = 44\mathbf{Z} + 16\mathbf{Z} \supseteq 16\mathbf{Z},$$

ce qui équivaut à (2.2.3.5).

De plus, si $c \in \mathbf{Z} \smallsetminus \{0\}$ est un diviseur commun à 44 et 16, alors il divise tous les éléments de $44\mathbf{Z} + 16\mathbf{Z} = 4\mathbf{Z}$; en particulier, c divise 4.

En résumé, (2.2.3.7) implique directement que l'entier 4 vérifie les propriétés (a) et (b) dans le théorème 1.6.2(1) (pour $a = 44$ et $b = 16$), d'où $4 = \mathrm{pgcd}(44, 16)$ et

$$44\mathbf{Z} + 16\mathbf{Z} = \mathrm{pgcd}(44, 16)\mathbf{Z}. \tag{2.2.3.8}$$

2.2.4 Algorithme d'Euclide et fractions continues (exemple) On peut itérer la formule (2.2.1.2) pour obtenir

$$\frac{44}{16} = 2 + \frac{12}{16}, \qquad \frac{16}{12} = 1 + \frac{4}{12}, \qquad \frac{12}{4} = 3,$$

ce qui implique que

$$\frac{44}{16} = 2 + \frac{1}{1 + \dfrac{1}{3}} = 2 + \frac{3}{4} = \frac{11}{4}. \tag{2.2.4.1}$$

L'objet qui apparaît dans (2.2.4.1) est un exemple d'une fraction continue (finie). Il s'avère que les coefficients dans la combinaison linéaire

$$4 = 3 \cdot 16 - 1 \cdot 44 \tag{2.2.4.2}$$

qu'on a trouvée en utilisant l'algorithme d'Euclide sont déterminés par la fraction continue (2.2.4.1) : il suffit de supprimer le dernier terme de la fraction pour obtenir

$$2 + \frac{1}{1} = \frac{3}{1}. \tag{2.2.4.3}$$

De même, on obtient les coefficients dans la combinaison linéaire

$$12 = (-2) \cdot 16 + 1 \cdot 44 \tag{2.2.4.4}$$

si l'on supprime les deux derniers termes dans (2.2.4.1) :

$$2 = \frac{2}{1}. \tag{2.2.4.5}$$

Les formules ci-dessus s'écrivent sous la forme matricielle suivante :

$$\begin{pmatrix}-16 & 44\end{pmatrix}\begin{pmatrix}0 & 1 & 2 & 3 & 11\\ 1 & 0 & 1 & 1 & 4\end{pmatrix} = \begin{pmatrix}44 & -16 & 12 & -4 & 0\end{pmatrix}. \tag{2.2.4.6}$$

On peut remplacer ici 44 et 16 par un couple quelconque d'entiers non nuls ; voir le paragraphe 2.4 ci-dessous.

2.3 Sous-groupes de Z, théorème de Bézout

2.3.1 Sous-groupes de Z Rappelons qu'un sous-ensemble $X \subset \mathbf{Z}$ est un sous-groupe (additif) de $\mathbf{Z}$ si $0 \in X$, et si $x \pm y \in X$ dès que $x, y \in X$. Voici quelques propriétés de base :

- si $a_i \in \mathbf{Z}$, alors $X = a_1\mathbf{Z} + \cdots + a_r\mathbf{Z} = \{a_1x_1 + \cdots + a_rx_r \mid x_i \in \mathbf{Z}\}$ est un sous-groupe de $\mathbf{Z}$.
- En particulier, $d\mathbf{Z} = (-d)\mathbf{Z}$ est un sous-groupe de $\mathbf{Z}$, pour tout $d \in \mathbf{Z}$.
- Si $X \subset \mathbf{Z}$ est un sous-groupe et $x_1, \ldots, x_r \in X$, alors $a_1x_1 + \cdots + a_rx_r \in X$, pour tous $a_i \in \mathbf{Z}$ (autrement dit, $\mathbf{Z}x_1 + \cdots + \mathbf{Z}x_r \subset X$).

2.3.2 Théorème (Structure de sous-groupes de $\mathbf{Z}$)**.** *Si $X \subset \mathbf{Z}$ est un sous-groupe, alors il existe $d \in \mathbf{N}$ (unique) tel que $X = d\mathbf{Z}$.*

Démonstration. Si $X = \{0\}$, alors $d = 0$. On suppose que $X \neq \{0\}$. Il faut montrer que l'on a $X = d\mathbf{Z}$, où $d \in \mathbf{N}_+$. On a $d = \min\{|a| \mid 0 \neq a \in d\mathbf{Z}\}$; nous allons définir d de la même façon en remplacant $d\mathbf{Z}$ par X. Le sous-ensemble $S := \{|a| \mid 0 \neq a \in X\} \subset \mathbf{N}_+$ étant non vide, le Principe de Minimalité 1.2.3 implique qu'il existe un élément minimal $d \in S$. On va montrer qu'on a bien $X = d\mathbf{Z}$. D'une part, X contient d ou $-d$ (ou les deux), ce qui implique que $d\mathbf{Z} = (-d)\mathbf{Z} \subseteq X$, d'après le troisième point dans 2.3.1. S'il existait $a \in X$ tel que $a \notin d\mathbf{Z}$, alors on pourrait soustraire de a un multiple convenable de d pour obtenir un élément non nul de X dont la valeur absolue soit plus petite que d : la division euclidienne de a par d implique qu'on a $a = qd + r$, où $q, r \in \mathbf{Z}$, $0 \leq r < d$ et $r \neq 0$ (car $a \notin d\mathbf{Z}$). On sait que $a \in A$ et $qd \in d\mathbf{Z} \subset X$; il en résulte que $0 \neq r = a - qd \in X$ et $|r| = r < d$. On a obtenu une contradiction vu la minimalité de d. Par conséquent chaque $a \in X$ appartient à $d\mathbf{Z}$, d'où $X = d\mathbf{Z}$. □

2.3.3 Théorème (Théorème de Bézout)**.** *Soient $a, b \in \mathbf{Z} \smallsetminus \{0\}$. Il existe un unique entier positif $d \in \mathbf{N}_+$ tel que $a\mathbf{Z} + b\mathbf{Z} = d\mathbf{Z}$. Il vérifie les propriétés (a) et (b) dans le théorème 1.6.2(1) :*
(a) $d \mid a$ et $d \mid b$;
(b) si $c \in \mathbf{Z} \smallsetminus \{0\}$, $c \mid a$ et $c \mid b$, alors $c \mid d$.
Autrement dit, on a $d = \mathrm{pgcd}(a, b)$ et $a\mathbf{Z} + b\mathbf{Z} = \mathrm{pgcd}(a, b)\mathbf{Z}$.

Démonstration. L'existence et unicité de $d \in \mathbf{N}_+$ tel que $a\mathbf{Z} + b\mathbf{Z} = d\mathbf{Z}$ est un cas particulier du théorème 2.3.2, pour $X = a\mathbf{Z} + b\mathbf{Z}$. On vérifie les propriétés (a) et (b) de la même façon que dans 2.2.3 : d'une part, $a\mathbf{Z} \subseteq a\mathbf{Z} + b\mathbf{Z} = d\mathbf{Z}$, d'où $d \mid a$ (idem pour $d \mid b$). D'autre part, si $c \in \mathbf{Z} \smallsetminus \{0\}$ divise a et b, alors $c\mathbf{Z} \subset \mathbf{Z}$ est un sous-groupe contenant a et b, ce qui implique que $c\mathbf{Z} \supseteq a\mathbf{Z} + b\mathbf{Z} = d\mathbf{Z}$ (d'après le troisième point dans 2.3.1), ce qui équivaut à $c \mid d$. □

2.3.4 Remarques La preuve de l'existence de $\mathrm{pgcd}(a, b)$ ci-dessus est inconditionnelle. Elle n'utilise pas l'unicité de factorisation. De plus, on obtient la caractérisation suivante de $\mathrm{pgcd}(a, b)$: c'est l'unique entier positif $d > 0$ tel que $a\mathbf{Z} + b\mathbf{Z} = d\mathbf{Z}$.

La relation $a\mathbf{Z} + b\mathbf{Z} = \mathrm{pgcd}(a, b)\mathbf{Z}$ équivaut à

$$\frac{1}{a}\mathbf{Z} + \frac{1}{b}\mathbf{Z} = \frac{1}{ab}(b\mathbf{Z} + a\mathbf{Z}) = \frac{\mathrm{pgcd}(a,b)}{ab}\mathbf{Z} = \frac{1}{\mathrm{ppcm}(a,b)}\mathbf{Z}.$$

On déduit du théorème 2.3.3 par récurrence que l'on a, pour tous $a_i \in \mathbf{Z} \smallsetminus \{0\}$,

$$a_1\mathbf{Z} + \cdots + a_r\mathbf{Z} = d\mathbf{Z},$$

où $d \in \mathbf{N}_+$ vérifie

$$\{\text{diviseurs communs à } a_1, \ldots, a_r\} = \{\text{diviseurs de } d\}.$$

Cette propriété caractérise $\mathrm{pgcd}(a_1, \ldots, a_r)$, ce qui implique que l'on a $d = \mathrm{pgcd}(a_1, \ldots, a_r)$ et

$$a_1\mathbf{Z} + \cdots + a_r\mathbf{Z} = \mathrm{pgcd}(a_1, \ldots, a_r)\mathbf{Z}.$$

2.3.5 Exercice. (1) Déterminer $\frac{2}{5}\mathbf{Z} + \frac{3}{7}\mathbf{Z}$.
(2) Soient $a_i \in \mathbf{Z} \smallsetminus \{0\}$. Montrer :

$$\frac{1}{a_1}\mathbf{Z} + \cdots + \frac{1}{a_r}\mathbf{Z} = \frac{1}{\mathrm{ppcm}(a_1, \ldots, a_r)}\mathbf{Z}.$$

2.3.6 Corollaire. *Soient $a, b, c \in \mathbf{Z} \smallsetminus \{0\}$. Si $c \mid a$ et $c \mid b$, alors $\mathrm{pgcd}(a/c, b/c) = \mathrm{pgcd}(a,b)/|c|$. En particulier, si $d = \mathrm{pgcd}(a,b)$, alors $\mathrm{pgcd}(a/d, b/d) = 1$. Par conséquent, $a/b = a'/b'$, où $a' = a/d$, $b' = b/d$ et $\mathrm{pgcd}(a', b') = 1$.*

Démonstration. On sait que $c \mid d$, ce qui implique qu'on peut diviser l'égalité $a\mathbf{Z} + b\mathbf{Z} = d\mathbf{Z}$ par c. On obtient $(a/c)\mathbf{Z} + (b/c)\mathbf{Z} = (d/c)\mathbf{Z} = (d/|c|)\mathbf{Z}$ avec $d/|c| > 0$, d'où $\mathrm{pgcd}(a/c, b/c) = \mathrm{pgcd}(a,b)/|c|$. □

2.3.7 Exercice. (1) Démontrer le corollaire 2.3.6 en utilisant le théorème 1.6.2(2).
(2) Montrer : si $\mathrm{pgcd}(a,b) = 1$, alors $\mathrm{pgcd}(a^m, b^n) = 1$ pour tous $m, n \in \mathbf{N}_+$.

2.3.8 Lemme. *Soient $a, b, c \in \mathbf{Z} \smallsetminus \{0\}$. Si $c \mid ab$ et $\mathrm{pgcd}(c,b) = 1$, alors $c \mid a$.*

Démonstration. D'après le théorème de Bézout on a $c\mathbf{Z} + b\mathbf{Z} = \mathrm{pgcd}(c,b)\mathbf{Z} = \mathbf{Z}$. On multiplie cette égalité par a ; on obtient

$$a\mathbf{Z} = ac\mathbf{Z} + ab\mathbf{Z} \subseteq ac\mathbf{Z} + c\mathbf{Z} \subseteq c\mathbf{Z} + c\mathbf{Z} = c\mathbf{Z}$$

(car $c\mathbf{Z} \supseteq ab\mathbf{Z}$), ce qui équivaut à $c \mid a$. □

2.3.9 Lemme (Lemme d'Euclide (bis))**.** *Soient $a, b \in \mathbf{Z} \smallsetminus \{0\}$, soit p un nombre premier. Si $p \mid ab$ et $p \nmid b$, alors $p \mid a$.*

Démonstration. L'entier positif $d := \mathrm{pgcd}(p,b)$ divise p, ce qui implique que $d = 1$ ou $d = p$. It divise aussi b, mais $p \nmid b$; il en résulte que $d = 1$. Le lemme 2.3.8 s'applique alors avec $c = p$. □

2.3.10 Remarque La preuve du lemme d'Euclide ci-dessus termine la démonstration de l'unicité de factorisation (le théorème 1.4.2). Une preuve moins abstraite du théorème de Bézout sera présentée dans le théorème 2.4.2 ci-dessous ; elle utilise l'algorithme d'Euclide.

2.3.11 Exercice. Soit p un nombre premier, soit $x \in \mathbf{Z}$. Montrer :
(1) Si $p \mid (x^2-1)$, alors $p \mid (x-1)$ ou $p \mid (x+1)$.
(2) Si $p^k \mid (x^2-1)$, $k>1$ et $p \neq 2$, alors $p^k \mid (x-1)$ ou $p^k \mid (x+1)$.
(3) Que se passe-t-il si $p=2$ dans (2) ?

2.3.12 Théorème (Une autre preuve d'irrationalité de $\sqrt[n]{a}$)**.** *Si $a, n \in \mathbf{N}_+$, alors il est équivalent :* $\sqrt[n]{a} \in \mathbf{Q} \iff \sqrt[n]{a} \in \mathbf{Z}$.

Démonstration. Si $\sqrt[n]{a} \in \mathbf{Q}$, alors $\sqrt[n]{a} = c/b$ avec $b, c \in \mathbf{N}_+$ tels que $\operatorname{pgcd}(c,b)=1$. L'entier $ab^n = c^n$ est divisible par c^n et $\operatorname{pgcd}(c^n, b^n) = \operatorname{pgcd}(c,b)^n = 1$. Le lemme 2.3.8 s'applique alors au triplet a, b^n, c^n ; on en déduit que $c^n = ab^n$ divise a. Ceci n'est possible que si $|b^n| = 1$, ce qui implique que $b=1$ et $\sqrt[n]{a} = c/b = c \in \mathbf{N}_+$. □

2.3.13 Racines rationnelles de polynômes On peut reformuler le théorème 2.3.12 de la façon suivante : "si $\alpha \in \mathbf{Q}$ est une racine du polynôme $X^n - a$ (où $a, n \in \mathbf{N}_+$), alors $\alpha \in \mathbf{Z}$." Que se passe-t-il si l'on remplace $X^n - a$ par un polynôme plus général ?

2.3.14 Théorème (Racines rationnelles de polynômes)**.** *Soient $a_0, \ldots, a_n \in \mathbf{Z}$, $a_0 \neq 0$, $n \geq 1$. Si $\alpha = a/b \in \mathbf{Q}$ (où $a, b \in \mathbf{Z} \smallsetminus \{0\}$ et $\operatorname{pgcd}(a,b)=1$) est une racine de l'équation polynômiale $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n = 0$, alors $a \mid a_n$ et $b \mid a_0$. En particulier, si $a_0 = 1$, alors $\alpha = a/b \in \mathbf{Z}$.*

Démonstration. On multiplie l'égalité

$$a_0\left(\frac{a}{b}\right)^n + a_1\left(\frac{a}{b}\right)^{n-1} + \cdots + a_{n-1}\left(\frac{a}{b}\right) + a_n = 0$$

par b^n ; on obtient

$$a_0a^n + a_1a^{n-1}b + \cdots + a_{n-1}ab^{n-1} + a_nb^n = 0.$$

La somme de tous les termes est égale à zéro et tous les termes sauf le dernier a_nb^n sont divisibles par a, ce qui implique que $a \mid a_nb^n$. On a $\operatorname{pgcd}(a, b^n) = 1$; on déduit du lemme 2.3.8 que $a \mid a_n$. De même, tous les termes sauf le premier a_0a^n sont divisibles par b, d'où $b \mid a_0a^n$. Le même raisonnement montre alors (en utilisant le fait que $\operatorname{pgcd}(b, a^n) = 1$) que $b \mid a_0$. □

2.3.15 Exercice. Trouver toutes les racines $\alpha \in \mathbf{Q}$ de l'équation $f(x) = x^3 + x^2 - 5x + 3 = 0$.

2.3.16 Terminologie On appelle un nombre complexe $\alpha \in \mathbf{C}$ qui est une racine d'une équation polynômiale

$$a_0\alpha^n + a_1\alpha^{n-1} + \cdots + a_n = 0$$

où $a_j \in \mathbf{Z}$ (avec $n \geq 1$ et $a_0 \neq 0$) un **nombre algébrique**. Si l'on a, de plus, $a_0 = 1$, on dit que α est un **entier algébrique**. La deuxième partie du théorème 2.3.14 affirme qu'un entier algébrique qui appartient à $\mathbf{Q}$ est un entier relatif usuel.

2.4 Algorithme d'Euclide

2.4.1 Algorithme d'Euclide (le cas général Soient $a, b \in \mathbf{Z} \smallsetminus \{0\}$. La division euclidienne de a par b nous permet d'écrire $a = qb + r$, où $0 \leq r < |b|$. On remplace le couple (a, b) par (b, r) et puis procède de la même manière ; on s'arrête quand on obtient un couple $(d, 0)$.

Chaque reste successif dans cette procédure sera donné par une combinaison linéaire explicite des entiers a et b ; il sera également divisible par d. On obtiendra d'ici une version faible du théorème de Bézout sous la forme $a\mathbf{Z} + b\mathbf{Z} = d\mathbf{Z}$ (ce qui implique que $|d| = \mathrm{pgcd}(a, b)$), et une relation de Bézout explicite $au + bv = d$ (où $u, v \in \mathbf{Z}$).

Plus précisement, on écrit $r_{-2} = a$, $r_{-1} = b$ et

$$\begin{aligned} a &= a_0 b + r_0 & 0 \leq r_0 < |b| \\ b &= a_1 r_0 + r_1 & 0 \leq r_1 < r_0 \\ r_0 &= a_2 r_1 + r_2 & 0 \leq r_2 < r_1 \\ &\vdots & \vdots \\ r_{k-2} &= a_k r_{k-1} + r_k & 0 = r_k < r_{k-1} \end{aligned} \tag{2.4.1.1}$$

Il existe toujours un entier $k \geq 0$ tel que $r_{k-1} > r_k = 0$, puisque la suite d'entiers positifs

$$|b| = |r_{-1}| > r_0 > r_1 > \cdots > r_{k-1} > r_k = 0$$

est strictement décroissante. On note $d := r_{k-1}$.

Tous les phénomènes qu'on a remarqués dans le paragraphe 2.2.3 dans le cas particulier $a = 44$ et $b = 16$ sont valables en général. Par exemple, les identités

$$\frac{r_i}{r_{i+1}} = a_{i+2} + \frac{1}{r_{i+1}/r_{i+2}} \qquad (0 \leq i + 2 \leq k)$$

impliquent qu'on a une fraction continue

$$\frac{a}{b} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_k}}} \tag{2.4.1.2}$$

2.4.2 Théorème (Propriétés de l'algorithme d'Euclide)**.** *(1) $d \mid r_i \quad (-2 \leq i \leq k)$*
(2) $r_i \in a\mathbf{Z} + b\mathbf{Z} \quad (-2 \leq i \leq k)$
(3) $d \mid a$, $d \mid b$ et il existe $u, v \in \mathbf{Z}$ tels que $au + bv = d$.
(4) $a\mathbf{Z} + b\mathbf{Z} = d\mathbf{Z}$ (version faible du théorème de Bézout).
(5) $|d| = \mathrm{pgcd}(a, b)$ et $a\mathbf{Z} + b\mathbf{Z} = \mathrm{pgcd}(a, b)\mathbf{Z}$ (version forte du théorème de Bézout).

Démonstration. (1) Récurrence décroissante sur i à partir de $i = k$ et $i = k - 1$: on a $r_k = 0$, $r_{k-1} = d$ et $r_i = a_{i+2} r_{i+1} + r_{i+2}$.
(2) Récurrence croissante sur i à partir de $i = -2$ et $i = -1$: on a $r_{-2} = a$, $r_{-1} = b$ et $r_{i+2} = r_i - a_{i+2} r_{i+1}$.
(3) Il s'agit d'un cas particulier de (1) pour $i = -2$, $i = -1$ et de (2) pour $i = k - 1$.
(4) Le raisonnement de 2.2.3 s'applique : (3) implique, d'une part, que $d\mathbf{Z} \supseteq a\mathbf{Z}$ et $d\mathbf{Z} \supseteq b\mathbf{Z}$, d'où $d\mathbf{Z} \supseteq a\mathbf{Z} + b\mathbf{Z}$, et d'autre part $d \in a\mathbf{Z} + b\mathbf{Z}$ implique que $d\mathbf{Z} \subseteq a\mathbf{Z} + b\mathbf{Z}$.
(5) est une conséquence de (4) ; voir la preuve du théorème 2.3.3. □

2.4.3 Relations de Bézout explicites L'algorithme d'Euclide fournit des entiers explicites $u_i, v_i \in \mathbf{Z}$ tels que $u_i a + v_i b = r_i$, pour chaque $-2 \leq i \leq k$. En particulier, on obtient $u = u_{k-1}$ et $v = v_{k-1}$ tels que $ua + vb = d = \mathrm{sgn}(d)\mathrm{pgcd}(a, b)$.

Si les entiers a et b ne sont pas trop grands on peut calculer les valeurs de u_i et v_i à la main ; voir l'exemple (2.2.3.1)–(2.2.3.4). En général, on peut exprimer les coefficients u_i, v_i en termes de la fraction continue (2.4.1.2) ; voir l'exemple 2.2.4. Voici les formules générales.

On fixe $j \geq 0$. Il faut écrire la fraction continue

$$[a_0, \ldots, a_j] := a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_j}}} \tag{2.4.3.1}$$

sous la forme p_j/q_j. Par exemple, on a

$$\frac{p_0}{q_0} = \frac{a_0}{1}, \qquad \frac{p_1}{q_1} = a_0 + \frac{1}{a_1} = \frac{a_0 a_1 + 1}{a_1}, \qquad \frac{p_2}{q_2} = a_0 + \frac{a_2}{a_1 a_2 + 1} = \frac{a_2(a_0 a_1 + 1) + a_0}{a_1 a_2 + 1}.$$

La table

j	-2	-1	0	1	2
a_j			a_0	a_1	a_2
p_j	0	1	a_0	$a_0 a_1 + 1$	$a_2(a_0 a_1 + 1) + a_0$
q_j	1	0	1	a_1	$a_1 a_2 + 1$

suggère qu'on a (si l'on pose $p_{-2} = q_{-1} = 0$ et $p_{-1} = q_{-2} = 1$)

$$p_j = a_j p_{j-1} + p_{j-2}$$
$$q_j = a_j q_{j-1} + q_{j-2}$$

($j \geq 0$), ce qui équivaut aux équations matricielles

$$\begin{pmatrix} p_j & p_{j-1} \\ q_j & q_{j-1} \end{pmatrix} = \begin{pmatrix} p_{j-1} & p_{j-2} \\ q_{j-1} & q_{j-2} \end{pmatrix} M_j, \qquad M_j = \begin{pmatrix} a_j & 1 \\ 1 & 0 \end{pmatrix}. \tag{2.4.3.2}$$

C'est bien le cas (voir le paragraphe 2.4.6 ci-dessous). On en déduit par récurrence les identités suivantes

$$\forall j \geq -1 \qquad M_0 \cdots M_j = \begin{pmatrix} p_j & p_{j-1} \\ q_j & q_{j-1} \end{pmatrix}, \tag{2.4.3.3}$$

ce qui implique que

$$\forall j \geq -1 \quad \begin{vmatrix} p_j & p_{j-1} \\ q_j & q_{j-1} \end{vmatrix} = (-1)^{j+1}, \quad \begin{pmatrix} p_j & p_{j-1} \\ q_j & q_{j-1} \end{pmatrix}^{-1} = (-1)^{j+1} \begin{pmatrix} q_{j-1} & -p_{j-1} \\ -q_j & p_j \end{pmatrix}.$$

De même, les relations $r_{j-2} = a_j r_{j-1} + r_j$ s'écrivent sous la forme matricielle

$$\forall j = 0, \ldots, k \qquad M_j \begin{pmatrix} r_{j-1} \\ r_j \end{pmatrix} = \begin{pmatrix} r_{j-2} \\ r_{j-1} \end{pmatrix}.$$

On obtient d'ici par récurrence les identités

$$\forall j = -1, \dots, k \qquad M_0 \cdots M_j \begin{pmatrix} r_{j-1} \\ r_j \end{pmatrix} = \begin{pmatrix} r_{-2} \\ r_{-1} \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix}$$

et

$$\forall j = -1, \dots, k \qquad \begin{pmatrix} r_{j-1} \\ r_j \end{pmatrix} = (-1)^{j+1} \begin{pmatrix} q_{j-1} & -p_{j-1} \\ -q_j & p_j \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}.$$

Les formules pour r_j s'écrivent sous la forme

$$\forall j = -2, \dots, k \qquad (-1)^j r_j = q_j a - p_j b = \begin{pmatrix} -b & a \end{pmatrix} \begin{pmatrix} p_j \\ q_j \end{pmatrix}. \tag{2.4.3.4}$$

Si on les met ensemble on obtient l'identité matricielle suivante :

$$\begin{pmatrix} -b & a \end{pmatrix} \begin{pmatrix} p_{-2} & p_{-1} & p_0 & \cdots & p_{k-1} & p_k \\ q_{-2} & q_{-1} & q_0 & \cdots & q_{k-1} & q_k \end{pmatrix} = \begin{pmatrix} a & -b & r_0 & \cdots & (-1)^j r_j & \cdots & (-1)^{k-1} d & 0 \end{pmatrix}. \tag{2.4.3.5}$$

On a déjà rencontré un cas particulier de cette formule dans (2.2.4.6).

En particulier, le cas $j = k - 1$ de (2.4.3.4) fournit une relation de Bézout explicite

$$q_{k-1} a - p_{k-1} b = (-1)^{k-1} d, \qquad |d| = \operatorname{pgcd}(a, b).$$

2.4.4 Exemples En résumé, si l'on applique l'algorithme d'Euclide au couple $a, b \in \mathbf{Z} \smallsetminus \{0\}$ on obtient des entiers a_j et r_j ($0 \leq j \leq k$) vérifiant (2.4.1.1). On pose $r_{-2} = a$ et $r_{-1} = b$. On calcule les entiers p_j et q_j ($-2 \leq j \leq k$) en utilisant les formules récursives (2.4.3.2). Il est commode d'écrire le résultat sous la forme d'une table

j	-2	-1	0	1	$\cdots$	$k-1$	k
a_j			a_0	a_1	$\cdots$	a_{k-1}	a_k
p_j	0	1	a_0	$a_0 a_1 + 1$	$\cdots$	p_{k-1}	p_k
q_j	1	0	1	a_1	$\cdots$	q_{k-1}	q_k

Les fractions continues (2.4.3.1) sont égales alors à

$$\forall j = 0, \dots, k \qquad [a_0, \dots, a_j] = \frac{p_j}{q_j}.$$

On a, d'une part, $\operatorname{pgcd}(p_j, q_j) = 1$, car $p_j q_{j-1} - q_j p_{j-1} = \pm 1$, et d'autre part $\operatorname{pgcd}(a, b) = |d|$, où $d = r_{k-1}$. En particulier, on en déduit pour $j = k$ que

$$\frac{a}{b} = [a_0, \dots, a_k] = \frac{p_k}{q_k}, \qquad |a/d| = |p_k|, \qquad |b/d| = |q_k|.$$

La formule matricielle (2.4.3.5) nous permet d'exprimer les entiers r_j (en particulier, $d = r_{k-1}$ et $\operatorname{pgcd}(a, b) = |d|$) sous la forme $u_j a + v_j b = r_j$ (d'où une **relation de Bézout explicite** $ua + vb = d$ pour a et b).

Exemple 1 : $a = 18$, $b = 11$. On calcule

$$18 = 1 \cdot 11 + 7, \qquad 11 = 1 \cdot 7 + 4, \qquad 7 = 1 \cdot 4 + 3, \qquad 4 = 1 \cdot 3 + 1, \qquad 3 = 3 \cdot 1 + 0$$

j	-2	-1	0	1	2	3	4
a_j			1	1	1	1	3
p_j	0	1	1	2	3	5	18
q_j	1	0	1	1	2	3	11

ce qui implique que l'on a

$$\mathrm{pgcd}(18,11)=1, \qquad 5\cdot 11+(-3)\cdot 18=1$$

et

$$\begin{pmatrix}-11 & 18\end{pmatrix}\begin{pmatrix}0 & 1 & 1 & 2 & 3 & 5\\ 1 & 0 & 1 & 1 & 2 & 3\end{pmatrix}=\begin{pmatrix}18 & -11 & 7 & -4 & 3 & -1\end{pmatrix}.$$

On peut aussi calculer directement

$$7=18-11, \qquad 4=11-(18-11)=2\cdot 11-18, \qquad 3=(18-11)-(2\cdot 11-18)=$$
$$=2\cdot 18-3\cdot 11, \qquad 1=(2\cdot 11-18)-(2\cdot 18-3\cdot 11)=5\cdot 11-3\cdot 18$$

ou

$$1+\cfrac{1}{1+\cfrac{1}{1+\frac{1}{1}}}=1+\frac{1}{1+\frac{1}{2}}=1+\frac{2}{3}=\frac{5}{3}.$$

Exemple 2 : $a=31$, $b=13$. On calcule

$$31=2\cdot 13+5, \qquad 13=2\cdot 5+3, \qquad 5=1\cdot 3+2, \qquad 3=1\cdot 2+1, \qquad 2=2\cdot 1+0$$

j	-2	-1	0	1	2	3	4
a_j			2	2	1	1	2
p_j	0	1	2	5	7	12	31
q_j	1	0	1	2	3	5	13

ce qui implique que l'on a

$$\mathrm{pgcd}(31,13)=1, \qquad 12\cdot 13+(-5)\cdot 31=1$$

et

$$\begin{pmatrix}-13 & 31\end{pmatrix}\begin{pmatrix}0 & 1 & 2 & 5 & 7 & 12\\ 1 & 0 & 1 & 2 & 3 & 5\end{pmatrix}=\begin{pmatrix}31 & -13 & 5 & -3 & 2 & -1\end{pmatrix}.$$

On peut aussi calculer directement

$$5=31-2\cdot 13, \qquad 3=13-2\cdot(31-2\cdot 13)=5\cdot 13-2\cdot 31,$$
$$2=(31-2\cdot 13)-(5\cdot 13-2\cdot 31)=3\cdot 31-7\cdot 13,$$
$$1=(5\cdot 13-2\cdot 31)-(3\cdot 31-7\cdot 13)=12\cdot 13-5\cdot 31$$

ou

$$2+\cfrac{1}{2+\cfrac{1}{1+\frac{1}{1}}}=2+\frac{1}{2+\frac{1}{2}}=2+\frac{2}{5}=\frac{12}{5}.$$

2.4.5 Algorithme d'Euclide modifié On peut modifier la division euclidienne qu'on a introduite dans la proposition 2.2.2 de la façon suivante : on autorise un **reste négatif**, mais on exige que sa valeur absolue soit minimale. On remplace alors les conditions

$$a = qb + r, \qquad 0 \leq r < |b|$$

par

$$a = q'b + r', \qquad |r'| \leq |b|/2.$$

Par exemple, on peut écrire

$$\begin{aligned} a &= 5q + 3 = 5(q+1) + (-2) \\ a &= 4q + 3 = 4(q+1) + (-1) \\ a &= 4q + 2 = 4(q+1) + (-2). \end{aligned}$$

Si b est impair, alors le couple (q', r') est unique. Il en est de même si b est pair et $r < |b|/2$. Si b est pair et $r = |b|/2$, alors il y a deux possibilités pour (q', r'), à savoir $a = qb + |b|/2$ et $a = (q + \mathrm{sgn}(b))b + (-|b|/2)$.

L'algorithme d'Euclide modifié utilise la division euclidienne modifieée qu'on vient d'introduire au lieu de la division euclidienne usuelle. Cette modification améliore l'efficacité de l'algorithme. Par exemple, les calculs qu'on a faits dans 2.2.3 pour $a = 44$ et $b = 16$ ont nécessité trois divisions euclidiennes. Par contre, il n'y a que deux divisions dans la version modifiée :

$$\begin{aligned} 44 &= 3 \cdot 16 + (-4) \\ 16 &= (-4) \cdot (-4) + 0 \\ -4 &= d' \end{aligned}$$

La fraction continue correspondante est égale à

$$\frac{44}{16} = 3 + \frac{1}{-4}$$

La table de coefficients

j	-2	-1	0	1
a_j			3	-4
p_j	0	1	3	-11
q_j	1	0	1	-4

nous donne les relations de Bézout explicites suivantes

$$1 \cdot 44 + (-3) \cdot 16 = -4, \qquad \mathrm{pgcd}(44, 16) = 4$$

et

$$\begin{pmatrix} -16 & 44 \end{pmatrix} \begin{pmatrix} 0 & 1 & 3 \\ 1 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 44 & -16 & -4 \end{pmatrix}.$$

On peut faire la même chose dans les deux exemples qu'on a considérés dans le paragraphe 2.4.4 :

Exemple 1 : $a = 18$, $b = 11$. On a

$$18 = 2 \cdot 11 + (-4), \qquad 11 = (-3) \cdot (-4) + (-1), \qquad -4 = 4 \cdot (-1) + 0, \qquad -1 = d',$$
$$-4 = 18 - 2 \cdot 11, \qquad -1 = 11 + 3(18 - 2 \cdot 11) = 3 \cdot 18 - 5 \cdot 11, \qquad 1 = 5 \cdot 11 - 3 \cdot 18.$$

La table

j	-2	-1	0	1	2
a_j			2	-3	4
p_j	0	1	2	-5	-18
q_j	1	0	1	-3	-11

nous donne les relations suivantes :

$$\mathrm{pgcd}(18, 11) = 1, \qquad 5 \cdot 11 + (-3) \cdot 18 = 1$$

et

$$\begin{pmatrix} -11 & 18 \end{pmatrix} \begin{pmatrix} 0 & 1 & 2 & -5 \\ 1 & 0 & 1 & -3 \end{pmatrix} = \begin{pmatrix} 18 & -11 & -4 & 1 \end{pmatrix}.$$

Exemple 2 : $a = 31$, $b = 13$. On a

$$31 = 2 \cdot 13 + 5, \qquad 13 = 3 \cdot 5 + (-2), \qquad 5 = (-2) \cdot (-2) + 1, \qquad -2 = (-2) \cdot 1 + 0, \qquad 1 = d',$$
$$5 = 31 - 2 \cdot 13, \qquad -2 = 13 - 3(31 - 2 \cdot 13) = 7 \cdot 13 - 3 \cdot 31,$$
$$1 = (31 - 2 \cdot 13) + 2(7 \cdot 13 - 3 \cdot 31) = 12 \cdot 13 - 5 \cdot 31$$

La table

j	-2	-1	0	1	2	3
a_j			2	3	-2	-2
p_j	0	1	2	7	-12	31
q_j	1	0	1	3	-5	13

nous donne les relations suivantes :

$$\mathrm{pgcd}(31, 13) = 1, \qquad 12 \cdot 13 + (-5) \cdot 31 = 1$$

et

$$\begin{pmatrix} -13 & 31 \end{pmatrix} \begin{pmatrix} 0 & 1 & 2 & 7 & -12 \\ 1 & 0 & 1 & 3 & -5 \end{pmatrix} = \begin{pmatrix} 31 & -13 & 5 & 2 & 1 \end{pmatrix}.$$

2.4.6 Fractions continues et matrices Revenons aux formules matricielles (2.4.3.2) et (2.4.3.3). D'où proviennent-elles ?

Le point clé est le fait que si l'on fait agir une matrice complexe $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in M_2(\mathbf{C})$ telle que $\det(M) \neq 0$ sur $\mathbf{C} \cup \{\infty\}$ par l'homographie

$$M(z) := \frac{Az + B}{Cz + D}$$

(où $M(\infty) = A/C$ et $M(-D/C) = \infty$), alors on a

$$M_1(M_2(z)) = (M_1M_2)(z), \qquad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}(z) = z. \tag{2.4.6.1}$$

La formule (2.4.6.1) est une conséquence de l'identification naturelle de la droite projective complexe $\mathbf{C} \cup \{\infty\} = \mathbf{P}^1(\mathbf{C})$ avec l'ensemble des droites complexes dans $\mathbf{C}^2$ qui passent par l'origine (autrement dit, avec l'ensemble des sous-espaces vectoriels de dimension 1 de $\mathbf{C}^2$). L'action linéaire standard de $M \in M_2(\mathbf{C})$ sur $\mathbf{C}^2$ transforme le sous-espace $\mathbf{C}\begin{pmatrix} z \\ 1 \end{pmatrix}$ en le sous-espace

$$M\big(\mathbf{C}\begin{pmatrix} z \\ 1 \end{pmatrix}\big) = \mathbf{C} \cdot M\begin{pmatrix} z \\ 1 \end{pmatrix} = \mathbf{C} \cdot \begin{pmatrix} A & B \\ C & D \end{pmatrix}\begin{pmatrix} z \\ 1 \end{pmatrix} = \mathbf{C} \cdot \begin{pmatrix} Az+B \\ Cz+D \end{pmatrix} = \mathbf{C} \cdot \begin{pmatrix} \frac{Az+B}{Cz+D} \\ 1 \end{pmatrix},$$

et le sous-espace $\mathbf{C}\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ em le sous-espace

$$M\big(\mathbf{C}\begin{pmatrix} 1 \\ 0 \end{pmatrix}\big) = \mathbf{C} \cdot M\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \mathbf{C} \cdot \begin{pmatrix} A & B \\ C & D \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \mathbf{C} \cdot \begin{pmatrix} A \\ C \end{pmatrix} = \mathbf{C} \cdot \begin{pmatrix} \frac{A}{C} \\ 1 \end{pmatrix}.$$

Le lien aux fractions continues provient de la formule

$$a + \frac{1}{z} = \frac{a \cdot z + 1}{1 \cdot z + 0} = \begin{pmatrix} a & 1 \\ 1 & 0 \end{pmatrix}(z),$$

qui implique que l'on a, en utilisant la notation de (2.4.3.1),

$$[a_0, \ldots, a_j, z] = M_0(M_1(\cdots(M_j(z))\cdots) = (M_0 \cdots M_j)(z), \qquad M_i = \begin{pmatrix} a_j & 1 \\ 1 & 0 \end{pmatrix} \tag{2.4.6.2}$$

(où $a_1, \ldots, a_j, z \in \mathbf{C}$). Si l'on définit $p_j, q_j \in \mathbf{C}$ par la formule

$$M_0 \cdots M_j = \begin{pmatrix} p_j & * \\ q_j & * \end{pmatrix},$$

alors on a

$$\begin{pmatrix} p_{j-1} & * \\ q_{j-1} & * \end{pmatrix}\begin{pmatrix} a_j & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} * & p_{j-1} \\ * & q_{j-1} \end{pmatrix},$$

ce qui implique que

$$M_0 \cdots M_j = \begin{pmatrix} p_j & p_{j-1} \\ q_j & q_{j-1} \end{pmatrix}.$$

On peut substituer $z = \infty$ dans (2.4.6.2) ; on obtient

$$[a_0, \ldots, a_j] = (M_0 \cdots M_j)(\infty) = \frac{p_j}{q_j},$$

ce qui termine la démonstration de la formule (2.4.3.3).

2.5 Equations $ax + by = c$ $\qquad (x, y \in \mathbf{Z})$

2.5.1 Exemple $44x + 16y = 6 \qquad (x, y \in \mathbf{Z})$.

Le terme à gauche $44x + 16y = 4(11x + 4y)$ est divisible par $4 = \text{pgcd}(44, 16)$, mais le terme à droite ne l'est pas : $4 \nmid 6$. Il en résulte qu'il n'y a pas de solutions.

2.5.2 Exemple $44x + 16y = 40 \qquad (x, y \in \mathbf{Z})$.

Dans ce cas le terme à droite est divisible par $4 = \text{pgcd}(44, 16)$. On divise l'équation ci-dessus par 4 ; on obtient l'équation

$$11x + 4y = 10 \qquad (x, y \in \mathbf{Z}), \tag{2.5.2.1}$$

où $\text{pgcd}(11, 4) = 1$.

On suppose qu'on connaît une solution particulière $x_1, y_1 \in \mathbf{Z}$ de (2.5.2.1) :

$$11x_1 + 4y_1 = 10. \tag{2.5.2.2}$$

On peut soustraire (2.5.2.2) de (2.5.2.1) ; on obtient

$$11(x - x_1) = 4(y_1 - y), \tag{2.5.2.3}$$

ce qui implique que $11 \mid 4(y_1 - y)$. On a $\text{pgcd}(11, 4) = 1$; on déduit du lemme 2.3.8 que $11 \mid (y_1 - y)$. Autrement dit, on a $y_1 - y = 11t$, où $t \in \mathbf{Z}$. On substitue cette valeur dans (2.5.2.3) ; on obtient $x - x_1 = 4t$. En résumé,

$$x = x_1 + 4t, \qquad y = y_1 - 11t \qquad (t \in \mathbf{Z}). \tag{2.5.2.4}$$

Réciproquement, les égalités (2.5.2.4) et (2.5.2.2) impliquent qu'on a bien

$$11x + 4y = 11(x_1 + 4t) + 4(y_1 - 11t) = 11x_1 + 4y_1 + (11 \cdot 4 - 4 \cdot 11)t = 10.$$

Il faut maintenant trouver une solution particulière $x_1, y_1 \in \mathbf{Z}$. La relation de Bézout

$$(-1) \cdot 44 + 3 \cdot 16 = 4$$

qu'on a établie dans (2.2.3.4) implique que

$$(-1) \cdot 11 + 3 \cdot 4 = 1. \tag{2.5.2.5}$$

On peut multiplier l'égalité ci-dessus par 10 ; on obtient une solution particulière

$$(-10) \cdot 11 + 30 \cdot 4 = 10$$

$x_1 = -10$, $y_1 = 30$ de (2.5.2.1), ce qui donne la solution générale

$$x = 4t - 10, \qquad y = 30 - 11t \qquad (t \in \mathbf{Z}). \tag{2.5.2.6}$$

2.5.3 Modifications Les constantes qui apparaîssent dans (2.5.2.6) sont assez grandes. On peut changer le paramètre t pour obtenir des constantes plus petites. Par exemple, la division euclidienne modifiée de 30 par 11, à savoir $30 = 3 \cdot 11 + (-3)$, implique que l'on a $y = -3 - 11(t - 3)$. Le changement de variables $t - 3 = s$ nous permet d'écrire $t = s + 3$ et $x = 4(s + 3) - 10 = 4s + 2$, d'où

$$x = 4s + 2, \qquad y = -3 - 11s \qquad (s \in \mathbf{Z}). \tag{2.5.3.1}$$

On peut introduire ce genre de modification avant qu'on commence les calculs. Par exemple, on a $10 = 2 \cdot 4 + 2$, ce qui nous permet de remplacer l'équation (2.5.2.1) par

$$11x + 4(y - 2) = 2. \tag{2.5.3.2}$$

Pour trouver une solution particulière $x_2, y_2 \in \mathbf{Z}$ de cette équation il suffit de multiplier (2.5.2.5) par 2 : on obtient $x_2 = -2$ et $y_2 - 2 = 6$ (donc $y_2 = 8$). Comme ci-dessus, on en déduit que

$$x = 4t - 2, \qquad y = 8 - 11t \qquad (t \in \mathbf{Z}). \tag{2.5.3.3}$$

On peut encore écrire ici $8 = 1 \cdot 11 + (-3)$ et $y = -3 - 11(t-1)$. La substitution $t - 1 = s$ conduit alors aux formules dans (2.5.3.1).

Voici le cas général.

2.5.4 Théorème. *Soient $a, b \in \mathbf{Z} \smallsetminus \{0\}$ et $c \in \mathbf{Z}$. On considère l'équation*

$$ax + by = c \qquad (x, y \in \mathbf{Z}). \tag{2.5.4.1}$$

(1) Si $d := \mathrm{pgcd}(a, b)$ ne divise pas c, alors (2.5.4.1) *n'a pas de solutions.*
(2) Si d divise c, alors (2.5.4.1) *a toujours une solution. Si $x_1, y_1 \in \mathbf{Z}$ est une telle solution, alors la solution générale de* (2.5.4.1) *est*

$$x = x_1 + (b/d)t, \qquad y = y_1 - (a/d)t \qquad (t \in \mathbf{Z}).$$

Démonstration. On procède de la même manière que dans les exemples ci-dessus.
(1) Le terme à gauche $ax + by$ est divisible par d, pour tous $x, y \in \mathbf{Z}$, mais c n'est pas divisible par d.
(2) Si d divise c, on peut diviser (2.5.4.1) par d ; on obtient une équation équivalente à (2.5.4.1)

$$a'x + b'y = c' \qquad (x, y \in \mathbf{Z}), \tag{2.5.4.2}$$

où $a' = a/d$, $b' = b/d$ et $c' = c/d$. On a $\mathrm{pgcd}(a', b') = d/d = 1$.

Si $x_1, y_1 \in \mathbf{Z}$ est une solution particulière de (2.5.4.2), on peut soustraire $a'x_1 + b'y_1 = c'$ de (2.5.4.2) ; on obtient

$$a'(x - x_1) = b'(y_1 - y), \tag{2.5.4.3}$$

d'où $a' \mid b'(y_1 - y)$. On a $\mathrm{pgcd}(a', b') = 1$, ce qui implique que $a' \mid (y_1 - y)$, d'où $y_1 - y = a't$ avec $t \in \mathbf{Z}$. On substitue cette relation dans (2.5.4.3) ; on obtient

$$x = x_1 + b't, \qquad y = y_1 - a't \qquad (t \in \mathbf{Z}).$$

Réciproquement, cette formule produit bien des solutions de (2.5.4.2), car

$$a'x + b'y = a'x_1 + b'y_1 + (a'b' - b'a')t = c'.$$

Pour montrer que l'équation (2.5.4.2) a une solution, on multiplie une relation de Bézout

$$a'u + b'v = \mathrm{pgcd}(a', b') = 1 \qquad (u, v \in \mathbf{Z})$$

par c' ; le couple $x_1 := c'u$, $y_1 := c'v$ sera alors une solution de (2.5.4.2).

La solution $(c'u, c'v)$ peut être assez grande. Les méthodes du paragraphe 2.5.3 nous permettent d'obtenir une solution particulière qui soit plus petite. □

2.5.5 Exercice. Résoudre $10x + 16y = 18$ $(x, y \in \mathbf{Z})$.

2.6 Numération en base b

2.6.1 Base 10 On peut interpréter l'écriture décimale de l'entier $n = 468$ en termes de la division euclidienne par 10 :

$$\begin{aligned} 468 &= 46 \cdot 10 + 8 \\ 46 &= 4 \cdot 10 + 6 \\ 4 &= 0 \cdot 10 + 4 \end{aligned} \qquad\qquad 468 = 4 \cdot 10^2 + 6 \cdot 10^1 + 8 \cdot 10^0$$

2.6.2 Base 7 Le même entier $n = 468$ s'écrit en base 7 de la manière suivante :

$$\begin{aligned} 468 &= 66 \cdot 7 + 6 \\ 66 &= 9 \cdot 7 + 3 \\ 9 &= 1 \cdot 7 + 2 \\ 1 &= 0 \cdot 7 + 1 \end{aligned} \qquad\qquad 468 = 1 \cdot 7^3 + 2 \cdot 7^2 + 3 \cdot 7^1 + 6 \cdot 7^0 = (1236)_7$$

2.6.3 Base générale On fixe un entier $b > 1$. Tout entier $n \in \mathbf{N}$ s'écrit en base b en utilisant des chiffres qui représentent les valeurs $0, 1, \ldots, b-1$ (par exemple, l'écriture hexadécimale en base $b = 16$ utilise les chiffres $0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F$). On écrit

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0 = (a_k \cdots a_1 a_0)_b \qquad (a_i \in \{0, 1, \ldots, b-1\}).$$

On calcule les chiffres a_i de n en base b par récurrence :

— $a_0 :=$ le reste de la division euclidienne de n par b,

— $n_1 := (n - a_0)/b$ le quotient de la division euclidienne de n par b,

— $a_1 :=$ le reste de la division euclidienne de n_1 par b,

— $n_2 := (n_1 - a_1)/b$ le quotient de la division euclidienne de n_1 par b, etc.

2.6.4 Première application : calcul des puissances On peut calculer les puissances a^m (même si $m \in \mathbf{N}$ est grand) d'une façon assez efficace en utilisant les carrés, les carrés des carrés, etc. Plus précisement, on écrit $m = \sum 2^{k_i}$ en base 2 et on calcule

$$a^2, \qquad (a^2)^2 = a^{2^2} = a^4, \qquad \big((a^2)^2\big)^2 = a^{2^3} = a^8, \qquad \cdots$$

On a, par exemple,

$$m = 105 = 64 + 32 + 8 + 1 = 2^6 + 2^5 + 2^3 + 2^0 = (1101001)_2, \qquad a^{105} = a^{64} \cdot a^{32} \cdot a^8 \cdot a,$$

ce qui nous permet de calculer a^{105} en n'effectuant que 9 produits :

$a \cdot a = a^2$	
$a^2 \cdot a^2 = a^4$	
$a^4 \cdot a^4 = a^8$	$a^8 \cdot a$
$a^8 \cdot a^8 = a^{16}$	
$a^{16} \cdot a^{16} = a^{32}$	$a^{32} \cdot (a^8 \cdot a)$
$a^{32} \cdot a^{32} = a^{64}$	$a^{64} \cdot (a^{32} \cdot (a^8 \cdot a)) = a^{105}$

2.6.5 Deuxième application : formule de Legendre pour $v_p(n!)$ **Exemple :** on va calculer $v_3(11!)$ (l'exposant de 3 dans la factorisation de 11!). On considère le produit

$$11! = 1 \cdot 2 \cdot \boxed{3} \cdot 4 \cdot 5 \cdot \boxed{6} \cdot 7 \cdot 8 \cdot \boxed{9} \cdot 10 \cdot 11.$$

Les seuls termes divisibles par 3 sont

$$3 = 3 \cdot 1, \qquad 6 = 3 \cdot 2, \qquad 9 = 3 \cdot 3.$$

On en déduit qu'on a

$$v_3(11!) = v_3(3 \cdot 6 \cdot 9) = v_3(3^3) + v_3(1 \cdot 2 \cdot 3) = 3 + v_3(3!).$$

De même, on a

$$3! = 1 \cdot 2 \cdot \boxed{3}, \qquad v_3(3!) = v_3(3) = 1 + v_3(1!) = 1,$$

ce qui implique que $v_3(11!) = 3 + 1 = 4$.

Le cas général : on va calculer par la même méthode la valeur de $v_p(n!)$, où $n \in \mathbf{N}_+$ et $p \in \mathcal{P}$. En écrivant $n = pn_1 + a_0$ avec $0 \leq a_0 < p$ on voit que les seuls termes qui sont divisibles par p dans le produit $n! = 1 \cdots n$ sont les entiers $p \cdot 1, p \cdot 2, \ldots p \cdot n_1$. On en déduit que

$$v_p(n!) = v_p(p^{n_1}(n_1)!) = n_1 + v_p((n_1)!), \qquad n_1 = \left\lfloor \frac{n}{p} \right\rfloor.$$

On utilise la notation $\lfloor x \rfloor$ pour la partie entière d'un nombre réel $x \in \mathbf{R}$: on a $\lfloor x \rfloor \in \mathbf{Z}$ et $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$.

La même procédure s'applique à n_1, etc. On obtient, par récurrence, (avec $n_0 = n$)

$$\begin{aligned} n_0 &= pn_1 + a_0 & 0 \leq a_0 < p \\ n_1 &= pn_2 + a_1 & 0 \leq a_1 < p \\ &\vdots & \vdots \\ n_{k-1} &= pn_k + a_{k-1} & 0 \leq a_{k-1} < p \\ n_k &= a_k & 0 \leq a_k < p \end{aligned}$$

où

$$n_i = \left\lfloor \frac{n_{i-1}}{p} \right\rfloor = \left\lfloor \frac{n}{p^i} \right\rfloor, \qquad v_p((n_i)!) = n_{i+1} + v_p((n_{i+1})!),$$

ce qui implique que

$$v_p(n!) = n_1 + \cdots + n_k = \sum_{i=1}^{k} \left\lfloor \frac{n}{p^i} \right\rfloor = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor. \tag{2.6.5.1}$$

On peut exprimer ce résultat en termes de l'écriture de n en base p : on a

$$n = a_k p^k + \cdots + a_1 p + a_0 = (a_k \cdots a_0)_p \qquad (a_i = 0, 1, \ldots, p-1)$$

et

$$\begin{aligned} v_p(n!) &= (a_k p^{k-1} + \cdots + a_2 p + a_1) + (a_k p^{k-2} + \cdots + a_3 p + a_2) + \cdots + a_k = \\ &= a_k(1 + p + \cdots + p^{k-1}) + a_{k-1}(1 + p + \cdots + p^{k-2}) + \cdots + a_2(1+p) + a_1 = \\ &= \frac{a_k(p^k - 1) + a_{k-1}(p^{k-1} - 1) \cdots + a_1(p-1)}{p-1} = \frac{n - s_p(n)}{p-1}, \end{aligned} \tag{2.6.5.2}$$

où

$$s_p(n) = a_k + a_{k-1} + \cdots + a_0$$

est la somme des chiffres de n en base p. La formule de Legendre (2.6.5.2) est valable pour tout $n \in \mathbf{N}$ (y compris $n = 0$).

2.6.6 Exercice. (1) Si $r \geq 1$ et $0 < a \leq p^r$, alors la valuation p-adique de $\binom{p^r}{a}$ est égale à $r - v_p(a)$.
(2) Soient $m, n \in \mathbf{N}$ et $p \in \mathcal{P}$. La valuation p-adique de $\binom{m+n}{m} = \frac{(m+n)!}{m!n!}$ est égale au nombre de retenus dans l'addition de m et n en base p.

3 Congruences, arithmétique sur $\mathbf{Z}/n\mathbf{Z}$

3.1 Notions de base

3.1.1 Introduction Soit n un entier positif. On est conduit à la notion de congruence modulo n si l'on ne considère que **le dernier chiffre** de l'écriture en base n (ou, ce qui revient au même, le reste de la division euclidienne par n) des entiers.

L'ensemble $\mathbf{Z}$ d'entiers relatifs se décompose naturellement en n classes selon le reste de la division par n. On peut effectuer les opérations usuelles (addition, soustraction, multiplication) avec ces classes. Autrement dit, le reste de la division par n de $a \pm b$ (resp. ab) ne dépend que des restes de a et b.

Prenons, par exemple, $n = 2$; on a

$$\mathbf{Z} = (2\mathbf{Z}) \cup (2\mathbf{Z}+1), \qquad \begin{array}{c} 2\mathbf{Z} = \{2k \mid k \in \mathbf{Z}\} = \{\text{entiers pairs}\} \\ 2\mathbf{Z}+1 = \{2k+1 \mid k \in \mathbf{Z}\} = \{\text{entiers impairs}\} \end{array}$$

$$\begin{array}{rr} (2k)+(2l) = 2(k+l) & \text{pair} + \text{pair} = \text{pair} \\ (2k)+(2l+1) = 2(k+l)+1 & \text{pair} + \text{impair} = \text{impair} \\ (2k+1)+(2l+1) = 2(k+l+1) & \text{impair} + \text{impair} = \text{pair} \\ (2k)\cdot(2l) = 2(2kl) & \text{pair} \cdot \text{pair} = \text{pair} \\ (2k)\cdot(2l+1) = 2(2kl+k) & \text{pair} \cdot \text{impair} = \text{pair} \\ (2k+1)\cdot(2l+1) = 2(2kl+k+l)+1 & \text{impair} \cdot \text{impair} = \text{impair} \end{array}$$

De même, on voit immédiatement que $276 + 389 \neq 667$ en considérant le reste de la division par 10, car $\ldots 6 + \ldots 9 = \ldots 5$.

D'ici jusqu'a fin du chapitre 3 on suppose que $m, n \geq 1$ sont des entiers strictement positifs.

3.1.2 Définition. Soient $a, b \in \mathbf{Z}$. On dit que a et b sont **congrus modulo** n s'ils ont le même reste de la division euclidienne par n (ce qui équivaut à $n|(a-b)$). **Notation :** $a \equiv b \pmod n$, ou $a \equiv b\ (n)$, ou $a \equiv b\ [n]$. La **classe de congruence modulo** n d'un entier relatif a est l'ensemble

$$a \pmod n := \{x \in \mathbf{Z} \mid x \equiv a \pmod n\} = \{a + ny \mid y \in \mathbf{Z}\} = a + n\mathbf{Z}.$$

On note $\mathbf{Z}/n\mathbf{Z}$ l'ensemble de toutes les classes de congruence modulo n.

3.1.3 Exemples On a $17 \equiv 7 \equiv -13 \pmod{10}$, d'où

$$17 \pmod{10} = 7 \pmod{10} = -13 \pmod{10} = \{7, 17, 27, \ldots, -3, -13, -23, \ldots\} = 10\mathbf{Z} + 7 = 10\mathbf{Z} - 3.$$

Il y a deux classes de congruence modulo 2, à savoir

$$\begin{array}{l} 0 \pmod 2 = \quad 2 \pmod 2 = -4 \pmod 2 = \{0, 2, 4, 6, \ldots, -2, -4, -6, \ldots\} = 2\mathbf{Z} \\ 1 \pmod 2 = -1 \pmod 2 = -7 \pmod 2 = \{1, 3, 5, 7, \ldots, -1, -3, -5, \ldots\} = 2\mathbf{Z}+1 \end{array}$$

(autrement dit, $\mathbf{Z}/2\mathbf{Z} = \{0 \pmod 2,\ 1 \pmod 2\}$) et trois classes de congruence modulo 3, à savoir

$$0 \pmod 3 = 3 \pmod 3 = -3 \pmod 3 = \{0, 3, 6, 9, \ldots, -3, -6, -9, \ldots\} = 3\mathbf{Z}$$
$$1 \pmod 3 = 4 \pmod 3 = -2 \pmod 3 = \{1, 4, 7, 10, \ldots, -2, -5, -8, \ldots\} = 3\mathbf{Z} + 1$$
$$2 \pmod 3 = 5 \pmod 3 = -1 \pmod 3 = \{2, 5, 8, 10, \ldots, -1, -4, -7, \ldots\} = 3\mathbf{Z} + 2 = 3\mathbf{Z} - 1$$

(ce qui implique que $\mathbf{Z}/3\mathbf{Z} = \{0 \pmod 3, \pm 1 \pmod 3\}$). En général, $\mathbf{Z}/n\mathbf{Z}$ consiste de n classes de congruence modulo n :

$$\mathbf{Z}/n\mathbf{Z} = \{1 \pmod n, 2 \pmod n, \ldots, n \pmod n\}$$

(où $n \pmod n = 0 \pmod n$). Si $n = 2k + 1$ est impair, alors on a

$$\mathbf{Z}/(2k+1)\mathbf{Z} = \{0 \pmod n, \pm 1 \pmod n, \pm 2 \pmod n, \ldots, \pm k \pmod n\}.$$

De même, si $n = 2k$ est pair, alors on a

$$\mathbf{Z}/2k\mathbf{Z} = \{0 \pmod n, \pm 1 \pmod n, \pm 2 \pmod n, \ldots, \pm(k-1) \pmod n, k \pmod n\}.$$

3.1.4 Proposition. *Si $a \equiv a' \pmod n$ et $b \equiv b' \pmod n$, alors*

$$a \pm b \equiv a' \pm b' \pmod n, \qquad ab \equiv a'b' \pmod n.$$

Démonstration. Il existe $x, y \in \mathbf{Z}$ tels que $a = a' + nx$ et $b = b' + ny$, ce qui implique que

$$a \pm b = a' \pm b' + n(x \pm y), \qquad ab = (a' + nx)(b' + ny) = a'b' + n(a'y + b'x + nxy).$$

□

3.1.5 Congruences modulo m et mn Il est important de comprendre des liens entre des congruences modulo deux entiers distincts.

On remarque d'abord qu'on a

$$a \equiv b \pmod{mn} \implies a \equiv b \pmod m \tag{3.1.5.1}$$

(par exemple, $a \equiv b \pmod{18}$ implique que $a \equiv b \pmod 6$). En effect, si $mn \mid (a - b)$, alors $m \mid (a - b)$. On peut reformuler le raisonnement ci-dessus en disant que $mn\mathbf{Z} \subseteq m\mathbf{Z}$, ce qui implique que $a + mn\mathbf{Z} \subseteq a + m\mathbf{Z}$.

Réciproquement, chaque classe de congruence modulo m est une réunion disjointe de n classes de congruence modulo mn.

Par exemple, on va décomposer la classe de congruence $6\mathbf{Z} + 1$ en réunion disjointe de trois classes de congruence modulo 18. On écrit d'abord

$$x \equiv 1 \pmod 6 \iff \exists\, y \in \mathbf{Z} \quad x = 6y + 1$$

et puis on remarque qu'il y a trois possibilités pour la classe de congruence de y modulo 3 :

$$y = 3z, \quad \text{ou} \quad y = 3z + 1, \quad \text{ou} \quad y = 3z + 2,$$

où $z \in \mathbf{Z}$. On en déduit qu'on a

$$x \equiv 1 \pmod 6 \iff \exists\, z \in \mathbf{Z} \quad \begin{cases} x = 6(3z) + 1 = 18z + 1, \text{ ou} \\ x = 6(3z + 1) + 1 = 18z + 7, \text{ ou} \\ x = 6(3z + 2) + 1 = 18z + 13, \end{cases}$$

ce qui équivaut à

$$x \equiv 1 \pmod 6 \iff \begin{cases} x \equiv 1 \pmod{18}, \text{ ou} \\ x \equiv 7 \pmod{18}, \text{ ou} \\ x \equiv 13 \pmod{18}. \end{cases}$$

En général, on a

$$\mathbf{Z} = \coprod_{b=0}^{n-1} (b + n\mathbf{Z}), \qquad a + m\mathbf{Z} = \coprod_{b=0}^{n-1} (a + m(b + n\mathbf{Z})) = \coprod_{b=0}^{n-1} ((a + bm) + mn\mathbf{Z})$$

(le symbole $\coprod$ signifie une réunion disjointe), ce qui implique qu'on a, pour $x \in \mathbf{Z}$,

$$x \equiv a \pmod m \iff x \equiv a, a + m, a + 2m, \ldots, a + (n-1)m \pmod{mn}. \tag{3.1.5.2}$$

3.1.6 Proposition. *Soient $m, n \geq 1$ et $a, b \in \mathbf{Z}$. Il est équivalent :*

$$a \equiv b \pmod m \iff na \equiv nb \pmod{mn}.$$

Démonstration. On remarque qu'on a des équivalences

$$a \equiv b \pmod m \iff m \mid (a-b) \iff mn \mid n(a-b) \iff na \equiv nb \pmod{mn}.$$

□

3.1.7 Proposition (Une propriété importante de congruences)**.** *Il est équivalent :*

$$\left.\begin{matrix} a \equiv b \pmod m \\ a \equiv b \pmod n \end{matrix}\right\} \iff a \equiv b \pmod{\operatorname{ppcm}(m,n)}$$

Démonstration. Il faut démontrer l'équivalence

$$\left.\begin{matrix} m \mid (a-b) \\ n \mid (a-b) \end{matrix}\right\} \iff \operatorname{ppcm}(m,n) \mid (a-b),$$

mais cet énoncé n'est rien d'autre que la caractérisation de $\operatorname{ppcm}(m,n)$:

$$\{\text{multiples de } m\} \cap \{\text{multiples de } n\} = \{\text{multiples de } \operatorname{ppcm}(m,n)\}.$$

□

3.1.8 Corollaire. *Soient $a, b \in \mathbf{Z}$, soit $n = p_1^{k_1} \cdots p_r^{k_r}$ la décomposition en facteurs premiers de $n \geq 1$. Il est équivalent :*

$$a \equiv b \pmod n \iff \forall i = 1, \ldots, r \quad a \equiv b \pmod{p_i^{k_i}}.$$

3.2 Valeurs de $a^k \pmod n$

3.2.1 Reformulation du petit théorème de Fermat Le petit théorème de Fermat se traduit en termes de congruences de la façon suivante :

$$\forall p \in \mathcal{P} \quad \forall a \in \mathbf{Z} \qquad a^p \equiv a \pmod p.$$

On va étudier le comportement de la suite des classes de congruence $1, a, a^2, a^3, \ldots \pmod n$.

3.2.2 Exemple : $a^k \pmod 3$ La table

$a \pmod 3$	$a^2 \pmod 3$	$a^3 \pmod 3$
0	$0^2 \equiv 0$	$0 \cdot 0 \equiv 0$
± 1	$(\pm 1)^2 \equiv 1$	$(\pm 1) \cdot 1 \equiv \pm 1$

nous dit que

$$\forall a \in \mathbf{Z} \quad a^3 \equiv a \pmod 3, \qquad a^2 \equiv \begin{cases} 0 \pmod 3, & 3 \mid a \\ 1 \pmod 3, & 3 \nmid a, \end{cases} \tag{3.2.2.1}$$

ce qui implique que

$$\forall a \in \mathbf{Z}\ \forall k \in \mathbf{N}_+ \quad a^{2k-1} \equiv a \pmod 3, \qquad a^{2k} \equiv \begin{cases} 0 \pmod 3, & 3 \mid a \\ 1 \pmod 3, & 3 \nmid a. \end{cases} \tag{3.2.2.2}$$

En particulier, nous avons démontré le petit théorème de Fermat pour $p = 3$ par cette méthode.
Application : soit $k \in \mathbf{Z}$; l'équation

$$x^2 - 3y^2 = 3k - 1 \qquad (x, y \in \mathbf{Z})$$

n'a pas de solutions, car

$$x^2 - 3y^2 \equiv x^2 \equiv 0, 1 \pmod 3, \qquad 3k - 1 \equiv -1 \not\equiv 0, 1 \pmod 3.$$

3.2.3 Exemple : $a^k \pmod 4$ La table

$a \pmod 4$	$a^2 \pmod 4$
0	$0^2 \equiv 0$
2	$2^2 \equiv 0$
± 1	$(\pm 1)^2 \equiv 1$

nous dit que

$$\forall a \in \mathbf{Z} \quad a^2 \equiv \begin{cases} 0 \pmod 4, & 2 \mid a \\ 1 \pmod 4, & 2 \nmid a, \end{cases} \tag{3.2.3.1}$$

ce qui implique que

$$\forall a \in \mathbf{Z}\ \forall k \in \mathbf{N}_+ \quad a^{2k} \equiv \begin{cases} 0 \pmod 4, & 2 \mid a \\ 1 \pmod 4, & 2 \nmid a. \end{cases} \tag{3.2.3.2}$$

Application : soit $k \in \mathbf{Z}$; l'équation

$$x^2 + y^2 = 4k + 3 \qquad (x, y \in \mathbf{Z})$$

n'a pas de solutions, car

$$4k + 3 \equiv 3 \pmod 4, \qquad x^2, y^2 \equiv 0, 1 \pmod 4, \qquad x^2 + y^2 \equiv 0, 1, 2 \pmod 4 \not\equiv 3 \pmod 4.$$

3.2.4 Exemple : $a^2 \pmod 8$ La table

$a \pmod 8$	$a^2 \pmod 8$
0	$0^2 \equiv 0$
± 2	$(\pm 2)^2 \equiv 4$
4	$4^2 \equiv 0$
± 1	$(\pm 1)^2 \equiv 1$
± 3	$(\pm 3)^2 \equiv 1$

nous dit que

$$\forall a \in \mathbf{Z} \quad a^2 \equiv \begin{cases} 0, 4 \pmod 8, & 2 \mid a \\ 1 \pmod 8, & 2 \nmid a. \end{cases} \tag{3.2.4.1}$$

Application : soit $k \in \mathbf{Z}$; l'équation

$$x^2 + y^2 + z^2 = 8k + 7 \qquad (x, y, z \in \mathbf{Z})$$

n'a pas de solutions, car

$8k+7 \equiv 7 \pmod 8$, $\quad x^2, y^2, z^2 \equiv 0, 1, 4 \pmod 8$, $\quad x^2+y^2+z^2 \equiv 0, 1, 2, 3, 4, 5, 6 \pmod 8 \not\equiv 7 \pmod 8$.

3.2.5 Exemple : $a^k \pmod 5$ La table

$a \pmod 5$	$a^2 \pmod 5$	$a^4 \pmod 5$	$a^5 \pmod 5$
0	$0^2 \equiv 0$	$0^2 \equiv 0$	$0 \cdot 0 \equiv 0$
± 1	$(\pm 1)^2 \equiv 1$	$1^2 \equiv 1$	$(\pm 1) \cdot 1 \equiv \pm 1$
± 2	$(\pm 2)^2 \equiv 4 \equiv -1$	$(-1)^2 \equiv 1$	$(\pm 2) \cdot 1 \equiv \pm 2$

nous dit que

$$\forall a \in \mathbf{Z} \quad a^5 \equiv a \pmod 5, \qquad a^4 \equiv \begin{cases} 0 \pmod 5, & 5 \mid a \\ 1 \pmod 5, & 5 \nmid a, \end{cases} \tag{3.2.5.1}$$

ce qui montre la validité du petit théorème de Fermat pour $p = 5$.

3.2.6 Exemple : $a^k \pmod{3^2}$ **pour** $3 \nmid a$ La table

$a \pmod{3^2}$	$a^3 \pmod{3^2}$	$a^6 \pmod{3^2}$
± 1	$(\pm 1)^3 \equiv \pm 1$	$(\pm 1)^2 \equiv 1$
± 2	$(\pm 2)^3 \equiv \pm 8 \equiv \mp 1$	$(\mp 1)^2 \equiv 1$
± 4	$(\pm 4)^3 \equiv \pm 64 \equiv \pm 1$	$(\pm 1)^2 \equiv 1$

nous dit que

$$\forall a \in \mathbf{Z} \quad \left[3 \nmid a \implies a^3 \equiv \pm 1 \pmod{3^2}, \qquad a^6 \equiv 1 \pmod{3^2}\right] \tag{3.2.6.1}$$

$$\forall a \in \mathbf{Z} \qquad a^3 \equiv 0, \pm 1 \pmod{3^2}. \tag{3.2.6.2}$$

Application : si $x, y, z \in \mathbf{Z}$ et $3 \nmid xyz$, alors $x^3, y^3, z^3 \equiv \pm 1 \pmod{3^2}$, ce qui implique que $x^3 + y^3 \equiv 0, \pm 2 \not\equiv z^3 \pmod{3^2}$.

3.2.7 Exemple : $a^k \pmod{3^3}$ pour $3 \nmid a$ On a montré dans 3.2.6 qu'on a $a^6 \equiv 1 \pmod{3^2}$, ce qui équivaut à

$$a^6 \equiv 1, 1+3^2, 1+2\cdot 3^2 \equiv 1, 10, -8 \pmod{3^3}.$$

La table

$a^6 \pmod{3^3}$	$a^{12} \pmod{3^3}$	$a^{18} \pmod{3^3}$
1	$1^2 \equiv 1$	$1 \cdot 1 \equiv 1$
10	$10^2 \equiv 100 \equiv -8$	$10 \cdot (-8) \equiv 1$
-8	$(-8)^2 \equiv \pm 64 \equiv 10$	$(-8) \cdot 10 \equiv 1$

nous dit que

$$\forall a \in \mathbf{Z} \quad \left[3 \nmid a \implies a^{18} \equiv 1 \pmod{3^3}\right]. \tag{3.2.7.1}$$

3.2.8 Exemple : $a^k \pmod{5^2}$ pour $5 \nmid a$ On a montré dans (3.2.5.1) que si $a \in \mathbf{Z}$ n'est pas divisible par 5, alors $a^4 \equiv 1 \pmod{5}$, ce qui équivaut à

$$a^4 \equiv 1,\ 1+5,\ 1+2\cdot 5,\ 1+3\cdot 5,\ 1+4\cdot 5 \equiv 1, 6, 11, -9, -4 \pmod{5^2}. \tag{3.2.8.1}$$

La table

$a^4 \pmod{5^2}$	$a^8 \pmod{5^2}$	$a^{16} \pmod{5^2}$	$a^{20} \pmod{5^2}$
1	$1^2 \equiv 1$	$1^2 \equiv 1$	$1 \cdot 1 \equiv 1$
-4	$(-4)^2 \equiv 16 \equiv -9$	$(-9)^2 \equiv 81 \equiv 6$	$(-4) \cdot 6 \equiv 1$
6	$6^2 \equiv 36 \equiv 11$	$11^2 \equiv 121 \equiv -4$	$6 \cdot (-4) \equiv 1$
-9	$(-9)^2 \equiv 6$	$6^2 \equiv 11$	$(-9) \cdot 11 \equiv 1$
11	$11^2 \equiv -4$	$(-4)^2 \equiv -9$	$11 \cdot (-9) \equiv 1$

montre alors que

$$\forall a \in \mathbf{Z} \quad \left[5 \nmid a \implies a^{20} \equiv 1 \pmod{5^2}\right]. \tag{3.2.8.2}$$

3.2.9 Le "Grand Théorème" de Fermat Il s'agit de l'énoncé suivant : si $n \geq 3$, alors l'équation

$$x^n + y^n = z^n \qquad (x, y, z \in \mathbf{Z}) \tag{3.2.9.1}$$

n'a pas de solutions avec $xyz \neq 0$. Fermat a démontré ce résultat pour $n = 4$ en utilisant sa méthode de descente infinie. Le cas général a été démontré par Wiles en 1995 (les travaux de Kummer au 19-ème siècle consacrés à ce problème ont été très importants, eux aussi).

Le résultat de Fermat mentionné ci-dessus implique qu'il suffit de considérer le cas lorsque n est un nombre premier $n = p > 2$. Il s'avère que, sous cette hypothèse, le cas $p \nmid xyz$ (le **premier cas**) est beaucoup plus facile que le cas $p \mid xyz$ (le **deuxième cas**).

Par exemple, nous avons démontré le premier cas du grand théorème de Fermat pour $p = 3$ dans le paragraphe 3.2.6. La preuve a utilisé des congruences modulo 3^2.

Une méthode plus sophistiquée due à Sophie Germain (sous une forme généralisée due à Legendre) permet de démontrer le premier cas pour tous les nombres premiers $p < 100$ (entre autres).

3.2.10 Exercice. (1) Déterminer toutes les valeurs possibles de $a^5 \pmod{5^2}$ lorsque $5 \nmid a$. [Indication : on pourra consulter la proposition 4.1.5 ci-dessous.]
(2) Montrer que $x^5 + y^5 \not\equiv z^5 \pmod{5^2}$ si $x, y, z \in \mathbf{Z}$ et $5 \nmid xyz$.
(3) Que se passe-t-il si l'on remplace 5 par 7 ?

3.2.11 Exercice. Soient $x, y, z \in \mathbf{Z}$. Montrer :
(1) $x^2 \equiv 0, 1 \pmod{3}$.
(2) Si $3 \mid (x^2 + y^2)$, alors $3 \mid x$ et $3 \mid y$.
(3) Si $x^2 + y^2 = 3z^2$, alors $3 \mid x$, $3 \mid y$ et $3 \mid z$.
(4) Si $x^2 + y^2 = 3z^2$, alors $x = y = z = 0$.
(5) Que se passe-t-il si l'on remplace 3 par 5 (resp. par 7) ?

3.2.12 Exercice. Soient $x, y, z \in \mathbf{Z}$. Montrer :
(1) $x^2 \equiv 0, 1, 4 \pmod{8}$.
(2) Si $4 \mid (x^2 + y^2 + z^2)$, alors $2 \mid x$, $2 \mid y$ et $2 \mid z$.
(3) Si $x^2 + y^2 + z^2 \equiv 3 \pmod{4}$, alors $2 \nmid x$, $2 \nmid y$, $2 \nmid z$ et $x^2 + y^2 + z^2 \equiv 3 \pmod{8}$.
(4) $x^2 + y^2 + z^2 \neq 4^k(8l + 7)$ $(k, l \in \mathbf{N})$.
[Le **théorème de trois carrés (Legendre, Gauss)** affirme que tout entier positif $n \neq 4^k(8l + 7)$ s'écrit sous la forme $n = x^2 + y^2 + z^2$ avec $x, y, z \in \mathbf{Z}$.]

3.3 Le théorème chinois

3.3.1 Exemple : $\mathbf{Z}/6\mathbf{Z}$ et $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$ On a vu dans (3.1.5.1) qu'une classe de congruence $x \pmod{6}$ modulo 6 détermine une classe $x \pmod{2}$ modulo 2, ainsi qu'une classe $x \pmod{3}$ modulo 3. Il est facile d'expliciter cette correspondance :

$x \pmod{6}$	$x \pmod{2}$	$x \pmod{3}$
0	0	0
1	1	1
2	0	2
3	1	0
4	0	1
5	1	2
$3a + 4b$	$a = a \cdot 1 + b \cdot 0$	$b = a \cdot 0 + b \cdot 1$

On peut remarquer que chaque combinaison possible

$$(0,0), (0,1), (0,2), (1,0), (1,1), (1,2)$$

apparaît une fois dans les deux dernières colonnes de la table. Autrement dit, une classe de congruence modulo 6 est détermimée d'une manière unique par un couple de classes de congruence respectifs modulo 2 et 3.

Voici une formulation scientifique : l'application

$$\begin{array}{ccc} \mathbf{Z}/6\mathbf{Z} & \longrightarrow & \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z} \\ x \pmod{6} & \mapsto & (x \pmod{2}, x \pmod{3}) \end{array} \tag{3.3.1.1}$$

est bijective : un élément quelconque de chaque côté correspond à un seul élément de l'autre côté. On a noté ici

$$X \times Y = \{(x, y) \mid x \in X,\, y \in Y\} \tag{3.3.1.2}$$

le produit cartésien d'ensembles X et Y.

La dernière ligne de la table ci-dessus fournit une formule explicite pour l'inverse de l'application bijective (3.3.1.1), à savoir

$$\begin{array}{ccc} \mathbf{Z}/6\mathbf{Z} & \longrightarrow & \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z} \\ 3a + 4b \pmod 6 & \mapsto & (a \pmod 2, b \pmod 3). \end{array} \tag{3.3.1.3}$$

Le contenu concret de cet énoncé est le suivant : étant donnés des entiers relatifs $a, b \in \mathbf{Z}$, le système

$$\left\{ \begin{array}{l} x \equiv a \pmod 2 \\ x \equiv b \pmod 3 \end{array} \right\} \tag{3.3.1.4}$$

à une unique solution modulo 6, à savoir

$$x \equiv 3a + 4b \pmod 6. \tag{3.3.1.5}$$

La formule (3.3.1.3) correspond à la formule

$$\begin{array}{ccc} & & \mathbf{R}^2 \longrightarrow \quad \mathbf{R} \times \mathbf{R} \\ \begin{pmatrix} a \\ b \end{pmatrix} = a \begin{pmatrix} 1 \\ 0 \end{pmatrix} + b \begin{pmatrix} 0 \\ 1 \end{pmatrix} & \mapsto & \qquad (a, b) \end{array} \tag{3.3.1.6}$$

qui exprime un vecteur quelconque dans le the plan $\mathbf{R}^2$ en termes de deux vectors

$$e_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \qquad e_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

de la base canonique de $\mathbf{R}^2$. Les classes de congruence $3 \pmod 6$ et $4 \pmod 6$ sont les solutions respectives de

$$\left\{ \begin{array}{l} 3 \equiv 1 \pmod 2 \\ 3 \equiv 0 \pmod 3 \end{array} \right\}, \qquad \left\{ \begin{array}{l} 4 \equiv 0 \pmod 2 \\ 4 \equiv 1 \pmod 3 \end{array} \right\} \tag{3.3.1.7}$$

Elles correspondent, donc, aux vecteurs e_1 et e_2. Il y a aussi une analogie entre les deux formules suivantes :

$$\left\{ \begin{array}{l} 3a + 4b \equiv a \pmod 2 \\ 3a + 4b \equiv b \pmod 3 \end{array} \right\}, \qquad \begin{pmatrix} a \\ b \end{pmatrix} = a \begin{pmatrix} 1 \\ 0 \end{pmatrix} + b \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{3.3.1.8}$$

Voici le cas général.

3.3.2 Théorème (Théorème chinois)**.** *Soient $m, n \geq 1$, $\operatorname{pgcd}(m, n) = 1$ et $a, b \in \mathbf{Z}$. Le système*

$$\left\{ \begin{array}{l} x \equiv a \pmod m \\ x \equiv b \pmod n \end{array} \right\} \tag{3.3.2.1}$$

a une unique solution modulo mn. Autrement dit, l'application

$$\begin{array}{ccc} \mathbf{Z}/mn\mathbf{Z} & \longrightarrow & \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z} \\ x \pmod{mn} & \mapsto & (x \pmod m, x \pmod n) \end{array}$$

est bijective.

Démonstration. **Unicité :** si l'on a $x \equiv y \equiv a \pmod m$ et $x \equiv y \equiv b \pmod n$, alors $m \mid (x-y)$ et $n \mid (x-y)$, ce qui implique que $x-y$ est divisible par $\mathrm{ppcm}(m,n) = mn/\mathrm{pgcd}(m,n) = mn$.
Construction : le but est de généraliser (3.3.1.7). On trouve d'abord les solutions respectives pour $(a,b) = (1,0)$ et $(a,b) = (0,1)$, et puis on prend leur combinaison linéaire convenable (comme dans (3.3.1.8)) pour obtenir une solution générale.

On applique l'algorithme d'Euclide au couple (m,n). On obtient un couple $u, v \in \mathbf{Z}$ vérifiant une relation de Bézout $mu + nv = \mathrm{pgcd}(m,n) = 1$. On en déduit

$$\left\{\begin{matrix} nv \equiv 1 \pmod m \\ nv \equiv 0 \pmod n \end{matrix}\right\}, \qquad \left\{\begin{matrix} mu \equiv 0 \pmod m \\ mu \equiv 1 \pmod n \end{matrix}\right\} \tag{3.3.2.2}$$

(voir (3.3.1.7)), d'où une solution

$$x \equiv a(nv) + b(mu) = a + (b-a)mu = b + (a-b)nv \equiv \left\{\begin{matrix} a\cdot 1 + b\cdot 0 \equiv a \pmod m \\ a\cdot 0 + b\cdot 1 \equiv b \pmod n \end{matrix}\right\}. \tag{3.3.2.3}$$

□

3.3.3 Remarques (1) Les entiers qui apparaîssent dans la formule $x \equiv a(nv) + b(mu) \pmod{mn}$ sont souvent assez grands. Si l'on écrit $av \equiv A \pmod m$ et $bu \equiv B \pmod n$ avec $|A|, |B|$ pas trop grand, alors on a $x \equiv nA + mB \pmod{mn}$ (d'après la proposition 3.1.6) avec $nA + mB$ pas trop grand, non plus.
(2) Les ensembles $\mathbf{Z}/mn\mathbf{Z}$ et $\mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$ ont le même cardinal. Par conséquent, si l'on sait que l'application dans le théorème est injective (ce qui équivaut à l'énoncé d'unicité), elle est automatiquement bijective. Ce raisonnement abstrait est plus rapide que celui dans la preuve du théorème 3.3.2. En revanche, il ne permet pas d'expliciter l'application inverse.

3.3.4 Système de congruences (exemple) On va résoudre le système suivant :

$$\left\{\begin{matrix} x \equiv 5 \pmod{27} \\ x \equiv 7 \pmod{37} \end{matrix}\right\}. \tag{3.3.4.1}$$

On applique d'abord l'algorithme d'Euclide modifié au couple $37, 27$:

$$37 = 1\cdot 27 + 10, \qquad 27 = 3\cdot 10 + (-3), \qquad 10 = (-3)\cdot(-3) + 1, \qquad -3 = (-3)\cdot 1 + 0.$$

On en déduit les combinaisons linéaires suivantes :

$$10 = 37 - 27, \qquad -3 = 27 - 3(37-27) = 4\cdot 27 - 3\cdot 37, \qquad 1 = (37-27) + 3(4\cdot 27 - 3\cdot 37) = 11\cdot 27 - 8\cdot 37.$$

On peut utiliser également la fraction continue

$$1 + \cfrac{1}{3 + \cfrac{1}{-3 + \frac{1}{-3}}} = 1 + \cfrac{1}{3 + \frac{-3}{10}} = 1 + \frac{10}{27} = \frac{37}{27}, \qquad 1 + \cfrac{1}{3 + \frac{1}{-3}} = 1 + \frac{3}{8} = \frac{11}{8}$$

ou la table

j	-2	-1	0	1	2	3
a_j			1	3	-3	-3
p_j	0	1	1	4	-11	37
q_j	1	0	1	3	-8	27

pour obtenir la même relation de Bézout explicite

$$11 \cdot 27 + (-8) \cdot 37 = 1.$$

Par conséquent, on a

$$x \equiv 5 \cdot (-8) \cdot 37 + 7 \cdot 11 \cdot 27 \equiv 7 + (7-5) \cdot 8 \cdot 37 \pmod{27 \cdot 37}$$

et $(7-5) \cdot 8 \equiv 16 \equiv -11 \pmod{27}$, ce qui implique que $(7-5) \cdot 8 \cdot 37 \equiv -11 \cdot 37 \pmod{27 \cdot 37}$ (d'après proposition 3.1.6), d'où

$$x \equiv 7 - 11 \cdot 37 \equiv -400 \equiv 599 \pmod{27 \cdot 37}$$

(car $27 \cdot 37 = 999$).

3.3.5 Une autre méthode On peut reformuler le système

$$\left\{\begin{matrix} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{matrix}\right\} \tag{3.3.5.1}$$

(où on n'impose aucune condition sur m et n) de la façon suivante : la première congruence équivaut à $x = a + my$, où $y \in \mathbf{Z}$. On substitue cet égalité dans la deuxième congruence ; on obtient

$$my \equiv b - a \pmod{n}. \tag{3.3.5.2}$$

On va étudier les congruences de ce type dans le paragraphe 3.4 ci-dessous.

On peut également remarquer que la deuxième congruence équivaut à l'existence de $z \in \mathbf{Z}$ tel que l'on ait $x = b + nz$. Si l'on met les deux conditions ensemble, on obtient l'équation $a + my = b + nz$ qui s'écrit aussi sous la forme

$$my - nz = b - a \qquad (y, z \in \mathbf{Z}) \tag{3.3.5.3}$$

(cet équation équivaut à la congruence (3.3.5.2)). On peut résoudre 3.3.5.3 (ou démontrer qu'il n'y a pas de soulutions) en utilisant la méthode qu'on a décrite dans la preuve du théorème 2.5.4. On obtient d'ici la solution du système (3.3.5.1).

3.3.6 Exercice. On suppose qu'on a $m_1, \ldots, m_r \geq 1$ et $\operatorname{pgcd}(m_i, m_j) = 1$ pour tous $1 \leq i < j \leq r$. Pour tous $a_1, \ldots, a_r \in \mathbf{Z}$ le système

$$\left\{\begin{matrix} x \equiv a_1 \pmod{m_1} \\ \vdots \\ x \equiv a_r \pmod{m_r} \end{matrix}\right\}$$

a une unique solution $x \pmod{m_1 \cdots m_r}$.

3.3.7 Exercice. (1) Soient $a, b \in \mathbf{Z}$. Montrer que le système

$$\left\{\begin{matrix} x \equiv a \pmod{4} \\ x \equiv b \pmod{6} \end{matrix}\right\}$$

a une solution si et seulement si $a \equiv b \pmod{2}$. Si c'est le cas, alors la solution est unique modulo 12.
(2) Que se passe-t-il si l'on remplace le couple $4, 6$ par un couple quelconque $m, n \in \mathbf{N}_+$?
(3) Y a-t-il un énoncé qui généralise à la fois (2) et l'exercice 3.3.6 ?

3.4 Congruences $ax \equiv b \pmod n$, éléments inversibles de $\mathbf{Z}/n\mathbf{Z}$

3.4.1 Inverse d'une classe de congruence Rappelons qu'on suppose que $n \geq 1$ est un entier (strictement) positif. On s'intéresse à la congruence

$$ax \equiv 1 \pmod n. \tag{3.4.1.1}$$

Une solution de cette congruence — s'il existe — se comportera comme l'inverse $a \pmod n$. Par exemple, la congruence $3 \cdot 5 \equiv 1 \pmod 7$ nous dit que $5 \pmod 7$ est inverse de $3 \pmod 7$.

3.4.2 Théorème (Eléments inversibles de $\mathbf{Z}/n\mathbf{Z}$)**.** *Si $a \in \mathbf{Z}$ et $n \geq 1$, alors la congruence $ax \equiv 1 \pmod n$ a une solution si et seulement si $\operatorname{pgcd}(a, n) = 1$. Si c'est le cas, alors il existe une unique solution $x \pmod n$; on dit que la classe de congruence $a \pmod n$ est **inversible** et que $x \pmod n$ est son **inverse**. **Notation :** La classe $x \pmod n$ sera notée $\frac{1}{a} \pmod n$ ou $a^{-1} \pmod n$. L'ensemble de tous les éléments inversibles de $\mathbf{Z}/n\mathbf{Z}$ sera noté $(\mathbf{Z}/n\mathbf{Z})^*$ ou $(\mathbf{Z}/n\mathbf{Z})^\times$.*

Démonstration. **Unicité :** si $ax \equiv ay \equiv 1 \pmod n$, alors $y \equiv 1 \cdot y \equiv (ax)y \equiv x(ay) \equiv x \cdot 1 \equiv x \pmod n$.
Existence : on a les équivalences suivantes

$$\exists x \in \mathbf{Z} \;\; ax \equiv 1 \pmod n \iff \exists x, y \in \mathbf{Z} \;\; ax+ny = 1 \iff 1 \in a\mathbf{Z}+n\mathbf{Z} = \operatorname{pgcd}(a, n)\mathbf{Z} \iff \operatorname{pgcd}(a, n) = 1.$$

□

3.4.3 Calcul de l'inverse de $a \pmod n$ Si n est petit, on peut souvent déterminer l'inverse directement. En général, on applique l'algorithme d'Euclide (modifié) pour obtenir $d = \operatorname{pgcd}(a, n)$ et une relation de Bézout explicite $au + nv = d$. La classe $a \pmod n$ est inversible si et seulement si $d = 1$. Si c'est le cas, alors on a $au \equiv 1 \pmod n$, ce qui implique que l'inverse de $a \pmod n$ est égal à $u \pmod n$.

Par exemple, les calculs dans le paragraphe 2.4.5 impliquent qu'on a

$$5{\cdot}11 \equiv 1 \pmod{18}, \quad 11^{-1} \pmod{18} = 5 \pmod{18}, \quad 12{\cdot}13 \equiv 1 \pmod{31}, \quad 13^{-1} \pmod{31} = 12 \pmod{31}.$$

3.4.4 Exercice. (1) Déterminer les éléments inversibles de $\mathbf{Z}/12\mathbf{Z}$. Calculer leurs inverses respectifs.
(2) Idem pour $\mathbf{Z}/18\mathbf{Z}$.
(3) Si les classes $a \pmod n$ et $b \pmod n$ sont inversibles, il en est de même de leur produit $ab \pmod n$, et son inverse est égal à $(ab)^{-1} \equiv a^{-1}b^{-1} \pmod n$.

3.4.5 Puissances de $a \pmod n$ Si $a \pmod n$ est une classe de congruence inversible, on définit pour tout $m \in \mathbf{N}_+$

$$a^{-m} \pmod n := (a^{-1})^m \pmod n,$$

ce qui est égal à $(a^m)^{-1} \pmod n$, d'après l'exercice 3.4.4(3).

3.4.6 Exercice. Si $a \pmod n$ est inversible, montrer que l'on a

$$\forall l, m \in \mathbf{Z} \quad a^l \cdot a^m \equiv a^{l+m} \pmod n, \qquad (a^l)^m \equiv a^{lm} \pmod n.$$

3.4.7 Division de congruences On suppose qu'on a $a, b, c \in \mathbf{Z}$, $a \neq 0$ et

$$ac \equiv b \pmod{n}. \tag{3.4.7.1}$$

On aimerait diviser la congruence (3.4.7.1) par a, si possible.

Cas 1 : a divise n. Dans ce cas a divise aussi b. La congruence (3.4.7.1) équivaut à l'existence de $y \in \mathbf{Z}$ tel que

$$ac + ny = b. \tag{3.4.7.2}$$

Les entiers n et b sont divisibles par a, ce qui implique que l'égalité (3.4.7.2) équivaut à

$$c + (n/a)y = b/a. \tag{3.4.7.3}$$

Par conséquent, la congruence (3.4.7.1) équivaut à

$$c \equiv (b/a) \pmod{n/a} \tag{3.4.7.4}$$

(voir la proposition 3.1.6).

Cas 2 : $\operatorname{pgcd}(a, n) = 1$. Le théorème 3.4.2 mous dit qu'il existe un unique inverse $a^{-1} \pmod{n}$ de $a \pmod{n}$. Si l'on multiplie (3.4.7.1) par $a^{-1} \pmod{n}$, on obtient

$$c \equiv ba^{-1} \pmod{n}. \tag{3.4.7.5}$$

Réciproquement, si l'on multiplie (3.4.7.5) par $a \pmod{n}$, on obtient la congruence du départ (3.4.7.1). En résumé, (3.4.7.5) équivaut à (3.4.7.1).

Cas 3 : le cas général. On pose $d := \operatorname{pgcd}(a, n)$; dans ce cas d divise b. On applique d'abord le Cas 1 avec d à la place de a ; on obtient

$$(a/d)c \equiv (b/d) \pmod{n/d}. \tag{3.4.7.6}$$

On a $\operatorname{pgcd}(a/d, n/d) = 1$, ce qui signifie que le Cas 2 s'applique à (3.4.7.6) ; on obtient

$$c \equiv (b/d)(a/d)^{-1} \pmod{n/d} \tag{3.4.7.7}$$

(ce qui équivaut à la congruence du départ (3.4.7.1)).

Exemple : on aimerait simplifier la congruence

$$12x \equiv 15 \pmod{21}, \tag{3.4.7.8}$$

ce qui équivaut à l'existence de $y \in \mathbf{Z}$ tel que

$$12x + 21y = 15.$$

On peut diviser cet égalité par 3 ; on obtient

$$4x + 7y = 5,$$

ce qui équivaut à la congruence

$$4x \equiv 5 \pmod{7}. \tag{3.4.7.9}$$

On a $4 \cdot 2 \equiv 1 \pmod{7}$. Si l'on multiplie (3.4.7.9) par $4^{-1} \pmod{7} = 2 \pmod{7}$, on obtient

$$x \equiv 2 \cdot 4x \equiv 2 \cdot 5 \equiv 3 \pmod{7}, \tag{3.4.7.10}$$

ce qui équivaut à la congruence du départ (3.4.7.8), d'après la discussion ci-dessus.

On peut traiter le cas général

$$ax \equiv b \pmod{n}$$

de la même façon. Voici le résultat.

3.4.8 Théorème. *Soient $a, b, n \in \mathbf{Z}$ avec $a \neq 0$ et $n \geq 1$; on pose $d := \mathrm{pgcd}(a, n)$.*
(1) Si $d \nmid b$, alors la congruence $ax \equiv b \pmod{n}$ n'a pas de solutions.
(2) Si $d \mid b$, alors la congruence $ax \equiv b \pmod{n}$ équivaut à $(a/d)x \equiv (b/d) \pmod{n/d}$, ce qui a une unique solution modulo n/d, à savoir $x \equiv (b/d)(a/d)^{-1} \pmod{n/d}$.

Démonstration. On a tout fait dans le paragraphe 3.4.7 (avec $c = x$). Si l'on ne s'intéresse pas à la formule explicite, le raisonnement suivant démontre directement l'existence et l'unicité des solutions.
Unicité : si $ax \equiv ay \equiv b \pmod{n}$, alors il existe $z \in \mathbf{Z}$ tel que $a(x - y) = nz$, ce qui implique que $(a/d)(x - y) = (n/d)z$ est divisible par n/d. On a $\mathrm{pgcd}(a/d, n/d) = 1$; on déduit du lemme 2.3.8 que n/d divise $x - y$, d'où $x \equiv y \pmod{n/d}$.
Existence : on a les équivalences suivantes

$$\exists x \in \mathbf{Z} \quad ax \equiv b \pmod{n} \iff \exists x, y \in \mathbf{Z} \quad ax + ny = b \iff b \in a\mathbf{Z} + n\mathbf{Z} = \mathrm{pgcd}(a, n)\mathbf{Z} \iff \mathrm{pgcd}(a, n) \mid b.$$

□

3.4.9 Exemple On va résoudre le système (3.3.4.1)

$$\left.\begin{aligned} x &\equiv 5 \pmod{27} \\ x &\equiv 7 \pmod{37} \end{aligned}\right\}$$

en utilisant les méthodes qu'on a introduites dans les paragraphes ci-dessus. La deuxième congruence équivaut à l'existence de $y \in \mathbf{Z}$ tel que $x = 7 + 37y$. On substitue cette relation dans la première congruence ; on obtient

$$5 \equiv x \equiv 7 + 37y \equiv 7 + 10y \pmod{27},$$

ce qui équivaut à $10y \equiv -2 \equiv 25 \pmod{27}$. On peut diviser cette congruence par 5 (car $\mathrm{pgcd}(5, 27) = 1$) ; on obtient $2y \equiv 5 \pmod{27}$ et $y \equiv 14 \cdot 2y \equiv 14 \cdot 5 \equiv -11 \pmod{27}$. Par conséquent, $y = -11 + 27z$ avec $z \in \mathbf{Z}$ et le système du départ équivaut à

$$x = 7 - 11 \cdot 37 + 27 \cdot 37z \equiv 7 - 11 \cdot 37 \equiv -400 \pmod{27 \cdot 37}.$$

3.4.10 Exercice. (1) Résoudre le système $21x \equiv 33 \pmod{45}$, $15x \equiv 6 \pmod{66}$.
(2) Résoudre le système $x \equiv 9 \pmod{15}$, $x \equiv 3 \pmod{16}$, $x \equiv 13 \pmod{17}$.

4 Fonction φ d'Euler, théorème d'Euler

4.1 Conséquences du petit théorème de Fermat

4.1.1 Introduction Soit $a \in \mathbf{Z}$. On a démontré les congruences suivantes dans le paragraphe 3.2 :

$$3 \nmid a \implies a^2 \equiv 1 \pmod 3, \qquad a^6 \equiv 1 \pmod{3^2}, \qquad a^{18} \equiv 1 \pmod{3^3}, \tag{4.1.1.1}$$

$$5 \nmid a \implies a^4 \equiv 1 \pmod 5, \qquad a^{20} \equiv 1 \pmod{5^2}. \tag{4.1.1.2}$$

On peut se demander s'il y a une règle plus générale, à savoir

$$\forall p \in \mathcal{P} \quad p \nmid a \implies a^{p-1} \equiv 1 \pmod p, \tag{4.1.1.3}$$

$$\implies a^{(p-1)p^{k-1}} \equiv 1 \pmod{p^k} \qquad (k \geq 1). \tag{4.1.1.4}$$

C'est bien le cas ; on va le déduire du petit théorème de Fermat

$$\forall p \in \mathcal{P} \quad \forall a \in \mathbf{Z} \qquad a^p \equiv a \pmod p \tag{4.1.1.5}$$

en utilisant la proposition 4.1.5 ci-dessous. Le corollaire 3.1.8 implique alors des congruences analogues modulo un entier quelconque $n = p_1^{k_1} \cdots p_r^{k_r} \geq 1$. En particulier, on en déduit le théorème d'Euler

$$\operatorname{pgcd}(a,n) = 1 \implies a^{\varphi(n)} \equiv 1 \pmod n, \qquad \varphi(n) = \varphi(p_1^{k_1}) \cdots \varphi(p_r^{k_r}), \qquad \varphi(p^k) = (p-1)p^{k-1} \tag{4.1.1.6}$$

ainsi que son amélioration (le théorème 4.1.11).

On va traiter la fonction d'Euler φ et le théorème d'Euler d'un point de vue plus conceptuel dans le paragraphe 4.2.

4.1.2 Proposition (Théorème d'Euler pour $n = p$)**.** *Si $p \in \mathcal{P}$ et $a \in \mathbf{Z}$, $p \nmid a$, alors on a $a^{p-1} \equiv 1 \pmod p$.*

Démonstration. Si l'on multiplie la congruence (4.1.1.5) (le petit théorème de Fermat) par l'inverse $a^{-1} \pmod p$ de $a \pmod p$ (un tel inverse bien existe, car $\operatorname{pgcd}(a,p) = 1$, par l'hypothèse) on obtient $a^p a^{-1} \equiv aa^{-1} \pmod p$, d'où

$$a^{p-1} \equiv a^{p-1} a a^{-1} \equiv a^p a^{-1} \equiv a a^{-1} \equiv 1 \pmod p.$$

□

4.1.3 Exercice. Montrer que l'on a $a^{m+10n} \equiv a^m \pmod{11}$, pour tous $a \in \mathbf{Z}$ et $m, n \geq 1$. Déterminer $b \in \{0, \ldots, 10\}$ tel que $b \equiv 2019^{9102} \pmod{11}$ sans calculatrice.

4.1.4 Amélioration de congruences par $x \mapsto x^p$ Le principe général est très simple : **l'application de Frobenius** $x \mapsto x^p$ améliore des congruences modulo des puissances de p, pour tout $p \in \mathcal{P}$.

Voici le cas le plus simple : si $a \equiv b \pmod 2$, alors $a = b + 2c$ avec $c \in \mathbf{Z}$, ce qui implique que

$$a^2 = (b+2c)^2 = b^2 + 4bc + 4c^2 \equiv b^2 \pmod{2^2}.$$

En général, on utilise la divisibilité de coefficients binomiaux $\binom{p}{j}$ $(0 < j < p)$ par p que l'on a démontrée dans la proposition 1.5.25.

4.1.5 Proposition. *Si $p \in \mathcal{P}$ et si $a, b \in \mathbf{Z}$ vérifient $a \equiv b \pmod{p^k}$ $(k \geq 1)$, alors $a^p \equiv b^p \pmod{p^{k+1}}$.*

Démonstration. Il existe $c \in \mathbf{Z}$ tel que $a = b + p^k c$, ce qui implique que

$$a^p = (b+p^k c)^p = b^p + \binom{p}{1} b^{p-1}(p^k c) + \binom{p}{2} b^{p-2}(p^k c)^2 + \cdots + \binom{p}{p-1} b(p^k c)^{p-1} + p^{pk} c^p.$$

Chaque terme $\binom{p}{j} b^{p-j}(p^k c)^j$ avec $0 < j < p$ est divisible par $p \cdot p^k = p^{k+1}$, d'après la proposition 1.5.25. Le dernier terme $p^{pk} c^p$ est aussi divisible par p^{k+1}, car $pk \geq 2k \geq k+1$. □

4.1.6 Proposition (Théorème d'Euler pour $n = p^k$)**.** *Si $p \in \mathcal{P}$ et si $a \in \mathbf{Z}$, $p \nmid a$, alors on a $a^{(p-1)p^{k-1}} \equiv 1 \pmod{p^k}$ pour tout $k \geq 1$.*

Démonstration. Le cas $k = 1$ a été démontré dans la proposition 4.1.2. Le cas général s'en déduit par récurrence, compte tenu de la proposition 4.1.5 : si l'on a $a^{(p-1)p^{k-1}} \equiv 1 \pmod{p^k}$, alors

$$a^{(p-1)p^k} \equiv (a^{(p-1)p^{k-1}})^p \equiv 1^p \equiv 1 \pmod{p^{k+1}}.$$

□

4.1.7 Amélioration pour $p = 2$ Le cas $p = 2$ de la proposition ci-dessus affirme qu'on a

$$2 \nmid a \implies a^2 \equiv 1 \pmod 4, \qquad a^4 \equiv 1 \pmod 8, \qquad a^8 \equiv 1 \pmod{16}, \qquad a^{16} \equiv 1 \pmod{32}, \qquad \cdots$$

Cependant, on a montré dans le paragraphe 3.2.4 une congruence plus forte

$$2 \nmid a \implies a^2 \equiv 1 \pmod 8,$$

qui implique, grâce à la proposition 4.1.5, qu'on a

$$2 \nmid a \implies a^2 \equiv 1 \pmod 8, \qquad a^4 \equiv 1 \pmod{16}, \qquad a^8 \equiv 1 \pmod{32}, \qquad \cdots \tag{4.1.7.1}$$

Voici une formulation générale de ce résultat (voir aussi l'exercice 1.1.7).

4.1.8 Proposition (Théorème d'Euler améliorée pour $n = 2^k$)**.** *Si $k \geq 3$ et $2 \nmid a$, alors $a^{2^{k-2}} \equiv 1 \pmod{2^k}$.*

4.1.9 Exemples modulo 15, 35 et 504 Que se passe-t-il modulo un entier qui n'est pas une puissance d'un nombre premier ? La réponse est simple : on peut combiner les résultats précédents valables pour plusieurs nombres premiers en utilisant la proposition 3.1.7 et son corollaire 3.1.8.

Par exemple, $n = 15 = 3 \cdot 5 = \operatorname{ppcm}(3,5)$. Si $\operatorname{pgcd}(a,15) = 1$ (ce qui équivaut à $3 \nmid a$ et $5 \nmid a$), alors

$$\left.\begin{array}{l} 3 \nmid a \implies a^{3-1} = a^2 \equiv 1 \pmod 3 \implies a^4 \equiv 1 \pmod 3 \\ 5 \nmid a \implies a^{5-1} = a^4 \equiv 1 \pmod 5 \end{array}\right\} \implies a^4 \equiv 1 \pmod{\operatorname{ppcm}(3,5)} \equiv 1 \pmod{15}.$$

De même, $n = 35 = 5 \cdot 7$. Si $\operatorname{pgcd}(a,35) = 1$, alors

$$\left.\begin{array}{l} 5 \nmid a \implies a^{5-1} = a^4 \equiv 1 \pmod 5 \implies a^{12} \equiv (a^4)^3 \equiv 1 \pmod 5 \\ 7 \nmid a \implies a^{7-1} = a^6 \equiv 1 \pmod 7 \implies a^{12} \equiv (a^6)^2 \equiv 1 \pmod 7 \end{array}\right\} \implies a^{12} \equiv 1 \pmod{\underbrace{\operatorname{ppcm}(5,7)}_{35}}.$$

Voici un exemple plus compliqué : $n = 504 = 7 \cdot 8 \cdot 9 = 2^3 \cdot 3^2 \cdot 7$. Si $\operatorname{pgcd}(a,504) = 1$, alors

$$\left.\begin{array}{lll} 2\nmid a & \Longrightarrow & a^2\equiv 1 \pmod{2^3} \Longrightarrow a^6\equiv (a^2)^3\equiv 1 \pmod{2^3} \\ 3\nmid a & \Longrightarrow & a^{(3-1)\cdot 3}\equiv a^6\equiv 1 \pmod{3^2} \\ 7\nmid a & \Longrightarrow & a^{7-1}\equiv a^6\equiv 1 \pmod 7 \end{array}\right\} \Longrightarrow a^6\equiv 1 \pmod{\underbrace{\operatorname{ppcm}(2^3,3^2,7)}_{504}}.$$

4.1.10 Notation : fonction d'Euler φ On va définir et étudier la fonction Euler dans le paragraphe 4.2 ci-dessous. On n'utilise ici que les formules explicites suivantes pour ses valeurs (voir le théorème 4.2.5).

Soient p et $k\geq 1$; on pose

$$\varphi(p^k) := (p-1)p^{k-1} = p^k - p^{k-1} = p^k(1-\tfrac{1}{p}).$$

La proposition 4.1.6 affirme alors que $a^{\varphi(p^k)}\equiv 1 \pmod{p^k}$ si $p\nmid a$.

Soit $n=p_1^{k_1}\cdots p_r^{k_r}$ $(r\geq 0,\ k_i\geq 1)$ la décomposition en facteurs premiers d'un entier $n\geq 1$; on pose

$$\varphi(n) := \varphi(p_1^{k_1})\cdots\varphi(p_r^{k_r}) = (p_1^{k_1}-p_1^{k_1-1})\cdots(p_r^{k_r}-p_r^{k_r-1}) = n(1-\tfrac{1}{p_1})\cdots(1-\tfrac{1}{p_r}).$$

4.1.11 Théorème (Théorème d'Euler amélioré)**.** *Soit $n=p_1^{k_1}\cdots p_r^{k_r}\geq 1$ entier (où p_i sont des nombres premiers distincts, $r\geq 0$, $k_i\geq 1$). Si $\operatorname{pgcd}(a,n)=1$ et si $u\geq 1$ est divisible par $\varphi(p_i^{k_i})=p_i^{k_i}-p_i^{k_i-1}$ pour tout $i=1,\dots,r$, alors*

$$a^u\equiv 1 \pmod n.$$

De plus, si $p_1=2$ et $k_1\geq 3$, alors on peut remplacer $\varphi(p_1^{k_1})=2^{k_1-1}$ ci-dessus par $\varphi(p_1^{k_1})/2=2^{k_1-2}$.

Démonstration. On a $u=\varphi(p_i^{k_i})v_i$ pour tout $i=1,\dots,r$. D'après la proposition 4.1.6, on a

$$a^{\varphi(p_i^{k_i})}\equiv 1 \pmod{p_i^{k_i}} \Longrightarrow a^u\equiv \left(a^{\varphi(p_i^{k_i})}\right)^{v_i}\equiv 1 \pmod{p_i^{k_i}}.$$

La proposition 3.1.7 implique alors que la congruence $a^u\equiv 1$ est valable modulo $\operatorname{ppcm}(p_1^{k_1},\dots,p_r^{k_r})=n$.

Si l'on a $p_1=2$ et $k_1\geq 3$, alors on applique la proposition 4.1.8 à la place de la proposition 4.1.6. □

4.1.12 Amélioration du théorème d'Euler (version optimale) La valeur minimum de u qui satisfait aux hypothèses du théorème précédent est égale à

$$u=\operatorname{ppcm}(\varphi(p_1^{k_1}),\dots,\varphi(p_r^{k_r})) \tag{4.1.12.1}$$

(comme ci-dessus, on remplace $\varphi(p_1^{k_1})$ par $\varphi(p_1^{k_1})/2$ si $p_1=2$ et $k_1\geq 3$).

4.1.13 Théorème (Théorème d'Euler)**.** *Soient $a,n\in\mathbf{Z}$ des entiers tels que $n\geq 1$ et $\operatorname{pgcd}(a,n)=1$. On a $a^{\varphi(n)}\equiv 1 \pmod n$.*

Démonstration. Il s'agit d'un cas particulier du théorème 4.1.11 avec $u=\varphi(n)$. Voici 4.2.9 ci-dessous pour une autre démonstration. □

4.1.14 Comparaison du théorème d'Euler et son amélioration On va comparer les deux versions du théorème d'Euler pour les trois valeurs $n=15, 35$ et 504 qu'on a traitées dans le paragraphe 4.1.9. Compte tenu des valeurs

$$\varphi(15)=\varphi(3)\varphi(5)=(3-1)(5-1)=8, \qquad \varphi(35)=\varphi(5)\varphi(7)=(5-1)(7-1)=24,$$
$$\varphi(504)=\varphi(2^3)\varphi(3^2)\varphi(7)=(2^3-2^2)(3^2-3^1)(7-1)=144,$$

le théorème d'Euler nous dit que l'on a

$$\begin{aligned} \mathrm{pgcd}(a,15)=1 &\implies a^8 \equiv 1 \pmod{15} \\ \mathrm{pgcd}(a,35)=1 &\implies a^{24} \equiv 1 \pmod{35} \\ \mathrm{pgcd}(a,504)=1 &\implies a^{144} \equiv 1 \pmod{504}. \end{aligned}$$

La version améliorée qui a été explicitée dans 4.1.9 est bien plus forte :

$$\begin{aligned} \mathrm{pgcd}(a,15)=1 &\implies a^4 \equiv 1 \pmod{15} \\ \mathrm{pgcd}(a,35)=1 &\implies a^{12} \equiv 1 \pmod{35} \\ \mathrm{pgcd}(a,504)=1 &\implies a^6 \equiv 1 \pmod{504}. \end{aligned}$$

4.1.15 Exercice. Sans calculatrice, déterminer $3^{15} \pmod{2^3}$, $3^{15} \pmod{5^3}$ puis $3^{15} \pmod{1000}$.

4.1.16 Exercice. Soit $a \in \mathbf{Z}$. Montrer :
(1) Si $2 \nmid a$ et $3 \nmid a$, alors $a^2 \equiv 1 \pmod{24}$.
(2) Si $2 \nmid a$, $3 \nmid a$ et $5 \nmid a$, alors $a^4 \equiv 1 \pmod{240}$.
(3) Si $2 \nmid a$ et $5 \nmid a$, alors $a^{100} \equiv 1 \pmod{1000}$.
(4) Si $b \in \mathbf{Z}$, alors $b^{100} \equiv 0, 1, 376, 625 \pmod{1000}$.

4.1.17 Exercice. Soit $a \in \mathbf{Z}$.
(1) Déterminer les valeurs possibles de $a^{12} \pmod 7$, $a^{12} \pmod{13}$ et $a^{12} \pmod{91}$.
(2) Idem pour a^6 à la place de a^{12}.
(3) Montrer : si $n \geq 1$ est un entier tel que $n \equiv 1 \pmod{12}$, alors on a $a^n \equiv a \pmod{91}$.

4.2 Fonction φ d'Euler

4.2.1 Notation On note $|X|$ le cardinal (le nombre d'éléments) d'un ensemble X. On a $|X \times Y| = |X| \cdot |Y|$. Rappelons la notation standard (où $n \in \mathbf{N}_+$) :

$$\begin{aligned} \mathbf{Z}/n\mathbf{Z} &= \{\text{classes de congruence } (\mathrm{mod}\, n)\} = \{1 \pmod n, 2 \pmod n, \ldots, n \pmod n\} \\ (\mathbf{Z}/n\mathbf{Z})^* &= \{\text{classes de congruence inversibles } (\mathrm{mod}\, n)\} = \{a \pmod n \mid 1 \leq a \leq n, \mathrm{pgcd}(a,n)=1\} \end{aligned}$$

On définit la **fonction d'Euler** $\varphi : \mathbf{N}_+ \longrightarrow \mathbf{N}_+$ de la manière suivante :

$$\varphi(n) := |(\mathbf{Z}/n\mathbf{Z})^*|\,. \tag{4.2.1.1}$$

Par exemple,

$$\begin{gathered} (\mathbf{Z}/1\mathbf{Z})^* = \{1 \pmod 1\}, \quad (\mathbf{Z}/2\mathbf{Z})^* = \{1 \pmod 2\}, \quad (\mathbf{Z}/3\mathbf{Z})^* = \{1 \pmod 3, 2 \pmod 3\}, \\ (\mathbf{Z}/4\mathbf{Z})^* = \{1 \pmod 4, 3 \pmod 4\}, \quad (\mathbf{Z}/5\mathbf{Z})^* = \{1 \pmod 5, 2 \pmod 5, 3 \pmod 5, 4 \pmod 5\}, \\ (\mathbf{Z}/6\mathbf{Z})^* = \{1 \pmod 6, 5 \pmod 6\}, \end{gathered}$$

d'où

$$\varphi(1)=1, \quad \varphi(2)=1, \quad \varphi(3)=2, \quad \varphi(4)=2, \quad \varphi(5)=4, \quad \varphi(6)=2.$$

4.2.2 Exemple : $(\mathbf{Z}/6\mathbf{Z})^*$ et $(\mathbf{Z}/2\mathbf{Z})^* \times (\mathbf{Z}/3\mathbf{Z})^*$ L'égalité $\varphi(6) = \varphi(2)\varphi(3)$ suggère qu'il faut étudier des liens au théorème chinois.

On reproduit ci-dessous la table qui explicite la correspondance entre $\mathbf{Z}/6\mathbf{Z}$ et $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$ (voir le paragraphe 3.3.1). Les carrés marquent les classes de congruence inversibles.

$x \pmod 6$	$x \pmod 2$	$x \pmod 3$
0	0	0
$\boxed{1}$	$\boxed{1}$	$\boxed{1}$
2	0	$\boxed{2}$
3	$\boxed{1}$	0
4	0	$\boxed{1}$
$\boxed{5}$	$\boxed{1}$	$\boxed{2}$

On voit qu'une classe de congruence $x \pmod 6$ est inversible dans $\mathbf{Z}/6\mathbf{Z}$ si et seulement si la classe de congruence $x \pmod 2$ est inversible dans $\mathbf{Z}/2\mathbf{Z}$ et la classe de congruence $x \pmod 3$ est inversible dans $\mathbf{Z}/3\mathbf{Z}$.

Autrement dit, si l'on considère l'application bijective

$$\begin{array}{ccc} \mathbf{Z}/6\mathbf{Z} & \longrightarrow & \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z} \\ x \pmod 6 & \mapsto & (x \pmod 2,\, x \pmod 3) \end{array}$$

qu'on a définie dans (3.3.1.1), alors le sous-ensemble $(\mathbf{Z}/6\mathbf{Z})^*$ correspond à $(\mathbf{Z}/2\mathbf{Z})^* \times (\mathbf{Z}/3\mathbf{Z})^*$. En particulier, les deux sous-ensembles ont même nombre d'éléments, ce qui explique l'égalité $\varphi(6) = \varphi(2)\varphi(3)$.

On va montrer maintenant qu'il s'agit d'un phénomène général.

4.2.3 Proposition. *Soient $a \in \mathbf{Z}$, $m, n \geq 1$ et $\operatorname{pgcd}(m,n) = 1$. La classe $a \pmod{mn}$ est inversible dans $\mathbf{Z}/mn\mathbf{Z}$ si et seulement si la classe $a \pmod m$ est inversible dans $\mathbf{Z}/m\mathbf{Z}$ et la classe $a \pmod n$ est inversible dans $\mathbf{Z}/n\mathbf{Z}$.*
Autrement dit, le sous-ensemble $(\mathbf{Z}/mn\mathbf{Z})^* \subset \mathbf{Z}/mn\mathbf{Z}$ correspond à $(\mathbf{Z}/m\mathbf{Z})^* \times (\mathbf{Z}/n\mathbf{Z})^* \subset \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$ sous l'aplication bijective $\mathbf{Z}/mn\mathbf{Z} \longrightarrow \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$ dans le théorème chinois 3.3.2.

Démonstration. Si $a \pmod{mn}$ est inversible dans $\mathbf{Z}/mn\mathbf{Z}$, alors il existe $b \in \mathbf{Z}$ tel que $ab \equiv 1 \pmod{mn}$, ce qui implique que $ab \equiv 1 \pmod m$ et $ab \equiv 1 \pmod n$.

Réciproquement, si $a \pmod m$ est inversible dans $\mathbf{Z}/m\mathbf{Z}$ et $a \pmod n$ est inversible dans $\mathbf{Z}/n\mathbf{Z}$, alors il existe $b, c \in \mathbf{Z}$ tels que $ab \equiv 1 \pmod m$ et $ac \equiv 1 \pmod n$. On a $\operatorname{pgcd}(m,n) = 1$; le théorème chinois implique qu'il existe $x \in \mathbf{Z}$ tel que $x \equiv b \pmod m$ et $x \equiv c \pmod n$. On en déduit que $ax \equiv ab \equiv 1 \pmod m$ et $ax \equiv ac \equiv 1 \pmod n$, d'où $ax \equiv 1 \pmod{\operatorname{ppcm}(m,n)} \equiv 1 \pmod{mn}$. □

4.2.4 Corollaire. *Si $m, n \geq 1$ et $\operatorname{pgcd}(m,n) = 1$, alors on a $\varphi(mn) = \varphi(m)\varphi(n)$.*

Démonstration. D'après la proposition 4.2.3, les ensembles $(\mathbf{Z}/mn\mathbf{Z})^*$ et $(\mathbf{Z}/m\mathbf{Z})^* \times (\mathbf{Z}/n\mathbf{Z})^*$ ont même nombre d'éléments. □

4.2.5 Théorème (Propriétés de $\varphi(n)$)**.** *(1) Si p est un nombre premier, alors $\varphi(p) = p - 1$.*
(2) Si p est un nombre premier et $k \geq 1$, alors $\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1) = p^k(1 - \frac{1}{p})$.
(3) Si $m, n \geq 1$ et $\operatorname{pgcd}(m,n) = 1$, alors $\varphi(mn) = \varphi(m)\varphi(n)$.
(4) Si $n = p_1^{k_1} \cdots p_r^{k_r}$ (où $r \geq 0$, p_i sont des nombres premiers distincts, $k_i \geq 1$), alors

$$\varphi(n) = \varphi(p_1^{k_1}) \cdots \varphi(p_r^{k_r}) = (p_1^{k_1} - p_1^{k_1-1}) \cdots (p_r^{k_r} - p_r^{k_r-1}) = n(1 - \tfrac{1}{p_1}) \cdots (1 - \tfrac{1}{p_r}) = n \prod_{p \mid n} (1 - \tfrac{1}{p}). \quad (4.2.5.1)$$

Démonstration. (1) $(\mathbf{Z}/p\mathbf{Z})^* = \{1 \pmod p,\ 2 \pmod p, \ldots,\ p-1 \pmod p\}$.
(2) Dans ce cas on a $(\mathbf{Z}/p^k\mathbf{Z})^* = \{a \pmod{p^k} \mid 1 \leq a \leq p^k,\ p \nmid a\} = \{a \pmod{p^k} \mid 1 \leq a \leq p^k\} \smallsetminus \{pb \pmod{p^k} \mid 1 \leq b \leq p^k/p\}$, ce qui implique que le cardinal de cet ensemble est ègal à $p^k - p^k/p$.
On a démontré le point (3) dans le corollaire 4.2.4. Le point (4) est une combinaison de (2) et (3). □

4.2.6 Remarques et exemples (1) Si p est un nombre premier, alors $\varphi(p^2) = p^2 - p = p(p-1) \neq (p-1)^2 = \varphi(p)^2$.
(2) $\varphi(120) = \varphi(2^3 \cdot 3 \cdot 5) = (2^3 - 2^2)(3-1)(5-1) = 4 \cdot 2 \cdot 4 = 32 = 2^5$.

4.2.7 Exercice. Montrer que $\varphi(2n)/\varphi(n)$ est égal à 1 (resp. à 2) si $2 \nmid n$ (resp. si $2 \mid n$). Que se passe-t-il si l'on remplace $2n$ par $3n$ (resp. par $6n$) ?

4.2.8 Inclusion-exclusion On peut démontrer la formule (4.2.5.1) pour $\varphi(n)$ directement en utilisant le principe d'inclusion-exclusion. Voici deux cas particuliers.
Exemple 1 : $n = 12 = 2^2 \cdot 3$ On a $\operatorname{pgcd}(x, 12) = 1 \iff 2 \nmid x$ et $3 \nmid x$.
Les sous-ensembles $A, B \subset \mathbf{Z}/12\mathbf{Z}$

$$A = \{1 \leq x \leq 12;\ 2 \mid x\} = \{2a \mid 1 \leq a \leq 6\} = \{2, 4, 6, 8, 10, 12\}$$
$$B = \{1 \leq x \leq 12;\ 3 \mid x\} = \{3b \mid 1 \leq b \leq 4\} = \{3, 6, 9, 12\}$$

vérifient

$$A \cap B = \{1 \leq x \leq 12;\ 6 \mid x\} = \{6c \mid 1 \leq c \leq 2\} = \{6, 12\}$$
$$A \cup B = \{1 \leq x \leq 12;\ x \pmod{12} \text{ n'est pas inversible}\} = \{2, 4, 6, 8, 10, 12, 3, 9\}$$
$$(\mathbf{Z}/12\mathbf{Z})^* = \{1 \leq x \leq 12;\ x \pmod{12} \text{ est inversible}\} = \mathbf{Z}/12\mathbf{Z} \smallsetminus (A \cup B) = \{1, 5, 7, 11\}.$$

Les formules

$$|A \cup B| = |A| + |B| - |A \cap B|, \qquad |A| = 12/2, \qquad |B| = 12/3, \qquad |A \cap B| = 12/6$$

impliquent qu'on a

$$\varphi(12) = 12 - |A \cup B| = 12 - |A| - |B| + |A \cap B| = 12\left(1 - \tfrac{1}{2} - \tfrac{1}{3} + \tfrac{1}{6}\right) = 12(1 - \tfrac{1}{2})(1 - \tfrac{1}{3}). \quad (4.2.8.1)$$

Exemple 2 : $n = p_1^{k_1} p_2^{k_2} p_3^{k_3}$ On a $\operatorname{pgcd}(x, n) = 1 \iff p_1 \nmid x$, $p_2 \nmid x$ et $p_3 \nmid x$. Si l'on définit des sous-ensembles $A, B, C \subset \mathbf{Z}/n\mathbf{Z}$ de la manière suivante

$$A = \{1 \leq x \leq n;\ p_1 \mid x\} = \{p_1 a \mid 1 \leq a \leq n/p_1\}$$
$$B = \{1 \leq x \leq n;\ p_2 \mid x\} = \{p_2 b \mid 1 \leq b \leq n/p_2\}$$
$$C = \{1 \leq x \leq n;\ p_3 \mid x\} = \{p_3 c \mid 1 \leq c \leq n/p_3\},$$

alors on a

$$A \cap B = \{1 \leq x \leq n;\ p_1 p_2 \mid x\}, \quad A \cap C = \{1 \leq x \leq n;\ p_1 p_3 \mid x\}, \quad B \cap C = \{1 \leq x \leq n;\ p_2 p_3 \mid x\},$$
$$A \cap B \cap C = \{1 \leq x \leq n;\ p_1 p_2 p_3 \mid x\}, \quad A \cup B \cup C = \{1 \leq x \leq n;\ x \pmod n \text{ n'est pas inversible}\},$$

ce qui implique que $\varphi(n) = n - |A \cup B \cup C|$ et

$$\begin{array}{c} |A| = n/p_1,\ |B| = n/p_2,\ |C| = n/p_3,\ |A \cap B| = n/p_1p_2, \\ |A \cap C| = n/p_1p_3,\ |B \cap C| = n/p_2p_3,\ |A \cap B \cap C| = n/p_1p_2p_3. \end{array} \tag{4.2.8.2}$$

La formule générale

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C| \tag{4.2.8.3}$$

implique alors qu'on a bien

$$\varphi(n) = n\left(1 - \tfrac{1}{p_1} - \tfrac{1}{p_2} - \tfrac{1}{p_3} + \tfrac{1}{p_1p_2} + \tfrac{1}{p_1p_3} + \tfrac{1}{p_2p_3} - \tfrac{1}{p_1p_2p_3}\right) = n\left(1 - \tfrac{1}{p_1}\right)\left(1 - \tfrac{1}{p_2}\right)\left(1 - \tfrac{1}{p_3}\right). \tag{4.2.8.4}$$

Exemple 3 : $n = p_1^{k_1} \cdots p_r^{k_r}$ Exercise pour le lecteur.

4.2.9 Théorème (Théorème d'Euler (bis))**.** *Soient $a, n \in \mathbf{Z}$ des entiers tels que $n \geq 1$ et $\operatorname{pgcd}(a, n) = 1$. On a $a^{\varphi(n)} \equiv 1 \pmod n$.*

Démonstration. Voici un raisonnement algébrique qui sera valable dans un cadre plus abstrait (voir le corollaire 7.5.9 ci-dessous). Notons $x_1 \pmod n, \ldots, x_{\varphi(n)} \pmod n$ les éléments invertibles de $\mathbf{Z}/n\mathbf{Z}$. On multiplie chaque $x_i \pmod n$ par $a \pmod n$; on obtient les éléments $ax_1 \pmod n, \ldots, ax_{\varphi(n)} \pmod n$. Chaque classe $ax_i \pmod n$ est inversible dans $\mathbf{Z}/n\mathbf{Z}$, et les classes $ax_i \pmod n$ sont distinctes (en effet, si $ax \equiv ay \pmod n$, alors $x \equiv a^{-1}ax \equiv a^{-1}ay \equiv y \pmod n$). On en déduit que

$$\{x_1 \pmod n, \ldots, x_{\varphi(n)} \pmod n\} = (\mathbf{Z}/n\mathbf{Z})^* = \{ax_1 \pmod n, \ldots, ax_{\varphi(n)} \pmod n\}. \tag{4.2.9.1}$$

Prenons, par exemple, $n = 12$ et $a = 5$. On a dans ce cas

$$\{1, 5, 7, 11 \pmod{12}\} = (\mathbf{Z}/12\mathbf{Z})^* = \{5, 1, 11, 7 \pmod{12}\}$$

(car $5 \cdot 1 \equiv 5$, $5 \cdot 5 \equiv 1$, $5 \cdot 7 \equiv 11$, $5 \cdot 11 \equiv 7 \pmod{12}$).

L'égalité (4.2.9.1) implique que le produit de toutes les classes de congruence inversibles est égal à la fois à

$$x := x_1 \cdots x_{\varphi(n)} \pmod n \tag{4.2.9.2}$$

et à

$$(ax_1) \cdots (ax_{\varphi(n)}) \pmod n \equiv a^{\varphi(n)}x \pmod n, \tag{4.2.9.3}$$

d'où

$$a^{\varphi(n)}x \equiv x \pmod n \tag{4.2.9.4}$$

La classe $x \pmod n$ est inversible, étant le produit de classes inversibles. Si l'on multiplie (4.2.9.4) par $x^{-1} \pmod n$, on obtient la congruence cherchée $a^{\varphi(n)} \equiv 1 \pmod n$. □

4.2.10 Corollaires du théorème d'Euler (1) Si $n = p$ est un nombre premier, alors $\varphi(p) = p - 1$ et on retrouve le fait qu'on a $a^{p-1} \equiv 1 \pmod{p}$ si $p \nmid a$ (voir la proposition 4.1.2).
(2) Plus généralement, si p est un nombre premier et $k \geq 1$, alors $\varphi(p^k) = (p-1)p^{k-1}$ et on obtient le fait que $a^{(p-1)p^{k-1}} \equiv 1 \pmod{p^k}$ si $p \nmid a$ (voir la proposition 4.1.6).
(3) Le petit théorème de Fermat est une conséquence immédiate de (1) : si $p \mid a$, alors $a^p \equiv 0 \equiv a \pmod{p}$, tandis que si $p \nmid a$, alors (1) implique que $a^p \equiv a \cdot a^{p-1} \equiv a \cdot 1 \equiv a \pmod{p}$. On s'est déjà apperçu dans la preuve de la proposition 4.1.2 que le raisonnement ci-dessus marchait aussi dans l'autre sens.
(4) Y a-t-il un analogue du petit théorème de Fermat $\pmod{n}$ si n n'est pas un nombre premier ? Autrement dit, existe-t-il un entier $m > 1$ tel que l'on ait $a^m \equiv a \pmod{n}$ pour tout $a \in \mathbf{Z}$? Voir la proposition 4.2.11 ci-dessous. Ce résultat nous sera utile dans le paragraphe 4.4.2 consacré aux applications à la cryptographie, ainsi que dans le paragraphe 5.3.

4.2.11 Proposition. *Soit $n > 1$ un entier.*
(1) S'il existe un nombre premiere p tel que $p^2 \mid n$, alors il n'y a aucun $m > 1$ vérifiant

$$\forall a \in \mathbf{Z} \quad a^m \equiv a \pmod{n}.$$

(2) Si $n = p_1 \cdots p_r$ est un produit de $r \geq 1$ nombres premiers distincts et si $m \geq 1$ vérifie $(p_i - 1) \mid (m-1)$ pour tout $i = 1, \ldots, r$ (ce qui équivaut à $\operatorname{ppcm}(p_1 - 1, \ldots, p_r - 1) \mid (m-1)$), alors on a

$$\forall a \in \mathbf{Z} \quad a^m \equiv a \pmod{n}.$$

Démonstration. (1) Si $a = p$ et $m > 1$, alors $p^2 \mid a^m$ et $p^2 \nmid a$, ce qui implique que $p^2 \nmid (a^m - a)$, d'où $n \nmid (a^m - a)$.
(2) D'après la proposition 3.1.7 et son corollaire 3.1.8, il suffit de montrer que l'on a

$$\forall a \in \mathbf{Z} \quad a^m \equiv a \pmod{p_i}$$

pour tout $i = 1, \ldots, r$. On écrit $(m-1) = (p_i - 1)t_i$. Si $p_i \mid a$, alors $a^m \equiv 0 \equiv a \pmod{p_i}$. Si $p_i \nmid a$, alors $a^{p_i - 1} \equiv 1 \pmod{p_i}$, d'où

$$a^m \equiv a \cdot (a^{p_i-1})^{t_i} \equiv a \cdot 1 \equiv a \pmod{p_i}.$$

□

4.2.12 Exemples (1) $\forall a \in \mathbf{Z} \quad a^{21} \equiv a \pmod{55}$. On a $n = 55 = 5 \cdot 11$ et $m - 1 = 20$.
(2) $\forall a \in \mathbf{Z} \quad a^{561} \equiv a \pmod{561}$. On a $m = n = 561 = 3 \cdot 11 \cdot 17$ et $m - 1 = 560 = 2^4 \cdot 5 \cdot 7$. L'entier 561 est un **nombre de Carmichael** selon la terminologie de la Définition 5.3.4 ci-dessous.

4.3 Structure de $(\mathbf{Z}/n\mathbf{Z})^*$

4.3.1 Motivation On sait que si les classes de congruence $a \pmod{n}$ et $b \pmod{n}$ sont inversibles dans $\mathbf{Z}/n\mathbf{Z}$, les classes $ab \pmod{n}$ et $a^{-1} \pmod{n}$ le sont aussi (autrement dit, $(\mathbf{Z}/n\mathbf{Z})^*$ est un groupe abélien pour la multiplication ; voir le chapitre 7 ci-dessous). Néanmoins, multiplication dans $(\mathbf{Z}/n\mathbf{Z})^*$ est beaucoup plus compliquée que l'addition dans $\mathbf{Z}/n\mathbf{Z}$.

On rencontre le même phénomène dans le monde réel : multiplication de nombres réels (positifs) est compliquée, mais on peut se ramener à l'addition en utilisant logarithme en base $a > 1$

$$\log_a : (\mathbf{R}_{>0}, \cdot) \longrightarrow (\mathbf{R}, +), \qquad \log_a(a^t) = t, \qquad \log_a(xy) = \log_a(x) + \log_a(y), \tag{4.3.1.1}$$

grâce au fait que tout nombre réel positif s'écrit a^t avec $t \in \mathbf{R}$.

Peut-on faire la même chose si l'on remplace $\mathbf{R}_{>0}$ par $(\mathbf{Z}/n\mathbf{Z})^*$? La réponse et "oui" si et seulement si tout élément de $(\mathbf{Z}/n\mathbf{Z})^*$ est une puissance d'une classe de congruence inversible $a \pmod n$ qu'on a fixée (on dit alors que $a \pmod n$ est un **générateur de** $(\mathbf{Z}/n\mathbf{Z})^*$ ou une **racine primitive modulo** n).

On va étudier maintenant l'existence d'un tel générateur pour quelques petites valeurs de n.

4.3.2 Générateurs de $(\mathbf{Z}/n\mathbf{Z})^*$ (exemples) Si $n = 3, 4, 6$, alors $(\mathbf{Z}/n\mathbf{Z})^* = \{\pm 1 \pmod n\}$, ce qui implique que $-1 \pmod n$ est un générateur de $(\mathbf{Z}/n\mathbf{Z})^*$.

Exemple 1 : $n = 5$.

$a \pmod 5$	$a^2 \pmod 5$	$a^3 \pmod 5$	$a^4 \pmod 5$
1	1	1	1
2	4	3	1
3	4	2	1
4	1	4	1

Les générateurs de $(\mathbf{Z}/5\mathbf{Z})^*$ sont les classes $2 \pmod 5$ et $3 \pmod 5 = 2^{-1} \pmod 5$.

Exemple 2 : $n = 7$.

$a \pmod 7$	$a^2 \pmod 7$	$a^3 \pmod 7$	$a^4 \pmod 7$	$a^5 \pmod 7$	$a^6 \pmod 7$
1	1	1	1	1	1
2	4	1	2	4	1
3	2	6	4	5	1
4	2	1	4	2	1
5	4	6	2	3	1
6	1	6	1	6	1

Les générateurs de $(\mathbf{Z}/7\mathbf{Z})^*$ sont les classes $3 \pmod 7$ et $5 \pmod 7 = 3^{-1} \pmod 7$.

Exemple 3 : $n = 8$.

$a \pmod 8$	$a^2 \pmod 8$	$a^3 \pmod 8$	$a^4 \pmod 8$
1	1	1	1
3	1	3	1
5	1	5	1
7	1	7	1

Il n'y a pas de générateurs de $(\mathbf{Z}/8\mathbf{Z})^*$.

Exemple 4 : $n = 9$.

$a \pmod 9$	$a^2 \pmod 9$	$a^3 \pmod 9$	$a^4 \pmod 9$	$a^5 \pmod 9$	$a^6 \pmod 9$
1	1	1	1	1	1
2	4	8	7	5	1
4	7	1	4	7	1
5	7	8	4	2	1
7	4	1	7	4	1
8	1	8	1	8	1

Les générateurs de $(\mathbf{Z}/9\mathbf{Z})^*$ sont les classes $2 \pmod 9$ et $5 \pmod 9 = 2^{-1} \pmod 9$.

Exemple 5 : $n = 15$**.** Il y a $\varphi(15) = (3-1)(5-1) = 8$ éléments inversibles modulo 15, mais on a montré dans le paragraphe 4.1.9 qu'on a $a^4 \equiv 1 \pmod{15}$ si $\operatorname{pgcd}(a, 15) = 1$. On en déduit que la suite des puissances $a^{4k+l} \equiv (a^4)^k a^l \equiv a^l \pmod{15}$ contient au plus 4 valeurs (qui correspondent à $l = 0, 1, 2, 3$), ce qui implique que $a \pmod{15}$ n'est jamais un générateur de $(\mathbf{Z}/15\mathbf{Z})^*$.

Le même raisonnement montre qu'un générateur de $(\mathbf{Z}/n\mathbf{Z})^*$ existe si et seulement si l'exposant $\varphi(n)$ dans le théorème d'Euler ne peut pas être amélioré (autrement dit, si et seulement si on a $u = \varphi(n)$ dans le théorème 4.1.11).

4.3.3 Définition. On suppose qu'on a $a, n \in \mathbf{Z}$, $n \geq 1$ et $\operatorname{pgcd}(a, n) = 1$. **L'ordre** d'une classe de congruence inversible $a \pmod n$ dans $(\mathbf{Z}/n\mathbf{Z})^*$ est le plus petit entier $d \geq 1$ tel que $a^d \equiv 1 \pmod n$ (le théorème d'Euler implique que que $d \leq \varphi(n)$). On a $a^{kd+l} \equiv (a^d)^k a^l \equiv 1^k \cdot a^l \equiv a^l \pmod n$, pour tous $k, l \in \mathbf{Z}$.

4.3.4 L'ordre de $a \pmod n$ **dans** $(\mathbf{Z}/n\mathbf{Z})^*$ **(exemples)** Les tables dans le paragraphe 4.3.2 nous permettent de déterminer l'ordre de toutes les classes de congruence inversibles $\pmod n$ pour $n = 4, 7, 8, 9$.

$a \pmod 5$	$1 \pmod 5$	$2 \pmod 5$	$3 \pmod 5$	$4 \pmod 5$
d	1	4	4	2

$a \pmod 7$	$1 \pmod 7$	$2 \pmod 7$	$3 \pmod 7$	$4 \pmod 7$	$5 \pmod 7$	$6 \pmod 7$
d	1	3	6	3	6	2

$a \pmod 8$	$1 \pmod 8$	$3 \pmod 8$	$5 \pmod 8$	$7 \pmod 8$
d	1	2	2	2

$a \pmod 9$	$1 \pmod 9$	$2 \pmod 9$	$4 \pmod 9$	$5 \pmod 9$	$7 \pmod 9$	$8 \pmod 9$
d	1	6	3	6	3	2

Dans les exemples ci-dessus, l'ordre de chaque élément $a \pmod{\in}(\mathbf{Z}/n\mathbf{Z})^*$ divise $\varphi(n)$. Il est égal à $\varphi(n)$ si et seulement si $a \pmod n$ est un générateur de $(\mathbf{Z}/n\mathbf{Z})^*$. On verra qu'il s'agit d'une propriété générale.

4.3.5 Exercice. Soit $n \in \mathbf{N}$. On pose $a_n = 3^n$, $b_n = 4^n$ et $c_n = 1018 \cdot 2018^n + 1026 \cdot 2019^n$.
(1) Que peut-on dire de valeurs de $a_n \pmod{13}$ et $b_n \pmod{13}$?
(2) Que peut-on dire de valeurs de $c_n \pmod{13}$? Quand est-ce qu'on a $c_n \equiv 0 \pmod{13}$ (resp. $c_n \equiv 3 \pmod{13}$) ?

4.3.6 Proposition. *Soient* $a, n \in \mathbf{Z}$, $n \geq 1$ *et* $\operatorname{pgcd}(a, n) = 1$. *On note* $d \geq 1$ *l'ordre de* $a \pmod n$ *dans* $(\mathbf{Z}/n\mathbf{Z})^*$.
(1) Pour $l \in \mathbf{Z}$*, il est équivalent :* $a^l \equiv 1 \pmod n \iff d \mid l$.
(2) Pour $l, m \in \mathbf{Z}$*, il est équivalent :* $a^l \equiv a^m \pmod n \iff d \mid (l-m) \iff l \equiv m \pmod d$.
(3) L'ensemble $\{a^m \mid m \in \mathbf{Z}\}$ *est égal à* $\{a, a^2, \ldots, a^d \equiv 1 \pmod n\}$ *; il a* d *éléments.*

Démonstration. (1) Si $l = dk$, alors $a^l \equiv (a^d)^k \equiv 1^k \equiv 1 \pmod n$. Réciproquement, supposons que $a^l \equiv 1 \pmod n$. La division euclidienne de l par d nous permet d'écrire $l = dq + r$, où $q, r \in \mathbf{Z}$, $0 \leq r < d$. On a $1 \equiv a^l \equiv (a^d)^q a^r \equiv 1 \cdot a^r \equiv a^r$; minimalité de d implique que $r = 0$, ce qui signifie que $l = dq$ est bien divisible par d.

(2) Les équivalences

$$a^l \equiv a^m \pmod n \iff (a^{-1})^m a^l \equiv (a^{-1})^m a^m \pmod n \iff a^{l-m} \equiv 1 \pmod n$$

sont automatiques, et la toute dernière condition équivaut à $d \mid (l-m)$, après (1).
(3) Tout $m \in \mathbf{Z}$ s'écrit sous la forme $m = kd + l$, où $k, l \in \mathbf{Z}$ et $1 \leq l \leq d$. On en déduit que $a^m \equiv (a^d)^k a^l \equiv a^l \pmod n$. Si $1 \leq i < j \leq d$, alors $0 < j - i < d$, ce qui implique que $d \nmid (j-i)$ et $a^i \not\equiv a^j \pmod n$, d'après (2). □

4.3.7 Corollaire. *L'ordre de chaque élément $a \pmod n$ de $(\mathbf{Z}/n\mathbf{Z})^*$ divise $\varphi(n)$ (car $a^{\varphi(n)} \equiv 1 \pmod n$, d'après le théorème d'Euler). Plus précisement, cet ordre divise $u := \operatorname{ppcm}(\varphi(p_1^{k_1}), \ldots, \varphi(p_r^{k_r}))$ si $n = p_1^{k_1} \cdots p_r^{k_r}$ (car $a^u \equiv 1 \pmod n$, d'après l'amélioration du théorème d'Euler (le théorème 4.1.11)). Si $p_1 = 2$ et $k_1 \geq 3$, on peut remplacer $\varphi(p_1^{k_1})$ par $\varphi(p_1^{k_1})/2$.*

4.3.8 Définition. Une classe de congruence inversible $a \pmod n \in (\mathbf{Z}/n\mathbf{Z})^*$ est un **générateur de** $(\mathbf{Z}/n\mathbf{Z})^*$ (ou une **racine primitive modulo** n) si $\{a^m \mid m \in \mathbf{Z}\} = (\mathbf{Z}/n\mathbf{Z})^*$ (autrement dit, si toute classe de congruence inversible $\pmod n$ est une puissance de $a \pmod n$).

4.3.9 Proposition. *Une classe de congruence inversible $a \pmod n$ est un générateur de $(\mathbf{Z}/n\mathbf{Z})^*$ si et seulement si son ordre est égal à $\varphi(n)$.*

Démonstration. Il s'agit d'un cas particulier de la proposition 4.3.6(3) (avec $d = \varphi(n)$). □

4.3.10 Calcul de l'ordre de $a \pmod n$ dans $(\mathbf{Z}/n\mathbf{Z})^*$ Exemple : $2 \pmod{67}$. Ici $n = 67$ est un nombre premier, d'où $\varphi(67) = 66 = 2 \cdot 3 \cdot 11$. On note d l'ordre de $2 \pmod{67}$ dans $(\mathbf{Z}/67\mathbf{Z})^*$. On sait que $d \mid 66$, d'après le corollaire 4.3.7.

On va montrer que $d = 66$. Si $d \neq 66$, alors il existe un nombre premier $p \mid 66$ tel que $d \mid (66/p)$. Selon les trois cas $p = 2, 3, 11$ on aura alors

$$\begin{aligned} d \mid 3 \cdot 11 &\Longrightarrow 2^{33} \equiv 1 \pmod{67}, \text{ ou} \\ d \mid 2 \cdot 11 &\Longrightarrow 2^{22} \equiv 1 \pmod{67}, \text{ ou} \\ d \mid 2 \cdot 3 &\Longrightarrow 2^{6} \equiv 1 \pmod{67}. \end{aligned}$$

Les calculs explicites

$$\begin{gathered} 2^6 \equiv 64 \equiv -3 \not\equiv 1 \pmod{67}, \quad 2^{12} \equiv (-3)^2 \equiv 9 \pmod{67}, \quad 2^{24} \equiv 9^2 \equiv 81 \equiv 14 \pmod{67}, \\ 2^{23} \equiv 2^{-1} \cdot 14 \equiv 7 \pmod{67}, \quad 2^{22} \equiv 2^{-1} \cdot 7 \equiv 2^{-1} \cdot (-60) \equiv -30 \not\equiv 1 \pmod{67}, \\ 2^{35} \equiv 2^{12} \cdot 2^{23} \equiv 9 \cdot 7 \equiv -4 \pmod{67}, \quad 2^{33} \equiv 2^{-2} \cdot (-4) \equiv -1 \not\equiv 1 \pmod{67} \end{gathered}$$

conduisent à une contradiction dans chacun de trois cas, ce qui implique qu'on a bien $d = 66$.

Le même raisonnement démontre l'énoncé général suivant.

4.3.11 Proposition. *Si $m \geq 1$ et $a^m \equiv 1 \pmod n$, alors il est équivalent :*
m est égal à l'ordre de $a \pmod n$ dans $(\mathbf{Z}/n\mathbf{Z})^* \iff a^{m/p} \not\equiv 1 \pmod n$ pour tout nombre premier $p \mid m$.

4.3.12 Exercice. Soit $a \in \mathbf{Z}$.
(1) Si $17 \nmid a$, il est équivalent : $a \pmod{17}$ est un générateur de $(\mathbf{Z}/17\mathbf{Z})^*$ (une racine primitive modulo

17) $\iff a^8 \neq 1 \pmod{17}$.
(2) Trouver un tel générateur.
(3) Si $3 \nmid a$, alors il est équivalent : $a \pmod{27}$ est un générateur de $(\mathbf{Z}/27\mathbf{Z})^*$ (une racine primitive modulo 27) $\iff a^6, a^9 \neq 1 \pmod{27}$.
(4) Trouver un tel générateur.

4.3.13 Proposition (Ordre de $a^k \pmod n$)**.** *Soit d l'ordre de $a \pmod n$ dans $(\mathbf{Z}/n\mathbf{Z})^*$. Si $k \neq 0$ est un entier non nul, alors l'ordre de $a^k \pmod n$ dans $(\mathbf{Z}/n\mathbf{Z})^*$ est égal à $d/\mathrm{pgcd}(d, |k|)$. En particulier, il est égal à d si et seulement si $\mathrm{pgcd}(d, |k|) = 1$.*

Démonstration. Si l'on note $e \geq 1$ l'ordre de $a^k \pmod n$, alors $|k|e \geq 1$ est le plus petit multiple positif de $|k|$ tel que $a^{|k|e} \equiv 1 \pmod n$. Cette congruence équivaut à la divisibilité de $|k|e$ par d, d'après la proposition 4.3.6(1). Autrement dit, $|k|e$ et le plus petit multiple commun à $|k|$ et d, d'où

$$e = \mathrm{ppcm}(d, |k|)/|k| = d/\mathrm{pgcd}(d, |k|).$$

□

4.3.14 Corollaire (Nombre de générateurs)**.** *(1) Si $a \pmod n$ est un générateur de $(\mathbf{Z}/n\mathbf{Z})^*$, alors l'ensemble de générateurs de $(\mathbf{Z}/n\mathbf{Z})^*$ est égal à $\{a^k \pmod n \mid 1 \leq k \leq \varphi(n), \mathrm{pgcd}(\varphi(n), k) = 1\}$.*
(2) Le nombre de générateurs de $(\mathbf{Z}/n\mathbf{Z})^*$ est égal soit à zéro, soit à $\varphi(\varphi(n))$.

Démonstration. (1) Il s'agit d'un cas particulier de la dernière affirmation dans la proposition 4.3.13. Le point (2) est une conséquence immédiate de (1). □

4.3.15 Proposition. *Supposons que $n = n_1 n_2$, où $n_1, n_2 > 2$ et $\mathrm{pgcd}(n_1, n_2) = 1$. Si $\mathrm{pgcd}(a, n) = 1$, alors $a^{\varphi(n)/2} \equiv 1 \pmod n$. En particuler, l'ordre de chaque classe de congruence inversible $a \pmod n$ dans $(\mathbf{Z}/n\mathbf{Z})^*$ divise $\varphi(n)/2$, ce qui implique que $(\mathbf{Z}/n\mathbf{Z})^*$ n'a aucun générateur.*

Démonstration. Les hypothèses impliquent que $2 \mid \varphi(n_i)$ et $\varphi(n) = \varphi(n_1)\varphi(n_2)$, d'où

$$\left.\begin{aligned} a^{\varphi(n)/2} &\equiv (a^{\varphi(n_1)})^{\varphi(n_2)/2} \equiv 1 \pmod{n_1} \\ a^{\varphi(n)/2} &\equiv (a^{\varphi(n_2)})^{\varphi(n_1)/2} \equiv 1 \pmod{n_2} \end{aligned}\right\} \implies a^{\varphi(n)/2} \equiv 1 \pmod n.$$

□

4.3.16 Théorème (Existence d'un générateur de $(\mathbf{Z}/n\mathbf{Z})^*$)**.** *Un générateur existe dans $(\mathbf{Z}/n\mathbf{Z})^* \iff n = 1, 2, 4, p^k, 2p^k$, où $p \neq 2$ est un nombre premier et $k \geq 1$.*

Démonstration. On ne démontrera ici que l'implication facile "$\Longrightarrow$". Quant à l'implication réciproque "$\Longleftarrow$", le point clé est la démonstration du fait que $(\mathbf{Z}/p\mathbf{Z})^*$ possède toujours un générateur si p est un nombre premier. Ce résultat est dû à Gauss (voir les théorèmes 5.5.2 et 5.5.4 ci-dessous).

Supposons que $(\mathbf{Z}/n\mathbf{Z})^*$ contient un générateur. Si l'on écrit $n = p_1^{k_1} \cdots p_r^{p_r}$ avec des nombres premiers $p_1 < \cdots < p_r$, la proposition 4.3.15 implique que n s'écrit sous la forme $n = 2^k, p^k$ ou $2p^k$ (où $k \geq 0$ et $p \neq 2$ est un nombre premier). Si $n = 2^k$ et $k \geq 3$, la proposition 4.1.8 nous dit que l'ordre de chaque élément de $(\mathbf{Z}/2^k\mathbf{Z})^*$ est inférieur ou égal à $\varphi(2^k)/2$, ce qui implique qu'il n'y a aucun générateur dans ce cas. □

4.3.17 Logarithme discret Supposons que $a \pmod n$ est un générateur de $(\mathbf{Z}/n\mathbf{Z})^*$ (ce qui implique que $n = 1, 2, 4, p^k$ ou $2p^k$, d'après le théorème 4.3.16). Pour toute classe de congruence inversible $x \pmod n$ il existe un unique entier $m \in \{0, 1, \ldots, \varphi(n) - 1\}$ tel que $x \equiv a^m \pmod n$. On appelle l'entier m le **logarithme discret** de $x \pmod n$ par rapport à $a \pmod n$.

Si l'on pose $l_a(x \pmod n) := m$, alors on a

$$l_a(xy \pmod n) \equiv l_a(x \pmod n) + l_a(y \pmod n) \pmod{\varphi(n)}. \tag{4.3.17.1}$$

4.3.18 Ecriture décimale de nombres rationnels Une telle écriture deviendra toujours périodique :

$$\frac{2}{3} = 0,666\ldots = 0,\overline{6} \qquad \frac{1}{15} = 0,0666\ldots = 0,0\overline{6} \qquad \frac{3}{7} = 0,428571428571\ldots = 0,\overline{428571}$$
$$\frac{16}{37} = 0,432432\ldots = 0,\overline{432}$$

Que peut-on dire de la longueur de la période ? On a, par exemple,

$$\frac{3}{7} = 0,\overline{428571} \implies 10^6 \cdot \frac{3}{7} = 428571,\overline{428571} \implies (10^6 - 1) \cdot \frac{3}{7} = 428571 \implies$$
$$\implies 7 \mid 3 \cdot (10^6 - 1) \implies 7 \mid (10^6 - 1) \implies 10^6 \equiv 1 \pmod 7.$$

L'ordre de $10 \pmod 7 = 3 \pmod 7$ dans $(\mathbf{Z}/7\mathbf{Z})^*$ est égal à 6, ce qui est aussi la longueur de la période de l'écriture décimale de $\frac{3}{7}$.

En général, soit $d \geq 1$ un entier. Le nombre réel $x := 0,\underbrace{\overline{000\cdots1}}_{d}$ vérifie

$$10^d x = 1,\underbrace{\overline{000\cdots1}}_{d} = 1 + x \implies x = \frac{1}{10^d - 1}.$$

Par exemple,

$$\frac{1}{9} = 0,1111\ldots = 0,\overline{1} \qquad \frac{1}{99} = 0,010101\ldots = 0,\overline{01} \qquad \frac{1}{999} = 0,001001001\ldots = 0,\overline{001}.$$

On en déduit que si l'on choisit des chiffres décimales $a_1, \ldots, a_d \in \{0, 1, \ldots, 9\}$ d'une manière quelconque, on aura

$$0,\overline{a_1 a_2 \cdots a_d} = (a_1 \cdots a_d)_{10} \cdot x = \frac{(a_1 \cdots a_d)_{10}}{10^d - 1}. \tag{4.3.18.1}$$

Par exemple,

$$0,\overline{432} = 432 \cdot 0,\overline{001} = \frac{432}{999} = \frac{27 \cdot 16}{27 \cdot 37} = \frac{16}{37}.$$

La formule (4.3.18.1) équivaut à l'énoncé suivant.

4.3.19 Proposition (Ecriture décimale de fractions)**.** *Supposons que* $0 < \frac{a}{b} < 1$*, où* $a, b \in \mathbf{N}_+$ *et* $\operatorname{pgcd}(b, 10) = 1$*; on note* $d \geq 1$ *l'ordre de* $10 \pmod b$ *dans* $(\mathbf{Z}/b\mathbf{Z})^*$*. On a alors* $10^d - 1 = bq$*, où* $q \in \mathbf{N}_+$ *et*

$$\frac{a}{b} = \frac{aq}{bq} = \frac{aq}{10^d - 1} = 0,\overline{a_1 a_2 \cdots a_d}, \qquad (a_1 \cdots a_d)_{10} = aq, \qquad 0 < aq < bq = 10^d - 1.$$

4.3.20 Exercice. (1) Que se passe-t-il si $\operatorname{pgcd}(b, 10) > 1$?
(2) Ecrire $0,15\overline{27} = 0,15272727\ldots$ sous la forme $\frac{a}{b}$.

4.4 Applications à la cryptographie

4.4.1 Création d'un secret en commun (Diffie–Hellman) Deux personnes (A = Alice et B = Bob) communiquent via un canal non sécurisé. Le but est de créer un secret en commun, en n'échangeant que des messages non sécurisés.

Données publiques : (i) un grand entier $n \geq 1$; (ii) une classe de congruence inversible $g \pmod n$ dont l'ordre dans $(\mathbf{Z}/n\mathbf{Z})^*$ est grand.

En pratique, $n = p$ est un "grand" nombre premier et $g \pmod p$ est un générateur de $(\mathbf{Z}/p\mathbf{Z})^*$.

Etape 1 : A choisit un entier secret $a \in \mathbf{Z}$ et communique à B la classe $g^a \pmod n$. B choisit un entier secret $b \in \mathbf{Z}$ et communique à A la classe $g^b \pmod n$.

Etape 2 : A calcule $(g^b)^a \equiv g^{ab} \pmod n$, et B calcule $(g^a)^b \equiv g^{ab} \pmod n$. La classe de congruence $g^{ab} \pmod n$ est leur secret en commun.

Et si un espion lisait leurs messages ? L'espion ne saurait que les valeurs de $g \pmod n$, $g^a \pmod n$ de $g^b \pmod n$.

En général, il est difficile de calculer la valeur de a (modulo l'ordre de $g \pmod n$) si l'on ne connaît que $g \pmod n$ et $g^a \pmod n$. Cependant, les experts continuent à améliorer les algorithmes dans ce domaine, ce qui signifie qu'on devrait utiliser à l'heure actuelle (octobre 2019) des nombres premiers $n = p > 2^{1000}$ (et tels que $p - 1$ soit divisible par un nombre premier pas trop petit).

4.4.2 Cryptographie à clé publique (Rivest–Shamir–Adleman : RSA) Le principe de la cryptographie à clé publique et le suivant. Le chiffrement se fait par un algorithme publique, le déchiffrement par un algorithme secret.

Plus précisement, on a besoin d'une application bijective $f : X \longrightarrow X$, où X est un grand ensemble fini, qui a la propriété suivante : f est facile à calculer, mais son inverse $g = f^{-1} : X \longrightarrow X$ est difficile à calculer. On utilise f (qu'on rend publique) pour chiffrement et g (qui reste secret) pour déchiffrement.

Le cryptosystème RSA a été découvert en 1973 par C. Cocks, un mathématicien à l'emploi des services de renseignements britanniques. Il a été découvert indépendamment et publié en 1977 par R. Rivest, A. Shamir et L. Adleman. On prend $X = \mathbf{Z}/n\mathbf{Z}$, où $n = pq$ est le produit de deux grands nombres premiers, et les applications

$$f(x) \equiv x^e \pmod n, \qquad g(y) \equiv y^d \pmod n, \tag{4.4.2.1}$$

où $d, e \geq 1$ sont des entiers bien choisis. Les deux applications sont l'inverses l'une à l'autre si et seulement si l'on a

$$\forall a \in \mathbf{Z} \quad a^{de} \equiv a \pmod n. \tag{4.4.2.2}$$

On a étudié des congruences de ce type dans la proposition 4.2.11(2), mais on va répéter le raisonnement ici.

4.4.3 Proposition (Congruences derrière RSA)**.** *Soit $n = pq$, où $p \neq q$ sont des nombres premiers. Si $d, e \geq 1$ sont des entiers tels que $(p-1) \mid (de-1)$ et $(q-1) \mid (de-1)$ (ce qui équivaut à $de \equiv 1 \pmod{\mathrm{ppcm}(p-1, q-1)}$), alors les applications $f, g : \mathbf{Z}/pq\mathbf{Z} \longrightarrow \mathbf{Z}/pq\mathbf{Z}$ suivantes*

$$f(x) \equiv x^e \pmod{pq}, \qquad g(y) \equiv y^d \pmod{pq}$$

sont l'inverses l'une à l'autre :

$$\forall x, y \in \mathbf{Z}/pq\mathbf{Z} \qquad g(f(x)) \equiv (x^e)^d \equiv x^{de} \equiv x \pmod{pq}, \qquad f(g(y)) \equiv (y^d)^e \equiv y^{de} \equiv y \pmod{pq}.$$

Démonstration. Soit $x \in \mathbf{Z}$. Si $p \mid x$, alors $x^{de} \equiv 0 \equiv x \pmod p$. Si $p \nmid x$, alors $x^{p-1} \equiv 1 \pmod p$. On a $de = 1 + (p-1)a$ avec $a \in \mathbf{N}$, d'où $x^{de} \equiv x \cdot (x^{p-1})^a \equiv x \pmod p$. Par conséquent, on a $x^{de} \equiv x \pmod p$

pour tout $x \in \mathbf{Z}$. De même, on a $x^{de} \equiv x \pmod{q}$ pour tout $x \in \mathbf{Z}$. Les deux congruences qu'on vient d'établir impliquent alors que $x^{de} \equiv x \pmod{pq}$, d'après la proposition 3.1.7 et son corollaire 3.1.8. □

4.4.4 RSA communication **Etape 1 :** La personne A choisit deux grands nombres premiers $p \neq q$ (il existe des algorithmes très efficaces qui permettent de décider si un entier est premier ou pas).

Etape 2 : A choisit un entier $e > 1$ (qui sera utilisé pour chiffrement) et puis calcule un entier $d > 1$ (qui sera utilisé pour déchiffrement) tel que

$$de \equiv 1 \pmod{\text{ppcm}(p-1, q-1)}. \tag{4.4.4.1}$$

Etape 3 : A rend publique le couple (pq, e) (la **clé publique**), mais garde secret d (la **clé secrète**).

Etape 4 : on peut envoyer à A un message chiffré de la façon suivante. Un message comportera des morceaux. Chaque morceau sera un élément de $\mathbf{Z}/pq\mathbf{Z}$. Ce morceau sera chiffré par l'application $x \pmod{pq} \mapsto y \equiv x^e \pmod{pq}$ (on remarque que les valeurs de e et pq sont connues !), et le résultat $y \equiv x^e \pmod{pq}$ sera envoyé à A via un canal non sécurisé.

Etape 5 : pour déchiffrer le message reçu, A va calculer $y \pmod{pq} \mapsto y^d \pmod{pq} \equiv x^{de} \equiv x \pmod{pq}$.

4.4.5 Remarques A peut aussi signer (ou authentifier) ses messages en utilisant sa clé secrète d (A envoie à B un couple $(y_1 \pmod{pq}, y_2 \pmod{pq})$, où $y_2 \equiv y_1^d \pmod{pq}$. B calcule $y_2^e \equiv (y_1^d)^e \pmod{pq}$ et vérifie qu'on a bien $y_2^e \equiv y_1 \pmod{pq}$).

En pratique, on n'utilise pas RSA pour chiffrer des messages, mais pour chiffrer des clés d'un cryptosystème plus conventionnel.

Ce qui est important ici est le fait que la connaissance de pq ne permet pas de déterminer facilement p et q, en général (décomposition en facteurs premiers est dificile, si l'on ne possède pas un ordinateur quantique). Si l'on connaissait les valeurs de p, q et e, on pourrait calculer facilement la clé secrète d en utilisant la congruence (4.4.4.1).

Ceci dit, il faut éviter certains mauvais choix de p et q. Par exemple, il faut choisir $p, q > 10^{150}$ d'une manière assez aléatoire, et p ne devrait pas être trop proche de q. De plus, il faut que $p-1$ soit divisible par un nombre premier pas trop petit (idem pour $q-1$).

5 Résultats plus avancés pour enthousiastes

5.1 Congruences $f(x) \equiv 0 \pmod{n}$

5.1.1 Proposition (Congruence $x^2 \equiv 1 \pmod{p^k}$)**.** *Soit p un nombre premier, soit $k \geq 1$. Les solutions de $x^2 \equiv 1 \pmod{p^k}$ sont*

$$\begin{cases} x \equiv \pm 1 \pmod{p^k}, & p \neq 2 \\ x \equiv \pm 1 \pmod{2^{k-1}}, & p = 2,\ k > 1. \end{cases}$$

Démonstration. Voir l'exercice 2.3.11. □

5.1.2 Corollaire. *Si p est un nombre premier et si $p \nmid a$, alors il est équivalent :*

$$a \equiv a^{-1} \pmod{p} \iff a \equiv \pm 1 \pmod{p}.$$

Démonstration. La congruence à gauche équivaut à $a \cdot a \equiv a \cdot a^{-1} \equiv 1 \pmod{p}$. □

5.1.3 Application du théorème chinois (exemple) On va résoudre la congruence

$$x^2 \equiv 1 \pmod{15}, \tag{5.1.3.1}$$

qui équivaut au système

$$\left\{\begin{matrix} x^2 \equiv 1 \pmod{3} \\ x^2 \equiv 1 \pmod{5} \end{matrix}\right\}$$

On peut combiner chacune des deux solutions $x \equiv \pm 1 \pmod{3}$ de la première congruence avec chacune des deux solutions $x \equiv \pm 1 \pmod{5}$ de la deuxième congruence pour obtenir une solution de (5.1.3.1). On obtiendra les $2 \cdot 2 = 4$ solutions suivantes :

$x \pmod{3}$	$x \pmod{5}$	$x \pmod{15}$
1	1	1
-1	-1	-1
1	-1	4
-1	1	-4

En résumé,

$$x^2 \equiv 1 \pmod{15} \iff x \equiv \pm 1, \pm 4 \pmod{15}.$$

5.1.4 Application du théorème chinois (principe général) Soit $f(x) = a_0 + a_1 x + \cdots + a_d x^d$ ($d \geq 0$, $a_i \in \mathbf{Z}$) un polynôme à coefficients dans $\mathbf{Z}$. On note

$$N(f; n) := |\{x \pmod{n} \mid f(x) \equiv 0 \pmod{n}\}|$$

(pour tout entier $n \geq 1$) le nombre de solutions $\pmod{n}$ de la congruence $f(x) \equiv 0 \pmod{n}$.

Si $m, n \geq 1$ et $\operatorname{pgcd}(m, n) = 1$, le théorème chinois implique que l'application bijective canonique

$$\mathbf{Z}/mn\mathbf{Z} \xrightarrow{\sim} \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$$

définit une bijection entre les sous-ensembles

$$\{x \pmod{mn} \mid f(x) \equiv 0 \pmod{mn}\} \subset \mathbf{Z}/mn\mathbf{Z}$$

et

$$\{x \pmod{m} \mid f(x) \equiv 0 \pmod{m}\} \times \{x \pmod{n} \mid f(x) \equiv 0 \pmod{n}\} \subset \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}.$$

En particulier,

$$\text{pgcd}(m,n) = 1 \implies N(f;mn) = N(f;m)N(f;n). \tag{5.1.4.1}$$

On a considéré le cas $m = 3$, $n = 5$ et $f(x) = x^2 - 1$ dans le paragraphe 5.1.3.

5.1.5 Exercice. (1) Si p est un nombre premier et $k \geq 1$, alors les solutions de $x^2 \equiv x \pmod{p^k}$ sont $x \equiv 0, 1 \pmod{p^k}$. [Indication : $x^2 - x = x(x-1)$.]
(2) Les solutions de $x^2 \equiv x \pmod{10^4}$ sont $x \equiv 0,\ 1,\ 625,\ 9376 \pmod{10^4}$.
(3) Pour tout $k \geq 1$, les solutions de $x^2 \equiv x \pmod{10^k}$ sont égales à $x \equiv 0, 1, e_k, 1 - e_k \pmod{10^k}$, où $e_k \equiv \cdots 0625 \pmod{10^k}$ et $1 - e_k \equiv \cdots 9376 \pmod{10^k}$.

5.1.6 Nombres 10-adiques Si l'on prend la limite $k \longrightarrow +\infty$ dans le point (3) de l'exercice 5.1.5, on obtient un nombre $e = \cdots 0625$ dont écriture décimale à une **infinité de chiffres à gauche** et qui vérifie $e^2 = e$ (ce qui implique que $1 - e = \cdots 9376$ vérifie aussi $(1-e)^2 = 1 - e$). Les deux nombres e et $1 - e$ sont des **entiers 10-adiques**. Voici un autre exemple : $a := \cdots 11111$, qui vérifie $9a = \cdots 99999$, d'où $9a + 1 = \cdots 00000 = 0$ et $a = -\frac{1}{9}$.

5.1.7 Congruences $x^2 \equiv a \pmod{n}$ (exemples) Calculons toutes les valeurs possibles des carrés $x^2 \pmod{p}$, où $p \neq 2$ est un nombre premier pas trop grand et $p \nmid x$.

$x \pmod 3$	± 1
$x^2 \pmod 3$	1

$x \pmod 5$	± 1	± 2
$x^2 \pmod 5$	1	$4 \equiv -1$

$x \pmod 7$	± 1	± 2	± 3
$x^2 \pmod 7$	1	$4 \equiv -3$	$9 \equiv 2$

$x \pmod{11}$	± 1	± 2	± 3	± 4	± 5
$x^2 \pmod{11}$	1	4	$9 \equiv -2$	$16 \equiv 5$	$25 \equiv 3$

$x \pmod{13}$	± 1	± 2	± 3	± 4	± 5	± 6
$x^2 \pmod{13}$	1	4	$9 \equiv -4$	$16 \equiv 3$	$25 \equiv -1$	$36 \equiv -3$

$x \pmod{17}$	± 1	± 2	± 3	± 4	± 5	± 6	± 7	± 8
$x^2 \pmod{17}$	1	4	$9 \equiv -8$	$16 \equiv -1$	$25 \equiv 8$	$36 \equiv 2$	$49 \equiv -2$	$64 \equiv -4$

$x \pmod{19}$	± 1	± 2	± 3	± 4	± 5	± 6	± 7	± 8	± 9
$x^2 \pmod{19}$	1	4	9	$16 \equiv -3$	$25 \equiv 6$	$36 \equiv -2$	$49 \equiv -8$	$64 \equiv 7$	$81 \equiv 5$

On peut extraire des tables ci-dessus les critères suivants concernant la résolubilité de la congruence $x^2 \equiv a \pmod{p}$, où l'on fixe $a = -1, \pm 3, 5$ et fait varier $p \nmid a$:

	OUI	NON
$x^2 \equiv -1 \pmod p$	$5, 13, 17$	$3, 7, 11, 19$
$x^2 \equiv -3 \pmod p$	$7, 13, 19$	$5, 11, 17$
$x^2 \equiv 3 \pmod p$	$11, 13$	$5, 7, 17, 19$
$x^2 \equiv 5 \pmod p$	$11, 19$	$3, 7, 13, 17$

La table précédente suggère qu'on a

— $x^2 \equiv -1 \pmod p$ a une solution $\overset{?}{\iff} p \equiv 1 \pmod 4$

— $x^2 \equiv -3 \pmod p$ a une solution $\overset{?}{\iff} p \equiv 1 \pmod 6$

— $x^2 \equiv 3 \pmod p$ a une solution $\overset{?}{\iff} p \equiv \pm 1 \pmod{12}$

— $x^2 \equiv 5 \pmod p$ a une solution $\overset{?}{\iff} p \equiv \pm 1 \pmod 5$

Toutes ces affirmations sont vraies. Il s'agit des cas particuliers de la **loi de réciprocité quadratique** (due à Gauss en général, et à Legendre dans certains cas), selon laquelle on a :

— $x^2 \equiv -1 \pmod p$ a une solution $\iff p \equiv 1 \pmod 4$

— $x^2 \equiv 2 \pmod p$ a une solution $\iff p \equiv \pm 1 \pmod 8$

— $x^2 \equiv (-1)^{(q-1)/2} q \pmod p$ a une solution $\iff x^2 \equiv p \pmod q$ a une solution

(ici, $p, q > 2$ sont des nombres premiers impairs distincts).

5.1.8 Exercice. (1) Trouver toutes les solutions de $x^2 \equiv -1 \pmod{35}$.
(2) Trouver toutes les solutions de $x^2 \equiv -1 \pmod{85}$.

5.1.9 Théorème. *Soit $p \neq 2$ un nombre premier. La congruence $x^2 \equiv -1 \pmod p$ a une solution $\iff$ $p \equiv 1 \pmod 4$.*

Démonstration. On va démontrer d'abord l'implication facile "$\Longrightarrow$" : si $x \in \mathbf{Z}$ vérifie $x^2 \equiv -1 \pmod p$, alors

$$\underbrace{(-1)^{\frac{p-1}{2}}}_{=\pm 1} \equiv (x^2)^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \pmod p.$$

Cette congruence implique l'égalité $(-1)^{\frac{p-1}{2}} = 1$ (car $-1 \not\equiv 1 \pmod p$), d'où $\frac{p-1}{2} = 2k$ et $p = 4k+1$ (avec $k \in \mathbf{Z}$).
Pour démontrer l'implication plus difficile "$\Longleftarrow$" on va utiliser le théorème de Wilson 5.1.10 ci-dessous. Si $p = 4k+1$, alors

$$-1 \equiv (p-1)! \equiv (4k)! \equiv 1 \cdot 2 \cdots (2k) \cdot \underbrace{(2k+1)}_{\equiv -2k} \cdots \underbrace{(4k)}_{\equiv -1} \equiv (2k)!\,(-1)^{2k} \cdot (2k)! = ((2k)!)^2 \pmod p.$$

□

5.1.10 Théorème (Théorème de Wilson)**.** *Si p est un nombre premier, alors on a $(p-1)! \equiv -1 \pmod p$.*

Démonstration. On peut supposer que $p \neq 2$. Par définition, $(p-1)! \equiv 1 \cdot 2 \cdots (p-1) \pmod p$ est congru au produit de toutes les classes inversibles $\pmod p$. On va mettre ensemble chaque classe et son inverse, si les deux classes sont distinctes. Par exemple, si $p = 7$, on peut récrire le produit $6! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6$ de la façon suivante :

$$6! = \underbrace{(2 \cdot 4)}_{\equiv 1} \cdot \underbrace{(3 \cdot 5)}_{\equiv 1} \cdot \underbrace{(1 \cdot 6)}_{\equiv -1} \equiv -1 \pmod 7.$$

En général, corollaire 5.1.2 nous dit qu'une classe de congruence inversible $a \not\equiv \pm 1 \pmod p$ fait partie d'un couple $a \pmod p$, $a^{-1} \pmod p$, où $a \not\equiv a^{-1} \pmod p$. Par conséquent,

$$(p-1)! \equiv (a \cdot a^{-1}) \cdot (b \cdot b^{-1}) \cdots (t \cdot t^{-1}) \cdot (1 \cdot (-1)) \equiv 1 \cdot (-1) \equiv -1 \pmod{p}.$$

□

5.1.11 Exercice. Soit $p \neq 2, 3$ un nombre premier. Si $x \in \mathbf{Z}$ vérifie $x^2 \equiv -3 \pmod{p}$, montrer :
(1) La classe de congruence $y := 2^{-1} \cdot (-1+x) \pmod{p}$ se comporte de la même manière que $\frac{1}{2}(-1+i\sqrt{3}) = e^{2\pi i/3} \in \mathbf{C}$: on a $y^2 + y + 1 \equiv 0 \pmod{p}$ et $y^3 \equiv 1 \not\equiv y \pmod{p}$.
(2) On écrit $p = 3k + a$, où $k \in \mathbf{Z}$ et $a \in \{1, 2\}$. Déduire de $y^{p-1} \equiv 1 \pmod{p}$ que $a = 1$ (autrement dit, que $p \equiv 1 \pmod{3}$).

5.1.12 Exercice. Si $x, y \in \mathbf{Z}$ et si $p \equiv 3 \pmod{4}$ est un nombre premier tel que $p \mid (x^2 + y^2)$, alors $p \mid x$ et $p \mid y$.

5.1.13 Congruences polynomiales qui ont beaucoup de solutions Un polynôme de degré $d \geq 1$ à coefficients complexes a au plus d racines complexes. Que se passe-t-il pour des congruences polynomiales ? On sait que la congruence quadratique

$$x^2 - 1 \equiv 0 \pmod{8}$$

a 4 solutions $x \equiv \pm 1, \pm 5$. De même, si $p_1, \ldots, p_r \neq 2$ sont des nombres premiers impairs distincts, alors la congruence quadratique

$$x^2 - 1 \equiv 0 \pmod{p_1 \cdots p_r}$$

a $2^r > 2$ solutions, d'après (5.1.4.1).

Le résultat suivant, qui est un cas particulier d'un résultat abstrait général qu'on va démontrer dans le théorème 9.2.7, montre que les congruences modulo des nombres premiers se comportent d'une façon plus raisonnable.

5.1.14 Théorème. *Soit p un nombre premier, soient $a_0, \ldots, a_d \in \mathbf{Z}$ et $p \nmid a_d$ $(d \geq 0)$. La congruence*

$$f(x) = a_0 + a_1 x + \cdots + a_d x^d \equiv 0 \pmod{p}$$

a au plus d solutions $\pmod{p}$.

Démonstration. Récurrence sur d. Le cas $d = 0$ est immédiat. On suppose que $d > 0$ et que le résultat est vrai pour les polynômes de degré $\deg < d$. Si $a \in \mathbf{Z}$ vérifie $f(a) \equiv 0 \pmod{p}$, alors les formules $x^k - a^k = (x-a)(x^{k-1} + ax^{k-2} + \cdots + a^{k-1})$ impliquent qu'on a une identité polynomiale

$$f(x) - f(a) = (x-a)g(x), \qquad g(x) = b_0 + b_1 x + \cdots + b_{d-1} x^{d-1}, \qquad b_i \in \mathbf{Z}, \qquad p \nmid b_{d-1} = a_d.$$

Si $b \not\equiv a \pmod{p}$ est une solution de $f(b) \equiv 0 \pmod{p}$, alors

$$(b-a)g(b) \equiv f(b) - f(a) \equiv 0 \pmod{p}.$$

La classe $b - a \not\equiv 0 \pmod{p}$ étant inversible $\pmod{p}$, on a $g(b) \equiv 0 \pmod{p}$. Par l'hypothèse de récurrence, cette congruence a au plus $d-1$ solutions $b \pmod{p}$. En ajoutant $a \pmod{p}$, on en déduit qu'il y a au plus d solutions de $f(x) \equiv 0 \pmod{p}$. □

5.1.15 Corollaire. *Soit p un nombre premier. Si $a_0, \ldots, a_d \in \mathbf{Z}$ $(d \geq 0)$ et si la congruence $f(x) = a_0 + a_1 x + \cdots + a_d x^d \equiv 0 \pmod{p}$ a au moins $d+1$ solutions $\pmod{p}$, alors $p \mid a_i$ pour chaque i, ce qui implique que l'on a $f(a) \equiv 0 \pmod{p}$ pour tout $a \in \mathbf{Z}$.*

5.1.16 Proposition (Une autre preuve du théorème de Wilson)**.** *Si p est un nombre premier, alors $(p-1)! \equiv -1 \pmod{p}$.*

Démonstration. Le polynôme

$$f(x) := (x^{p-1} - 1) - \prod_{j=1}^{p-1} (x - j)$$

a coefficients dans $\mathbf{Z}$, son degré est égal à $\deg(f) < p-1$, et on a $f(x) \equiv 0 \pmod{p}$ pour $p-1$ classes distinctes $x \equiv 1, \ldots, p-1 \pmod{p}$. Le corollaire 5.1.15 implique alors que tous les coefficients de $f(x)$ sont divisible par p, d'où

$$f(0) \equiv 0 \pmod{p}, \qquad f(0) = -1 + (-1)^p (p-1)!$$

□

5.2 Nombres premiers dans une progression arithmétique

5.2.1 Nombres premiers modulo 4 et 6 Rappelons (voir l'exercice 1.1.8) qu'un nombre premier $p \neq 2$ (resp. $p \neq 2, 3$) satisfait à $p \equiv \pm 1 \pmod{4}$ (resp. $p \equiv \pm 1 \pmod{6}$)

5.2.2 Proposition. *Il y a une infinité de nombres premiers $p \equiv -1 \pmod{4}$.*

Démonstration. Il faut démontrer l'énoncé suivant : si $p_1, \ldots, p_r \equiv -1 \pmod{4}$ sont des nombres premiers $(r \geq 0)$, alors il existe un nombre premier $p \equiv -1 \pmod{4}$ tel que $p \neq p_1, \ldots, p_r$. Soit $N := 4p_1 \cdots p_r - 1 \geq 4 \cdot 1 - 1 = 3$. On a $N \equiv -1 \pmod{4}$. On écrit $N = q_1 \cdots q_s$, où q_j sont des nombres premiers (pas forcément distincts). On a $q_j \neq 2$ (car $2 \nmid N$), d'où $q_j \equiv \pm 1 \pmod{4}$. Si $q_j \equiv 1 \pmod{4}$ pour tout $j = 1, \ldots, r$, alors $N \equiv 1 \pmod{4}$, ce qui n'est pas vrai. Il en résulte qu'il existe $p = q_j$ tel que $p \not\equiv 1 \pmod{4}$, ce qui implique que $p \equiv -1 \pmod{4}$. On remarque que $p \mid N$. S'il existe i tel que $p = p_i$, alors $p \mid 4p_1 \cdots p_r = N + 1$, d'où $p \mid (N+1) - N$, ce qui est impossible. Cette contradiction montre que $p \neq p_1, \ldots, p_r$. □

5.2.3 Exercice. Il y a une infinité de nombres premiers $p \equiv -1 \pmod{6}$.

5.2.4 Proposition. *Il y a une infinité de nombres premiers $p \equiv 1 \pmod{4}$.*

Démonstration. Il faut démontrer l'énoncé suivant : si $p_1, \ldots, p_r \equiv 1 \pmod{4}$ sont des nombres premiers $(r \geq 0)$, alors il existe un nombre premier $p \equiv 1 \pmod{4}$ tel que $p \neq p_1, \ldots, p_r$. Soit $N := (2p_1 \cdots p_r)^2 + 1 \geq 2^2 + 1 = 5$, soit $p \mid N$ un nombre premier qui divise N. On a $p \neq 2$, car $2 \nmid N$. L'entier $x := 2p_1 \cdots p_r \in \mathbf{Z}$ vérifie $x^2 \equiv -1 \pmod{p}$. La partie "facile" du théorème 5.1.9 implique que $p \equiv 1 \pmod{4}$. S'il existe i tel que $p = p_i$, alors $p \mid (2p_1 \cdots p_r)^2 = N - 1$, d'où $p \mid N - (N-1)$, ce qui est impossible. Cette contradiction montre que $p \neq p_1, \ldots, p_r$. □

5.2.5 Exercice. Il y a une infinité de nombres premiers $p \equiv 1 \pmod{6}$.
[Indication : modifier la démonstration de la proposition 5.2.4 en utilisant l'exercise 5.1.11 à la place du théorème 5.1.9.

5.2.6 Exercice. Il y a une infinité de nombres premiers $p \equiv 5 \pmod{12}$.
[Indication : combiner la méthode de la proposition 5.2.4 et celle de l'exercice 5.2.3.]

5.2.7 Exercice. Il y a une infinité de nombres premiers $p \equiv 7 \pmod{12}$.
[Indication : combiner la méthode de la proposition 5.2.2 et celle de l'exercice 5.2.5.]

5.2.8 Exercice. Que faut-il savoir pour qu'on puisse démontrer qu'il y a une infinité de nombres premiers $p \equiv 11 \pmod{12}$ (en utilisant la même méthode) ?

5.2.9 Exercice. (1) $(x^{12}-1)/((x^6-1)(x^2+1)) = x^4 - x^2 + 1 = (x^2-1)^2 + x^2 = (x^2 - \frac{1}{2})^2 + \frac{3}{4}$.
(2) Si p est un nombre premier et si la congruence $x^4 - x^2 + 1 \equiv 0 \pmod{p}$ a une solution, alors $p \equiv 1 \pmod{12}$.
(3) Il y a une infinité de nombres premiers $p \equiv 1 \pmod{12}$.

5.2.10 Exercice. (1) Si $p \neq 2$ est un nombre premier et si la congruence $x^4 \equiv -1 \pmod{p}$ a une solution, alors $p \equiv 1 \pmod{8}$.
(2) Il y a une infinité de nombres premiers $p \equiv 1 \pmod{8}$.
(3) Si $p \neq 2$ est un nombre premier et si la congruence $x^{2^k} \equiv -1 \pmod{p}$ a une solution, alors $p \equiv 1 \pmod{2^{k+1}}$.
(4) Pour tout $n \geq 2$ il y a une infinité de nombres premiers $p \equiv 1 \pmod{2^n}$.

5.2.11 Résultats plus généraux Des méthodes élémentaires analogues permettent de démontrer qu'il y a une infinité de nombres premiers $p \equiv a \pmod{n}$ lorsque $a^2 \equiv 1 \pmod{n}$. Le résultat général suivant est dû à Dirichlet.

5.2.12 Théorème (Théorème de Dirichlet sur les nombres premiers dans une progression arithmétique)**.** *Si* $\operatorname{pgcd}(a, n) = 1$*, alors il y a une infinité de nombres premiers* $p \equiv a \pmod{n}$*. Plus précisement, on a*

$$\sum_{\substack{p \in \mathcal{P} \\ p \equiv a \pmod{n}}} \frac{1}{p} = +\infty. \tag{5.2.12.1}$$

5.2.13 Méthode de Dirichlet Avant Dirichlet, Euler a montré que l'on a

$$\sum_{p \in \mathcal{P}} \frac{1}{p} = +\infty.$$

On peut reformuler la méthode d'Euler de la façon suivante : le point de départ est l'identité

$$\prod_{p \in \mathcal{P}} \frac{1}{1 - p^{-s}} = \sum_{n=1}^{\infty} n^{-s} \qquad (s > 1)$$

(qui exprime l'unicité de factorisation dans $\mathbf{Z}$ d'une manière analytique), puis on développe chaque terme du produit en utilisant la formule

$$-\log(1 - T) = \sum_{k=1}^{\infty} \frac{T^k}{k}.$$

Le passage à la limite $s \longrightarrow 1+$ permet de conclure.

On peut démontrer le cas le plus simple $n = 4$, $a = \pm 1$ du théorème de Dirichlet 5.2.12 de la même façon si l'on considère aussi le produit

$$\prod_{\substack{p\in\mathcal{P}\\ p\equiv 1 \pmod 4}} \frac{1}{1-p^{-s}} \prod_{\substack{p\in\mathcal{P}\\ p\equiv -1 \pmod 4}} \frac{1}{1+p^{-s}} = 1 - 3^{-s} + 5^{-s} - 7^{-s} + 9^{-s} \cdots \qquad (s>1).$$

5.3 Nombres pseudopremiers, nombres de Carmichael

5.3.1 Question Selon le petit théorème de Fermat, on a $a^p \equiv a \pmod p$ pour tout $a \in \mathbf{Z}$ si p est un nombre premier. Est-ce que cette propriété caractérise les nombres premiers ?

5.3.2 Définition. Un entier $n > 1$ est un **nombre pseudopremier en base** $a \in \mathbf{Z}$ si n n'est pas un nombre premier et si l'on a $a^n \equiv a \pmod n$.

5.3.3 Exemple : $2^{341} \equiv 2 \pmod{341}$ Si $a = 2$ et $n = 341 = 11 \cdot 31$, alors on a $2^5 = 32$ et

$$\left.\begin{aligned} 2^5 \equiv 1 \pmod{31} &\Longrightarrow 2^{10} \equiv 1 \pmod{31}\\ 2^5 \equiv -1 \pmod{11} &\Longrightarrow 2^{10} \equiv 1 \pmod{11}\end{aligned}\right\} \Longrightarrow 2^{10} \equiv 1 \pmod{11\cdot 31} \Longrightarrow$$
$$\Longrightarrow 2^{341-1} \equiv (2^{10})^{34} \equiv 1 \pmod{11\cdot 31} \Longrightarrow 2^{341} \equiv 2 \pmod{11\cdot 31}.$$

5.3.4 Définition. Un entier $n > 1$ est un **nombre de Carmichael** si c'est un nombre pseudopremier en base quelconque (autrement dit, si n n'est pas un nombre premier et si l'on a $a^n \equiv a \pmod n$ pour tout $a \in \mathbf{Z}$).

5.3.5 Proposition. *Un entier $n > 1$ est un nombre de Carmichael $\iff$ $n = p_1 \cdots p_r$ est un produit de $r \geq 2$ nombres premiers distincts tels que $\forall i = 1, \ldots, r \quad (p_i - 1) \mid (n-1)$.*

Démonstration. L'implication '$\Longleftarrow$' est un cas particulier de la proposition 4.2.11(2). L'implication '$\Longrightarrow$' : la proposition 4.2.11(1) implique qu'un nombre de Carmichael n est sans facteur carré, d'où $n = p_1 \cdots p_r$ ($r \geq 2$, car $n > 1$ n'est pas un nombre premier). Pour démontrer que $p_i - 1$ divise $n - 1$ on va utiliser le fait qu'il existe un générateur $a_i \pmod{p_i}$ de $(\mathbf{Z}/p_i\mathbf{Z})^*$ (voir le théorème 5.5.2). On a $p_i \nmid a_i$ et $a_i^n \equiv a_i \pmod{p_i}$, ce qui implique que $a_i^{n-1} \equiv 1 \pmod{p_i}$. On en déduit que $n-1$ est divisible par l'ordre de $a_i \pmod{p_i} \in (\mathbf{Z}/p_i\mathbf{Z})^*$, mais cet ordre est égal à $p_i - 1$. □

5.3.6 Exemple : $n = 561$ Le nombre de Carmichael le plus petit est $n = 561 = 3\cdot 11\cdot 17$, car $3-1 = 2$, $11 - 1 = 2 \cdot 5$, $17 - 1 = 2^4$ et $561 - 1 = 2^4 \cdot 5 \cdot 7$.

5.3.7 Remarque On sait qu'il y a une infinité de nombres de Carmichael.

5.3.8 Exercice. Montrer : si $n = p_1 \cdots p_r$ est un nombre de Carmichael, alors $r \geq 3$.

5.4 Formule de Möbius

5.4.1 Fractions $\frac{1}{n}, \frac{2}{n}, \ldots, \frac{n}{n}$ On sait que chaque nombre rationnel $\frac{a}{n}$ ($a, n \in \mathbf{Z}$, $n \geq 1$) s'écrit sous la forme réduite si l'on divise le numérateur et le dénominateur par leur plus grand commun diviseur $m = \operatorname{pgcd}(a, n)$:

$$a = ma', \qquad n = mn', \qquad \frac{a}{n} = \frac{a'}{n'}, \qquad \operatorname{pgcd}(a', n') = 1. \tag{5.4.1.1}$$

Que se passe-t-il si l'on applique cette procédure à tous les nombres rationnels $\frac{a}{n}$ ($a \in \mathbf{Z}$) à dénominateur $n \geq 1$? Il suffit de se borner aux numérateurs dans l'intervalle $1 \leq a \leq n$, car $\frac{a+n}{n} = \frac{a}{n} + 1$ et $\operatorname{pgcd}(a + n, n) = \operatorname{pgcd}(a, n)$.

Exemple : Si $n = 6$, alors

$$\frac{1}{6} = \frac{1}{6}, \qquad \frac{2}{6} = \frac{1}{3}, \qquad \frac{3}{6} = \frac{1}{2}, \qquad \frac{4}{6} = \frac{2}{3}, \qquad \frac{5}{6} = \frac{5}{6}, \qquad \frac{6}{6} = \frac{1}{1},$$
$$\left\{\frac{1}{6}, \frac{2}{6}, \frac{3}{6}, \frac{4}{6}, \frac{5}{6}, \frac{6}{6}\right\} = \left\{\frac{1}{1}\right\} \cup \left\{\frac{1}{2}\right\} \cup \left\{\frac{1}{3}, \frac{2}{3}\right\} \cup \left\{\frac{1}{6}, \frac{5}{6}\right\}.$$

En général : Si $n \geq 1$ est quelconque, on obtient à partir des fractions $\frac{a}{n}$ $(1 \leq a \leq n)$ les fractions qui s'écrivent $\frac{b}{d}$, où $d \mid n$, $1 \leq b \leq d$ et $\mathrm{pgcd}(b, d) = 1$, d'où

$$\left\{\frac{a}{n} \,\middle|\, 1 \leq a \leq n\right\} = \bigcup_{d|n} \left\{\frac{b}{d} \,\middle|\, 1 \leq b \leq d,\ \mathrm{pgcd}(b, d) = 1\right\} \tag{5.4.1.2}$$

(une réunion disjointe). Le comptage du nombre d'éléments de chaque côté implique que l'on a

$$\forall n \geq 1 \qquad n = \sum_{d|n} \varphi(d). \tag{5.4.1.3}$$

5.4.2 Formule de Möbius Les égalités (5.4.1.3) $(n \geq 1)$ forment un système d'équations linéaires pour les valeurs de $\varphi(d)$ $(d \geq 1)$.

Plus généralement, étant donnée une function $f : \mathbf{N}_+ \longrightarrow \mathbf{C}$ on peut considérer la fonction $g : \mathbf{N}_+ \longrightarrow \mathbf{C}$ suivante

$$g(n) = \sum_{d|n} f(d). \tag{5.4.2.1}$$

Explicitement,

$$g(1) = f(1), \quad g(2) = f(2) + f(1), \quad g(3) = f(3) + f(1), \quad g(4) = f(4) + f(2) + f(1), \quad \cdots$$

Ces relations permettent d'exprimer les valeurs de f en termes des valeurs de g :

$$f(1) = g(1), \quad f(2) = g(2) - g(1), \quad f(3) = g(3) - g(1), \quad f(4) = g(4) - g(2), \quad \cdots$$

En général, $f(n)$ est donnée par la **formule de Möbius**

$$f(n) = \sum_{n=dm} \mu(d)\, g(m) = \sum_{d|n} \mu(d)\, g\big(\frac{n}{d}\big) = \sum_{d|n} \mu\big(\frac{n}{d}\big)\, g(d), \tag{5.4.2.2}$$

où $\mu : \mathbf{N}_+ \longrightarrow \{0, \pm 1\}$ est la **fonction de Möbius** :

$$\mu(n) := \begin{cases} 1, & n = 1 \\ (-1)^r, & n = p_1 \cdots p_r,\ p_i \text{ nombres premiers distincts} \\ 0, & \exists p \in \mathcal{P} \quad p^2 \mid n. \end{cases} \tag{5.4.2.3}$$

En effect, la fonction μ vérifie

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & n = 1 \\ 0, & n > 1, \end{cases} \tag{5.4.2.4}$$

ce qui implique que si l'on commence par une function $g : \mathbf{N}_+ \longrightarrow \mathbf{C}$ et si l'on définit $f : \mathbf{N}_+ \longrightarrow \mathbf{C}$ par la formule (5.4.2.2), alors on a bien

$$\sum_{d|n} f(d) = \sum_{d|n} \sum_{d=em} \mu(e)\, g(m) = \sum_{m|n} g(m) \sum_{e|\frac{n}{m}} \mu(e) = \sum_{m|n} g(m) \left\{ \begin{matrix} 1, & \frac{n}{m} = 1 \\ 0, & \frac{n}{m} > 1 \end{matrix} \right\} = g(n).$$

5.4.3 Exercice. Démontrer la formule (5.4.2.4). [Indication : écrire $n = p_1^{k_1} \cdots p_r^{k_r}$.]

5.4.4 Fonction $\varphi(n)$ La formule de Möbius s'applique à (5.4.1.3) ; on obtient

$$\varphi(n) = \sum_{d|n} \mu(d)\, \frac{n}{d}\,.$$

On écrit $n = p_1^{k_1} \cdots p_r^{k_r}$. Les seuls diviseurs $d \mid n$ avec $\mu(d) \neq 0$ sont $d = p_{i_1} \cdots p_{i_s}$, où $1 \leq i_1 < \cdots < i_s \leq r$. On en déduit que

$$\frac{\varphi(n)}{n} = \sum_{d|n} \frac{\mu(d)}{d} = \sum_{s=0}^{r} (-1)^s \sum_{1 \leq i_1 < \cdots < i_s \leq r} \frac{1}{p_{i_1} \cdots p_{i_s}} = \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right) = \prod_{p|n} \left(1 - \frac{1}{p}\right). \quad (5.4.4.1)$$

5.4.5 Exercice. On définit une généralisation de la fonction d'Euler $\varphi_M : \mathbf{N}_+ \longrightarrow \mathbf{C}$ (qui dépend d'un entier $M \geq 1$) de la façon suivante :

$$\varphi_M(n) := |\{(a_1, \ldots, a_M) \mid 1 \leq a_i \leq n,\ \mathrm{pgcd}(a_1, \ldots, a_M, n) = 1\}|.$$

Montrer :

$$\sum_{d|n} \varphi_M(n) = n^M.$$

Démontrer une formule pour $\varphi_M(n)$ qui généralise (5.4.4.1).

5.5 Structure de $(\mathbf{Z}/p^k\mathbf{Z})^*$

5.5.1 $p \neq 2$ On va montrer que dans ce cas il existe toujours un générateur de $(\mathbf{Z}/p^k\mathbf{Z})^*$. Le point principal est une démonstration de ce résultat pour $k = 1$.

5.5.2 Théorème (Gauss)**.** *Pour tout nombre premier p il existe un générateur de $(\mathbf{Z}/p\mathbf{Z})^*$ (une classe de congruence inversible $a \pmod p$ telle que $(\mathbf{Z}/p\mathbf{Z})^* = \{a, a^2, \ldots, a^{p-1} \pmod p\}$).*

Démonstration. On sait que $a \pmod p \in (\mathbf{Z}/p\mathbf{Z})^*$ est un générateur de $(\mathbf{Z}/p\mathbf{Z})^*$ si et seulement si son ordre est égal à $p - 1$. On note $\psi(d)$ (pour chaque $d \geq 1$) le nombre d'éléments de $(\mathbf{Z}/p\mathbf{Z})^*$ dont l'ordre est égal à d. On sait que $\psi(d) = 0$ si $d \nmid (p-1)$, ce qui implique que

$$\sum_{d|(p-1)} \psi(d) = |(\mathbf{Z}/p\mathbf{Z})^*| = p - 1 = \sum_{d|(p-1)} \varphi(d). \quad (5.5.2.1)$$

Le point clé est une preuve de l'implication suivante :

$$\psi(d) \neq 0 \implies \psi(d) = \varphi(d). \quad (5.5.2.2)$$

En effet, compte tenu de (5.5.2.1), on en déduit que

$$\forall d \mid (p-1) \quad \psi(d) = \varphi(d).$$

En particulier, le nombre de générateurs de $(\mathbf{Z}/p\mathbf{Z})^*$ est égal à $\psi(p-1) = \varphi(p-1) > 0$.

On va maintenant démontrer (5.5.2.2). Supposons que $d \mid (p-1)$ et qu'il existe une classe inversible $a \pmod p$ d'ordre d. On a une inclusion

$$\{a, a^2, \dots, a^d \pmod p\} \subseteq \{x \pmod p \mid x^d - 1 \equiv 0 \pmod p\}.$$

L'ensemble à gauche à d éléments, tandis que celui à droite a au plus $\deg(x^d-1) = d$ éléments, grâce au théorème 5.1.14 (c'est ici qu'on utilise le fait que p est un nombre premier). On en déduit que les deux ensembles sont égaux :

$$\{a, a^2, \dots, a^d \pmod p\} = \{x \pmod p \mid x^d - 1 \equiv 0 \pmod p\}.$$

Le reste est facile : un élément $x \pmod p$ d'ordre d vérifie $x^d - 1 \equiv 0 \pmod p$, ce qui implique qu'il existe $k = 1, \dots, d$ tel que $x \equiv a^k \pmod p$. D'après la proposition 4.3.13, l'ordre de $a^k \pmod p$ est égal à d si et seulement si $\operatorname{pgcd}(k, p) = 1$, ce qui est vrai pour $\varphi(d)$ valeurs de k. L'implication (5.5.2.2) est démontrée. □

5.5.3 Proposition (Amélioration de congruences par $x \mapsto x^p$ est uniforme)**.** *Supposons que p est un nombre premier, $k \geq 1$, $p^k > 2$ et que $a, b \in \mathbf{Z}$ vérifient $p \nmid a$, $a \equiv b \pmod{p^k}$ et $a \not\equiv b \pmod{p^{k+1}}$. Alors on a $a^p \equiv b^p \pmod{p^{k+1}}$ et $a^p \not\equiv b^p \pmod{p^{k+2}}$.*
[L'hypothèse $p^k > 2$ est nécessaire : on a $1 \equiv 3 \pmod 2$ et $1 \not\equiv 3 \pmod{2^2}$, mais $1^2 \equiv 3^2 \pmod{2^3}$.]

Démonstration. Il existe $c \in \mathbf{Z}$ tel que $a = b + p^k c$ et $p \nmid c$, d'où

$$a^p - b^p = (b + p^k c)^p - b^p = \binom{p}{1} b^{p-1}(p^k c) + \binom{p}{2} b^{p-2}(p^k c)^2 + \cdots + \binom{p}{p-1} b (p^k c)^{p-1} + p^{pk} c^p.$$

On a vu dans la preuve de la proposition 4.1.5 que chaque terme à droite est divisible par p^{k+1}. Le premier terme $\binom{p}{1} b^{p-1}(p^k c) = p^{k+1} b^{p-1} c$ n'est pas divisible par p^{k+2}, car $p \nmid b$ et $p \nmid c$. Les termes $\binom{p}{j} b^{p-j}(p^k c)^j$ avec $1 < j < p$ sont tous divisibles par $p \cdot (p^k)^2 = p^{2k+1}$; en particulier, ils sont divisibles par p^{k+2}. Le dernier terme $p^{pk} c^p$ est divisible aussi par p^{k+2}, car l'hypothèse $p^k > 2$ implique que $pk - (k+2) = (p-1)k - 2 \geq 0$. Par conséquent, on a $a^p - b^p \equiv p^{k+1} b^{p-1} c \not\equiv 0 \pmod{p^{k+2}}$. □

5.5.4 Théorème. *Soit $p \neq 2$ un nombre premier, soit $k > 1$.*
(1) Si $a \in \mathbf{Z}$, $p \nmid a$, $a^{p-1} \not\equiv 1 \pmod{p^2}$ et si $a \pmod p$ est un générateur de $(\mathbf{Z}/p\mathbf{Z})^*$, alors $a \pmod{p^k}$ est un générateur de $(\mathbf{Z}/p^k\mathbf{Z})^*$ (autrement dit, on a $(\mathbf{Z}/p^k\mathbf{Z})^* = \{a, a^2, \dots, a^{(p-1)p^{k-1}} \pmod{p^k}\}$).
(2) Un générateur de $(\mathbf{Z}/p^k\mathbf{Z})^*$ existe toujours.
(3) Un générateur de $(\mathbf{Z}/2p^k\mathbf{Z})^*$ existe toujours.

Démonstration. (1) On note d l'ordre de $a \pmod{p^k}$. On sait, d'une part, que $d \mid (p-1)p^{k-1}$. D'autre part, la congruence $a^d \equiv 1 \pmod{p^k}$ implique que $a^d \equiv 1 \pmod p$, d'où $(p-1) \mid d$, car $a \pmod p$ est un générateur de $(\mathbf{Z}/p\mathbf{Z})^*$. On en déduit que $d = (p-1)p^l$ avec $0 \leq l \leq k-1$. Il faut montrer que $l = k-1$, mais cet égalité est une conséquence des propriétés suivantes : $p > 2$, $a^{p-1} \not\equiv 1 \pmod{p^2}$ et $a^{p-1} \equiv 1 \pmod p$, grâce à la proposition 5.5.3 : on obtient successivement $a^{(p-1)p} \not\equiv 1 \pmod{p^3}$, …, $a^{(p-1)p^{k-2}} \not\equiv 1 \pmod{p^k}$.
(2) D'après le théorème 5.5.2, il existe $a \in \mathbf{Z}$ tel que $a \pmod p$ est un générateur of $(\mathbf{Z}/p\mathbf{Z})^*$. Si $a^{p-1} \not\equiv 1 \pmod{p^2}$, alors $a \pmod{p^k}$ est un générateur de $(\mathbf{Z}/p^k\mathbf{Z})^*$, d'après (1). Si $a^{p-1} \equiv 1 \pmod{p^2}$, alors

$b := a(1+p) \equiv a \pmod{p}$ et $b^{p-1} \equiv a^{p-1}(1+\binom{p-1}{1}p) \equiv 1-p \not\equiv 1 \pmod{p^2}$, ce qui implique que $b \pmod{p^k}$ est un générateur de $(\mathbf{Z}/p^k\mathbf{Z})^*$.

(3) Soit $a \pmod{p^k}$ un générateur de $(\mathbf{Z}/p^k\mathbf{Z})^*$. Quitte à remplacer a par $a+p^k$ on peut supposer que $2 \nmid a$; dans ce cas $a \pmod{2p^k}$ sera un générateur de $(\mathbf{Z}/2p^k\mathbf{Z})^* = (\mathbf{Z}/2\mathbf{Z})^* \times (\mathbf{Z}/p^k\mathbf{Z})^* = \{1\} \times (\mathbf{Z}/p^k\mathbf{Z})^*$. □

5.5.5 $p = 2$ Il s'avère que dans ce cas $(\mathbf{Z}/2^k\mathbf{Z})^*$ $(k \geq 3)$ n'a pas de générateurs, mais il existe un "générateur au signe près".

5.5.6 Théorème. *Soit $k > 1$. Si $a \in \mathbf{Z}$ vérifie $a \equiv 1 \pmod{2^2}$ et $a \not\equiv 1 \pmod{2^3}$ (par exemple, si $a = 5$), alors on a $(\mathbf{Z}/2^k\mathbf{Z})^* = \{\pm a, \pm a^2, \ldots, \pm a^{2^{k-2}} \pmod{2^k}\}$.*

Démonstration. On a une décomposition

$$(\mathbf{Z}/2^k\mathbf{Z})^* = X_+ \cup X_-, \qquad X_\pm = \{x \pmod{2^k} \mid x \equiv \pm 1 \pmod{2^2}\}, \qquad |X_\pm| = \tfrac{1}{2}\varphi(2^k) = 2^{k-2}.$$

L'hypothèse $a \in X_+$ implique que $a^k \in X_+$, pour tout $k \in \mathbf{Z}$. On va suivre la même démarche que celle dans la preuve du théorème 5.5.4(2). Les hypothèses $a \equiv 1 \pmod{2^2}$ et $a \not\equiv 1 \pmod{2^3}$ impliquent successivement, grâce à la proposition 5.5.3, que l'on a $a^2 \equiv 1 \pmod{2^3}$ et $a^2 \not\equiv 1 \pmod{2^4}$, …, $a^{2^{k-3}} \equiv 1 \pmod{2^{k-1}}$ et $a^{2^{k-3}} \not\equiv 1 \pmod{2^k}$, et $a^{2^{k-2}} \equiv 1 \pmod{2^k}$. En particulier, l'ordre de $a \pmod{2^k}$ est égal à 2^{k-2}, ce qui implique que les deux ensembles

$$\{a, a^2, \ldots, a^{2^{k-2}} \pmod{2^k}\} \subseteq X_+$$

ont le même nombre d'éléments $2^{k-2} = |X_+|$. On en déduit qu'il sont égaux, d'où

$$X_+ = \{a, a^2, \ldots, a^{2^{k-2}} \pmod{2^k}\}, \qquad X_- = \{-a, -a^2, \ldots, -a^{2^{k-2}} \pmod{2^k}\}.$$

□

6 Algèbre – motivation

6.1 Introduction

6.1.1 Théorie abstraite L'objectif de la partie algébrique abstraite du cours est d'introduire des groupes (surtout des groupes abéliens), des anneaux (surtout des anneaux commutatifs) et des corps. De nombreux exemples liés à la partie arithmétique du cours accompagneront la théorie abstraite.

On a déjà rencontré plusieurs exemples de groupes, d'anneaux et de corps :

— si $X \subset \mathbf{C}$ est un sous-groupe additif on peut effectuer des opérations "+" et "−" vérifiant des règles usuelles dans X (X est un groupe abélien pour addition) ;

— si $A \subset \mathbf{C}$ est un sous-anneau on peut effectuer des opérations "+", "−" et "$\cdot$" vérifiant des règles usuelles dans A (A est un anneau commutatif) ;

— si $A \subset \mathbf{C}$ est un sous-corps on peut aussi effectuer division par des éléments non nuls dans A ;

— $\mathbf{Z}/n\mathbf{Z}$ est un anneau commutatif (il est muni des opérations "+", "−" et "$\cdot$") qui n'est pas un sous-anneau de $\mathbf{C}$;

— si p est un nombre premier, alors $\mathbf{Z}/p\mathbf{Z}$ est un corps (c'est un anneau commutatif dans lequel tout élément non nul a admet l'inverse multiplicatif $a^{-1} = 1/a$) ;

— l'ensemble $M_2(\mathbf{R})$ des matrices 2×2 à coefficients réels est un anneau non commutatif (il est muni des opérations "+", "−" et "$\cdot$", mais la multiplication matricielle n'est pas commutative : en général, $M \cdot N \neq N \cdot M$).

On peut rencontrer beaucoup de groupes en géométrie (groupes de symétrie), mais dans ce cours on ne s'intéressera pas trop à cet aspect de la théorie.

6.1.2 Exemple important : anneaux de polynômes L'objectif de la partie algébrique concrète du cours est l'étude algébrique des anneaux de polynômes en une variable. Le point le plus important du cours est le fait que l'anneau $\mathbf{Z} = \{0, \pm 1, \pm 2, \ldots\}$ des entiers relatifs se comporte de la même manière que l'anneau $K[X] = \{f(X) = a_0 + a_1 X + \cdots + a_n X^n \mid a_j \in K,\, n \geq 0\}$ des polynômes en une variable à coefficients dans un corps K (on peut prendre, par exemple, $K = \mathbf{Q}, \mathbf{R}$ ou $\mathbf{C}$).

Dans les deux cas respectifs on a une notion de divisibilité qui a les mêmes propriétés : division euclidienne, algorithme d'Euclide, théorème de Bézout, le pgcd, lemme d'Euclid et l'unicité de factorisation.

Par conséquent, la théorie des congruences (par exemple, le théorème chinois) fonctionne de la même façon dans les deux cas. Il ne s'agit pas d'une théorie abstraite ; on verra que des congruences entre polynômes apparaîssent naturellement en algèbre, analyse et algèbre linéaire.

Arithmétique	Algèbre
$\mathbf{Z}$	$K[X]$
$n \in \mathbf{Z}$	$f = f(X) \in K[X]$
$a \equiv b \pmod{n}$	$u(X) \equiv v(X) \pmod{f}$
$\mathbf{Z}/n\mathbf{Z}$	$K[X]fK[X] = K[X]/(f)$
$\mathbf{Z}^* = \{\pm 1\}$	$K[X]^* = K^* = K \smallsetminus \{0\}$
nombres premiers p	polynômes irréductibles unitaires $g(X)$
$n = \pm \prod p^{v_p(n)}$	$f(X) = c \prod g(X)^{v_g(f)}$

6.2 Polynômes

6.2.1 Division euclidienne **Exemple 1 : $\mathbf{R}[X]/(X) = \mathbf{R}$.** En effet, tout polynôme $g(X) = b_0 + b_1X + \cdots + b_nX^n$ ($b_j \in \mathbf{R}$) s'écrit d'une façon unique

$$g(X) = Xh(X) + r, \qquad h(X) \in \mathbf{R}[X], \qquad r \in \mathbf{R},$$
$$h(X) = b_1 + b_2X + \cdots + b_nX^{n-1}, \qquad r = b_0 = g(0),$$

ce qui signifie que l'ensemble des classes de congruence modulo X est égal à

$$\mathbf{R}[X]/(X) = \{r \pmod X \mid r \in \mathbf{R}\}.$$

Plus précisement, les applications

$$\mathbf{R} \longrightarrow \mathbf{R}[X]/(X), \qquad r \mapsto r \pmod X,$$
$$\mathbf{R}[X]/(X) \longrightarrow \mathbf{R}, \qquad g(X) \pmod X \mapsto g(0)$$

sont inverses l'une à l'autre ; elles sont compatibles avec des opérations algébriques (addition, soustraction, multiplication).

Exemple 2 : $\mathbf{R}[Y]/(Y - a) = \mathbf{R}$. Soit $a \in \mathbf{R}$. Après un changement de variables $X = Y - a$ dans l'exemple 1 on écrit $g(X) = g(Y - a) = b_0 + b_1(Y - a) + \cdots + b_n(Y - a)^n = c_0 + c_1Y + \cdots + c_nY^n = h(Y)$. On obtient, comme avant,

$$\mathbf{R}[Y]/(Y - a) = \{r \pmod{(Y - a)} \mid r \in \mathbf{R}\}$$

et deux applications compatibles avec des opérations algébriques qui sont inverses l'une à l'autre :

$$\mathbf{R} \longrightarrow \mathbf{R}[Y]/(Y - a), \qquad r \mapsto r \pmod{(Y - a)},$$
$$\mathbf{R}[Y]/(Y - a) \longrightarrow \mathbf{R}, \qquad h(Y) \pmod{(Y - a)} \mapsto h(a)$$

On dit que **évaluation en $Y = a$**

$$\mathrm{ev}_a : \mathbf{R}[Y] \longrightarrow \mathbf{R}, \qquad h(Y) \mapsto h(a)$$

induit un isomorphisme d'anneaux

$$\overline{\mathrm{ev}}_a : \mathbf{R}[Y]/(Y - a) \xrightarrow{\sim} \mathbf{R}. \tag{6.2.1.1}$$

Exemple 3 : Construction de C. On va construire $\mathbf{C}$ en utilisant des polynômes à coefficients réels. Avant de commencer, on doit répondre à la question fondamentale suivante : **c'est quoi exactement, $\mathbf{C}$** ? Bien sûr, $\mathbf{C} = \{a + bi \mid a, b \in \mathbf{R}\}$, mais i**, c'est quoi** ? On ne peut pas répondre à cette question, mais on sait ce qui est i^2 : on a $i^2 = -1$. Autrement dit, chaque fois que i^2 apparaît, on le remplace par -1.

On peut aussi dire qu'on remplace $i^2 + 1$ (ainsi que tous les multiples de $i^2 + 1$) par 0.

On fait la même chose quand on travaille avec des congruences $\pmod n$: on fait des calculs usuels avec des entiers et on remplace tous les multiples de n par 0.

Cette analogie suggère qu'on devrait considérer des congruences modulo $X^2 + 1$ pour des polynômes réels. Pour le faire, il faut comprendre d'abord la division euclidienne par $X^2 + 1$. On a, par exemple,

$$X^3+2X^2+5=(X^2+1)X+(2X^2-X+5),\qquad 2X^2-X+5=(X^2+1)\cdot 2-X+3,$$
$$X^3+2X^2+5=(X^2+1)(X+2)+(3-X).$$

En général, tout polynôme $g(X)\in\mathbf{R}[X]$ s'écrit d'une façon unique

$$g(X)=(X^2+1)h(X)+(a+bX),\qquad h(X)\in\mathbf{R}[X],\qquad a,b\in\mathbf{R},\tag{6.2.1.2}$$

ce qui implique que l'on a

$$g(X)\ (\mathrm{mod}\,(X^2+1))=a+bX\ (\mathrm{mod}\,(X^2+1))$$

et

$$\mathbf{R}[X]/(X^2+1)=\{a+bX\ (\mathrm{mod}\,(X^2+1))\mid a,b\in\mathbf{R}\}=\{a+bI\mid a,b\in\mathbf{R}\}$$

($a+bI=a'+b'I\iff a=a'$ et $b=b'$), où

$$I=X\ (\mathrm{mod}\,(X^2+1))\in\mathbf{R}[X]/(X^2+1),\qquad I^2+1=X^2+1\ (\mathrm{mod}\,(X^2+1))=0\ (\mathrm{mod}\,(X^2+1)).$$

Autrement dit, on a bien

$$\boxed{\mathbf{R}[X]/(X^2+1)=\mathbf{C}}.\tag{6.2.1.3}$$

Plus précisement, évaluation en i induit un isomorphisme d'anneaux (une bijection compatible avec des opérations algébriques)

$$\overline{\mathrm{ev}}_i:\mathbf{R}[X]/(X^2+1)\xrightarrow{\sim}\mathbf{C},\qquad g(X)\ (\mathrm{mod}\,(X^2+1))\mapsto g(i).\tag{6.2.1.4}$$

Remarquons que $-i$ est aussi une racine de X^2+1, ce qui signifie qu'il y a un autre isomorphisme d'anneaux

$$\overline{\mathrm{ev}}_{-i}:\mathbf{R}[X]/(X^2+1)\xrightarrow{\sim}\mathbf{C},\qquad g(X)\ (\mathrm{mod}\,(X^2+1))\mapsto g(-i)=\overline{g(i)},\tag{6.2.1.5}$$

qu'on obtient à partir de (6.2.1.4) si on applique la conjugation complexe.

Exemple 4 : Construction de corps. En général, si K est un corps et si $f(X)\in K[X]$ est un polynôme **irréductible** de degré $\deg(f)=d\geq 1$, alors l'anneau quotient $L=K[X]/(f)$ est un corps contenant K. Tout élément de L s'écrit d'une façon unique

$$a_0+a_1\alpha+\cdots+a_{d-1}\alpha^{d-1},\qquad a_j\in K,\qquad \alpha=X\ (\mathrm{mod}\,f(X))\in L,\qquad f(\alpha)=0.\tag{6.2.1.6}$$

Par exemple, $\mathbf{Q}[X]/(X^2+1)=\{a+bi\mid a,b\in\mathbf{Q}\}$.

On va s'intéresser surtout au cas $K=\mathbf{Z}/p\mathbf{Z}$, où p est un nombre premier. Le corps L sera alors un corps fini à p^d éléments (et tout corps fini peut être construit de cette façon).

Exemple 5 : Interpolation. Si $f(X)=(X-a_1)\cdots(X-a_n)$ avec $a_1,\ldots,a_n\in\mathbf{C}$ distincts, on peut décrire l'anneau quotient $\mathbf{C}[X]/(f)$ en termes d'interpolation de Lagrange (il s'agit de trouver un polynôme de degré $\deg<n$ à partir de la connaissance de ses valeurs en $a_1,\ldots,a_n$).

7 Groupes

7.1 Définition et exemples

7.1.1 Groupes de transformations Les groupes seront traités ici d'un point de vue abstrait, mais il est important de savoir que beaucoup de groupes apparaîssent dans le cadre concret suivant.

Un tel groupe "concret" est tout simplement un ensemble G d'applications inversibles $g : X \longrightarrow X$ (où X est un ensemble donné) qui est stable par composition (si $g, h \in G$, alors $g \circ h \in G$), par inverse (si $g \in G$, alors $g^{-1} \in G$) et qui contient l'identité $\mathrm{id} : X \longrightarrow X$. Exemple : $X = \mathbf{R}^2$ et $G = \{\text{rotations de } \mathbf{R}^2 \text{ autour d'origine}\}$.

Cependant, il est important de séparer G et X, car le même groupe abstrait peut agir sur beaucoup d'ensembles (dans l'exemple ci-dessus, G agit sur l'ensemble des points de $\mathbf{R}^2$ mais aussi sur l'ensemble des droites). Si l'on oublie X, ce qui restera sera l'ensemble G muni d'opération binaire "$\circ$" (pour tous $g, h \in G$ on a un élément $g \circ h \in G$) et d'un élément distingué $\mathrm{id} \in G$. Leur propriétés apparaîssent, sous une forme abstraite, dans la Définition 7.1.3 ci-dessous.

7.1.2 Exemple : $G = \mathbf{Z}$ Voici un autre exemple d'un groupe : l'ensemble des entiers relatifs $\mathbf{Z} = \{0, \pm 1, \pm 2, \ldots\}$ muni d'opération "+" (et de l'opération inverse "$-$").

Ces opérations vérifient les identités suivantes (pour tous $a, b, c \in \mathbf{Z}$).

$$\begin{aligned} &(1) \quad (a+b)+c = a+(b+c) \\ &(2) \quad a+0 = 0+a = a \\ &(3) \quad a+(-a) = (-a)+a = 0 \\ &(4) \quad a+b = b+a \end{aligned} \tag{7.1.2.1}$$

7.1.3 Définition (Définition d'un groupe)**.** Un **groupe** est un couple $(G, *)$, où G est un ensemble et $* : G \times G \longrightarrow G$ est une opération binaire (une règle qui assigne à chaque couple $g, h \in G$ un élément $g * h \in G$) qui vérifient les trois axiomes suivants.

$$\begin{aligned} &(1) \quad \textbf{(Associativité)} \quad \forall g, h, k \in G \quad (g*h)*k = g*(h*k) \\ &(2) \quad \textbf{(Elément neutre)} \quad \exists e \in G \; \forall g \in G \quad g*e = e*g = g \\ &(3) \quad \textbf{(Inverse)} \quad \forall g \in G \; \exists h \in G \quad g*h = h*g = e \end{aligned}$$

Si, de plus, la propriété suivante est satisfaite

$$(4) \quad \textbf{(Commutativité)} \quad \forall g, h \in G \quad g*h = h*g \tag{7.1.3.1}$$

on dit que $(G, *)$ est un **groupe abélien** (ces groupes portent le nom de N.H. Abel (1802–1829), un mathématicien norvégien).

7.1.4 Unicité On montrera dans la proposition 7.1.6 ci-dessous que $e \in G$ dans l'Axiome (2) est unique (**l'élément neutre de** G), et que $h \in G$ dans l'Axiome (3) (qui dépend de g) est aussi unique (**l'inverse de** g).

7.1.5 Exemples de groupes (1) Exemple $(G, *) = (\mathbf{Z}, +)$ de 7.1.2 : on a $G = \mathbf{Z}$, $* = +$, l'élément neutre est $e = 0$ et l'inverse de $a \in \mathbf{Z}$ est égal à $-a$.
(2) $(\mathbf{R}, +)$ (plus généralement, tout sous-groupe additif de $\mathbf{C}$) est un groupe abélien dans lequel $e = 0$ et l'inverse de a est égal à $-a$.
(3) $(\mathbf{R} \smallsetminus \{0\}, \cdot)$ et $(\mathbf{C} \smallsetminus \{0\}, \cdot)$ sont des groupes abéliens dans lesquels $e = 1$ et l'inverse de a est égal à a^{-1}.

(4) $(\mathbf{Z}\smallsetminus\{0\},\cdot)$ **n'est pas** un groupe : les Axiomes (1) et (2) sont satisfaits (avec $e=1$), mais $g=a\in\mathbf{Z}\smallsetminus\{0\}$ vérifie l'Axiome (3) si et seulement s'il existe $b\in\mathbf{Z}\smallsetminus\{0\}$ tel que $ab=ba=1$. Un tel élément b n'existe que si $a=\pm1$. On en déduit que le sous-ensemble $(\{\pm1\},\cdot)$ est bien un groupe (abélien).
(5) On note $GL_2(\mathbf{R}) := \{M\in M_2(\mathbf{R}) \mid \det(M)\neq 0\}$ l'ensemble des matrices inversibles réelles 2×2. Le couple $(GL_2(\mathbf{R}),\cdot)$ est un groupe, avec $e=I=\begin{pmatrix}1&0\\0&1\end{pmatrix}$. En effect, multiplication matricielle vérifie $(M\cdot N)\cdot P = M\cdot(N\cdot P)$ et $M\cdot I = I\cdot M = M$. L'inverse de $M=\begin{pmatrix}a&b\\c&d\end{pmatrix}$ est la matrice $M^{-1} = (ad-bc)^{-1}\begin{pmatrix}d&-b\\-c&a\end{pmatrix}$. Ce groupe n'est pas abélien, car $M\cdot N\neq N\cdot M$ pour $M=\begin{pmatrix}0&1\\0&0\end{pmatrix}$, $N=\begin{pmatrix}0&0\\1&0\end{pmatrix}$.
(6) $(\mathbf{Z}/n\mathbf{Z},+)$ est un groupe abélien, où $e=0 \pmod n$ et l'inverse de $a \pmod n$ est $(-a) \pmod n$.
(7) $((\mathbf{Z}/n\mathbf{Z})^*,\cdot)$ est un groupe abélien, où $e=1 \pmod n$ et l'inverse d'une classe de congruence inversible $a \pmod n$ est $a^{-1} \pmod n$.

7.1.6 Proposition. *Soit $(G,*)$ un groupe.*
*(1) **(Associativité supérieure)** Si $n\geq 3$ et si $g_1,\dots,g_n\in G$, alors l'élément $g_1*\cdots g_n\in G$ ne dépend de l'ordre dans lequel on met des parenthèses (par exemple, on a $(g_1*(g_2*g_3))*g_4 = (g_1*g_2)*(g_3*g_4) = ((g_1*g_2)*g_3)*g_4 = \cdots$).*
*(2) **L'élément neutre** $e\in G$ dans l'Axiome (2) de* (7.1.3.1) ***est unique**.*
(3) Pour tout $g\in G$ l'élément $h\in G$ dans l'Axiome (3) de (7.1.3.1) *est unique. On le note g^{-1} et on l'appelle **l'inverse de** g.*
*(4) **(Inverse à gauche = inverse à droite)** Si $g,h\in G$ vérifient $g*h=e$, alors $h=g^{-1}$ et $g=h^{-1}$ (d'où $h*g=e$).*
(5) Pour tous $g,h\in G$ on a $(g*h)^{-1}=h^{-1}*g^{-1}$ et $(g^{-1})^{-1}=g$.
(6) Si $g,h,k\in G$ vérifient $g*h=g*k$ ou $h*g=k*g$, alors $h=k$.

Démonstration. (1) Exercice. (2) Si e,e' vérifient $g*e=e*g=g$ et $h*e'=e'*h=h$ pour tous $g,h\in G$, alors $e'=e*e'=e$ (on prend $g=e'$ et $h=e$). (3) De même, si $g*h=h*g=e=g*h'=h'*g$, alors $h=h*e=h*(g*h')=(h*g)*h'=e*h'=h'$. (4) Si $g*h=e$, alors $g^{-1}=g^{-1}*e=g^{-1}*(g*h)=(g^{-1}*g)*h=e*h=h$. (5) L'identité $(g*h)*(h^{-1}*g^{-1}) = (g*(h*h^{-1}))*g^{-1} = (g*e)*g^{-1} = g*g^{-1} = e$ implique, grâce à (4), que $(g*h)^{-1}$ est égal à $h^{-1}*g^{-1}$. (6) Si $g*h=g*k$, alors $g^{-1}*(g*h)=g^{-1}*(g*k)$. Le terme à gauche est égal à $(g^{-1}*g)*h=e*h=h$ et celui à droite à $(g^{-1}*g)*k=e*k=k$. On raisonne de même pour traiter le cas $h*g=k*g$. □

7.1.7 Notation (1) Dans un groupe nonabélien on utilise souvent la notation multiplicative : on écrit $e=1$ et on supprime le symbole pour l'opération. Les formules dans la proposition 7.1.6 deviennent alors

$$(g_1(g_2g_3))g_4 = (g_1g_2)(g_3g_4) = ((g_1g_2)g_3)g_4, \qquad (gh)^{-1}=h^{-1}g^{-1}, \qquad g^{-1}gh=eh=h. \tag{7.1.7.1}$$

(2) Dans un groupe abélien on peut choisir soit la **notation multiplicative** ci-dessus, soit la **notation additive**, où $e=0$, on note l'opération "+", et l'inverse de $x\in G$ est noté $-x$. Les deux premières formules de (7.1.7.1) deviennent alors

$$(x_1+(x_2+x_3))+x_4 = (x_1+x_2)+(x_3+x_4) = ((x_1+x_2)+x_3)+x_4, \qquad -(x+y)=(-y)+(-x)=(-x)+(-y) \tag{7.1.7.2}$$

(la dernière égalité est une conséquence du fait que le groupe $(G,+)$ est abélien).

7.1.8 Groupe produit Si $(G,*)$ et $(H,\square)$ sont des groupes, leur **produit** est le groupe

$$(G \times H, \triangle), \qquad G \times H = \{(g,h) \mid g \in G,\, h \in H\}, \qquad (g,h)\triangle(g',h') = (g * g', h \square h'). \tag{7.1.8.1}$$

On a $e_{G\times H} = (e_G, e_H)$ et $(g,h)^{-1} = (g^{-1}, h^{-1})$ dans ce groupe.
Exemple : $(\mathbf{R},+) \times (\mathbf{R},+) = (\mathbf{R}^2,+)$.

7.2 Sous-groupes

7.2.1 Exemple : $\mathbf{Z} \subset \mathbf{R}$ Le groupe additif $(\mathbf{Z},+)$ est un sous-groupe de $(\mathbf{R},+)$.

7.2.2 Définition. Soit $(G,*)$ un groupe. Un sous-ensemble $H \subset G$ est un **sous-groupe** de $(G,*)$ si $(H,*)$ (muni de l'opération $*$ qui provient de G) est un groupe.
[Si c'est le cas, alors l'unicité de l'élément neutre et de l'inverse implique que $e_H = e_G =: e$, et que l'inverse h^{-1} de tout $h \in H$ est le même dans G et dans H.]

7.2.3 Proposition. *Soit $(G,*)$ un groupe, soit $H \subset G$ un sous-ensemble. Il est équivalent :*
(1) H est un sous-groupe de $(G,*)$.
(2) $e_G \in H$ et on a, pour tous $h,h' \in H$, $h * h' \in H$ et $h^{-1} \in H$.
(3) $H \neq \emptyset$ et on a, pour tous $h,h' \in H$, $h' * h^{-1} \in H$.

Démonstration. (1) et (2) sont équivalents par définition (grâce à l'unicité de l'élément neutre et de l'inverse).
(2) $\Longrightarrow$ (3) : H est bien non vide, car $e = e_G \in H$. Si $h,h' \in H$, alors $h^{-1} \in H$, d'où $h' * h^{-1} \in H$.
(3) $\Longrightarrow$ (2) : H étant non vide, il existe $k \in H$, ce qui implique que $k * k^{-1} = e \in H$. Si $h,h' \in H$, alors $e * h^{-1} = h^{-1} \in H$, d'où $h' * (h^{-1})^{-1} = h' * h \in H$. □

7.2.4 Exemples de sous-groupes (1) Les sous-ensembles $\{e\}$ et G sont des sous-groupes de $(G,*)$.
(2) D'après le théorème 2.3.2, les sous-groupes de $(\mathbf{Z},+)$ sont les sous-ensembles $d\mathbf{Z}$ ($d \in \mathbf{N}$).
(3) Soit X un ensemble non vide. On note $(S_X,\circ)$ le groupe des permutations de X (l'opération étant la composition) :

$$S_X := \{\text{applications bijectives } \alpha : X \longrightarrow X\}, \qquad (\beta\circ\alpha)(x) = \beta(\alpha(x)), \qquad \beta\circ\alpha : X \xrightarrow{\alpha} X \xrightarrow{\beta} X.$$

L'élément neutre est l'application identité $e = \mathrm{id}_X$ ($\mathrm{id}(x) = x$, pour tout $x \in X$).

Lorsque $X = \{1,2,\ldots,n\}$ ($n \geq 1$), on appelle $S_X = S_n$ le **groupe symétrique** d'un ensemble à n éléments. On écrit une permutation $\alpha \in S_n$ de la façon suivante :

$$\alpha = \begin{pmatrix} 1 & 2 & \cdots & n \\ \alpha(1) & \alpha(2) & \cdots & \alpha(n) \end{pmatrix}, \qquad e = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}.$$

Si $n > 2$, alors le groupe S_n n'est pas abélien. Par exemple, si $n = 3$, alors

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \qquad \beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \qquad \beta\circ\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \neq \alpha\circ\beta = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

Si $Y \subset X$ est un sous-ensemble, alors

$$H := \{\alpha \in S_X \mid \alpha(Y) = Y\}$$

est un sous-groupe de S_X. Par exemple, si $X = \{1,2,\ldots,n\}$ et $Y = \{n\}$, alors $S_X = S_n$ et $H = S_{n-1}$.

(4) Soit V un espace vectoriel sur un corps K. Le **groupe linéaire général**

$$GL(V) := \{\alpha : V \longrightarrow V \mid \alpha \text{ est bijective et } K\text{-linéaire}\} \subset S_V$$

est un sous-groupe de S_V. Lorsque $V = K^n$ (un élément de K^n étant un vecteur colonne), alors toute application linéaire $\alpha : K^n \longrightarrow K^n$ s'écrit matriciellement $\alpha(x) = Ax$, où $A \in M_n(K)$. La composition de deux applications linéaires $\alpha : x \mapsto Ax$ et $\beta : y \mapsto By$ est égale à $\beta \circ \alpha : x \mapsto B(Ax) = (BA)x$. Par conséquent, on peut identifier

$$GL(V) = GL(K^n) = \{x \mapsto Ax \ (x \in K^n) \mid A \in M_n(K), \det(A) \neq 0\}$$

au groupe matriciel

$$GL_n(K) = \{A \in M_n(K) \mid \det(A) \neq 0\}$$

(dont l'opération est le produit matriciel). Le **groupe linéaire spécial**

$$SL_n(K) := \{A \in M_n(K) \mid \det(A) = 1\}$$

est un sous-groupe de $GL_n(K)$.

(5) On peut combiner des applications linéaires et des translations dans le cadre de (4). On obtient le **groupe affine général**

$$GA(V) := \{x \mapsto \alpha(x) + a \ (x \in V) \mid \alpha \in GL(V), a \in V\} \subset S_V.$$

Le groupe des **translations**

$$\{x \mapsto x + a \ (x \in V) \mid a \in V\} \subset GA(V)$$

est un sous-groupe de $GA(V)$.

Si $V = K^n$, alors le groupe affine général

$$GA_n(K) = GA(K^n) = \{x \mapsto Ax + a \ (x \in K^n) \mid A \in GL_n(K), a \in K^n\}$$

s'écrit sous la forme matricielle suivante

$$GA_n(K) = \left\{ \begin{pmatrix} A & a \\ 0 & 1 \end{pmatrix} \mid A \in GL_n(K), a \in K^n \right\},$$

car la composition des applications $x \mapsto Ax + a$ et $y \mapsto By + b$ est égale à $x \mapsto B(Ax + a) + b = (BA)x + (Ba + b)$ et

$$\begin{pmatrix} B & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} A & a \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} BA & Ba + b \\ 0 & 1 \end{pmatrix}.$$

(6) Si $n \geq 1$, alors le **groupe orthogonal**

$$O(n) := \{A \in M_n(\mathbf{R}) \mid {}^tAA = I\}$$

(où on a noté ${}^tA$ la matrice transposée) est un sous-groupe de $GL_n(\mathbf{R})$. Le **groupe orthogonal spécial**

$$SO(n) := \{A \in O(n) \mid \det(A) = 1\} = O(n) \cap SL_n(\mathbf{R})$$

est un sous-groupe de $O(n)$ et aussi de $SL_n(\mathbf{R})$.

Si $n = 2$, alors $SO(2)$ est le groupe des matrices qui représentent les rotations de $\mathbf{R}^2$ autour d'origine.

De même, le **groupe unitaire**

$$U(n) := \{A \in M_n(\mathbf{C}) \mid {}^tA\overline{A} = I\}$$

est un sous-groupe de $GL_n(\mathbf{C})$. Le **groupe unitaire spécial**

$$SU(n) := \{A \in U(n) \mid \det(A) = 1\} = U(n) \cap SL_n(\mathbf{C})$$

est un sous-groupe de $U(n)$ et aussi de $SL_n(\mathbf{C})$.

(7) Soit $n \geq 1$ un entier. L'ensemble des **racines n-ièmes d'unité**

$$\mu_n := \{z \in \mathbf{C} \mid z^n = 1\}$$

est un sous-groupe de $(\mathbf{C} \smallsetminus \{0\}, \cdot)$. Par exemple,

$$\mu_1 = \{1\}, \qquad \mu_2 = \{\pm 1\}, \qquad \mu_3 = \{1, \tfrac{-1 \pm i\sqrt{3}}{2}\}, \qquad \mu_4 = \{\pm 1, \pm i\}, \qquad \mu_6 = \{\pm 1, \tfrac{1 \pm i\sqrt{3}}{2}, \tfrac{-1 \pm i\sqrt{3}}{2}\}.$$

(8) Soit $a \in \mathbf{C} \smallsetminus \{0\}$ un nombre complexe non nul. L'ensemble de toutes les puissances de a

$$\langle a \rangle := \{a^n \mid n \in \mathbf{Z}\} \tag{7.2.4.1}$$

est un sous-groupe de $(\mathbf{C} \smallsetminus \{0\}, \cdot)$. Par exemple,

$$\begin{gathered} \langle -1 \rangle = \{-1, 1\} = \mu_2, \qquad \langle i \rangle = \{i, i^2 = -1, i^3 = -i, i^4 = 1\} = \mu_4, \\ \langle -i \rangle = \{i, (-i)^2 = -1, (-i)^3 = i, (-i)^4 = 1\} = \mu_4. \end{gathered} \tag{7.2.4.2}$$

(9) Le **centre** $Z(G) := \{z \in G \mid \forall g \in G \quad zg = gz\}$ de $(G, *)$ est un sous-groupe de $(G, *)$. Remarqueons que l'on a $Z(G) = G \iff (G, *)$ est abélien.

7.2.5 Exercice. Montrer : $O(n)$ (resp. $U(n)$) est bien un sous-groupe de $GL_n(\mathbf{R})$ (resp. de $GL_n(\mathbf{C})$).

7.2.6 Proposition. *Soit $(G, *)$ un groupe. L'intersection $H := \bigcap_{i \in I} H_i \subset G$ de n'importe quel ensemble de sous-groupes $H_i \subset G$ $(i \in I)$ est un sous-groupe de $(G, *)$.*

Démonstration. Tout H_i contient l'élément neutre e de G, ce qui implique que $e \in H$. Si $h, h' \in H = \bigcap H_i$, alors $h' * h^{-1} \in H_i$ (car H_i est un sous-groupe), d'où $h' * h^{-1} \in \bigcap_{i \in I} H_i = H$. □

7.2.7 Définition (Sous-groupe engendré par un sous-ensemble)**.** Soit $(G, *)$ un groupe. Si $S \subset G$ est un sous-ensemble non vide, alors l'intersection

$$\langle S \rangle := \bigcap_{\substack{H \subset (G,*) \\ S \subset H}} H$$

de tous les sous-groupes $H \subset (G, *)$ contenant S est le plus petit sous-groupe $(G, *)$ contenant S. On dit que $\langle S \rangle$ est **le sous-groupe de $(G, *)$ engendré par S**. Si $S = \{g\}$ contient un seul élément g, on dit que $\langle g \rangle := \langle \{g\} \rangle \subset G$ est **le sous-groupe cyclique engendré par g**.

7.2.8 Exemple : sous-groupes cycliques de $\mathbf{C}^*$ Soit $a \in \mathbf{C} \smallsetminus \{0\}$. Tout sous-groupe de $(\mathbf{C} \smallsetminus \{0\}, \cdot)$ contenant a contient aussi les éléments suivants (pour tous les entiers $n \geq 1$) :

$$\begin{gathered} 1, \quad a, \quad a^2 = a \cdot a, \quad a^3 = a \cdot a \cdot a, \quad \cdots \quad a^n = \underbrace{a \cdot a \cdots a}_{n \text{ fois}}, \quad \cdots \quad a^{-1}, \\ (a^{-1})^2 = a^{-2}, \cdots \quad a^{-n} = \underbrace{a^{-1} \cdot a^{-1} \cdots a^{-1}}_{n \text{ fois}}, \end{gathered} \tag{7.2.8.1}$$

ce qui implique que

$$\langle a \rangle = \{a^n \mid n \in \mathbf{Z}\} \tag{7.2.8.2}$$

est bien donné par la formule (7.2.4.1).

7.2.9 Isométries de $\mathbf{R}^n$ On utilise le produit scalaire standard

$$(x \mid y) := {}^t xy = x_1 y_1 + \cdots x_n y_n, \qquad x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbf{R}^n, \qquad y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \in \mathbf{R}^n$$

pour définir la **norme** $\|x\| := (x \mid x)^{1/2}$ et la **distance** $d(x, y) := \|x - y\|$ $(x, y \in \mathbf{R}^n)$ dans $\mathbf{R}^n$.

Une **isométrie de $\mathbf{R}^n$** est une application $f : \mathbf{R}^n \longrightarrow \mathbf{R}^n$ qui conserve la distance :

$$\forall x, y \in \mathbf{R}^n \quad d(f(x), f(y)) = d(x, y). \tag{7.2.9.1}$$

Par exemple, toute translation $f(x) = x + a$ $(a \in \mathbf{R}^n)$ est une isométrie.

On peut montrer que toute isométrie vérifiant $f(0) = 0$ est une application $\mathbf{R}$-linéaire $x \mapsto Ax$ $(A \in M_n(\mathbf{R}))$ (exercice !). La propriété (7.2.9.1) équivaut alors à

$$\forall x, y \in \mathbf{R}^n \quad (Ax \mid Ay) = (x \mid y) \iff \forall x, y \in \mathbf{R}^n \quad {}^t x({}^t AA)y = {}^t xy \iff {}^t AA = I_n \iff A \in O(n).$$

Par conséquent,

$$\{\text{Isométries de } \mathbf{R}^n\} = \{x \mapsto Ax + a \ (x \in \mathbf{R}^n) \mid A \in O(n),\ a \in \mathbf{R}^n\} \subset GA_n(\mathbf{R}).$$

7.3 Groupes cycliques, sous-groupes cycliques

La formule (7.2.8.2) se généralise de la façon suivante.

7.3.1 Puissances de $g \in G$ Soit $(G, *)$ un groupe, soit $g \in G$. On définit les puissances entières $g^n \in G$ $(n \in \mathbf{Z})$ de la manière suivante (voir le paragraphe 3.4.5).

$$g^0 := e, \qquad g^m := \underbrace{g * g * \cdots * g}_{m \text{ fois}}, \qquad g^{-m} := \underbrace{g^{-1} * g^{-1} * \cdots * g^{-1}}_{m \text{ fois}} \qquad (m \in \mathbf{N}_+). \tag{7.3.1.1}$$

7.3.2 Proposition. *Si $(G, *)$ est un groupe et si $g \in G$, alors on a*

$$\forall m, n \in \mathbf{Z} \qquad g^m * g^n = g^{m+n} = g^n * g^m, \qquad (g^m)^n = g^{mn}. \tag{7.3.2.1}$$

Démonstration. On a, par exemple, $g^3 * g^{-5} = g * g * g * g^{-1} * g^{-1} * g^{-1} * g^{-1} * g^{-1} = g^{-1} * g^{-1} = g^{-2}$. On laisse le cas général au lecteur. □

7.3.3 Corollaire. *Le sous-groupe cyclique $\langle g\rangle \subset G$ est égal à $\{g^n \mid n \in \mathbf{Z}\}$ (en particulier, ce groupe est abélien). On a $\langle g\rangle = \langle g^{-1}\rangle$.*

7.3.4 Définition. On dit qu'un groupe $(G, *)$ est **cyclique** et que $g \in G$ est son **générateur** si $G = \langle g\rangle = \{g^n \mid n \in \mathbf{Z}\}$.
[D'après le corollaire 7.3.3, si g est un générateur de G, alors g^{-1} l'est aussi.]

7.3.5 Notation multiplicative et notation additive Comparons l'écriture multiplicative (valable dans un groupe quelconque) avec l'écriture additive (valable dans un groupe abélien).

Notation multiplicative $(G, *)$ groupe quelconque	Notation additive $(G, +)$ groupe abélien
$g * h = gh$	$g + h = h + g$
$e = 1$	$e = 0$
g^{-1}	$-g$
gh^{-1}	$g + (-h) = (-h) + g$
$(gh)^{-1} = h^{-1}g^{-1}$	$-(g + h) = (-h) + (-g) = (-g) + (-h)$
$g^m := \underbrace{g \cdots g}_{m \text{ fois}} \quad (m > 0)$	$mg := \underbrace{g + \cdots + g}_{m \text{ fois}}$
$g^{-m} := (g^{-1})^m = (g^m)^{-1}$	$(-m)g := m(-g) = -(mg)$
$\langle g\rangle = \{g^n \mid n \in \mathbf{Z}\} = \langle g^{-1}\rangle$	$\langle g\rangle = \{ng \mid n \in \mathbf{Z}\} = \langle -g\rangle$

7.3.6 Exemples de groupes cycliques (1) Pour tout $d \in \mathbf{Z}$, $(d\mathbf{Z}, +) = \langle d\rangle = ((-d)\mathbf{Z}, +) = \langle -d\rangle \subset \mathbf{Z}$ est un sous-groupe cyclique de $(\mathbf{Z}, +)$. On a montré dans le théorème 2.3.2 que chaque sous-groupe de $\mathbf{Z}$ s'écrit sous cette forme.

(2) Pour tout $z \in \mathbf{C}$, le sous-groupe cyclique de $(\mathbf{C}, +)$ engendré par z est égal à $\langle z\rangle = \{0, \pm z, \pm 2z, \pm 3z, \ldots\} \subset \mathbf{C}$.

(3) Pour tout $n \in \mathbf{N}_+$, $(\mathbf{Z}/n\mathbf{Z}, +)$ est un groupe cyclique engendré par $1 \pmod n$ (et aussi par $-1 \pmod n$). On va déterminer l'ensemble de tous les générateurs de ce groupe dans l'exemple 3 du paragraphe 7.5.3 (voir aussi 7.5.7).

(4) On c'est appercu dans le paragraphe 4.3.2 que le groupe $((\mathbf{Z}/7\mathbf{Z})^*, \cdot)$ est cyclique. Il est engendré par $3 \pmod 7$ (et aussi par $5 \pmod 7$).

(5) Pour tout $n \in \mathbf{N}_+$, le groupe des racines n-ièmes d'unité est cyclique :

$$\mu_n = \{z \in \mathbf{C} \mid z^n = 1\} = \{e^{2\pi ik/n} = \cos(\tfrac{2\pi ik}{n}) + i\sin(\tfrac{2\pi ik}{n}) = (e^{2\pi i/n})^k \mid 1 \le k \le n\} = \langle e^{2\pi i/n}\rangle.$$

(6) Pour tout $n \in \mathbf{N}_+$, le groupe des rotations de $\mathbf{R}^2$ autour d'origine qui conservent un polygône régulier à n côtés (dont le centre est à l'origine) forment un groupe cyclique (un sous-groupe de $SO(2)$)

$$C_n = \{r, r^2, \ldots, r^n = \mathrm{id}\} = \langle r\rangle,$$

où r^k est la rotation d'angle $\frac{2\pi k}{n}$.

7.3.7 Exercice. Y a-t-il un lien entre l'exemple (5) et l'exemple (6) dans le paragraphe 7.3.6 ?

7.4 Morphismes de groupes

7.4.1 Exponentielle Il est important de comprendre des liens entre des groupes différents. Par exemple, l'exponentielle

$$\exp : (\mathbf{R}, +) \longrightarrow (\mathbf{R} \smallsetminus \{0\}, \cdot), \qquad \exp(x) = e^x \tag{7.4.1.1}$$

établie un lien entre les opérations (addition et multiplication) dans les deux groupes :

$$\exp(x + y) = \exp(x) \cdot \exp(y). \tag{7.4.1.2}$$

C'est un cas particulier de la notion générale suivante.

7.4.2 Définition. Soient $(G, *), (H, \square)$ des groupes. Un **morphisme de groupes** $f : (G, *) \longrightarrow (H, \square)$ est une application $f : G \longrightarrow H$ telle que $\forall g, g' \in G \quad f(g * g') = f(g) \square f(g')$.

7.4.3 Exemples de morphismes de groupes (1) $f : G \longrightarrow H$, $f(g) = e_H$ pour tout $g \in G$.

(2) $\mathrm{id} : G \longrightarrow G$, $\mathrm{id}(g) = g$ pour tout $g \in G$.

(3) $f = [\times 6] : (\mathbf{Z}, +) \longrightarrow (3\mathbf{Z}, +)$, $f(n) = 6n$. On a $6(m + n) = 6m + 6n$.

(4) $\exp : (\mathbf{R}, +) \longrightarrow (\mathbf{R} \smallsetminus \{0\}, \cdot)$, $\exp(x) = e^x$. On a $e^{x+y} = e^x e^y$.

(5) $\exp : (\mathbf{C}, +) \longrightarrow (\mathbf{C} \smallsetminus \{0\}, \cdot)$, $\exp(x + iy) = e^{x+iy} = e^x(\cos(y) + i \sin(y))$. On a $e^{z+z'} = e^z e^{z'}$.

(6) $\det : (GL_n(\mathbf{R}), \cdot) \longrightarrow (\mathbf{R} \smallsetminus \{0\}, \cdot)$, $\det(MN) = \det(M)\det(N)$.

(7) Si $(G, *)$ est un groupe et $g \in G$, alors l'application $f : \mathbf{Z} \longrightarrow G$ définie par $f(n) = g^n$ est un morphisme de groupes, car $g^{m+n} = g^m g^n$.

(8) Si $(G, *)$ est un groupe et $H \subset G$ est un sous-groupe, alors l'inclusion $H \hookrightarrow G$ est un morphisme de groupes.

(9) La projection canonique $\mathrm{pr} : (\mathbf{Z}, +) \longrightarrow (\mathbf{Z}/n\mathbf{Z}, +)$, $\mathrm{pr}(a) = a \pmod n$. On a $(a + b) \pmod n = (a \pmod n) + (b \pmod n)$.

(10) La projection verticale $f : (\mathbf{R}^2, +) \longrightarrow (\mathbf{R}, +)$, $f(\begin{pmatrix} x \\ y \end{pmatrix}) = x$.

(11) Si $f_1 : (G, *) \longrightarrow (H, \square)$ et $f_2 : (H, \square) \longrightarrow (K, \triangle)$ sont des morphismes de groupes, leur composition $f_2 \circ f_1 : (G, *) \longrightarrow (H, \square) \longrightarrow (K, \triangle)$ $((f_2 \circ f_1)(g) = f_2(f_1(g)))$ l'est aussi.

(12) Si $f_i : G_i \longrightarrow H_i$ $(i = 1, 2)$ sont des morphismes de groupes, alors $f_1 \times f_2 : G_1 \times G_2 \longrightarrow H_1 \times H_2$ l'est aussi.

7.4.4 Proposition. *Si $f : (G, *) \longrightarrow (H, \square)$ est un morphisme de groupes, alors :*
(1) $f(e_G) = e_H$.
(2) $\forall g \in G \quad f(g^{-1}) = f(g)^{-1}$.
*(3) Si l'application $f : G \longrightarrow H$ est bijective, alors son inverse $f^{-1} : (H, \square) \longrightarrow (G, *)$ est aussi un morphisme de groupes. On dit que f est un **isomorphisme de groupes** (ce qui implique que f^{-1} est aussi un isomorphisme de groupes).*
[Dans ce cas les propriétés algébriques des deux groupes sont "les mêmes", mais l'application f fait partie des données.]
(4) Si l'application f est injective, elle définit un isomorphisme de groupes $f : (G, *) \xrightarrow{\sim} (\mathrm{Im}(f), \square)$.

Démonstration. (1) $\forall g \in G \quad f(g) \square e_H = f(g) = f(g * e_G) = f(g) \square f(e_G)$, d'où $e_H = f(e_G)$. Le point (2) est une conséquence du fait que $f(g) \square f(g^{-1}) = f(g * g^{-1}) = f(e_G) = e_H$.
(3) Si f est bijective et $h, h' \in H$, alors il existe unique $g, g' \in G$ tels que $h = f(g)$ et $h' = f(g')$ $(g = f^{-1}(h)$, $g' = f^{-1}(h'))$. L'identité $h \square h' = f(g) \square f(g') = f(g * g')$ implique que $f^{-1}(h \square h') = g * g' = f^{-1}(h) * f^{-1}(h')$,

ce qu'il fallait démontrer dans (3). Le point (4) est une conséquence immédiate des définitions, car l'injectivité de f implique que $f : G \longrightarrow \mathrm{Im}(f)$ est bijective. □

7.4.5 Définition. Le noyau et **l'image** d'un morphisme de groupes $f : (G, *) \longrightarrow (H, \square)$ sont définis par les formules respectives suivantes :

$$\mathrm{Ker}(f) := \{g \in G \mid f(g) = e_H\} \subset G, \qquad \mathrm{Im}(f) := \{f(g) \mid g \in G\} \subset H.$$

7.4.6 Proposition. *Si $f : (G, *) \longrightarrow (H, \square)$ est un morphisme de groupes, alors :*
(1) $\mathrm{Ker}(f)$ *est un sous-groupe de* G.
(2) $\mathrm{Im}(f)$ *est un sous-groupe de* H.
(3) Soient $g, g' \in G$. Il est équivalent : $f(g) = f(g') \iff g^{-1} * g' \in \mathrm{Ker}(f) \iff g' * g^{-1} \in \mathrm{Ker}(f)$.

Démonstration. (1) On sait que $f(e_G) = e_H$, d'où $e_G \in \mathrm{Ker}(f)$. Si $g, g' \in \mathrm{Ker}(f)$, alors $f(g) = f(g') = e_H$. Il en résulte que $f(g^{-1}) = f(g)^{-1} = e_H^{-1} = e_H$ et $f(g * g') = f(g) \square f(g') = e_H \square e_H = e_H$, d'où $g^{-1}, g * g' \in \mathrm{Ker}(f)$.
(2) De même, $e_H = f(e_G) \in \mathrm{Im}(f)$. Si $h, h' \in \mathrm{Im}(f)$, alors il existe $g, g' \in G$ tels que $h = f(g)$ et $h' = f(g')$. Par conséquent, $h^{-1} = f(g)^{-1} = f(g^{-1}) \in \mathrm{Im}(f)$ et $h \square h' = f(g) \square f(g') = f(g * g') \in \mathrm{Im}(f)$.
(3) $f(g) = f(g') \iff e_H = f(g)^{-1} \square f(g') = f(g^{-1} * g') \iff g^{-1} * g' \in \mathrm{Ker}(f)$. La deuxième équivalence peut être démontrée de la même façon. □

7.4.7 Exemples de $\mathrm{Ker}(f)$ **et** $\mathrm{Im}(f)$ Nous allons décrire le noyau et l'image de chacun de morphismes de groupes qu'on a vus dans le paragraphe 7.4.3.

(1) Le morphisme trivial $f(g) = e_H$: $\mathrm{Ker}(f) = G$, $\mathrm{Im}(f) = \{e_H\}$.

(2) L'identité $\mathrm{id} : G \longrightarrow G$: $\mathrm{Ker}(\mathrm{id}) = \{e_G\}$, $\mathrm{Im}(f) = G$.

(3) $f : (\mathbf{Z}, +) \longrightarrow (3\mathbf{Z}, +)$, $f(n) = 6n$: $\mathrm{Ker}(f) = \{0\}$, $\mathrm{Im}(f) = (6\mathbf{Z}, +)$.

(4) $f = \exp : (\mathbf{R}, +) \longrightarrow (\mathbf{R} \smallsetminus \{0\}, \cdot)$: $\mathrm{Ker}(f) = \{0\}$, $\mathrm{Im}(f) = (\mathbf{R}_{>0}, \cdot)$.

(5) $f = \exp : (\mathbf{C}, +) \longrightarrow (\mathbf{C} \smallsetminus \{0\}, \cdot)$: $\mathrm{Ker}(f) = \{x + iy \in \mathbf{C} \mid e^x(\cos(y) + i\sin(y)) = 1\} = 2\pi i\mathbf{Z}$, $\mathrm{Im}(f) = (\mathbf{C} \smallsetminus \{0\}, \cdot)$.

(6) $\det : (GL_n(\mathbf{R}), \cdot) \longrightarrow (\mathbf{R} \smallsetminus \{0\}, \cdot)$: $\mathrm{Ker}(\det) = SL_n(\mathbf{R})$, $\mathrm{Im}(\det) = (\mathbf{R} \smallsetminus \{0\}, \cdot)$.

(7) $f : (\mathbf{Z}, +) \longrightarrow (G, *)$, $f(n) = g^n$: $\mathrm{Im}(f) = \langle g \rangle$.

(8) $f : H \hookrightarrow (G, *)$: $\mathrm{Ker}(f) = \{e_H\} = \{e_G\}$, $\mathrm{Im}(f) = H$.

(9) $f = \mathrm{pr} : (\mathbf{Z}, +) \longrightarrow (\mathbf{Z}/n\mathbf{Z}, +)$: $\mathrm{Ker}(\mathrm{pr}) = (n\mathbf{Z}, +)$, $\mathrm{Im}(\mathrm{pr}) = \mathbf{Z}/n\mathbf{Z}$.

(10) La projection verticale $f : (\mathbf{R}^2, +) \longrightarrow (\mathbf{R}, +)$: $\mathrm{Ker}(f) = \{\begin{pmatrix} 0 \\ y \end{pmatrix} \mid y \in \mathbf{R}\}$, $\mathrm{Im}(f) = \mathbf{R}$.

7.4.8 Exemples d'isomorphismes (1) L'identité $\mathrm{id} : G \longrightarrow G$.

(2) Conjugaison par $g \in G$: $f : G \longrightarrow G$, $f(h) = ghg^{-1}$. Dans ce cas on a $g(hh')g^{-1} = (ghg^{-1})(gh'g^{-1})$. L'inverse de f est $f^{-1}(g) = g^{-1}hg$, car $g^{-1}ghg^{-1}g = ehe = h$.

(3) Si $m, n \in \mathbf{N}_+$ et $\mathrm{pgcd}(m, n) = 1$, alors l'application dans le théorème chinois

$$f : (\mathbf{Z}/mn\mathbf{Z}, +) \longrightarrow (\mathbf{Z}/m\mathbf{Z}, +) \times (\mathbf{Z}/n\mathbf{Z}, +), \qquad f(a \pmod{mn}) = (a \pmod{m}, a \pmod{n})$$

est un morphisme de groupes bijectif, donc un isomorphisme de groupes.

7.4.9 Exercice. Un **automorphisme** d'un groupe G est un isomorphisme de groupes $G \longrightarrow G$. Montrer :
(1) $\mathrm{Aut}(G) := \{\text{automorphismes de } G\}$ est un sous-groupe de S_G.
(2) L'application $G \longrightarrow \mathrm{Aut}(G)$ qui assigne à $g \in G$ la conjugaison par g (voir l'exemple 2 dans le paragraphe 7.4.8) est un morphisme de groupes. On appelle son image le groupe des **automorphismes intérieurs** de G.
(3) Déterminer le noyau de $G \longrightarrow \mathrm{Aut}(G)$.

7.4.10 Proposition. *Un morphisme de groupes $f : (G, *) \longrightarrow (H, \square)$ est injectif $\iff \mathrm{Ker}(f) = \{e_G\}$.*

Démonstration. Par définition, f est injectif si, pour $g, g' \in G$, l'égalité $f(g) = f(g')$ équivaut à $g = g'$. On a

$$\begin{aligned} g = g' &\iff g' * g^{-1} = e_G \\ f(g) = f(g') &\iff g' * g^{-1} \in \mathrm{Ker}(f), \end{aligned}$$

ce qui implique que les conditions $g = g'$ et $f(g) = f(g')$ sont équivalents si et seulement si $\{e_G\} = \mathrm{Ker}(f)$. □

7.4.11 Corollaire. *Si $f : (G, *) \longrightarrow (H, \square)$ est un morphisme de groupes tel que $\mathrm{Ker}(f) = \{e_G\}$, alors f est injectif, ce qui implique que f définit un isomorphisme de groupes $f : (G, *) \xrightarrow{\sim} (\mathrm{Im}(f), \square)$.*

7.4.12 Exemple : exp et log Le morphisme de groupes (7.4.1.1) donné par l'exponentielle induit un isomorphisme de groupes

$$\exp : (\mathbf{R}, +) \xrightarrow{\sim} (\mathbf{R}_{>0}, \cdot).$$

Son inverse (qui est aussi un isomorphisme de groupes) est donné par le logarithme naturel

$$\ln : (\mathbf{R}_{>0}, \cdot) \xrightarrow{\sim} (\mathbf{R}, +).$$

7.4.13 Exercice. Soit $f : (G, *) \longrightarrow (H, \square)$ un morphisme de groupes.
(1) L'image $f(G_1) = \{f(g) \mid g \in G_1\}$ d'un sous-groupe G_1 de G est un sous-groupe de H.
(2) L'image réciproque $f^{-1}(H_1) = \{g \in G \mid f(g) \in H_1\}$ d'un sous-groupe H_1 de H est un sous-groupe de G.
(3) Sous les hypothèses de (1) et (2) on a $G_1 \subseteq f^{-1}(f(G_1))$ et $f(f^{-1}(H_1)) \subseteq H_1$.
(4) Trouver un exemple où $G_1 \neq f^{-1}(f(G_1))$ et $f(f^{-1}(H_1)) \neq H_1$.

7.4.14 Plongement de G dans S_G (Cayley) Soit $(G, *)$ un groupe. Les translations à gauche

$$L(g) : G \longrightarrow G, \qquad h \mapsto g * h$$

par des éléments $g \in G$ sont des applications bijectives vérifiant

$$L(e) = \mathrm{id}, \qquad L(g * g') = L(g) \circ L(g'), \qquad L(g)(e) = g,$$

ce qui implique que l'application

$$L : G \longrightarrow S_G, \qquad g \mapsto L(g)$$

est un morphisme de groupes injectif. En particulier, tout groupe fini d'ordre $|G| = n$ est isomorphe à un sous-groupe $\mathrm{Im}(L) \subset S_G \xrightarrow{\sim} S_n$ de S_n.

7.5 Ordre, (sous-)groupes cycliques, théorème de Lagrange

7.5.1 Introduction On a étudié les puissances des classes de congruence inversibles $(\mathrm{mod}\, n)$ dans le paragraphe 4.3. On fera maintenant la même chose dans le cadre général suivant.

7.5.2 Définition (Ordre)**.** Soit $(G, *)$ un groupe, soit $g \in G$. **L'ordre de** G est le nombre d'éléments $|G|$ de G ($|G| \in \mathbf{N}_+ \cup \{\infty\}$). **L'ordre de** g est $\min\{k \in \mathbf{N}_+ \mid g^k = e\}$ (si $g^k \neq e$ pour tout $k \in \mathbf{N}_+$, on dit que l'ordre de g est infini).

7.5.3 Exemples (1) Si $G = ((\mathbf{Z}/n\mathbf{Z})^*, \cdot)$, alors on retrouve la Définition 4.3.3.

(2) Si $(G, +)$ est un groupe abélien dans lequel on utilise l'écriture additive, alors l'ordre de $g \in G$ est $\min\{k \in \mathbf{N}_+ \mid kg = 0\}$ (ou ∞).

(3) Si $G = (\mathbf{Z}/m\mathbf{Z}, +)$ et $g = a \pmod m$ (où $a \in \mathbf{Z} \smallsetminus \{0\}$), alors on a $kg = ka \pmod m$, ce qui implique que l'ordre de g est égal à

$$d = \min\{k \geq 1 \mid ka \equiv 0 \pmod m\}.$$

Autrement dit, $d|a| \geq 1$ est le plus petit multiple positif de $|a|$ qui est divisible par m, d'où $d|a| = \mathrm{ppcm}(|a|, m)$ et $d = \mathrm{ppcm}(|a|, m)/|a| = m/\mathrm{pgcd}(|a|, m)$. En particulier, on a $d = m$ si et seulement si $\mathrm{pgcd}(|a|, m) = 1$ (cf. la proposition 4.3.13 et sa démonstration).

7.5.4 Groupes cycliques On va montrer maintenant qu'un groupe cyclique est déterminé, à un isomorphisme près, par son ordre. Plus précisement, il est isomorphe à $(\mathbf{Z}/m\mathbf{Z}, +)$ si son ordre m est fini (resp. à $(\mathbf{Z}, +)$ si son ordre est infini). De plus, tout sous-groupe d'un groupe cyclique est cyclique.

7.5.5 Proposition. *Soit $(G, *)$ un groupe, soit $g \in G$. On considère le morphisme de groupes $f : (\mathbf{Z}, +) \longrightarrow G$ défini par $f(n) = g^n$ (son image est le sous-groupe cyclique $\langle g \rangle$ de G engendré par g).*
(1) Si l'ordre de $g \in G$ est infini, alors $\mathrm{Ker}(f) = \{0\}$ *et f induit un isomorphisme de groupes $(\mathbf{Z}, +) \xrightarrow{\sim} \langle g \rangle$. Un élément g^k ($k \in \mathbf{Z}$) est un générateur du groupe cyclique $\langle g \rangle$ si et seulement si $k = \pm 1$. L'ensemble des sous-groupes de $\langle g \rangle$ est égal à $\{\langle g^d \rangle \mid d \in \mathbf{N}\}$.*
(2) Si l'ordre de $g \in G$ est égal à $m \in \mathbf{N}_+$, alors $\mathrm{Ker}(f) = m\mathbf{Z}$.

Démonstration. On a, par définition, $\mathrm{Ker}(f) = \{n \in \mathbf{Z} \mid g^n = e\}$. C'est un sous-groupe de $(\mathbf{Z}, +)$, ce qui implique qu'il existe $m \in \mathbf{N}$ tel que $\mathrm{Ker}(f) = m\mathbf{Z}$. L'ordre de g est égal à $\min\{k \in \mathrm{Ker}(f) = m\mathbf{Z} \mid k > 0\}$, donc à m si $m > 0$ (resp. à ∞ si $m = 0$), ce qui donne la description de $\mathrm{Ker}(f)$ dans (1) et (2).

En particulier, si l'ordre de g est infini, alors $\mathrm{Ker}(f) = \{0\}$, ce qui implique que le morphisme de groupes f est injectif et induit un isomorphisme de groupes $(\mathbf{Z}, +) \xrightarrow{\sim} (\mathrm{Im}(f), *) = \langle g \rangle$. Par conséquent, f définit une bijection entre l'ensemble des sous-groupes $\{d\mathbf{Z} \mid d \in \mathbf{N}\}$ de $\mathbf{Z}$ et l'ensemble des sous-groupes $\{f(d\mathbf{Z}) = \langle g^d \rangle\}$ de $\langle g \rangle$. L'élément $f(k) = g^k$ est un générateur de $\langle g \rangle$ si et seulement si k est un générateur de $\mathbf{Z}$, ce qui équivaut à $k\mathbf{Z} = \mathbf{Z} \iff k = \pm 1$. □

7.5.6 Théorème. *Soit $(G, *)$ un groupe, soit $g \in G$ un élément d'ordre $m \in \mathbf{N}_+$.*
(1) Soit $k \in \mathbf{Z}$; il est équivalent : $g^k = e \iff m \mid k$.
(2) Soient $k, l \in \mathbf{Z}$; il est équivalent : $g^k = g^l \iff m \mid (k - l) \iff k \equiv l \pmod m$.
(3) Le sous-groupe $\{g^k \mid k \in \mathbf{Z}\} = \langle g \rangle$ est égal à $\{g, g^2, \ldots, g^m = e\}$; il a m éléments.
(4) L'application $\overline{f} : \mathbf{Z}/m\mathbf{Z} \longrightarrow \langle g \rangle$ définie par $\overline{f}(k \pmod m) = g^k$ est bien définie. C'est un isomorphisme de groupes $\overline{f} : \mathbf{Z}/m\mathbf{Z} \xrightarrow{\sim} \langle g \rangle$.
(5) Si $k \in \mathbf{Z} \smallsetminus \{0\}$, alors l'ordre de g^k est égal à $m/\mathrm{pgcd}(|k|, m)$.
(6) Le groupe cyclique $\langle g \rangle$ (d'ordre m) a $\varphi(m)$ générateurs.
(7) Plus généralement, le nombre d'éléments de $\langle g \rangle$ d'ordre $d \in \mathbf{N}_+$ est égal à zéro (resp. à $\varphi(d)$) si d ne divise pas m (resp. si d divises m).

(8) L'ensemble des sous-groupes de $\langle g\rangle$ est égal à $\{\langle g^d\rangle \mid d \mid m\}$ (où $\langle g^d\rangle$ est un groupe cyclique d'ordre m/d).

Démonstration. (1), (2) Soit $f : (\mathbf{Z}, +) \longrightarrow G$ le morphisme de groupes $f(k) = g^k$. On a $g^k = e \iff k \in \mathrm{Ker}(f)$, mais on sait que $\mathrm{Ker}(f) = m\mathbf{Z}$, d'après la proposition 7.5.5(2). Par conséquent, $g^k = g^l \iff g^{k-l} = g^k(g^l)^{-1} = e \iff m \mid (k-l)$.
(3) Tout $k \in \mathbf{Z}$ s'écrit $k = ma + l$, où $a, l \in \mathbf{Z}$ et $1 \leq l \leq m$. On a $g^k = (g^m)^a g^l = g^l$, et les m éléments $g, g^2, \ldots, g^m = e$ sont distincts, grâce à (2).
(4) Si $k \equiv l \pmod m$, alors $g^k = g^l$, ce qui implique que l'application $\overline{f}$ est bien définie. On a $\overline{f}((k \pmod m) + (l \pmod m)) = \overline{f}(k \pmod m)\overline{f}(l \pmod m))$, car le terme à gauche est égal à $\overline{f}((k+l) \pmod m) = g^{k+l}$ et celui à droite à $g^k g^l$. Autrement dit, $\overline{f}$ est un morphisme de groupes. L'application $\overline{f}$ est bijective, d'après (3).
(5) L'ordre de g^k et le plus petit entier $d \geq 1$ tel que $(g^k)^d = g^{dk} = e$, ce qui équivaut à $m \mid dk$. Il en résulte que $d|k|$ est le plus petit multiple positif de $|k|$ qui est divisible par m, ce qui implique que $d|k| = \mathrm{ppcm}(|k|, m)$ et $d = \mathrm{ppcm}(|k|, m)/|k| = m/\mathrm{pgcd}(|k|, m)$.
(6) Le groupe cyclique $\langle g\rangle$ a m éléments $g, g^2, \ldots, g^m = e$. Parmi ces éléments, g^k est un générateur de $\langle g\rangle$ si et seulement si son ordre $m/\mathrm{pgcd}(|k|, m)$ est égal à m, ce qui équivaut à $\mathrm{pgcd}(k, m) = 1$. Il y a $\varphi(m)$ valeurs possibles de k tels que $\mathrm{pgcd}(k, m) = 1$ et $1 \leq k \leq m$.
(7) D'après (5), l'ordre de n'importe quel élément $g, g^2, \ldots, g^m = e$ de $\langle g\rangle$ est un diviseur de m. Réciproquement, étant donné un diviseur $d \mid m$, l'ordre de g^k $(1 \leq k \leq m)$ est égal à d si et seulement si $m/\mathrm{pgcd}(k, m) = d$, ce qui équivaut à $\mathrm{pgcd}(k, m) = m/d$, donc à $k = (m/d)k'$, $1 \leq k' \leq d$, $m = (m/d)d$ et $\mathrm{pgcd}(k', d) = 1$. Il y a $\varphi(d)$ valeurs possibles de tels k'.
(8) Pour tout diviseur $d \mid m$, $\langle g^d\rangle = \{g^d, g^{2d}, \ldots, (g^d)^{m/d} = g^m = e\}$ est un sous-groupe cyclique de $\langle g\rangle$ d'ordre m/d. Réciproquement, si H est un sous-groupe de $\langle g\rangle$, alors $A := \{k \in \mathbf{Z} \mid g^k \in H\}$ est un sous-groupe de $\mathbf{Z}$ contenant $m\mathbf{Z}$. Par conséquent, on a $A = d\mathbf{Z}$, où $d \in \mathbf{Z}$ et $d \mid m$. □

7.5.7 Résumé : propriétés des (sous-)groupes cycliques (1) L'ordre de $g \in G$ (fini ou pas) est égal à l'ordre $|\langle g\rangle|$ du groupe cyclique engendré par g.

(2) Un groupe cyclique G d'ordre infini a deux générateurs. Un choix d'un générateur $g \in G$ définit un isomorphisme de groupes $f : (\mathbf{Z}, +) \xrightarrow{\sim} G$, $f(k) = g^k$. L'autre générateur est g^{-1}.

(3) Un groupe cyclique G d'ordre $m \in \mathbf{N}_+$ a $\varphi(m)$ générateurs. Un choix d'un générateur $g \in G$ définit un isomorphisme de groupes $\overline{f} : (\mathbf{Z}/m\mathbf{Z}, +) \xrightarrow{\sim} G$, $f(k \pmod m) = g^k$. Les autres générateurs sont g^k, où $k \pmod m \in (\mathbf{Z}/m\mathbf{Z})^*$ (i.e., où $\mathrm{pgcd}(k, m) = 1$).

(4) Par exemple, $G = \mu_m = (\{z \in \mathbf{C} \mid z^m = 1\}, \cdot)$ est engendré par $g = e^{2\pi i/m}$, et l'application $\overline{f} : (\mathbf{Z}/m\mathbf{Z}, +) \longrightarrow \mu_m$, $k \pmod m \mapsto e^{2\pi ki/m}$ est un isomorphisme de groupes.

(5) On peut montrer que tout groupe abélien fini est isomorphe à un produit de groupes cycliques $(\mathbf{Z}/n_1\mathbf{Z}, +) \times \cdots \times (\mathbf{Z}/n_r\mathbf{Z}, +)$, où $r \geq 0$, $n_1 > 1$ et $n_1 \mid n_2 \mid \cdots \mid n_r$. On peut démontrer ce résultat, par exemple, en utilisant l'algorithme d'Euclide et des opérations élémentaires pour des matrices à coefficients dans $\mathbf{Z}$.

7.5.8 Théorème (Lagrange)**.** *Si G est un groupe fini et $H \subset G$ est un sous-groupe, alors $|H|$ divise $|G|$.*

Démonstration. Voir le théorème 7.6.15 et le paragraphe 7.6.19 ci-dessous. □

7.5.9 Corollaire (Lagrange)**.** *Si G est un groupe fini et $g \in G$, alors l'ordre de g (qui est égal à l'ordre du sous-groupe cyclique $\langle g\rangle \subset G$) divise $|G|$. Par conséquent, on a $g^{|G|} = e$.*

Démonstration. On va démontrer le corollaire dans le cas particulier lorsque le groupe G est **abélien**. Soit $m = |G|$, $G = \{g_1, \ldots, g_m\}$. On fixe $g \in G$. Les égalités $gg_i = gg_j \iff g_i = g_j$ sont équivalentes, d'après

la proposition 7.1.6(6). Il en résulte que les éléments $gg_1, \ldots, gg_m$ sont distincts, ce qui implique que l'on a $G = \{gg_1, \ldots, gg_m\}$. Le groupe G étant abélien, le produit de ses éléments dans un ordre quelconque donne toujours le même résultat. En particulier, on a

$$g_1 g_2 \cdots g_m = (gg_1)(gg_2)\cdots(gg_m) = g^m g_1 g_2 \cdots g_m \quad \Longrightarrow \quad e = g^m$$

(on applique la proposition 7.1.6(6)). □

7.5.10 Théorème de Lagrange $\Longrightarrow$ théorème d'Euler Si $G = ((\mathbf{Z}/n\mathbf{Z})^*, \cdot)$, alors $|G| = \varphi(n)$ et $g = a \pmod n$, où $a \in \mathbf{Z}$ et $\operatorname{pgcd}(a, n) = 1$. L'identité $g^{|G|} = e$ équivaut à $a^{\varphi(n)} \equiv 1 \pmod n$, et la preuve ci-dessus est une version abstraite de la preuve du théorème d'Euler 4.2.9.

7.6 Le groupe quotient G/H (le cas abélien)

7.6.1 Introduction L'objectif de ce paragraphe est de développer une version abstraite de la construction du groupe additif $(\mathbf{Z}/n\mathbf{Z}, +)$.

D'ici jusqu'a fin du paragraphe 7.6 on fixe les données suivantes.

— Un groupe abélien $(G, +)$; on va utiliser la notation additive (l'élément neutre est $e = 0$ et l'inverse de $a \in G$ sera noté $-a$). Pour $a, b \in G$ on note $a-b := a+(-b) = (-b)+a$; on a $-(a-b) = b+(-a) = b-a$ et $(a-b)+(b-c) = a-c$.

— Un sous-groupe $H \subset G$.

On aimerait définir et étudier la notion de congruence modulo H dans G. Il faut garder en tête l'exemple fondamental $G = \mathbf{Z}$ et $H = n\mathbf{Z}$.

7.6.2 Définition. Soit $a \in G$; on note $a + H := \{a + h \mid h \in H\} \subset G$. On appelle les sous-ensembles $a + H \subset G$ les **classes modulo H dans G**.

7.6.3 Exemples (1) Si $G = \mathbf{Z}$, $H = n\mathbf{Z}$ et $a \in \mathbf{Z}$, alors $a + n\mathbf{Z} = \{b \in \mathbf{Z} \mid a \equiv b \pmod n\}$ (voir le chapitre 3).

(2) Si $G = (\mathbf{R}^2, +)$, $0 \neq u \in \mathbf{R}^2$ et $H = (\mathbf{R}u, +)$, alors les éléments de G correspondent aux points d'un plan, H est une droite qui passe par l'origine du plan, et $a + H$ est l'unique droite contenant a qui est parallèle à H. En particuler, si $a, b \in \mathbf{R}^2$, alors les classes $a + H$ et $b + H$ sont soit disjointes, soit égales. On va montrer maintenant qu'il s'agit d'une propriété générale.

7.6.4 Proposition. *Si $a, b \in G$, alors on a*

$$\begin{cases} a + H = b + H, & \text{si } a - b \in H \\ (a + H) \cap (b + H) = \emptyset, & \text{si } a - b \notin H. \end{cases}$$

L'application $H \longrightarrow a + H$, $h \mapsto a + h$ est bijective, son inverse étant $a' \mapsto a' - a$. En particulier, si H est fini, alors $|a + H| = |H|$.

Démonstration. Si $(a + H) \cap (b + H) \neq \emptyset$, alors il existe $h_1, h_2 \in H$ tels que $a + h_1 = b + h_2$, d'où $a - b = h_2 - h_1 \in H$. Réciproquement, si $h_0 := a - b \in H$, alors on a, pour tout $h \in H$, $a+h = b+(h+h_0) \in b+H$ et $b+h = a+(h-h_0) \in a+H$. On en déduit que $a + H \subseteq b + H$ et $b + H \subseteq a + H$, d'où $a + H = b + H$. La deuxième partie de la proposition est immédiate, car $(a + h) - a = h$ et $a + (a' - a) = a'$. □

7.6.5 Corollaire. *L'ensemble G est une réunion disjointe des classes modulo H. On note G/H l'ensemble de ces classes (on prend chaque classe une seule fois).*

7.6.6 Définition. On dit que $a, b \in G$ sont **congrus modulo** H (et on écrit $a \equiv b \pmod{H}$) si $a - b \in H$. D'après la proposition 7.6.4, cette condition équivaut à $a + H = b + H$. Remarquons qu'on a $a + H = \{c \in G \mid c \equiv a \pmod{H}\}$. Pour simplifier la notation on écrit souvent $\overline{a} \in G/H$ plutôt que $a + H \in G/H$.

L'indice de H dans G, noté $(G : H) := |G/H|$, est le nombre de classes modulo H dans G (par exemple, $(\mathbf{Z} : n\mathbf{Z}) = n$ et $(\mathbf{R} : \mathbf{Z}) = \infty$).

7.6.7 Proposition. *Soient $a, b, c \in G$.*
(1) $a \equiv a \pmod{H}$.
(2) Si $a \equiv b \pmod{H}$, alors $b \equiv a \pmod{H}$.
(3) Si $a \equiv b \pmod{H}$ et $b \equiv c \pmod{H}$, alors $a \equiv c \pmod{H}$.

Démonstration. Les trois affirmations sont des conséquences immédiates du fait que $a \equiv b \pmod{H}$ équivaut à $a + H = b + H$. □

7.6.8 Proposition. *Si $a, b, a', b' \in G$, alors*

$$\left.\begin{matrix} a \equiv a' \pmod{H} \\ b \equiv b' \pmod{H} \end{matrix}\right\} \implies \left\{\begin{matrix} a + b \equiv a' + b' \pmod{H} \\ -a \equiv -a' \pmod{H} \end{matrix}\right.$$

Démonstration. Si $a - a', b - b' \in H$, alors $(-a) - (-a') = -(a - a') \in H$ et $(a + b) - (a' + b') = (a - a') + (b - b') \in H$, car H est un sous-groupe de G et l'opération "+" vérifie $x + y = y + x$. □

7.6.9 Vers G/H On est prêt à montrer que l'ensemble G/H des classes modulo H dans G admet une structure naturelle d'un groupe abélien (ce qui va généraliser $(\mathbf{Z}/n\mathbf{Z}, +)$).

Il y a une projection naturelle

$$\mathrm{pr} : G \longrightarrow G/H, \qquad a \mapsto a + H = \overline{a}$$

qui assigne à un élément $a \in G$ l'unique classe modulo H contenant a.

7.6.10 Théorème. *Soit H un sous-groupe d'un groupe abélien $(G, +)$.*
*(1) L'ensemble G/H des classes modulo H dans G a une structure naturelle d'un groupe abélien (le **groupe quotient** de G par H) telle que*

(Opération)	$(a + H) + (b + H) = (a + b) + H$
(Inverse)	$-(a + H) = (-a) + H$
(Elément neutre)	$0_{G/H} = 0_G + H$

(2) La projection $\mathrm{pr} : G \longrightarrow G/H$ est un morphisme de groupes (surjectif).
(3) $\mathrm{Ker}(\mathrm{pr}) = H$.

Démonstration. (1) Les opérations sont **bien définies :** il faut montrer que les égalités $a + H = a' + H$ et $b + H = b' + H$ impliquent que $(a + b) + H = (a' + b') + H$ et $(-a) + H = (-a') + H$. On l'a démontré dans la proposition 7.6.8.

Associativité : il faut montrer que l'on a, pour tous $a, b, c \in G$,

$$(a + H) + ((b + H) + (c + H)) \stackrel{?}{=} ((a + H) + (b + H)) + (c + H)$$

C'est une conséquence du fait que le terme à gauche (resp. à droite) est égal à $(a + (b + c)) + H$ (resp. à $((a + b) + c) + H$).

Commutativité : il faut montrer que l'on a, pour tous $a, b \in G$,

$$(a+H)+(b+H) \stackrel{?}{=} (b+H)+(a+H)$$

C'est une conséquence du fait que le terme à gauche (resp. à droite) est égal à $(a+b)+H$ (resp. à $(b+a)+H$).

Elément neutre : il faut montrer que l'on a, pour tout $a \in G$,

$$(a+H)+(0+H) \stackrel{?}{=} a+H \stackrel{?}{=} (0+H)+(a+H)$$

C'est une conséquence du fait que le terme à gauche (resp. à droite) est égal à $(a+0)+H = a+H$ (resp. à $(0+a)+H = a+H$).

Inverse : il faut montrer que l'on a, pour tout $a \in G$,

$$(a+H)+((-a)+H) \stackrel{?}{=} 0+H \stackrel{?}{=} ((-a)+H)+(a+H)$$

C'est une conséquence du fait que le terme à gauche (resp. à droite) est égal à $(a+(-a))+H = 0+H$ (resp. à $((-a)+a)+H = 0+H$).

(2) Pour tous $a, b \in H$, on a

$$\mathrm{pr}(a+b) = (a+b)+H = (a+H)+(b+H) = \mathrm{pr}(a)+\mathrm{pr}(b).$$

(3) $a \in \mathrm{Ker}(\mathrm{pr}) \iff a+H = 0+H \iff a-0 \in H \iff a \in H.$ □

7.6.11 Remarque La preuve montre que les formules dans (1) sont déteminées par (2).

7.6.12 Exemples de G/H (le cas abélien) (1) Si $G = (\mathbf{Z}, +)$ et $H = n\mathbf{Z}$, alors $(G/H, +) = (\mathbf{Z}/n\mathbf{Z}, +)$ est l'ensemble des classes de congruence $(\mathrm{mod}\, n)$.

(2) Si $G = (\mathbf{R}^2, +)$ et $H = (\mathbf{R}u, +)$, où $0 \neq u \in \mathbf{R}^2$, alors H est une droite dans le plan G et G/H est l'ensemble de toutes les droites dans G qui sont parallèles à H. Dans cet exemple G/H n'est pas seulement un groupe abélien, mais un espace vectoriel réel (car G et H le sont). Choisissons $u' \in \mathbf{R}^2$ tel que u et u' soient linéairement indépendants sur $\mathbf{R}$. Dans ce cas $H' = \mathbf{R}u'$ est une droite dans le plan G qui est transverse à H, ce qui implique que l'application

$$H' \hookrightarrow G \xrightarrow{\mathrm{pr}} G/H \tag{7.6.12.1}$$

est bijective (son inverse envoie une droite $a+H$ parallèle à H sur l'intersection $(a+H) \cap H'$). L'application (7.6.12.1) est un morphisme de groupes bijectif, donc un isomorphisme de groupes.

En général, si V est un espace vectoriel sur un corps K et $W \subset V$ un sous-espace vectoriel, alors le groupe quotient $(V/W, +)$ a une structure naturelle d'un espace vectoriel sur K (**l'espace quotient** de V par W) si l'on définit multiplication par un scalaire $t \in K$ par

$$t(v+W) = (tv)+W, \qquad v \in V, \qquad t \in K.$$

Il faut vérifier les identités suivantes

$$(t+t')(v+W) \stackrel{?}{=} t(v+W)+t'(v+W)$$
$$t(t'(v+W)) \stackrel{?}{=} (tt')(v+W)$$
$$t((v+W)+(v'+W)) \stackrel{?}{=} t(v+W)+t(v'+W)$$

$(t, t' \in K,\ v, v' \in V)$, ce qui est facile.

Comme avant, si $W' \subset V$ est un sous-espace supplémentaire à W (autrement dit, si $V = W \oplus W'$), alors l'application linéaire

$$W' \hookrightarrow V \xrightarrow{\text{pr}} V/W \tag{7.6.12.2}$$

est bijective (son inverse envoie $a+W$ sur l'intersection $(a+W) \cap W'$). Il s'agit, donc, d'un isomorphisme des espaces vectoriels.

(3) $G = (\mathbf{R}, +)$, $H = 2\pi\mathbf{Z}$. Le quotient $(\mathbf{R}/2\pi\mathbf{Z}, +)$ admet l'interprétation géometrique suivante.

Pour tout $\alpha \in \mathbf{R}$ on note $R(\alpha)$ la rotation autour d'origine dans $\mathbf{R}^2$ d'angle orienté α. Ces rotations forment un groupe abélien (que l'on note $SO(2)$) par rapport à la composition. Plus précisement, on a

$$R(\alpha) = R(\beta) \iff \alpha \equiv \beta \pmod{2\pi\mathbf{Z}} \iff \alpha + 2\pi\mathbf{Z} = \beta + 2\pi\mathbf{Z} \tag{7.6.12.3}$$

$$R(\alpha) \circ R(\beta) = R(\alpha + \beta), \tag{7.6.12.4}$$

ce qui nous dit que l'application

$$\mathbf{R}/2\pi\mathbf{Z} \xrightarrow{\sim} SO(2), \qquad \alpha + 2\pi\mathbf{Z} \mapsto R(\alpha) \tag{7.6.12.5}$$

est un isomorphisme de groupes. Autrement dit, un angle orienté dans le plan $\mathbf{R}^2$ n'est rien d'autre qu'une classe $\alpha + 2\pi\mathbf{Z} \in \mathbf{R}/2\pi\mathbf{Z}$ des nombres réels modulo des multiples entiers de 2π.

7.6.13 Exercice. Déterminer l'ordre de $\frac{m}{n} + \mathbf{Z} \in (\mathbf{Q}/\mathbf{Z}, +)$, où $m, n \in \mathbf{Z}$, $n \geq 1$ et $\text{pgcd}(m, n) = 1$.

7.6.14 Notation multiplicative Si l'on utilise la notation multiplicative pour le groupe abélien $(G, \cdot)$ et son sous-groupe $H \subset G$, alors les classes modulo H dans G sont définies par

$$gH := \{gh \mid h \in H\}, \tag{7.6.14.1}$$

où $g \in G$. Comme avant, deux classes sont soit disjointes, soit égales. Plus précisement, $gH = g'H \iff g^{-1}g' \in H$.

L'ensemble G/H des classes est un groupe abélien pour l'opération $(gH)(g'H) = (gg')H$. L'élément neutre est $eH = H$ et l'inverse de gH est égal à $(gH)^{-1} = g^{-1}H$.

7.6.15 Théorème (Lagrange, le cas abélien)**.** *Si G est un groupe abélien fini et $H \subset G$ est un sous-groupe, alors on a $|G| = |H| \cdot |G/H|$. En particulier, $|H|$ divise $|G|$.*

Démonstration. On sait que G est une réunion disjointe de $|G/H|$ classes modulo H, et que le nombre d'éléments de chaque classe $a + H$ est égal à $|a + H| = |H|$. □

7.6.16 Théorème (théorème de l'homomorphisme, le cas abélien)**.** *Soit $(G, *)$ un groupe abélien, soit $f : (G, *) \longrightarrow (H, \square)$ un morphisme de groupes. L'application*

$$\begin{array}{rcl} \overline{f} : (G/\operatorname{Ker}(f), *) & \longrightarrow & (\operatorname{Im}(f), \square) \\ g \operatorname{Ker}(f) & \mapsto & f(g) \end{array}$$

est un isomorphisme de groupes. [On utilise la notation multiplicative pour G et $G/\operatorname{Ker}(f)$; voir le paragraphe 7.6.14.]

Démonstration. L'application $\overline{f}$ est **bien définie :** si $g \operatorname{Ker}(f) = g' \operatorname{Ker}(f)$, alors $g^{-1}g' \in \operatorname{Ker}(f)$, ce qui implique que $f(g') = f(gg^{-1}g') = f(g)f(g^{-1}g') = f(g) \square e_H = f(g)$.

L'application $\overline{f}$ est un **morphisme de groupes :**

$$\overline{f}((g\,\mathrm{Ker}(f))(g'\,\mathrm{Ker}(f))) = \overline{f}(gg'\,\mathrm{Ker}(f)) = f(gg') = f(g)\square f(g') = \overline{f}(g\,\mathrm{Ker}(f))\square\overline{f}(g'\,\mathrm{Ker}(f)).$$

Pour terminer la démonstration il suffit de vérifier que le noyau de $\overline{f}$ est trivial, compte tenu du corollaire 7.4.11. Si $g\,\mathrm{Ker}(f)$ appartient à $\mathrm{Ker}(\overline{f})$, alors $f(g) = e_H$, ce qui implique que $g \in \mathrm{Ker}(f)$, d'où $g\,\mathrm{Ker}(f) = \mathrm{Ker}(f)$ est bien l'élément neutre de $G/\mathrm{Ker}(f)$. □

7.6.17 Théorème de l'homomorphisme : exemples (1) Si $\mathrm{Ker}(f) = \{e_G\}$, on retrouve le corollaire 7.4.11 (pour un groupe abélien G).

(2) L'exponentielle $\exp : (\mathbf{C}, +) \longrightarrow (\mathbf{C}\smallsetminus\{0\}, \cdot)$ est un morphisme de groupes tel que $\mathrm{Ker}(\exp) = (2\pi i\mathbf{Z}, +)$ et $\mathrm{Im}(\exp) = \mathbf{C} \smallsetminus \{0\}$. Il induit un isomorphisme de groupes

$$(\mathbf{C}/2\pi i\mathbf{Z}, +) \xrightarrow{\sim} (\mathbf{C} \smallsetminus \{0\}, \cdot), \qquad z + 2\pi i\mathbf{Z} \mapsto e^z.$$

(3) Soit $(G, *)$ un groupe, soit $g \in G$ un élément d'ordre fini $m \in \mathbf{N}_+$. Le morphisme de groupes $f : (\mathbf{Z}, +) \longrightarrow (G, *)$ défini par $f(n) = g^n$ (voir le paragraphe 7.4.3, l'exemple 7) vérifie $\mathrm{Im}(f) = \langle g\rangle$ et $\mathrm{Ker}(f) = (m\mathbf{Z}, +)$. Il définit un isomorphisme de groupes

$$\overline{f} : (\mathbf{Z}/m\mathbf{Z}, +) \xrightarrow{\sim} \langle g\rangle, \qquad k + m\mathbf{Z} \mapsto g^k$$

que l'on a déjà vu dans le théorème 7.5.6(4).

(4) Une petite modification de l'exponentielle $f : (\mathbf{C}, +) \longrightarrow (\mathbf{C} \smallsetminus \{0\}, \cdot)$, $f(z) = e^{2\pi iz}$ est un morphisme de groupes surjectif vérifiant $\mathrm{Ker}(f) = (\mathbf{Z}, +)$. Il définit des isomorphismes de groupes

$$(\mathbf{C}/\mathbf{Z}, +) \xrightarrow{\sim} (\mathbf{C} \smallsetminus \{0\}, \cdot), \qquad (\mathbf{R}/\mathbf{Z}, +) \xrightarrow{\sim} (\{e^{2\pi i\alpha} \mid \alpha \in \mathbf{R}\}, \cdot) = (\{z \in \mathbf{C} \mid |z| = 1\}, \cdot) = U(1),$$
$$(\tfrac{1}{n}\mathbf{Z}/\mathbf{Z}, +) \xrightarrow{\sim} (\{z \in \mathbf{C} \mid z^n = 1\}, \cdot) = \mu_n, \qquad (\mathbf{Q}/\mathbf{Z}, +) \xrightarrow{\sim} \bigcup_{n\geq 1} \mu_n = \{\text{racines d'unité dans } \mathbf{C}\}.$$

7.6.18 Propriété universelle de G/H Soit H un sous-groupe d'un groupe abélien G. Pour tout morphisme de groupes $f : G \longrightarrow G'$ tel que $H \subset \mathrm{Ker}(f)$ il existe un unique morphisme de groupes $f' : G/H \longrightarrow G'$ vérifiant

$$f = f' \circ \mathrm{pr} : G \longrightarrow G/H \longrightarrow G'.$$

Cette formule est équivalente à $f'(gH) = f(g)$ pour tout $g \in G$. La condition $H \subset \mathrm{Ker}(f)$ implique que $f(g) = f(gh)$ pour tout $h \in H$, ce qui signifie que f' est bien défini (c'est un morphisme de groupes, car f l'est).

7.6.19 Que se passe-t-il si G n'est pas abélien ? Si $(G, *)$ est un groupe quelconque et $H \subset G$ est un sous-groupe, il faut distinguer **les classes à gauche (resp. à droite) de H dans G**

$$gH := \{gh \mid h \in H\} \subset G, \qquad Hg := \{hg \mid h \in H\} \subset G \qquad (g \in G).$$

La proposition 7.6.4 est encore valable, sous la forme suivante :

— $gH \cap g'H \neq \emptyset \iff g^{-1}g' \in H \iff gH = g'H$.

— L'application $H \longrightarrow gH$, $h \mapsto gh$ est bijective (son inverse $gH \longrightarrow H$ étant $g' \mapsto g^{-1}g'$).

Par conséquent, G est une réunion disjointe des classes gH, et le nombre d'éléments (fini ou infini) de chaque classe gH est le même que celui de H.

Si l'on note G/H l'ensemble des classes gH, on en déduit que $|G| = |H| \cdot |G/H|$ (voir la preuve du théorème 7.6.15).

De même, on note $H\backslash G$ l'ensemble des classes Hg. L'application $G/H \longrightarrow H\backslash G$, $gH \mapsto Hg^{-1}$ est bijective. L'indice de H dans G est défini par $(G : H) := |G/H| = |H\backslash G|$.

Il est naturel de se demander si l'ensemble G/H est un groupe pour l'opération

$$(g_1H)(g_2H) \stackrel{?}{=} (g_1g_2)H. \tag{7.6.19.1}$$

En général, la réponse est "non". Ce qui se passe c'est que la proposition 7.6.8 n'est pas valable en général dans le cas non-abélien, ce qui signifie que la formule (7.6.19.1) ne permet pas de définir une opération bien définie sur G/H.

Ce dont on a besoin à la place de la proposition 7.6.8 est la propriété suivante :

$$\left.\begin{matrix} g_1H = g_1'H \\ g_2H = g_2'H \end{matrix}\right\} \stackrel{?}{\Longrightarrow} (g_1g_2)H = (g_1'g_2')H. \tag{7.6.19.2}$$

On peut récrire cette condition sous la forme $(g_1g_2)H = (g_1h_1g_2h_2)H$ pour tous $g_i \in G$ et $h_i \in H$, ce qui équivaut à $g_2H = h_1g_2H$, donc à $H = g_2^{-1}h_1g_2H$ et $g_2^{-1}h_1g_2 \in H$ (pour tous $g_2 \in G$ et $h_1 \in H$). Autrement dit, il nous faut

$$\forall g \in G \quad g^{-1}Hg \subseteq H.$$

Si l'on applique cette condition avec g et g^{-1}, on obtient une condition équivalente

$$\forall g \in G \quad g^{-1}Hg = H. \tag{7.6.19.3}$$

Un sous-groupe $H \subset G$ qui vérifie (7.6.19.3) s'appelle un **sous-groupe distingué de** G (notation : $H \lhd G$). Cette propriété équivaut à $gH = Hg$ (pour tout $g \in G$), ce qui implique que

$$gH = g'H \implies Hg^{-1} = (gH)^{-1} = (g'H)^{-1} = Hg'^{-1} \implies g^{-1}H = g'^{-1}H. \tag{7.6.19.4}$$

En résumé, si $H \lhd G$ est un sous-groupe distingué, alors (7.6.19.2) et (7.6.19.4) impliquent que G/H est un groupe pour l'opération (7.6.19.1). Le reste du théorème 7.6.10 est vrai aussi : la projection $\mathrm{pr} : G \longrightarrow G/H$ définie par $\mathrm{pr}(g) = gH$ est un morphisme de groupes surjectif et $\mathrm{Ker}(\mathrm{pr}) = H$.

Réciproquement, le noyau de chaque morphisme de groupes $f : (G, *) \longrightarrow (H, \square)$ est un sous-groupe distingué de G. En effet, si $g' \in \mathrm{Ker}(f)$, alors $f(g') = e_H$ et $f(g^{-1}g'g) = f(g)^{-1}\square f(g')\square f(g) = f(g)^{-1}\square e_H \square f(g) = f(g)^{-1}\square f(g) = e_H$, d'où $g^{-1}g'g \in \mathrm{Ker}(f)$.

En particulier, les sous-groupes distingués de G sont précisement les noyaux des morphismes de groupes $G \longrightarrow G'$.

L'énoncé (ainsi que la démonstration) du théorème de l'homomorphisme 7.6.16 est alors valable pour n'importe quel morphisme de groupes.

La propriété universelle de G/H dans le paragraphe 7.6.18 est valable pour tout groupe G et tout sous-groupe distingué $H \lhd G$.

8 Anneaux

8.1 Définition et exemples

8.1.1 Exemple : $A = \mathbf{Z}$ L'exemple fondamental d'un anneau (commutatif) est l'ensemble des entiers relatifs $\mathbf{Z} = \{0, \pm 1, \pm 2, \cdots\}$ muni des opérations "+" et "$\cdot$". On a vu d'autres anneaux, par exemple $\mathbf{Z}/n\mathbf{Z}$ et des anneaux de matrices $M_k(\mathbf{R})$ (qui sont non-commutatifs si $k > 1$).

8.1.2 Définition. Un **anneau** (unitaire) est un triple $(A, +, \cdot)$, où A est un ensemble muni des opérations binaires $a, b \mapsto a + b$ (addition) et $a, b \mapsto a \cdot b = ab$ (multiplication) vérifiant les axiomes suivants.

(1) **(Structure additive)** $(A, +)$ est un groupe abélien avec un élément neutre $0 = 0_A$ et inverse $a \mapsto -a$

(2) **(Associativité)** $\forall a, b, c \in A \quad (a \cdot b) \cdot c = a \cdot (b \cdot c)$

(3) **(Unité)** $\exists 1 = 1_A \in A \; \forall a \in A \quad a \cdot 1 = 1 \cdot a = a$

(4) **(Distributivité)** $\forall a, b, c \in A \quad (a + b) \cdot c = (a \cdot c) + (b \cdot c), \quad a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ (8.1.2.1)

8.1.3 Définition. Si la propriété suivante est satisfaite

(5) **(Commutativité)** $\forall a, b \in A \quad a \cdot b = b \cdot a$

on dit que A est un **anneau commutatif**.

8.1.4 Propriétés de base

— $\forall a \in A \quad 0 \cdot a = a \cdot 0 = 0$ (car $0 \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a$).

— 1 **est unique :** s'il existe $1, 1' \in A$ tels que $\forall a, b \in A \quad a \cdot 1 = 1 \cdot a = a$ et $b \cdot 1' = 1' \cdot b = b$, alors on obtient pour $a = 1'$ et $b = 1$ que $1' = 1 \cdot 1' = 1$.

— $0 = 1$ dans $A \iff A = \{0\}$ (**l'anneau nul**). En effet, si $0 \neq 1$ dans A, alors $A \neq \{0\}$. Réciproquement, si $0 = 1$ dans A, alors on a $a = a \cdot 1 = a \cdot 0 = 0$ pour tout $a \in A$.

8.1.5 Exemples d'anneaux

(1) Anneaux commutatifs $\mathbf{Z}$, $\mathbf{Z}/n\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$, $\mathbf{Z} + i\mathbf{Z}$, $\mathbf{Z} + 2i\mathbf{Z}$, $\mathbf{Q} + i\mathbf{Q}$.

(2) Anneaux de matrices (non-commutatifs) $M_n(\mathbf{R})$, $M_n(\mathbf{C})$ $(n > 1)$. L'unité est la matrice identité $I = I_n$.

(3) Plus généralement, si V est un espace vectoriel sur un corps K, alors l'ensemble des endomorphismes K-linéaires de V

$$\mathrm{End}_K(V) := \{\alpha : V \longrightarrow V \mid \alpha \text{ est } K - \text{ linéaire}\}$$

est un anneau pour les opérations $(\alpha + \beta)(v) = \alpha(v) + \beta(v)$ et $(\beta \circ \alpha)(v) = \beta(\alpha(v))$ $(v \in V)$. L'unité est l'identité $\mathrm{id}_V : v \mapsto v$.

Bien sûr, si $V = K^n$, alors $\mathrm{End}_K(K^n) = M_n(K)$ (voir l'exemple (4) dans le paragraphe 7.2.4).

(4) Si A est un anneau quelconque (pas forcément commutatif), alors l'ensemble $M_n(A)$ des matrices $n \times n$ à coefficients dans A est un anneau pour addition et multiplication matricielle.

(5) Si A est un anneau commutatif, il en est de même pour l'anneau de polynômes $A[T] = \{a_0 + a_1 T + \cdots + a_d T^d \mid d \geq 0, \, a_i \in A\}$ en une variable à coefficients dans A. Par récurrence, on obtient des anneaux $A[T_1, \ldots, T_n]$ de polynômes en plusieures variables.

(6) On rencontre parfois des anneaux sans unité, mais il est très souvent le cas qu'il existe des "unités approximatives". Exemple : $A = \{\alpha \in \mathrm{End}_K(V) \mid \dim_K(\mathrm{Im}(\alpha)) < \infty\}$, où V est un espace vectoriel de dimension infinie sur un corps K.

8.1.6 Définition. Soit A un anneau. Un élément $a \in A$ est **inversible dans** A s'il existe $b \in A$ tel que $ab = ba = 1$. Un tel élément $b \in A$ est **unique** ; on l'appelle **l'inverse de** a et on écrit $b = a^{-1}$. L'ensemble des éléments inversibles de A

$$A^* := \{a \text{ inversible dans } A\}$$

est un groupe pour le produit (l'élément neutre étant 1). On appelle A^* **le groupe multiplicatif de** A.

8.1.7 Remarques sur l'inverse (1) Unicité de l'inverse : si $ab = ba = 1 = ac = ca$, alors $b = b \cdot 1 = b(ac) = (ba)c = 1 \cdot c = c$.

(2) $(A^*, \cdot)$ est un groupe : on a $1 \in A^*$, car $1 \cdot 1 = 1$. Si $a, a' \in A^*$, alors $ab = ba = 1 = a'b' = b'a'$ avec $b = a^{-1}$, $b' = a'^{-1}$. On en déduit que $(aa')(b'b) = a(a'b')b = a \cdot 1 \cdot b = ab = 1$ et $(b'b)(aa') = b'(ba)a' = b' \cdot 1 \cdot a' = b'a' = 1$. En particulier, $ab \in A^*$ et l'inverse $(ab)^{-1}$ de ab est égal à $b'a' = b^{-1}a^{-1}$ (voir aussi la proposition 7.1.6(5)). Si $a \in A^*$, alors $aa^{-1} = a^{-1}a = 1$, ce qui implique que $a^{-1} \in A^*$ et $(a^{-1})^{-1} = a$.

(3) Le raisonnement dans (1) ci-dessus montre un peu plus : si $b, c \in A$ vérifient $ba = 1 = ac$, alors $b = b \cdot 1 = b(ac) = (ba)c = 1 \cdot c = c$. Autrement dit, si $a \in A$ admet un **inverse à gauche** $b \in A$ ainsi qu'un **inverse à droite** $c \in A$, alors $b = c$, et cet élément est unique.

8.1.8 Eléments inversibles (exemples) (1) $\mathbf{R}^* = (\mathbf{R} \smallsetminus \{0\}, \cdot)$, $\mathbf{C}^* = (\mathbf{C} \smallsetminus \{0\}, \cdot)$, $\mathbf{Q}^* = (\mathbf{Q} \smallsetminus \{0\}, \cdot)$, $(\mathbf{Q} + \mathbf{Q}i)^* = ((\mathbf{Q} + \mathbf{Q}i) \smallsetminus \{0\}, \cdot)$, $\mathbf{Z}^* = (\{\pm 1\}, \cdot)$, $(\mathbf{Z} + \mathbf{Z}i)^* = (\{\pm 1, \pm i\}, \cdot)$, $(\mathbf{Z} + \mathbf{Z}\sqrt{2})^* = (\{\pm(1+\sqrt{2})^n \mid n \in \mathbf{Z}\}, \cdot)$, $(\mathbf{Z} + \mathbf{Z}\frac{1+\sqrt{5}}{2})^* = (\{\pm(\frac{1+\sqrt{5}}{2})^n \mid n \in \mathbf{Z}\}, \cdot)$.

(2) Soit A un anneau. Le groupe multiplicatif de l'anneau de matrices $M_n(A)$ sera noté

$$GL_n(A) := M_n(A)^* = \{M \in M_n(A) \mid \exists N \in M_n(A) \quad MN = NM = I_n\}.$$

8.1.9 Proposition. *Si A est un anneau commutatif, alors*

$$\begin{aligned} GL_n(A) &= \{M \in M_n(A) \mid \det(M) \in A^*\} \\ &= \{M \in M_n(A) \mid \exists N \in M_n(A) \quad MN = I_n\} \\ &= \{M \in M_n(A) \mid \exists N \in M_n(A) \quad NM = I_n\} \end{aligned}$$

Démonstration. Si $M, N \in M_n(A)$ vérifient $MN = I_n$, alors on a $\det(M)\det(N) = \det(I_n) = 1$, d'où $\det(M), \det(N) \in A^*$.
Réciproquement, si l'on note $\mathrm{adj}(M) \in M_n(A)$ la **matrice adjointe** de M (rappelons que $(-1)^{i+j}\mathrm{adj}(M)_{ij}$ est le déterminant de la matrice $(n-1) \times (n-1)$ qu'on obtient si l'on supprime la i-ème colonne et la j-ème ligne de M), alors on a

$$M \cdot \mathrm{adj}(M) = \mathrm{adj}(M) \cdot M = \det(M) I_n. \tag{8.1.9.1}$$

Par exemple, si $n = 2$, alors

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \qquad \mathrm{adj}(M) = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}, \qquad M \cdot \mathrm{adj}(M) = \mathrm{adj}(M) \cdot M = \begin{pmatrix} ad-bc & 0 \\ 0 & ad-bc \end{pmatrix}.$$

Si $\det(M) \in A^*$, alors les formules (8.1.9.1) impliquent que la matrice $N := (\det(M))^{-1}\mathrm{adj}(M) \in M_n(A)$ vérifie $MN = NM = I_n$. □

8.1.10 Exercice. Donner un exemple d'un élément a d'un anneau A qui a un inverse à gauche mais aucun inverse à droite (et réciproquement).
[Indication : on pourra prendre $A = \mathrm{End}_K(V)$, où V est un espace vectoriel de dimension infinie.]

8.1.11 Anneau produit Soient A_1, A_2 des anneaux. Leur produit

$$A = A_1 \times A_2 = \{(a_1, a_2) \mid a_i \in A_i\}$$

est un anneau muni des opérations

$$(a_1,a_2)+(b_1,b_2)=(a_1+b_1,a_2+b_2),\qquad (a_1,a_2)\cdot(b_1,b_2)=(a_1\cdot b_1,a_2\cdot b_2),$$
$$0_A=(0_{A_1},0_{A_2}),\qquad 1_A=(1_{A_1},1_{A_2}).$$

On a

$$A^*=A_1^*\times A_2^*=\{(a_1,a_2)\mid a_i\in A_i^*\},\qquad (a_1,a_2)^{-1}=(a_1^{-1},a_2^{-1}).$$

8.2 Sous-anneaux

8.2.1 Définition. Un **sous-anneau** d'un anneau A est un sous-ensemble $B\subset A$ qui est un anneau pour les opérations "$+$" et "$\cdot$" de A (ce qui implique que B a le même zéro 0 et la même unité 1 que A, que $B^*\subset A^*\cap B$ et que l'inverse de tout $b\in B^*$ est le même dans B et dans A).

8.2.2 Exemple : $\mathbf{Z}\subset\mathbf{C}$ $\mathbf{Z}$ est un sous-anneau de $\mathbf{C}$ et on a $\mathbf{Z}^*=\{\pm1\}\subsetneq\mathbf{Z}\cap\mathbf{C}^*=\mathbf{Z}\smallsetminus\{0\}$.

8.2.3 Proposition. *Soit $B\subset A$ un sous-ensemble d'un anneau A. Il est équivalent :*
(1) B est un sous-anneau de A ;
(2) $0_A,1_A\in B$ et $\forall b,b'\in B\quad b-b',bb'\in B$.
[En particulier, la Définition 8.2.1 est bien une généralisation de la définition d'un sous-anneau de $\mathbf{C}$ dans la Définition 1.5.18.]

Démonstration. L'implication (1) $\Longrightarrow$ (2) est automatique. Il faut montrer que (2) implique (1). On sait, d'après la proposition 7.2.3(3), que (2) implique que $(B,+)$ est un groupe abélien. Le reste est automatique. □

8.2.4 Exemples de sous-anneaux de $\mathbf{C}$ La proposition 8.2.3 implique que les sous-ensembles suivants de $\mathbf{C}$ sont tous des sous-anneaux de $\mathbf{C}$:

$$A_1=\mathbf{Z}+\mathbf{Z}\sqrt{6},\qquad A_2=\mathbf{Q}+\mathbf{Q}\sqrt{6},\qquad A_3=\mathbf{Z}+\mathbf{Z}\sqrt[3]{2}+\mathbf{Z}\sqrt[3]{4},\qquad A_4=\mathbf{Q}+\mathbf{Q}\sqrt[3]{2}+\mathbf{Q}\sqrt[3]{4}.\quad (8.2.4.1)$$

8.2.5 Exercice. (1) Tout sous-anneau de $\mathbf{C}$ contient $\mathbf{Z}$.
(2) Déterminer le plus petit sous-anneau de $\mathbf{C}$ contenant $2\sqrt{6}$ (resp. $\sqrt[4]{2}$, resp. $\sqrt{6}/2$).

8.2.6 Centre d'un anneau Le **centre**

$$Z(A):=\{z\in A\mid \forall a\in A\quad za=az\}$$

d'un anneau A est un sous-anneau de A. L'anneau A est commutatif $\iff Z(A)=A$.

8.2.7 Exercice. Soit A un anneau, soit $n\geq 1$. Montrer :

$$Z(M_n(A))=Z(A)\cdot I_n=\{a\cdot I_n\mid a\in Z(A)\}.$$

8.2.8 Exemple : C en tant qu'un sous-anneau de $M_2(\mathbf{R})$ Un nombre complexe $z = x + iy$ est donné par un couple de nombres réels $\begin{pmatrix} x \\ y \end{pmatrix}$, ce qui conduit à une identification des espaces vectoriels réels

$$\mathbf{C} \xrightarrow{\sim} \mathbf{R}^2, \qquad z = x + iy \mapsto \begin{pmatrix} x \\ y \end{pmatrix}$$

Cette identification nous permet d'écrire toute application $\mathbf{C}$-linéaire $\mathbf{C} \longrightarrow \mathbf{C}$ (i.e., une matrice complexe 1×1) comme une application $\mathbf{R}$-linéaire $\mathbf{R}^2 \longrightarrow \mathbf{R}^2$ (i.e., une matrice réelle 2×2).

Explicitement, multiplication par un nombre complexe $w = a+bi$ (que l'on a fixé) d'un nombre complexe variable $z = x + yi$ définit une application $\mathbf{R}$-linéaire

$$z = x + yi \mapsto wz = (a + bi)(x + yi) = (ax - by) + (bx + ay)i \tag{8.2.8.1}$$

$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} ax - by \\ bx + ay \end{pmatrix} = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \tag{8.2.8.2}$$

qui est représentée par la matrice $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$.

La représentation matricielle des nombres complexes qu'on vient de construire

$$M : \mathbf{C} \longrightarrow M_2(\mathbf{R}), \qquad M(a + bi) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \tag{8.2.8.3}$$

a les propriétés suivantes :

— $\forall a \in \mathbf{R} \quad M(a) = a \cdot I_2$ (en particulier, $M(1) = I_2$) ;
— $M(w + w') = M(w) + M(w')$ (car $(w + w')z = wz + w'z$) ;
— $M(ww') = M(w)M(w')$ (car $(ww')z = (ww')z$) ;
— $M(w) = 0 \iff w = 0$;
— plus généralement, $M(w) = M(w') \iff w = w'$.

Ces propriétés impliquent que l'on peut considérer $\mathbf{C}$ en tant qu'un sous-anneau de $M_2(\mathbf{R})$, dès que l'on identifie $w \in \mathbf{C}$ à la matrice $M(w)$. Plus précisement, si l'on utilise le langage de la Définition 8.4.1 ci-dessous, M est un morphisme injectif d'anneaux.

En résumé, $\mathbf{C} = M_1(\mathbf{C}) = \mathrm{End}_{\mathbf{C}}(\mathbf{C})$ est un sous-anneau de $\mathrm{End}_{\mathbf{R}}(\mathbf{C}) = \mathrm{End}_{\mathbf{R}}(\mathbf{R}^2) = M_2(\mathbf{R})$.

8.2.9 Exemple (suite) La restriction de M à l'ensemble des éléments inversibles de $\mathbf{C}$ fournit un morphisme de groupes injectif

$$M : \mathbf{C}^* \hookrightarrow GL_2(\mathbf{R}).$$

Remarquons que si $\alpha \in \mathbf{R}$, alors la matrice

$$M(e^{i\alpha}) = r(\alpha) = \begin{pmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{pmatrix}$$

représente la rotation de $\mathbf{R}^2$ autour d'origine d'angle orienté α. On déduit d'ici quatre versions algébriques différentes du groupe contenant toutes ces rotations :

$$\mathbf{R}/2\pi\mathbf{Z}, \qquad U(1) = \{z \in \mathbf{C} \mid z\overline{z} = 1\}, \qquad SO(2) = \{a \in M_2(\mathbf{R}) \mid {}^tAA = I_2\}, \qquad \{r(\alpha) \mid \alpha \in \mathbf{R}\}.$$

Voici des isomorphismes explicites entre ces groupes.

$$\mathbf{R}/2\pi\mathbf{Z} \xrightarrow{\sim} U(1), \qquad \alpha + 2\pi\mathbf{Z} \mapsto e^{i\alpha}; \qquad M : U(1) \xrightarrow{\sim} \{r(\alpha) \mid \alpha \in \mathbf{R}\} = SO(2).$$

8.3 Anneaux intègres, corps

8.3.1 Exemples (1) Produit de deux nombres complexes non nuls est toujours non nul.

(2) Dans l'anneau $A = \mathbf{Z}/6\mathbf{Z}$, les éléments $a = 2 \pmod 6 \in \mathbf{Z}/6\mathbf{Z} \smallsetminus \{0 \pmod 6\}$ et $b = 3 \pmod 6 \in \mathbf{Z}/6\mathbf{Z} \smallsetminus \{0 \pmod 6\}$ sont non nuls, mais leur produit est nul : $ab = 6 \pmod 6 = 0 \pmod 6$.

8.3.2 Définition. Soit A un anneau **commutatif**.
(1) On dit que A est un **anneau intègre** si $A \neq \{0\}$ et si le produit de deux éléments non nuls de A est non nul :

$$\forall a, b \in A \smallsetminus \{0\} \quad ab \neq 0$$

(formulation équivalente : $ab = 0 \Longrightarrow a = 0$ ou $b = 0$).
(2) A est un **corps** si $A \neq \{0\}$ et si tout élément non nul de A est inversible :

$$A \smallsetminus \{0\} = A^*.$$

(3) Un **sous-corps** d'un corps K est un sous-anneau de K qui est un corps.

8.3.3 Exemples et remarques (1) $\mathbf{Q}, \mathbf{R}, \mathbf{C}$ and $\mathbf{Q} + \mathbf{Q}i$ sont des corps (plus précisement, des sous-corps de $\mathbf{C}$), tandis que $\mathbf{Z}$ et $\mathbf{Z} + \mathbf{Z}i$ sont des anneaux intègres qui ne sont pas des corps.

(2) Il existe des anneaux non-commutatifs $A \neq \{0\}$ tels que $A \smallsetminus \{0\} = A^*$ (par exemple, l'anneau $\mathbf{H}$ des quaternions de Hamilton). On dit qu'un tel anneau est un **corps gauche** ou une **algèbre à division**.

(3) Si A est un anneau et si $a, b \in A$ vérifient $ab = 0$ et $a \in A^*$, alors $b = a^{-1}ab = a^{-1} \cdot 0 = 0$. Par conséquent, tout corps est un anneau intègre.

(4) Tout sous-anneau d'un anneau intègre (en particulier, tout sous-anneau d'un corps) est un anneau intègre.

(5) Réciproquement, on peut montrer que tout anneau intègre A est un sous-anneau d'un corps K qu'on construit en termes des fractions dont les numérateurs et dénominateurs appartient à A (exemple : $\mathbf{Z} \subset \mathbf{Q}$). On a

$$K = \left\{ \frac{a}{b} \mid a, b \in A,\, b \neq 0 \right\}, \qquad \frac{a}{b} = \frac{c}{d} \iff ad - bc = 0 \in A, \quad \frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd},$$
$$0_K = \frac{0}{1}, \qquad 1_K = \frac{1}{1},$$

mais il faut montrer que les conditions ci-dessus ne sont pas contradictoires, que les axiomes (8.1.2.1) sont vérifiés par K, et que K est bien un corps, avec l'inverse $(\frac{a}{b})^{-1} = \frac{b}{a}$. On dit que K est le **corps des fractions de** A.

8.3.4 Exercice. Lesquels parmi les anneaux A_j dans (8.2.4.1) sont des corps ?

8.3.5 Proposition. *Soit $n \geq 1$ un entier. Il est équivalent :*
(1) $\mathbf{Z}/n\mathbf{Z}$ est un corps.
(2) $\mathbf{Z}/n\mathbf{Z}$ est un anneau intègre.
(3) $n = p$ st un nombre premier.

Démonstration. (1) $\Longrightarrow$ (2) : cette implication est automatique.
(2) $\Longrightarrow$ (3) : on suit l'exemple 2 du paragraphe 8.3.1. Si $n \neq p$ n'est pas un nombre premier, alors soit $n = 1$ (où $\mathbf{Z}/n\mathbf{Z} = \{0\}$), soit $n = kl$ avec des entiers $1 < k, l < n$. Les classes de congruence $a = k \pmod n$ et $b = l \pmod n$ $\mathbf{Z}/n\mathbf{Z}$ sont alors non nuls dans $\mathbf{Z}/n\mathbf{Z}$, mais leur produit est nul : $ab = kl \pmod n = 0 \pmod n \in \mathbf{Z}/n\mathbf{Z}$.

(3) $\Longrightarrow$ (1) : si $n = p$ est un nombre premier, alors $\varphi(p) = p - 1 > 0$, ce qui implique que $(\mathbf{Z}/p\mathbf{Z})^* = \mathbf{Z}/p\mathbf{Z} \smallsetminus \{0\} \neq \emptyset$. □

8.3.6 Un anneau intègre fini est un corps L'implication non triviale (2) $\Longrightarrow$ (1) dans la proposition 8.3.5 est un cas particulier de l'énoncé abstrait suivant.

8.3.7 Proposition. *Soit $A \neq \{0\}$ un anneau commutatif qui a un nombre fini d'éléments. Il est équivalent :*

(1) A est un corps.
(2) A est un anneau intègre.

Démonstration. L'implication (1) $\Longrightarrow$ (2) est automatique. Réciproquement, si (2) est vrai, alors l'application

$$m_a : A \longrightarrow A, \qquad b \mapsto ab$$

est injective, pour tout $a \in A \smallsetminus \{0\}$. Une application injective entre deux ensembles finis du même cardinal est bijective. Par conséquent, il existe $b \in A$ tel que $1 = m_a(b) = ab$, ce qui signifie que a est inversible et $b = a^{-1}$. □

8.3.8 Un anneau intègre de dimension fini (sur un corps) est un corps La proposition 8.3.7 admet l'analogue suivant dans un cadre d'algèbre linéaire.

8.3.9 Exercice. On suppose que A est un anneau commutatif et que K est un corps qui est un sous-anneau de A. Montrer :
(1) A est un K-espace vectoriel par rapport à la restriction à $K \times A \longrightarrow A$ de la multiplication $A \times A \longrightarrow A$.
(2) Si la dimension de A sur K est finie, alors il est équivalent : A est un corps $\iff$ A est un anneau intègre.
(3) Résoudre l'exercise 8.3.4 en utilisant (2).

8.3.10 Divisibilité Soit A un anneau commutatif. On définit la notion de divisibilité dans A de la façon usuelle : si $a, b \in A$, on dit que b **divise** a (notation : $b \mid a$) s'il existe $c \in A$ tel que $a = bc$ (ce qui équivaut à $bA \supseteq aA$).

Les propriétés de divisibilité qu'on a vu dans le paragraphe 1.1.5 restent valables, avec les modifications suivantes :

- $b \mid 1 \iff b \in A^*$
- si $u \in A^*$, alors il est équivalent : $b \mid a \iff b \mid au$
- si A est un anneau intègre, si $a, b \in A \smallsetminus \{0\}$ vérifient $b \mid a$ et $a \mid b$, alors il existe $u \in A^*$ tel que $b = au$.

8.3.11 Eléments irréductibles Soit A un anneau intègre. Un élément $a \in A$ est **irréductible dans** A si l'on a :

- $a \neq 0$
- $a \notin A^*$
- a n'est pas un produit non trivial : si $a = bc$ avec $b, c \in A$, alors $b \in A^*$ ou $c \in A^*$ (mais pas simultanément, car $a \notin A^*$).

A noter : si a est irréductible dans A et si $u \in A^*$, alors au l'est aussi.

Exemple : $\{$éléments irréductibles dans $\mathbf{Z}\} = \{\pm p \mid p \text{ prime}\}$.

8.4 Morphismes d'anneaux

8.4.1 Définition. Soient A, B des anneaux. Une application $f : A \longrightarrow B$ est un **morphisme d'anneaux** si l'on a :
(1) $\forall a, a' \in A \quad f(a + a') = f(a) + f(a')$.
(2) $\forall a, a' \in A \quad f(aa') = f(a)f(a')$.
(3) $f(1_A) = 1_B$.

8.4.2 Remarques et exemples (1) La condition (1) dans la Définition 8.4.1 implique que f définit un morphisme de groupes additifs $f : (A, +) \longrightarrow (B, +)$ (d'où $f(0_A) = 0_B$ et $f(-a) = -f(a)$ pour tout $a \in A$). De même, les conditions (2) et (3) impliquent que $f(A^*) \subset B^*$ et que f définit un morphisme de groupes multiplicatifs $f : (A^*, \cdot) \longrightarrow (B^*, \cdot)$ (en particulier, si $a \in A^*$, alors $f(a) \in B^*$ et $f(a)^{-1} = f(a^{-1})$).

(2) La projection $\mathrm{pr} : \mathbf{Z} \longrightarrow \mathbf{Z}/n\mathbf{Z}$, $\mathrm{pr}(a) = a \pmod n$ est un morphisme d'anneaux.

(3) De même, l'application $\mathbf{Z}/mn\mathbf{Z} \longrightarrow \mathbf{Z}/n\mathbf{Z}$ définie par $a \pmod{mn} \mapsto a \pmod n$ est un morphisme d'anneaux.

(4) Soient A_1, A_2 des anneaux. Les projections $A_1 \xleftarrow{\mathrm{pr}_1} A_1 \times A_2 \xrightarrow{\mathrm{pr}_2} A_2$, $\mathrm{pr}_j(a_1, a_2) = a_j$ sont des morphismes d'anneaux.

(5) L'inclusion d'un sous-anneau $B \hookrightarrow A$ est un morphisme d'anneaux.

(6) **Attention :** les conditions (1) et (2) dans la Définition 8.4.1 **n'impliquent pas** (3), en général. Par exemple, l'application $f : \mathbf{Z}/6\mathbf{Z} \longrightarrow \mathbf{Z}/6\mathbf{Z}$ définie par $f(a \pmod 6) := 3a \pmod 6$ vérifie $3(a + a') \equiv 3a + 3a' \pmod 6$ et $3(aa') \equiv (3a)(3a') \pmod 6$ (since $3 \equiv 3^2 \pmod 6$), mais $3 \cdot 1 \not\equiv 1 \pmod 6$.

(7) De même, les inclusions $A_1 \xrightarrow{i_1} A_1 \times A_2 \xleftarrow{i_2} A_2$ définies par $i_1(a_1) = (a_1, 0)$ et $i_2(a_2) = (0, a_2)$ vérifient les conditions (1) et (2) dans la Définition 8.4.1, mais (3) n'est pas satisfaite (si $A_1, A_2 \neq \{0\}$).

(8) Pour tout anneau A il existe un unique morphisme d'anneaux $f : \mathbf{Z} \longrightarrow A$. En effet, un tel morphisme v'erifie $f(0) = 0_A$, $f(1) = 1_A$, $f(2) = f(1+1) = f(1)+f(1) = 1_A+1_A$, $f(3) = f(2)+f(1) = 1_A+1_A+1_A$, $f(-1) = -f(1) = -1_A$, $f(-2) = -(1_A + 1_A)$ etc. Autrement dit, si l'on définit, pour $m \in \mathbf{N}_+$ et $a \in A$,

$$m \cdot a := \underbrace{a + \cdots + a}_{m \text{ fois}}, \qquad (-m) \cdot a := -\underbrace{a + \cdots + a}_{m \text{ fois}}, \qquad 0 \cdot a := 0_A,$$

alors f est forcément défini par $f(n) = n \cdot 1_A$ ($n \in \mathbf{Z}$), ce qui montre l'unicité de f. Réciproquement, la proposition 7.3.2 avec $G = (A, +)$ et $g = 1_A$ affirme que $f(m)+f(n) = f(m+n)$. La propriété multiplicative $f(mn) = f(m)f(n)$ est une conséquence de la distributivité 8.1.2.1(4). On a aussi $f(1) = 1_A$.

Remarquons que $f(\mathbf{Z}) = \{n \cdot 1_A \mid n \in \mathbf{Z}\} \subset Z(A)$ est contenu dans le centre $Z(A)$ de A.

(9) Si $f : A \longrightarrow B$ et $g : B \longrightarrow C$ sont des morphismes d'anneaux, leur composition $g \circ f : A \longrightarrow B \longrightarrow C$ l'est aussi.

(10) Si $f_i : A_i \longrightarrow B_i$ ($i = 1, 2$) sont des morphismes de groupes, alors $f_1 \times f_2 : A_1 \times A_2 \longrightarrow B_1 \times B_2$ l'est aussi.

(11) Si p est un nombre premier et si A est un anneau commutatif tel que $p \cdot 1_A = 0_A$, alors l'application $\varphi : A \longrightarrow A$ définie par $\varphi(a) = a^p$ est un morphisme d'anneaux (on l'appelle le **morphisme de Frobenius**). En effet, $\varphi(1_A) = 1_A$, $\varphi(ab) = (ab)^p = a^p b^p = \varphi(a)\varphi(b)$ et

$$\varphi(a + b) = (a + b)^p = a^p + b^p + \sum_{j=1}^{p-1} \binom{p}{j} a^j b^{p-j} = a^p + b^p = \varphi(a) + \varphi(b),$$

car $\binom{p}{j} \in p\mathbf{Z}$ si $1 \leq j \leq p - 1$. Pour tout $n \geq 1$, la composition $\varphi \circ \cdots \circ \varphi : A \longrightarrow A$ de n exemplaires de φ est définie par $a \mapsto \varphi_q(a) = a^q$, où $q = p^n$. D'après (9), c'est aussi un morphisme d'anneaux.

8.4.3 Proposition. *Si un morphisme d'anneaux $f : A \longrightarrow B$ est bijectif, alors son inverse $f^{-1} : B \longrightarrow A$ est aussi un morphisme d'anneaux. On dit que f est un* ***isomorphisme d'anneaux*** *(ce qui implique que f^{-1} est aussi un isomorphisme d'anneaux).*

Démonstration. Soient $b, b' \in B$; on pose $a = f^{-1}(b), a' = f^{-1}(b') \in A$. Les identités $f(a + a') = f(a) + f(a') = b + b'$ et $f(aa') = f(a)f(a') = bb'$ impliquent que $f^{-1}(b + b') = a + a' = f^{-1}(b) + f^{-1}(b')$ et $f^{-1}(bb') = aa' = f^{-1}(b)f^{-1}(b')$. On a aussi $f^{-1}(1_B) = f^{-1}(f(1_A)) = 1_A$. Par conséquent $f^{-1} : B \longrightarrow A$ est un morphisme d'anneaux. □

8.4.4 Exemple : le théorème chinois Soient $m, n \geq 1$ des entiers tels que $\mathrm{pgcd}(m, n) = 1$. L'application bijective

$$f : \mathbf{Z}/mn\mathbf{Z} \longrightarrow \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}, \qquad f(a \pmod{mn}) = (a \pmod{m}, a \pmod{n})$$

dans le théorème chinois est un morphisme d'anneaux. Il s'agit, donc, d'un isomorphisme d'anneaux.

8.4.5 Exercice. Expliquer, un utilisant le théorème chinois, pouquoi l'exemple 6 dans le paragraphe 8.4.2 est un cas particulier de l'exemple 7.

8.4.6 Définition. Le noyau et **l'image** d'un morphisme d'anneaux $f : A \longrightarrow B$ sont définis, respectivement, par

$$\mathrm{Ker}(f) := \{a \in A \mid f(a) = 0\} \subset A, \qquad \mathrm{Im}(f) := \{f(a) \mid a \in A\} \subset B.$$

8.4.7 Proposition. *Si $f : A \longrightarrow B$ est un morphisme d'anneaux, alors on a :*
(1) $\mathrm{Im}(f)$ *est un sous-anneaux de B.*
(2) Si f est injectif, alors f définit un isomorphisme d'anneaux $A \xrightarrow{\sim} \mathrm{Im}(f)$.
(3) Soient $a, a' \in A$. Il est équivalent : $f(a) = f(a') \iff a' - a \in \mathrm{Ker}(f)$.
(4) f est injectif $\iff \mathrm{Ker}(f) = \{0\}$.

Démonstration. (1) On sait que $f(1_A) = 1_B$ et $f(0_A) = 0_B$, d'où $0_B, 1_B \in \mathrm{Im}(f)$. Si $b, b' \in \mathrm{Im}(f)$, alors il existe $a, a' \in A$ tels que $b = f(a)$ et $b' = f(a')$. Par conséquent, $b - b' = f(a - a') \in \mathrm{Im}(f)$ et $bb' = f(aa') \in \mathrm{Im}(f)$. D'après la proposition 8.2.3, $\mathrm{Im}(f)$ est bien un sous-anneau de B.
(2) C'est une conséquence des définitions.
(3) C'est un cas particulier de la proposition 7.4.6(3), avec $G = (A, +)$ et $H = (B, +)$. On peut aussi raisonner directement : $f(a) = f(a') \iff 0 = f(a') - f(a) = f(a' - a) \iff a' - a \in \mathrm{Ker}(f)$.
(4) C'est un cas particulier de la proposition 7.4.10 avec $G = (A, +)$ et $H = (B, +)$ (ou une conséquence directe de (3)). □

8.4.8 Corollaire. *Si un morphisme d'anneaux $f : A \longrightarrow B$ vérifie $\mathrm{Ker}(f) = \{0\}$, alors il est injectif, ce qui implique que f définit un isomorphisme d'anneaux $f : A \xrightarrow{\sim} \mathrm{Im}(f)$.*

8.4.9 $\mathrm{Ker}(f), \mathrm{Im}(f)$ **: Exemples** (1) L'inclusion d'un sous-anneaux $B \subset A$: $\mathrm{Ker} = \{0\}$, $\mathrm{Im} = B$.
(2) Projection $\mathrm{pr} : \mathbf{Z} \longrightarrow \mathbf{Z}/n\mathbf{Z}$: $\mathrm{Ker}(\mathrm{pr}) = n\mathbf{Z}$, $\mathrm{Im}(\mathrm{pr}) = \mathbf{Z}/n\mathbf{Z}$.
(3) Projection $\mathbf{Z}/mn\mathbf{Z} \longrightarrow \mathbf{Z}/n\mathbf{Z}$: $\mathrm{Ker} = n\mathbf{Z}/mn\mathbf{Z}$, $\mathrm{Im}(\mathrm{pr}) = \mathbf{Z}/n\mathbf{Z}$.
(4) Projections $\mathrm{pr}_j : A_1 \times A_2 \longrightarrow A_j$ $(\mathrm{pr}(a_1, a_2) = a_j)$: $\mathrm{Im}(\mathrm{pr}_j) = A_j$, $\mathrm{Ker}(\mathrm{pr}_1) = \{0\} \times A_2$, $\mathrm{Ker}(\mathrm{pr}_2) = A_1 \times \{0\}$.

8.4.10 Exercice. (1) Sous les hypothèses du paragraphe 8.4.2, exemple 4, les éléments

$$e_1 := i_1(1_{A_1}) = (1_{A_1}, 0_{A_2}) = (1, 0) \in A_1 \times A_2, \qquad e_2 := i_2(1_{A_2}) = (0_{A_1}, 1_{A_2}) = (0, 1) \in A_1 \times A_2$$

satisfont aux propriétés suivantes (ils forment un **système complet d'idempotents orthogonaux centraux dans** $A_1 \times A_2$) :

(e_1, e_2 sont centraux)	$e_1, e_2 \in Z(A_1 \times A_2)$
(e_1, e_2 sont idempotents)	$e_1^2 = e_1,\ e_2^2 = e_2$
(e_1, e_2 sont orthogonaux)	$e_1 e_2 = e_2 e_1 = 0$
	$e_1 + e_2 = 1$

(2) Réciproquement, si A est un anneau et si $e_1, e_2 \in A$ sont des éléments de A qui satisfont aux quatre propriétés dans (1), alors le sous-ensemble $A_j := e_j A = A e_j = \{e_j a = a e_j \mid a \in A\} \subset A$ muni des opérations "+" et "$\cdot$" de A est un anneau avec unité e_j ($j = 1, 2$), et l'application

$$A \longrightarrow A_1 \times A_2, \qquad a \mapsto (e_1 a, e_2 a)$$

et un isomorphisme d'anneaux.

8.4.11 Exercice. Soit A un anneau commutatif. On sait qu'il existe un unique morphisme d'anneaux $\mathbf{Z} \longrightarrow A$. Peut-on classifier les morphismes d'anneaux $\mathbf{Z} \times \mathbf{Z} \longrightarrow A$?

8.4.12 Exercice. Soient $(G, +)$ et $(H, +)$ des groupes abéliens. Montrer :
(1) L'ensemble $\mathrm{Hom}_{Ab}(G, H) := \{\text{morphismes de groupes } f : G \longrightarrow H\}$ est un groupe abélien pour l'opération $(f_1 + f_2)(g) := f_1(g) + f_2(g)$.
(2) L'ensemble $\mathrm{End}_{Ab}(G) := \mathrm{Hom}_{Ab}(G, G)$ est un anneau, où le produit de $f_1, f_2 \in \mathrm{End}_{Ab}(G)$ est la composition $f_f \circ f_2$.
(3) $\mathrm{End}_{Ab}((\mathbf{Z}, +)) = \mathbf{Z}$ et $\mathrm{End}_{Ab}((\mathbf{Z}^2, +)) = M_2(\mathbf{Z})$.

8.5 L'anneau quotient A/I

8.5.1 Introduction L'objectif de ce paragraphe est de développer une version abstraite de la construction de l'anneau $(\mathbf{Z}/n\mathbf{Z}, +, \cdot)$.

8.5.2 Multiplication de congruences D'ici jusqu'a fin du paragraphe 8.5 on suppose que

— A est un anneau ;

— $I \subset (A, +)$ est un sous-groupe additif.

On va utiliser la notation du paragraphe 7.6 : si $a, b \in A$, on écrit $a \equiv b \pmod I$ si et seulement si $a - b \in I$ (ce qui équivaut à $a + I = b + I$).

D'après la proposition 7.6.8 on peut additionner et soustraire des congruences : on a, pour tous $a, b, a', b' \in A$,

$$\left.\begin{matrix} a \equiv a' \pmod I \\ b \equiv b' \pmod I \end{matrix}\right\} \implies a \pm b \equiv a' \pm b' \pmod I.$$

Quand est-ce qu'on peut multiplier des congruences $\pmod I$? Autrement dit, quand est-ce qu'on a

$$\left.\begin{matrix} a \equiv a' \pmod I \\ b \equiv b' \pmod I \end{matrix}\right\} \overset{?}{\implies} ab \equiv a'b' \pmod I \ ? \tag{8.5.2.1}$$

Si l'implication 8.5.2.1 est valable, alors la preuve du théorème 7.6.10 implique que l'ensemble $A/I = \{a + I \mid a \in A\}$ des classes de congruence $\pmod I$ dans A est un anneau pour lequel la projection $\mathrm{pr} : A \longrightarrow A/I$ ($\mathrm{pr}(a) = a + I$) est un morphisme d'anneaux.

8.5.3 Multiplication de congruences : exemples (1) Si $A = \mathbf{Z}$ et $I = n\mathbf{Z}$, alors (8.5.2.1) est vrai.
(2) Si $A = \mathbf{R}$ et $I = 2\pi\mathbf{Z}$, alors (8.5.2.1) **n'est pas vrai**. En effet, on a, pour tout $a \in \mathbf{R} \smallsetminus \mathbf{Z}$,

$$\begin{aligned} a &\equiv a \pmod{2\pi\mathbf{Z}} \\ 0 &\equiv 2\pi \pmod{2\pi\mathbf{Z}} \\ \underbrace{a \cdot 0}_{0} &\not\equiv \underbrace{a \cdot 2\pi}_{2\pi a} \pmod{2\pi\mathbf{Z}} \end{aligned}$$

Par conséquent, **on ne peut pas multiplier deux angles** $\alpha, \beta \in \mathbf{R}/2\pi\mathbf{Z}$.

8.5.4 Théorème. *Un sous-groupe additif $I \subset (A, +)$ d'un anneau A vérifie* (8.5.2.1) *si et seulement si $AI \subset I$ et $IA \subset I$; autrement dit, si*

$$\forall a \in A \ \forall x \in I \quad ax \in I,\ xa \in I.$$

Si c'est le cas, on dit que I est un ***idéal (bilatère)*** *de A.*

Démonstration. Soient $a \in A$ et $x \in I$. Si (8.5.2.1) est vrai, alors on a

$$\left.\begin{matrix} a \equiv a \pmod{I} \\ 0 \equiv x \pmod{I} \end{matrix}\right\} \implies a \cdot 0 \equiv a \cdot x \pmod{I} \implies ax \in I \tag{8.5.4.1}$$

et

$$\left.\begin{matrix} 0 \equiv x \pmod{I} \\ a \equiv a \pmod{I} \end{matrix}\right\} \implies 0 \cdot a \equiv x \cdot a \pmod{I} \implies xa \in I. \tag{8.5.4.2}$$

Réciproquement, si $ax \in I$ et $xa \in I$ dès que $a \in A$ et $x \in I$, alors

$$\left.\begin{matrix} a \equiv a' \pmod{I} \\ b \equiv b' \pmod{I} \end{matrix}\right\} \implies a - a', b - b' \in I \implies ab - a'b' = (a - a')b + a'(b - b') \in IA + AI \subset I + I \subset I. \tag{8.5.4.3}$$

□

8.5.5 Exemples d'idéaux (bilatères) (1) $\{0\}$ et A sont des idéaux (bilatères) de A.
(2) Un sous-ensemble non vide $I \subset A$ est un idéal (bilatère) si (et seulement si)

$$\forall x, y \in I \ \forall a \in A \quad x + y \in I,\ ax \in I,\ xa \in I.$$

En effet, si l'on prend $a = 0_A$ resp. $a = -1_A$ on obtient que $0_A \in I$ et $-x \in I$ si $x \in I$. On en déduit que I est un sous-groupe de $(A, +)$, d'après la proposition 7.2.3(3).
(3) Si I, J sont des idéaux (bilatères) de A, alors $I + J := \{x + y \mid x \in I, y \in J\}$, $I \cap J$ et $IJ := \{x_1y_1 + \cdots + x_ry_r \mid r \geq 0, x_i \in I, y_i \in J\}$ le sont aussi.
(4) Le noyau $\mathrm{Ker}(f) = \{a \in A \mid f(a) = 0_B\}$ de tout morphisme d'anneaux $f : A \longrightarrow B$ est un idéal (bilatère) de A. En effet, $\mathrm{Ker}(f)$ est un sous-groupe de $(A, +)$, et si $a \in A$ et $x \in \mathrm{Ker}(f)$, alors $f(x) = 0$ et $f(ax) = f(a)f(x) = f(a) \cdot 0 = 0$, ce qui implique que $ax \in \mathrm{Ker}(f)$ (de même, $f(xa) = f(x)f(a) = 0 \cdot f(a) = 0$, d'où $xa \in \mathrm{Ker}(f)$).
(5) Réciproquement, le théorème 8.5.9 ci-dessous affirme que tout idéal (bilatère) $I \subset A$ est le noyau d'un morphisme (surjectif) d'anneaux $A \longrightarrow A/I$. Par conséquent, on a

$$\{\text{idéaux (bilatères) de } A\} = \{\text{noyaux des morphismes d'anneaux } A \longrightarrow B\} = \\ = \{\text{noyaux des morphismes surjectifs d'anneaux } A \longrightarrow B\}$$

(6) Si $f : A \longrightarrow B$ est un morphisme d'anneaux et si $J \subset B$ est un idéal (bilatère) de B, alors $I := f^{-1}(J) = \{a \in A \mid f(a) \in J\}$ est un idéal (bilatère) de A.

(7) Si l'anneau A est commutatif, alors les conditions $ax \in I$ et $xa \in I$ dans le théorème 8.5.4 sont équivalentes. On supprime l'adjectif "bilatère" et on dit tout simplement que I est un **idéal de** A.

(8) Soit A un anneau commutatif. L'exemple le plus simple d'un idéal $I \subset A$ est **l'idéal principal engendré par** $x \in A$

$$(x) := xA = Ax = \{ax \mid a \in A\}$$

qui contient tous les multiples de x. On a $(x) = (ux)$, pour tout élément inversible $u \in A^*$.

Plus généralement, si $x_1, \ldots, x_r \in A$, alors le sous-ensemble

$$(x_1, \ldots, x_r) := (x_1) + \cdots + (x_r) = Ax_1 + \cdots + Ax_r = \{a_1x_1 + \cdots + a_rx_r \mid a_i \in A\}$$

est un idéal de A que l'on appelle **l'idéal engendré par** $x_1, \ldots, x_r$ (il est contenu dans chaque idéal $I \subset A$ contenant $x_1, \ldots, x_r$).

(9) Un sous-ensemble $I \subset \mathbf{Z}$ est un idéal $\iff$ $I \subset (\mathbf{Z}, +)$ est un sous-groupe additif ($\iff$ $I = d\mathbf{Z} = (d) = (-d)$, où $d \in \mathbf{N}$). Autrement dit, tout idéal de $\mathbf{Z}$ est principal.

(10) Si A est un anneau commutatif est si $I \subset A$ est un idéal contenant un élément inversible $u \in A^*$, alors I contient $u \cdot (u^{-1}a) = a$, pour tout $a \in A$; par conséquent, $I = A = (1)$.

(11) En particulier, si $A = K$ est un corps, les seuls idéaux de K sont $(0) = \{0\}$ et $(1) = K$, car tout élément non nul de K est inversible.

(12) Un sous-ensemble $I \subset \mathbf{Z}/n\mathbf{Z}$ est un idéal $\iff$ il existe $d \mid n$ tel que $I = d\mathbf{Z}/n\mathbf{Z}$.

(13) Si l'anneau A n'est pas commutatif, on peut définir deux notions plus faibles d'idéaux. Un sous-groupe $I \subset (A, +)$ du groupe additif de A est un **idéal à gauche** (resp. un **idéal à droite**) si l'on a $ax \in I$ (resp. $xa \in I$), pour tout $a \in A$ et $x \in I$. En particulier, I est un idéal bilatère $\iff$ c'est un idéal à gauche et un idéal à droite.

Exemple : soit $A = M_n(K)$, où K est un corps. On note, pour tout sous-espace vectoriel $W \subset K^n$,

$$I_W := \{M \in M_n(K) \mid \text{toutes les colonnes de } M \text{ appartiennent à } W\},$$
$${}^tI_W := \{M \in M_n(K) \mid \text{toutes les colonnes de } {}^tM \text{ appartiennent à } W\}.$$

On peut montrer que l'on a

$$\{\text{idéaux à droite de } M_n(K)\} = \{I_W \mid W \subset K^n\}, \qquad \{\text{idéaux à gauche } M_n(K)\} = \{{}^tI_W \mid W \subset K^n\},$$
$$\{\text{idéaux bilatères de } M_n(K)\} = \{\{0\}, M_n(K)\}.$$

8.5.6 Exercice. Soient $m, n \in \mathbf{Z} \smallsetminus \{0\}$. Montrer :

$$(m) + (n) = (\text{pgcd}(m, n)), \qquad (m)(n) = (mn), \qquad (m) \cap (n) = (\text{ppcm}(m, n)).$$

8.5.7 Exercice. Soit K un corps, soit $B \neq \{0\}$ un anneau. Montrer que tout morphisme d'anneaux $f : K \longrightarrow B$ est injectif. Que se passe-t-il si l'on remplace K par $M_n(K)$, où $n > 1$?

8.5.8 Exercice. Soit A un anneau commutatif.
(1) Un élément $a \in A$ est dit **nilpotent** s'il existe un entier $n \geq 1$ tel que $a^n = 0$. Montrer que le **nilradical de** A $\mathrm{Nil}(A) := \{a \in A \mid a \text{ est nilpotent}\}$ est un idéal de A.
(2) Si A est un anneau intègre, alors $\mathrm{Nil}(A) = \{0\} = (0)$.
(3) Déterminer $\mathrm{Nil}(\mathbf{Z}/6\mathbf{Z})$, $\mathrm{Nil}(\mathbf{Z}/12\mathbf{Z})$ et $\mathrm{Nil}(\mathbf{Z}/n\mathbf{Z})$, pour tout $n \in \mathbf{N}_+$.
(4) Si $f : A \longrightarrow B$ est un morphisme d'anneaux commutatifs, alors on a $f(\mathrm{Nil}(A)) \subset \mathrm{Nil}(B)$. En particulier, si B est un anneau intègre, alors $\mathrm{Nil}(A) \subset \mathrm{Ker}(f)$.
(5) Plus généralement, si $I \subset A$ est un idéal, montrer que $\sqrt{I} := \{a \in A \mid \exists n \geq 1\ a^n \in I\}$ (le **radical de** I) est un idéal de A (on a $\sqrt{(0)} = \mathrm{Nil}(A)$).

8.5.9 Théorème. *Si $I \subset A$ est un idéal (bilatère) d'un anneau A, alors l'ensemble $A/I = \{a+I \mid a \in A\}$ des classes de congruence $(\mathrm{mod}\, I)$ dans A est un anneaux pour les opérations suivantes :*

$$\begin{aligned}
&\textbf{\textit{(Addition)}} && (a+I)+(b+I) = (a+b)+I \\
&\textbf{\textit{(Multiplication)}} && (a+I)\cdot(b+I) = ab+I \\
&\textbf{\textit{(Zéro)}} && 0_{A/I} = 0_A + I \\
&\textbf{\textit{(Unité)}} && 1_{A/I} = 1_A + I
\end{aligned}$$

(2) La projection $\mathrm{pr} : A \longrightarrow A/I$ $(\mathrm{pr}(a) = a + I)$ *est un morphisme (surjectif) d'anneaux.*
(3) $\mathrm{Ker}(\mathrm{pr}) = I$.

Démonstration. (1) Les opérations "+" et "$\cdot$" on A/I sont bien définies, d'après la proposition 7.6.8 et le théorème 8.5.4, respectivement. Il faut vérifier les axiomes (8.1.2.1). On a démontré (1) dans le théorème 7.6.10. Les axiomes d'associativité, unité et distributivité pour A/I sont des conséquences respectives des mêmes propriétés de A, grâce aux identités suivantes :

$$\begin{aligned}
((a+I)\cdot(b+I))\cdot(c+I) = (ab+I)\cdot(c+I) = (ab)c+I, \\
(a+I)\cdot((b+I)\cdot(c+I)) = (a+I)\cdot(bc+I) = a(bc)+I,
\end{aligned}$$

$$\begin{aligned}
(a+I)\cdot(1+I) = (a\cdot 1+I) = (a+I), \\
(1+I)\cdot(a+I) = (1\cdot a+I) = (a+I),
\end{aligned}$$

et

$$\begin{aligned}
((a+I)+(b+I))\cdot(c+I) = ((a+b)+I)\cdot(c+I) = (a+b)c+I, \\
(a+I)\cdot(c+I)+(b+I)\cdot(c+I) = (ac+I)+(bc+I) = (ac+bc)+I
\end{aligned}$$

(de même pour $a(b+c)$).
Le point (2) est automatique (réciproquement, la validité de (2) impose les formules dans la définition des opérations dans A/I), et le point (3) a été démontré dans le théorème 7.6.10. □

8.5.10 Remarques (1) Si $I = \{0\}$, alors $A/I = A$.
(2) Si $I = A$, alors $A/I = \{0\}$.
(3) Si l'anneau A est commutatif, alors A/I l'est aussi.

8.5.11 Eléments inversibles de A/I (le cas commutatif) Soit $I \subset A$ un idéal d'un anneau commutatif A, soit $a \in A$. Il est équivalent (voir la preuve du théorème 3.4.2) :

$$\begin{aligned} a \pmod I = a + I \in A/I \text{ est inversible dans } A/I &\iff \exists u \in A \quad au \equiv 1 \pmod I \\ &\iff \exists u \in A \ \exists y \in I \quad au + y = 1 \\ &\iff 1 \in aA + I = (a) + I \\ &\iff (a) + I = A. \end{aligned} \tag{8.5.11.1}$$

En particulier, si $I = (b) = bA$ est un idéal principal, alors

$$a \pmod b = a + (b) \in A/(b) \text{ est inversible dans } A/(b) \iff 1 \in aA + bA \iff aA + bA = A. \tag{8.5.11.2}$$

Explicitement, si on trouve $u, v \in A$ tels que $au+bv = 1$, alors $au \equiv 1 \pmod b$, ce qui signifie que $u \pmod b$ est l'inverse de $a \pmod b$ dans $A/(b)$.

8.5.12 Théorème (théorème de l'homomorphisme)**.** *Soit $f : A \longrightarrow B$ un morphisme d'anneaux. L'application*

$$\begin{array}{ccc} \overline{f} : A/\operatorname{Ker}(f) & \longrightarrow & \operatorname{Im}(f) \\ a + \operatorname{Ker}(f) & \mapsto & f(a) \end{array}$$

est un isomorphisme d'anneaux.

Démonstration. D'après le théorème 7.6.16, l'application $\overline{f}$ is bien définie et bijective, et on a $\overline{f}(x + y) = \overline{f}(x) + \overline{f}(y)$. Il faut démontrer les propriétés (2) et (3) de la Définition 8.4.1 : on a bien $\overline{f}(1_A + \operatorname{Ker}(f)) = f(1_A) = 1_B$ et

$$\forall a, b \in A \quad \overline{f}((a+\operatorname{Ker}(f))(b+\operatorname{Ker}(f))) = \overline{f}(ab+\operatorname{Ker}(f)) = f(ab) = f(a)f(b) = \overline{f}(a+\operatorname{Ker}(f))\overline{f}(b+\operatorname{Ker}(f)).$$

□

8.5.13 Reformulation Le théorème 8.5.12 implique que tout morphisme d'anneaux $f : A \longrightarrow B$ s'écrit d'une façon naturelle

$$f : A \xrightarrow{\text{pr}} A/\operatorname{Ker}(f) \xrightarrow{\overline{f}} \operatorname{Im}(f) \xrightarrow{i} B, \tag{8.5.13.1}$$

où pr est la projection sur l'anneau quotient, $\overline{f}$ est un isomorphisme et i est l'inclusion d'un sous-anneau.

Voici deux cas particuliers importants :

$$\begin{aligned} f \text{ est injectif} &\iff \text{pr} = \text{id} \iff \overline{f} : A \xrightarrow{\sim} \operatorname{Im}(f), \\ f \text{ est surjectif} &\iff i = \text{id} \iff \overline{f} : A/\operatorname{Ker}(f) \xrightarrow{\sim} B. \end{aligned}$$

On a une décomposition analogue

$$f : G \xrightarrow{\text{pr}} A/\operatorname{Ker}(f) \xrightarrow{\overline{f}} \operatorname{Im}(f) \xrightarrow{i} H \tag{8.5.13.2}$$

d'un morphisme de groupes quelconque $f : G \longrightarrow H$.

8.5.14 Exercice. Soit I un idéal (bilatère) d'un anneau A.
(1) Si $\overline{J} \subset A/I$ est un idéal (bilatère) de A/I, alors $J := \mathrm{pr}^{-1}(\overline{J}) = \{a \in A \mid a \pmod I \in \overline{J}\}$ est un idéal (bilatère) de A contenant I, et $\overline{J} = J/I$.
(2) Réciproquement, si $J \supset I$ est un idéal (bilatère) de A, alors J/I est un idéal (bilatère) de A/I et $J = \mathrm{pr}^{-1}(J/I)$.

8.5.15 Exercice. Soit $I \subset A$ un idéal d'un anneau commutatif A. Montrer : $\mathrm{Nil}(A/I) = \sqrt{I}/I$ (voir l'exercise 8.5.8).

8.5.16 Caractéristique d'un anneau Soit A un anneau. On sait qu'il existe un unique morphisme d'anneaux $f : \mathbf{Z} \longrightarrow A$, à savoir, $f(n) = n \cdot 1_A$. L'image de f est contenue dans le centre $Z(A)$ de A.

Cas 1. $\mathrm{Ker}(f) = 0$. On dit que la **caractéristique de A est nulle**. L'application f est injective dans ce cas et on peut considérer $\mathbf{Z}$ en tant que sous-anneau de A si l'on identifie $n \in \mathbf{Z}$ avec son image $f(n) = n \cdot 1_A \in A$.

Cas 2. $\mathrm{Ker}(f) \neq 0$. Dans ce cas $\mathrm{Ker}(f)$ est un idéal non nul de $\mathbf{Z}$, ce qui implique que $\mathrm{Ker}(f) = m\mathbf{Z}$, où $m \geq 1$. On appelle l'entier m la **caractéristique de** A.

On a $m = 1$ si et seulement si $f(1) = 0$, ce qui équivaut à $A = \{0\}$. Par conséquent, on a $m > 1$ si $A \neq \{0\}$.

D'après le théorème 8.5.12, f définie un isomorphisme d'anneaux $\overline{f} : \mathbf{Z}/m\mathbf{Z} \xrightarrow{\sim} \mathrm{Im}(f)$, ce qui implique qu'on peut considérer $\mathbf{Z}/m\mathbf{Z}$ en tant que sous-anneau de A si l'on identifie $n \pmod m = n + m\mathbf{Z} \in \mathbf{Z}/m\mathbf{Z}$ avec son image $f(n) = n \cdot 1_A \in A$.

8.5.17 Caractéristique d'un corps On peut dire plus lorsque $A = K$ est un corps.

Si la caractéristique de K est nulle, alors $\mathbf{Z}$ est un sous-anneau de K, via $n \mapsto n \cdot 1_K$ ($n \in \mathbf{Z}$). Pour tout $n \in \mathbf{Z} \smallsetminus \{0\}$, l'élément $n \cdot 1_K \neq 0_K$ est inversible dans K, ce qui implique que le morphisme injectif d'anneaux

$$\mathbf{Z} \hookrightarrow K, \qquad n \mapsto n \cdot 1_K$$

s'étend d'une façon unique à un morphisme d'anneaux (qui est forcément injectif, grâce à l'exercice 8.5.7)

$$\mathbf{Q} \hookrightarrow K, \qquad \frac{m}{n} = mn^{-1} \mapsto (m \cdot 1_K)(n \cdot 1_K)^{-1}. \tag{8.5.17.1}$$

En particulier, il existe un seul morphisme d'anneaux $\mathbf{Q} \longrightarrow K$, celui défini par la formule (8.5.17.1). Ce morphisme est injectif et $\mathbf{Q}$ s'identifie à son image, qui est un sous-corps de K.

Si la caractéristique de K est $m > 0$, alors $\mathbf{Z}/m\mathbf{Z}$ est un sous-anneau de K, via $n \pmod m \mapsto n \cdot 1_K$ ($n \in \mathbf{Z}$). Puisque le corps K est un anneau intègre, il en est de même de $\mathbf{Z}/m\mathbf{Z}$, ce qui implique que $m = p$ est un **nombre premier**, d'après la proposition 8.3.5. L'anneau $\mathbf{Z}/p\mathbf{Z}$ est alors un corps ; on le note $\mathbf{F}_p$.

Voici un résumé du raisonnement ci-dessus.

8.5.18 Proposition. *Soit K un corps.*
(1) Si la caractéristique de K est nulle, alors $\mathbf{Q}$ est un sous-corps de K via l'application $\frac{m}{n} = mn^{-1} \mapsto (m \cdot 1_K)(n \cdot 1_K)^{-1}$.
(2) Si la caractéristique de K est $m \geq 1$, alors $m = p$ est un nombre premier et $\mathbf{Z}/p\mathbf{Z} = \mathbf{F}_p$ est un sous-corps de K via l'application $n \pmod p \mapsto n \cdot 1_K$.

9 Anneau A[X]

D'ici jusqu'a fin du chapitre 9 on suppose que A est un anneau commutatif.

9.1 Définition et propriétés de base de $A[X]$

9.1.1 Polynômes Un polynôme en une variable (disons, X) à coefficients dans A est une somme formelle

$$a = a(X) = a_0 + a_1X + \cdots + a_mX^m = a_mX^m + \cdots + a_1X + a_0 \qquad (m \geq 0,\ a_i \in A).$$

Par définition, un polynôme ne change pas si l'on ajoute quelques termes où les coefficients sont nuls. Par exemple :

$$a_0 + a_1X + \cdots + a_mX^m = a_0 + a_1X + \cdots + a_mX^m + 0 \cdot X^{m+1} + 0 \cdot X^{m+2}.$$

Il est commode d'ajouter tous les termes ultérieurs avec des coefficients nuls $a_{m+1} = a_{m+2} = \cdots = 0$. Le polynôme $a = a(X)$ deviendra alors

$$a = a(X) = \sum_{i=0}^{\infty} a_iX^i, \qquad a_i \in A, \qquad \text{tous sauf un nombre fini de } a_i \text{ sont nuls.}$$

Un tel polynôme s'identifie à la suite des coefficients

$$(a_0, a_1, a_2, \ldots) = (a_i)_{i\in\mathbf{N}}, \qquad a_i \in A, \qquad \text{tous sauf un nombre fini de } a_i \text{ sont nuls.}$$

Si l'on se donne un autre polynôme

$$b = b(X) = \sum_{i=0}^{\infty} b_iX^i, \qquad b_i \in A, \qquad \text{tous sauf un nombre fini de } a_i \text{ sont nuls,}$$

on peut calculer la somme et le produit de a et b par le calcul formel usuel :

$$\begin{aligned} a + b &= (a_0 + a_1X + a_2X^2 + \cdots) + (b_0 + b_1X + b_2X^2 + \cdots) = \\ &= (a_0 + b_0) + (a_1 + b_1)X + (a_2 + b_2)X^2 + \cdots \\ ab &= (a_0 + a_1X + a_2X^2 + \cdots)(b_0 + b_1X + b_2X^2 + \cdots) = \\ &= (a_0b_0) + (a_0b_1 + a_1b_0)X + (a_0b_2 + a_1b_1 + a_2b_0)X^2 + \cdots \end{aligned}$$

ce qui s'écrit en termes des coefficients de la manière suivante :

$$\begin{aligned} &(a_0, a_1, a_2, \ldots) + (b_0, b_1, b_2, \ldots) = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \ldots) \\ &(a_0, a_1, a_2, \ldots) \cdot (b_0, b_1, b_2, \ldots) = (c_0, c_1, c_2, \ldots), \qquad c_k = \sum_{i+j=k} a_ib_j. \end{aligned} \tag{9.1.1.1}$$

On utilise ces formules pour définir l'anneaux de polynômes $A[X]$.

9.1.2 Définition. L'anneau de polynômes $A[X]$ en une variable X à coefficients dans un anneau commutatif A est l'ensemble

$$A[X] = \{a = (a_0, a_1, a_2, \ldots) \mid a_i \in A, \text{ tous sauf un nombre fini de } a_i \text{ sont nuls}\}.$$

L'addition et la multiplication dans $A[X]$ sont définies par les formules (9.1.1.1). Muni de ces opérations, $A[X]$ est un anneau commutatif avec zéro $0 = (0, 0, 0, \ldots)$ et unité $1 = (1, 0, 0, \ldots)$.

9.1.3 Remarques sur $A[X]$ (1) On laisse au lecteur la vérification du fait que les opérations (9.1.1.1) sur $A[X]$ sont bien définies et satisfont aux axiomes 8.1.2.1.

(2) Si l'on supprime la condition "tous sauf un nombre fini de a_i sont nuls" dans la définition, on obtient l'anneau

$$A[[X]] = \{\sum_{i=0}^{\infty} a_i X^i \mid a_i \in A\}$$

de séries formelles à coefficients dans A, dont $A[X]$ est un sous-anneau.

(3) $A \subset A[X]$ est un sous-anneau de $A[X]$, où $\alpha \in A$ correspond au polynôme constant $(\alpha, 0, 0, \ldots) = \alpha + 0 \cdot X + 0 \cdot X^2 + \cdots$.

(4) Pour tout polynôme $a \in A[X]$ il existe un entier $m \geq 0$ tel que $a_i = 0$ pour tout $i > m$. On écrit alors

$$a = a(X) = a_0 + a_1 X + \cdots + a_m X^m = a_m X^m + \cdots + a_1 X + a_0.$$

Si $a \neq 0$, alors on peut choisir $m \geq 0$ ci-dessus de telle manière que $a_m \neq 0$ (m est unique). On définit le **degré de** a par $\deg(a) := m$. En particulier, on a $a \in A \smallsetminus \{0\} \iff \deg(a) = 0$.

Le degré du polynôme nul est défini par $\deg(0) := -\infty$. On a alors $\deg(ab) = \deg(a) + \deg(b) = -\infty$ si $a = 0$ ou $b = 0$.

(5) Un polynôme $a = a_m X^m + \cdots + a_1 X + a_0$ de degré $m \geq 0$ est dit **unitaire** si $a_m = 1$.

9.1.4 Exemple : $\deg(ab) \neq \deg(a) + \deg(b)$ On considère l'anneau de polynômes $(\mathbf{Z}/4\mathbf{Z})[X]$. Pour tout $m \in \mathbf{Z}$, on note $\overline{m}$ la classe de congruence $m \pmod 4 \in \mathbf{Z}/4\mathbf{Z}$. On a $\overline{2} + \overline{2} = \overline{0} = \overline{2} \cdot \overline{2}$, ce qui implique que le polynôme $a = \overline{1} + \overline{2}X \in (\mathbf{Z}/4\mathbf{Z})[X]$ vérifie

$$\deg(a) = 1, \qquad a^2 = \overline{1}^2 + (\overline{2} + \overline{2})X + \overline{2}^2 X^2 = \overline{1}, \qquad \deg(a^2) = 0, \qquad a = a^{-1} \in (\mathbf{Z}/4\mathbf{Z})[X])^*.$$

9.1.5 Proposition. *Soient $a, b \in A[X] \smallsetminus \{0\}$. On écrit $a = a_m X^m + \cdots + a_0$ et $b = b_n X^n + \cdots + b_0$, où $m = \deg(a) \geq 0$ et $n = \deg(b) \geq 0$.*
(1) $\deg(a + b) \leq \max(\deg(a), \deg(b))$.
(2) $\deg(ab) \leq \deg(a) + \deg(b)$.
(3) Si $a_m \in A^*$, alors $\deg(ab) = \deg(a) + \deg(b)$.
(4) Si A est un anneau intègre, alors $\deg(ab) = \deg(a) + \deg(b)$.

Démonstration. (1) Si $i > m$ et $i > n$, alors $a_i = b_i = 0$, d'où $a_i + b_i = 0$.
(2) L'identité $ab = a_m b_n X^{m+n} + \cdots + a_0 b_0$ implique que $\deg(ab) \leq m+n$, et que l'équalité $\deg(ab) = m+n$ équivaut à $a_m b_n \neq 0$.
(3) Les hypothèses $a_m \in A^*$ and $b_n \neq 0$ impliquent que $a_m b_n \neq 0$, car $b_n = a_m^{-1}(a_m b_n)$ (voir le paragraphe 8.3.3, Remarque 3).
(4) Les hypothèses $a_m, b_n \neq 0$ impliquent que $a_m b_n \neq 0$, car A est un anneau intègre. □

9.1.6 Corollaire. *Si A est un anneau intègre, il en est de même de $A[X]$, et $A[X]^* = A^*$.*

Démonstration. Si $a, b \in A[X] \smallsetminus \{0\}$, alors $ab \neq 0$, d'après la proposition 9.1.5(4) (ou sa preuve), ce qui signifie que $A[X]$ est un anneau intègre. L'inclusion $A^* \subset A[X]^*$ est automatique. Réciproquement, si l'on a $ab = 1$ avec $a, b \in A[X]$, alors $0 = \deg(1) = \deg(ab) = \deg(a) + \deg(b)$, d'où $\deg(a) = \deg(b) = 0$, ce qui équivaut à $a, b \in A \smallsetminus \{0\}$. L'identité $ab = 1$ implique que $a, b \in A^*$. □

9.1.7 Exercice. (1) $(A_1 \times A_2)[X] = A_1[X] \times A_2[X]$.
(2) Si $A = A_1 \times \cdots \times A_r$ et si $A_1, \ldots, A_r$ sont des anneaux intègres, alors $A[X]^* = A^*$.
(3) Si $n = p_1 \cdots p_r$ est un produit de nombres premiers distincts, alors on a $((\mathbf{Z}/n\mathbf{Z})[X])^* = (\mathbf{Z}/n\mathbf{Z})^*$.
(4) Que peut-on dire de $((\mathbf{Z}/n\mathbf{Z})[X])^*$ en général $(n \geq 1)$?

9.1.8 Exercice. Supposons que $a = a_0 + a_1X + \cdots + a_mX^m \in A[X]$, $a_0 \in A^*$ et que les éléments $a_1, \ldots, a_m \in A$ sont nilpotents dans A (voir l'exercice 8.5.8). Montrer : $a \in (A[X])^*$.
[Indication : on pourra considérer $(a_0 - a)^n$, où $n > 0$ est un entier assez grand.]

9.2 Racines d'un polynôme

9.2.1 Morphisme d'évaluation Supposons que $a = a_mX^m + \cdots + a_0 \in A[X]$, où A est un sous-anneau d'un anneau commutatif B, et que $\beta \in B$. La **valeur de** a **en** β est définie par

$$a(\beta) := a_m\beta^m + \cdots + a_0 = \sum_{i=0}^{m} a_i\beta^i \in B.$$

Si $a(\beta) = 0$, on dit que β **est une racine de** a.

Il est utile de changer le point de vue traditionnel. Au lieu de fixer $a \in A[X]$ et faire varier $\beta \in B$, on fixe $\beta \in B$ et fait varier $a \in A[X]$.

9.2.2 Proposition. *L'application "évaluation en* β*"*

$$\mathrm{ev}_\beta : A[X] \longrightarrow B, \qquad a \mapsto a(\beta)$$

est un morphisme d'anneaux qui vérifie $\mathrm{ev}_\beta(a) = a$*, pour tout* $a \in A$*.*

Démonstration. Il faut montrer que l'on a bien

$$(a + b)(\beta) = a(\beta) + b(\beta), \qquad (ab)(\beta) = a(\beta)b(\beta), \qquad 1(\beta) = 1.$$

Pour démontrer l'énoncé au milieu (qui est le seul parmi les trois qui n'est pas immédiat) on calcule

$$(ab)(\beta) = \sum_{k\geq 0}\Big(\sum_{i+j=k} a_ib_j\beta^k\Big) = \Big(\sum_{i\geq 0} a_i\beta^i\Big)\Big(\sum_{j\geq 0} b_j\beta^j\Big) = a(\beta)b(\beta).$$

□

9.2.3 Caractérisation des racines Quand est-ce que $\beta \in A$ est une racine d'un polynôme $a = \sum_{k=0}^{m} a_kX^k \in A[X]$? On va montrer que la réponse est la même que dans le cas $A = \mathbf{C}$, à savoir :

$$a(\beta) = 0 \iff (X - \beta) \mid a \iff a \equiv 0 \ (\mathrm{mod}\,(X - \beta)). \tag{9.2.3.1}$$

En effet, si $a(X) = (X - \beta)b(X)$ avec $b \in A[X]$, alors $a(\beta) = (\beta - \beta)b(\beta) = 0$, d'après la proposition 9.2.2 (en particulier, $a \notin A \smallsetminus \{0\}$). Réciproquement, les formules

$$X^k - \beta^k = (X - \beta)(X^{k-1} + \beta X^{k-2} + \cdots + \beta^{k-1}) \qquad (k \geq 1)$$

impliquent que la différence

$$a - a(\beta) = a(X) - a(\beta) = (X - \beta)\sum_{k=1}^{m} a_k(X^{k-1} + \beta X^{k-2} + \cdots + \beta^{k-1}) \tag{9.2.3.2}$$

est divisible par $(X-\beta)$ in $A[X]$, d'où

$$a(X) \equiv a(\beta) \pmod{(X-\beta)}. \tag{9.2.3.3}$$

En particulier, si $a(\beta) = 0$, alors $(X-\beta) \mid a$. Voici une reformulation plus abstraite de la discussion ci-dessus.

9.2.4 Proposition. *Soit $\beta \in A$. Le morphisme d'évaluation $\mathrm{ev}_\beta : A[X] \longrightarrow A$ vérifie $\mathrm{Ker}(\mathrm{ev}_\beta) = (X-\beta)$, ce qui implique qu'il induit un isomorphisme d'anneaux*

$$\overline{\mathrm{ev}}_\beta : A[X]/(X-\beta) \xrightarrow{\sim} A, \qquad a \pmod{(X-\beta)} \mapsto a(\beta).$$

Son inverse est égal à la composition $A \hookrightarrow A[X] \xrightarrow{\mathrm{pr}} A[X]/(X-\beta)$. Autrement dit, l'ensemble des classes de congruence dans $A[X]$ modulo $(X-\beta)$ est égal à $\{\alpha \pmod{(X-\beta)} \mid \alpha \in A\}$, où $\alpha_1 \not\equiv \alpha_2 \pmod{(X-\beta)}$ si $\alpha_1 \neq \alpha_2$.

9.2.5 Développement de Taylor d'un polynôme La congruence (9.2.3.2) admet une version plus raffinée modulo $(X-\beta)^2$ comme suit. On définit le **polynôme dérivé** de $a = a(X) = \sum_{k=0}^m a_k X^k$ par

$$a' = a'(X) := \sum_{k=1}^{m} k a_k X^{k-1} \in A[X], \qquad k a_k := \underbrace{a_k + \cdots + a_k}_{k \text{ fois}} \in A.$$

Si l'on met ensemble (9.2.3.2) et (9.2.3.3), on obtient que le polynôme

$$a - a(\beta) - (X-\beta)a'(\beta) \tag{9.2.5.1}$$

est divisible par $(X-\beta)^2$ in $A[X]$, d'où

$$a(X) \equiv a(\beta) + (X-\beta)a'(\beta) \pmod{(X-\beta)^2} \equiv a(\beta) + (X-\beta)a'(X) \pmod{(X-\beta)^2}. \tag{9.2.5.2}$$

Y a-t-il des congruences modulo des puissances supérieures de $(X-\beta)$?

9.2.6 Exercice. (Formule de Taylor) Pour tout entier $n \geq 0$ on a

$$a(X) \equiv \sum_{k=0}^{n} (D_k a)(\beta)\,(X-\beta)^k \pmod{(X-\beta)^{n+1}}, \tag{9.2.6.1}$$

où $D_k a = \sum_{i \geq k} \binom{i}{k} a_i X^{i-k} \in A[X]$.
[Si $A = \mathbf{C}$, alors on a $k!(D_k a)(X) = (d/dX)^k a(X)$.]

9.2.7 Théorème. *Si A est un anneau intègre, alors un polynôme non nul $a \in A[X] \smallsetminus \{0\}$ a au plus $\deg(a)$ racines distinctes dans A.*

Démonstration. On suit la preuve du théorème 5.1.14. Soit $d := \deg(a)$. Si $d = 0$, alors $a \in A \smallsetminus \{0\}$ et il n'y a aucune racine. Supposons que $d > 0$ et que le résultat est vrai pour tous les polynômes de degré $\deg < d$. Si $\alpha \in A$ est une racine de a, alors $a = (X-\alpha)b$ avec un polynôme $b \in A[X] \smallsetminus \{0\}$ de degré $\deg(b) = d-1$. Si $\beta \in A$, $\beta \neq \alpha$ et $a(\beta) = 0$, alors $0 = a(\beta) = (\beta-\alpha)b(\beta)$. Par l'hypothèse, A est un anneau intègre et $\beta - \alpha \neq 0$, ce qui implique que $b(\beta) = 0$. Il y a au plus $\deg(b) = d-1$ valeurs possibles de β, par l'hypothèse de récurrence. En ajoutant α, on obtient au plus $(d-1)+1 = d$ racines de a dans A.

□

9.2.8 Remarque On a vu dans le paragraphe 5.1.13 des exemples de polynômes $a \in (\mathbf{Z}/n\mathbf{Z})[X]$ de degré $\deg(a) = 2$ qui ont (au moins) quatre racines dans $\mathbf{Z}/n\mathbf{Z}$ (pour $n = 8$ ou $n = p_1 \cdots p_r$, où $r \geq 2$ et $p_i \neq 2$ sont des nombres premiers distincts).

9.2.9 Exercice. Soit $p \neq 2$ un nombre premier. Donner un exemple d'un polynôme unitaire $a \in (\mathbf{Z}/p^2\mathbf{Z})[X]$ de degré $\deg(a) < p^2$ tel que $\forall \alpha \in \mathbf{Z}/p^2\mathbf{Z} \quad a(\alpha) = 0$.

9.3 Division euclidienne dans $A[X]$

9.3.1 Introduction Les classes de congruence $(\mathrm{mod}\, n)$ dans $\mathbf{Z}$ correspondent aux restes de la division euclidienne par $n \geq 1$ dans $\mathbf{Z}$. Pour comprendre les classes de congruence $(\mathrm{mod}\, b)$ dans $A[X]$ il faut comprendre les restes de la division euclidienne par $b \in A[X]$ dans $A[X]$.

9.3.2 Anneau quotient $A[X]/(b)$ Soit $b \in A[X]$. Les congruences dans $A[X]$ modulo b (plus précisement, modulo l'idéal principal $(b) = bA[X]$ engendré par b) sont définies de la façon usuelle :

$$a \equiv \widetilde{a} \ (\mathrm{mod}\, b) \iff b \mid (a - \widetilde{a}) \iff \exists c \in A[X] \quad a - \widetilde{a} = bc.$$

Les classes de congruence $(\mathrm{mod}\, b)$ forment un anneau commutatif $A[X]/(b) = A[X]/bA[X]$ par rapport aux opérations usuelles : si l'on note $\overline{a} = a + (b) = a \ (\mathrm{mod}\, b)$ l'image dans $A[X]/(b)$ d'un polynôme $a \in A[X]$ (i.e., la classe de congruence de a modulo b), alors

$$a \ (\mathrm{mod}\, b) \pm \widetilde{a} \ (\mathrm{mod}\, b) = (a \pm \widetilde{a}) \ (\mathrm{mod}\, b), \qquad (a \ (\mathrm{mod}\, b)) \cdot (\widetilde{a} \ (\mathrm{mod}\, b)) = a\widetilde{a} \ (\mathrm{mod}\, b).$$

On a aussi

$$a \ (\mathrm{mod}\, b) \text{ est inversible dans } A[X]/(b) \iff 1 \in aA[X] + bA[X] \iff aA[X] + bA[X] = A[X], \quad (9.3.2.1)$$

d'après (8.5.11.2). Si $u, v \in A[X]$ vérifient $au + bv = 1$, alors $au \equiv 1 \ (\mathrm{mod}\, b)$ et $u \ (\mathrm{mod}\, b)$ est l'inverse de $a \ (\mathrm{mod}\, b)$ dans $A[X]/(b)$.

Il y a un **élément distingué** dans $A[X]/(b)$, à savoir, la classe de la variable X. Cette classe $\overline{X} = X \ (\mathrm{mod}\, b) \in A[X]/(b)$ est une racine de l'équation polynomiale

$$b(\overline{X}) = 0 \in A[X]/(b), \quad (9.3.2.2)$$

car $b(\overline{X}) = \overline{b(X)}$ et $b(X) \equiv 0 \ (\mathrm{mod}\, b)$.

Dans le cas le plus simple (mais non trivial) $b = X - \beta$ ($\beta \in A$) que l'on a considéré dans la proposition 9.2.4, l'anneau quotient $A[X]/(X - \beta)$ s'identifie à A via le morphisme d'évaluation $\overline{\mathrm{ev}}_\beta$, et $\overline{X}$ correspond à la valeur $\mathrm{ev}_\beta(X) = X(\beta) = \beta \in A$.

L'objectif du paragraphe 9.3 est décrire l'anneau quotient $A[X]/(b)$ pour les polynômes b dont le coefficient dominant est inversible dans A (cette condition est toujours satisfaite si $A = K$ est un corps). L'util principal sera la division euclidienne pour des polynômes.

9.3.3 Division euclidienne (exemples) (1) Division de $a = a(X) = 2X^3 + 2X^2 - X + 1 \in \mathbf{Q}[X]$ par $b = b(X) = 2X + 3$. On calcule

$$\begin{aligned}
\boxed{2X^3} + 2X^2 - X + 1 &= (2X + 3)X^2 + (-X^2 - X + 1), \\
\boxed{-X^2} - X + 1 &= (2X + 3)(-\tfrac{1}{2}X) + (\tfrac{1}{2}X + 1), \\
\boxed{\tfrac{1}{2}X} + 1 &= (2X + 3) \cdot \tfrac{1}{4} + \tfrac{1}{4}, \\
2X^3 + 2X^2 - X + 1 &= (X^2 - \tfrac{1}{2}X + \tfrac{1}{4})(2X + 3) + \tfrac{1}{4}.
\end{aligned}$$

Dans ce genre de calculs on manipule d'une façon purement formel les coefficients des polynômes qui apparaissent :

	X^3	X^2	X	1
b			2	3
a	2	2	-1	1
X^2b	2	3		
$a - X^2b$		-1	-1	1
$-\frac{1}{2}Xb$		-1	$-\frac{3}{2}$	
$a - (X^2 - \frac{1}{2}X)b$			$\frac{1}{2}$	1
$\frac{1}{4}b$			$\frac{1}{2}$	$\frac{3}{4}$
$a - (X^2 - \frac{1}{2}X + \frac{1}{4})b$				$\frac{1}{4}$

(2) Division de $a = a(X) = X^3 - 2X^2 - 7X + 3 \in \mathbf{Q}[X]$ par $b = b(X) = 2X^2 + 4X - 1$. On a

$$\begin{aligned}
\boxed{X^3} - 2X^2 - 7X + 3 &= (2X^2 + 4X - 1)(\tfrac{1}{2}X) + (-4X^2 - \tfrac{13}{2}X + 3),\\
\boxed{-4X^2} - \tfrac{13}{2}X + 3 &= (2X^2 + 4X - 1)(-2) + (\tfrac{3}{2}X + 1),\\
2X^3 - 2X^2 - 7X + 3 &= (\tfrac{1}{2}X - 2)(2X^2 + 4X - 1) + (\tfrac{3}{2}X + 1),
\end{aligned}$$

ce qui s'écrit aussi

	X^3	X^2	X	1
b		2	4	-1
a	1	-2	-7	3
$\frac{1}{2}Xb$	1	2	$-\frac{1}{2}$	
$a - \frac{1}{2}Xb$		-4	$-\frac{13}{2}$	3
$-2b$		-4	-8	2
$a - (\frac{1}{2}X - 2)b$			$\frac{3}{2}$	1

(3) Division de $a = \sum_{k=0}^{m} a_k X^k \in A[X]$ par $b = X - \beta$ ($\beta \in A$) équivaut à la formule (9.2.3.2).

9.3.4 Proposition. *Supposons que $b = b_nX^n + \cdots + b_0 \in A[X]$, $\deg(b) = n \geq 0$ et $b_n \in A^*$. Alors, pour tout $a \in A[X]$, il existe un unique couple $q, r \in A[X]$ tel que*

$$a = bq + r, \qquad \deg(r) < \deg(b).$$

On a $b \mid a$ dans $A[X]$ si et seulement si $r = 0$.

Démonstration. Si $n = 0$, alors $b = b_0 \in A^*$ et $q = b_0^{-1}a$, $r = 0$. Supposons que $n > 0$.
Unicité : si $a = bq + r = b\widetilde{q} + \widetilde{r}$ et $\deg(r), \deg(\widetilde{r}) < \deg(b)$, alors $b(q - \widetilde{q}) = \widetilde{r} - r$, ce qui implique que

$$\deg(b) > \deg(\widetilde{r} - r) = \deg(b(q - \widetilde{q})) = \deg(b) + \deg(q - \widetilde{q})$$

(on a utilisé ici l'hypothèse $b_n \in A^*$ et la proposition 9.1.5(3)). Par conséquent, $\deg(q - \widetilde{q}) < 0$, ce qui signifie que $q - \widetilde{q} = 0$, d'où $q = \widetilde{q}$ et $r = \widetilde{r}$.

Existence : récurrence sur $m = \deg(a)$, $a = a_m X^m + \cdots + a_0$. Si $m < n$, alors on peut prendre $q = 0$, $r = a$. Si $m \geq n$, alors

$$a = (a_m b_n^{-1} X^{m-n})b + c, \qquad c \in A[X], \qquad \deg(c) < m.$$

Par l'hypothèse de récurrence, il existe $\widetilde{q}, \widetilde{r} \in A[X]$ tels que $c = b\widetilde{q} + \widetilde{r}$ et $\deg(\widetilde{r}) < \deg(b)$, ce qui implique que

$$a = b(a_m b_n^{-1} X^{m-n} + \widetilde{q}) + \widetilde{r}, \qquad \deg(\widetilde{r}) < \deg(b).$$

Divisibilité : si $r = 0$, alors $a = bq$ est divisible par b dans $A[X]$. Réciproquement, si $a = bc$ avec $c \in A[X]$, alors on a $a = cb + 0$ et $\deg(0) = -\infty < \deg(b)$, d'où $r = 0$ par l'unicité. □

9.3.5 Corollaire. *Soit $A \subset \widetilde{A}$ un sous-anneau d'un anneau commutatif $\widetilde{A}$, soit $a \in A[X]$. Supposons que $b = b_n X^n + \cdots + b_0 \in A[X]$, $\deg(b) = n \geq 0$ et $b_n \in A^*$. Il est équivalent :*

$$b \mid a \text{ dans } A[X] \iff b \mid a \text{ dans } \widetilde{A}[X].$$

[Attention : on ne peut pas supprimer l'hypothèse $b_n \in A^*$ (par exemple, 2 divise 1 dans $\mathbf{C}[X]$, mais pas dans $\mathbf{Z}[X]$)].

Démonstration. Puisque $b_n \in A^* \subset \widetilde{A}^*$, il existe un unique couple $q, r \in A[X]$ (resp. $\widetilde{q}, \widetilde{r} \in \widetilde{A}[X]$) tel que

$$a = bq + r, \qquad \deg(r) < \deg(b), \qquad a = b\widetilde{q} + \widetilde{r}, \qquad \deg(\widetilde{r}) < \deg(b).$$

L'unicité implique que $\widetilde{q} = q$ et $\widetilde{r} = r$, d'où

$$b \mid a \text{ dans } A[X] \iff r = 0 \iff \widetilde{r} = 0 \iff b \mid a \text{ dans } \widetilde{A}[X].$$

□

9.3.6 Conséquences pour $A[X]/(b)$ Supposons que $b = b_n X^n + \cdots + b_0 \in A[X]$, $\deg(b) = n \geq 0$ et $b_n \in A^*$. La proposition 9.3.4 nous dit que pour tout polynomial $a \in A[X]$ il existe un unique polynôme $r \in A[X]$ de degré $\deg(r) < n$ tel que

$$a \equiv r \pmod{b}.$$

Autrement dit, si l'on écrit

$$A[X]_{\deg<n} := \{r \in A[X] \mid \deg(r) < n\} = \{r_0 + r_1 X + \cdots + r_{n-1} X^{n-1} \mid r_j \in A\}$$

(bien sûr, on a $A[X]_{\deg<0} = \{0\}$), alors la composition

$$A[X]_{\deg<n} \hookrightarrow A[X] \xrightarrow{\text{pr}} A[X]/(b) \tag{9.3.6.1}$$

est **bijective :**

$$\begin{aligned} A[X]/(b) &= \{r \pmod{b} \mid r \in A[X], \deg(r) < n\} \\ &= \{r_0 + r_1 X + \cdots + r_{n-1} X^{n-1} \pmod{b} \mid r_j \in A\} \\ &= \{r_0 + r_1 \overline{X} + \cdots + r_{n-1} \overline{X}^{n-1} \mid r_j \in A\}, \end{aligned} \tag{9.3.6.2}$$

où $\overline{X} = X \pmod{b} \in A[X]/(b)$ (la classe $\pmod{b}$ de la variable X) vérifie $b(\overline{X}) = 0$, comme l'on a vu dans (9.3.2.2). Si l'on note cette classe $\alpha := X \pmod{b} \in A[X]/(b)$, alors on a

$$A[X]/(b) = \{r(\alpha) \mid r \in A[X],\, \deg(r) < n\} = \{r_0 + r_1\alpha + \cdots + r_{n-1}\alpha^{n-1} \mid r_j \in A\},$$
$$b(\alpha) = b_n\alpha^n + \cdots + b_0 = 0, \tag{9.3.6.3}$$

où des n-uplets distincts $(r_0, \ldots, r_{n-1})$ $(r_j \in A)$ correspondent aux éléments distincts de $A[X]/(b)$.

L'application (9.3.6.1) est A-linéaire : elle est compatible avec les opérations "+" et "multiplication par une constante $c \in A$" les deux côtés. On calcule le produit $(a \pmod b)) \cdot (\widetilde{a} \pmod b))$ en écrivant $a\widetilde{a} = qb + r$, où $\deg(r) < n$; on a alors $(a \pmod b)) \cdot (\widetilde{a} \pmod b)) = r \pmod b)$.

Si l'on utilise la notation de (9.3.6.3) pour les éléments de $A[X]/(b)$, alors on a $a(\alpha)\widetilde{a}(\alpha) = r(\alpha)$.

10 Anneau K[X]

D'ici jusqu'a fin du chapitre 10 on suppose que K est un corps.

10.1 Propriétés de base de $K[X]$

10.1.1 Rappels Rappelons qu'un corps est un anneau commutatif non nul dans lequel tout élément non nul est inversible. Exemples : $K = \mathbf{Q}, \mathbf{R}, \mathbf{C}, \mathbf{Q} + \mathbf{Q}i$ ou $\mathbf{Z}/p\mathbf{Z} = \mathbf{F}_p$ (où p est un nombre premier).

Voici quelques conséquences de la propriété $K^* = K \smallsetminus \{0\}$:

- $K[X]$ est un anneau intègre et on a $K[X]^* = K^* = K \smallsetminus \{0\} = \{a \in K[X] \mid \deg(a) = 0\}$.
- $\deg(ab) = \deg(a) + \deg(b)$ pour tous $a, b \in K[X]$.
- Tout polynôme non nul $a = a_nX^n + \cdots + a_0$ s'écrit d'une façon unique $a = a_n(a_n^{-1}a)$, où $a_n \in K^*$ et $a_n^{-1}a = X^n + \cdots + a_n^{-1}a_0 \in K[X]$ est un polynôme **unitaire** $(n = \deg(a) \geq 0)$.
- Un polynôme non constant $a \in K[X] \smallsetminus K$ est **irréductible dans** $K[X]$ au sens du paragraphe 8.3.11 si $a \neq bc$ avec des polynômes non constants $b, c \in K[X] \smallsetminus K$. Par exemple, a est irréductible dans $K[X]$ si $\deg(a) = 1$. On note $\mathcal{P}_K$ l'ensemble de tous les polynômes **irréductibles unitaires** (non constants) dans $K[X]$. Remarquons qu'on a $\{\pi \in \mathcal{P}_K \mid \deg(\pi) = 1\} = \{X - \alpha \mid \alpha \in K\}$.

On verra que l'anneau de polynômes $K[X]$ ressemble beaucoup à l'anneau des entiers relatifs $\mathbf{Z}$. En particulier, les éléments de $\mathcal{P}_K$ sont des analogues des nombres premiers.

Par exemple, la plupart de la discussion dans le paragraphe 1.1.5 s'applique presque sans modifications :

10.1.2 Proposition (Existence de factorisation)**.** *Tout polynôme non nul $a \in K[X] \smallsetminus \{0\}$ s'écrit $a = \lambda\pi_1 \cdots \pi_r$, où $\lambda \in K^*$, $r \geq 0$ et $\pi_j \in \mathcal{P}_K$.*

Démonstration. Récurrence sur $\deg(a)$ (voir la preuve de la proposition 1.2.1 par récurrence sur n). □

10.1.3 Proposition (Critère d'irréductibilité)**.** *Soit $a \in K[X] \smallsetminus K$ un polynôme non constant. Les propriétés suivantes sont équivalentes.*
(1) a n'est pas irréductible dans $K[X]$.
(2) Il existe $b \in K[X] \smallsetminus K$ tel que $\deg(b) \leq \frac{1}{2}\deg(a)$ et $b \mid a$.
(3) Il existe $\pi \in \mathcal{P}_K$ tel que $\deg(\pi) \leq \frac{1}{2}\deg(a)$ et $\pi \mid a$.

Démonstration. La propriété (1) implique que $a = bc$ avec des polynômes non nuls b, c tels que $\deg(b) \leq \deg(c)$; on a alors $b \mid a$ et $2\deg(b) \leq \deg(b) + \deg(c) = \deg(bc) = \deg(a)$, ce qui montre (2). La propriété (2) implique qu'il existe $\pi \in \mathcal{P}_K$ qui divise b ; on a alors $\pi \mid a$ et $\deg(\pi) \leq \deg(b) \leq \frac{1}{2}\deg(a)$. □

10.1.4 Corollaire. *Si $a \in K[X]$ est un polynôme de degré $\deg(a) \in \{2,3\}$, alors il est équivalent :*

$$a \text{ est irréductible dans } K[X] \iff a \text{ n'a pas de racines dans } K.$$

Démonstration. En effet, $\pi \in \mathcal{P}_K$ vérifie (3) dans la proposition 10.1.3 si et seulement si $\pi = X - \alpha$, où $\alpha \in K$ et $a(\alpha) = 0$. □

10.1.5 Exemples (1) Si $n \in \{2,3\}$, $a \in \mathbf{N}_+$ et $\sqrt[n]{a} \notin \mathbf{N}_+$, alors le polynôme $X^n - a$ n'a pas de racines dans $\mathbf{Q}$ (d'après le théorème 1.5.11), ce qui implique qu'il est irréductible dans $\mathbf{Q}[X]$.

(2) Ce n'est plus vrai si $n = 4$, car

$$X^4 + 4 = (X^2 - 2X + 2)(X^2 + 2X + 2).$$

10.2 Division euclidienne dans $K[X]$, conséquences

10.2.1 Division euclidienne dans $K[X]$ La proposition suivante correspond à la proposition 2.2.2 dans le cadre arithmétique.

10.2.2 Proposition. *Si $a, b \in K[X]$ et $b \neq 0$, alors il existe un unique couple $q, r \in K[X]$ tel que*

$$a = bq + r, \qquad \deg(r) < \deg(b).$$

On a $b \mid a$ dans $K[X]$ si et seulement si $r = 0$.

Démonstration. C'est un cas particulier de la proposition 9.3.4 pour $A = K$. L'hypothèse clé $b_n \in K^*$ ($n = \deg(b)$) dans cette proposition est une conséquence automatique du fait que $b \neq 0$. □

10.2.3 Conséquences Tous les énoncés qu'on a déduits de la proposition 2.2.2 dans les chapitres 2 et 3 ont des analogues immédiats dans $K[X]$. Voici quelques uns.

10.2.4 Algorithme d'Euclide, relations de Bézout Soient $a, b \in K[X] \smallsetminus \{0\}$. La division euclidienne itérée dans $K[X]$ (voir le paragraphe 2.4) produit des éléments

$$d \in K[X] \smallsetminus \{0\}, \qquad u, v \in K[X]$$

tels que

$$\left.\begin{array}{l} d \mid a, \;\; d \mid b \\ d = au + bv \end{array}\right\} \implies aK[X] + bK[X] = dK[X]. \tag{10.2.4.1}$$

Autrement dit, l'idéal $(a, b) = (a) + (b) = (d)$ de $K[X]$ est principal, engendré par d. C'est une version faible du théorème de Bézout pour $K[X]$.

10.2.5 Plus grand commun diviseur La relation (10.2.4.1) implique que

$$\begin{array}{l} d \mid a, \;\; d \mid b \\ \text{si } c \in K[X] \smallsetminus \{0\} \text{ et } c \mid a, \;\; c \mid b, \text{ alors } c \mid d. \end{array} \tag{10.2.5.1}$$

L'élément d dans (10.2.4.1) est unique à un facteur multiplicatif appartenant à $K[X]^* = K^* = K \smallsetminus \{0\}$ près. Il sera unique s'il on exige que d soit **unitaire**.

On dit alors que d est le **plus grand commun diviseur** de a et b ; on le note $\operatorname{pgcd}(a, b) := d$. La relation

$$aK[X] + bK[X] = \mathrm{pgcd}(a,b)K[X]. \tag{10.2.5.2}$$

est une version forte du théorème de Bézout pour $K[X]$.

10.2.6 Exemples Revenons aux exemples du paragraphe 9.3.3.
(1) $a = 2X^3 + 2X^2 - X + 1$, $b = 2X + 3 \in \mathbf{Q}[X]$. On sait que

$$2X^3 + 2X^2 - X + 1 = (X^2 - \tfrac{1}{2}X + \tfrac{1}{4})(2X + 3) + \tfrac{1}{4},$$

ce qui implique que $\mathrm{pgcd}(a,b) = 1$ et

$$4(2X^3 + 2X^2 - X + 1) + (-4X^2 + 2X - 1)(2X + 3) = 1.$$

(2) $a = X^3 - 2X^2 - 7X + 3$, $b = 2X^2 + 4X - 1 \in \mathbf{Q}[X]$. On sait que

$$2X^3 - 2X^2 - 7X + 3 = (\tfrac{1}{2}X - 2)(2X^2 + 4X - 1) + (\tfrac{3}{2}X + 1),$$

mais il faut faire encore une division euclidienne :

$$2X^2 + 4X - 1 = (\tfrac{4}{3}X + \tfrac{16}{9})(\tfrac{3}{2}X + 1) - \tfrac{25}{9},$$

d'où $\mathrm{pgcd}(a,b) = 1$ et

$$-\tfrac{25}{9} = b - (\tfrac{4}{3}X + \tfrac{16}{9})(a - (\tfrac{1}{2}X - 2)b) = -\tfrac{4}{9}(3X + 4)a + \tfrac{b}{9}(6X^2 - 16X - 23),$$

$$\tfrac{4}{25}(3X + 4)a + \tfrac{1}{25}(-6X^2 + 16X + 23)b = 1.$$

10.2.7 Idéaux de $K[X]$ Il s'avère que **tout idéal de $K[X]$ est principal**. En effet, si $I \subset K[X]$ est un idéal non nul et si $b \in I \smallsetminus \{0\}$ est un élément de degré minimum, alors le raisonnement dans la preuve du théorème 2.3.2 montre que l'on a $I = (b) = bK[X]$.

De même, b est unique à un élément de K^* près. Il sera unique si l'on exige que b soit unitaire.

10.2.8 Lemme d'Euclide Comme dans les paragraphes 1.4 et 2.3, on déduit de la version faible (10.2.4.1) du théorème de Bézout le lemme d'Euclid dans $K[X]$, ce qui implique l'unicité de factorisation dans $K[X]$.

10.2.9 Lemme (Lemme d'Euclide dans $K[X]$)**.** *Si $\pi \in \mathcal{P}_K$, $a, b \in K[X] \smallsetminus \{0\}$, $\pi \mid ab$ et $\pi \nmid b$, alors $\pi \mid a$.*

10.2.10 Théorème (Unicité de factorisation dans $K[X]$)**.** *Tout polynôme non nul $a \in K[X] \smallsetminus \{0\}$ admet une unique factorisation*

$$a = \lambda \prod_{\pi \in \mathcal{P}_K} \pi^{v_\pi(a)} \qquad (\lambda \in K^*),$$

où $v_\pi(a) \in \mathbf{N}$ et $v_\pi(a) = 0$ pour tous sauf un nombre fini de $\pi \in \mathcal{P}_K$.

10.2.11 Valuations π-adiques Les exposants v_π dans le théorème 10.2.10 se comportent de la même manière que les valuations p-adiques des entiers. Toutes les propriétés dans la proposition 1.5.4 son encore valables, avec la modification suivante : on a $v_\pi(a) = v_\pi(b)$ pour tout $\pi \in \mathcal{P}_K$ si et seulement si $a = \lambda b$ avec $\lambda \in K^*$.

10.2.12 Plus petit commun multiple Comme dans le théorème 1.6.2, on a

$$\forall a, b \in K[X] \smallsetminus \{0\} \quad \operatorname{pgcd}(a,b) = \prod_{\pi \in \mathcal{P}_K} \pi^{\min(v_\pi(a), v_\pi(b))}.$$

De même, si l'on définit le **plus petit commun multiple** de a et b par

$$m = \operatorname{ppcm}(a,b) := \prod_{\pi \in \mathcal{P}_K} \pi^{\max(v_\pi(a), v_\pi(b))},$$

alors le polynôme m est unitaire, c'est un multiple commun à a et b, et tout multiple commun à a et b est un multiple de m, comme dans le théorème 1.6.3.

On a $\operatorname{pgcd}(a,b)\operatorname{ppcm}(a,b) = \lambda ab$, où $\lambda \in K^*$.

10.3 Corps algébriquement clos

10.3.1 Théorème Fondamental de l'Algèbre Ce théorème affirme que tout polynôme complexe non constant admet une racine complexe (selon la terminologie de la Définition 10.3.2 ci-dessous, le corps des nombres complexes est **algébriquement clos**). Malgré son nom, il s'agit d'un théorème de l'analyse.

10.3.2 Définition. Un corps K est **algébriquement clos** si pour tout $f \in K[X] \smallsetminus K$ il existe $\alpha \in K$ tel que $f(\alpha) = 0$.

10.3.3 Proposition. *Si K est un corps algébriquement clos et si $f \in K[X]$, $\deg(f) = n \geq 0$, alors il existe $\alpha_1, \ldots, \alpha_n \in K$ (pas forcément distincts) et $a_n \in K \smallsetminus \{0\}$ tels que $f = a_n(X - \alpha_1)\cdots(X - \alpha_n)$.*

Démonstration. Récurrence sur n. Il n'y a rien à démontrer si $n = 0$. Supposons que $n > 0$ et que l'énoncé et vrai pour tous les polynômes de degré $\deg < n$. Il existe $\alpha_1 \in K$ tel que $f(\alpha_1) = 0$, ce qui implique que $f = (X - \alpha_1)f_1$ avec $f_1 \in K[X]$, d'après (9.2.3.1). On a $\deg(f_1) = n - 1$; l'hypothèse de récurrence nous dit alors que l'on a $f_1 = a_n(X - \alpha_2)\cdots(X - \alpha_n)$ avec $\alpha_j \in K$ and $a_n \in K \smallsetminus \{0\}$, d'où $f = a_n(X - \alpha_1)\cdots(X - \alpha_n)$. □

10.3.4 Théorème (Théorème Fondamental de l'Algèbre)**.** *Pour tout $f \in \mathbf{C}[X] \smallsetminus \mathbf{C}$ il existe $\alpha \in \mathbf{C}$ tel que $f(\alpha) = 0$.*

Démonstration. La démonstration ci-dessous (due à Argand) utilise les résultats analytiques suivants.

- **Compacité :** toute fonction continue $F : D_R \longrightarrow \mathbf{R}$ définie sur un disque fermé $D_R = \{z \in \mathbf{C} \mid |z| \leq R\}$ atteint son inf : il existe $z_0 \in D_R$ tel que $F(z_0) = \inf_{z \in D_R} F(z)$.
- **Existence des racines m-ièmes :** pour tout $z \in \mathbf{C}$ tel que $|z| = 1$ et tout entier $m \geq 1$ il existe $w \in \mathbf{C}$ tel que $w^m = z$.

Le polynôme $f(z) = a_n z^n + \cdots + a_0$ $(n = \deg(f) \geq 1)$ vérifie

$$\lim_{\substack{z \in \mathbf{C} \\ |z| \to +\infty}} f(z)/z^n = a_n \neq 0,$$

ce qui implique qu'il existe $R > 0$ tel que $|f(z)| > |f(0)|$ si $z \in \mathbf{C}$ et $|z| > R$. Par conséquent, on a

$$\inf_{z \in \mathbf{C}} |f(z)| = \inf_{|z| \leq R} |f(z)| = |f(z_0)|,$$

où $z_0 \in \mathbf{C}$, $|z_0| \leq R$. Cet égalité implique que $f(z_0) = 0$, d'après le lemme 10.3.5 ci-dessous, donc z_0 est une racine de f. □

10.3.5 Lemme (Argand)**.** *Si $f \in \mathbf{C}[z] \smallsetminus \mathbf{C}$, $z_0 \in \mathbf{C}$ et $f(z_0) \neq 0$, alors il existe, pour tout $r > 0$, un nombre complexe $z \in \mathbf{C}$ tel que $|z - z_0| < r$ et $|f(z)| < |f(z_0)|$.*

Démonstration. On considère le polynôme $g(z) := f(z_0 + z)/f(z_0)$. On a

$$g(z) = 1 + b_m z^m + z^{m+1}(b_{m+1} + \cdots + b_n z^{n-m-1}) = 1 + b_m z^m + h(z), \qquad b_m \neq 0, \qquad (1 \leq m \leq n).$$

Il faut trouver $z \in \mathbf{C}$ tel que $|z| < r$ et $|g(z)| < 1$. L'idée est simple : si $|z| > 0$ est petit, alors le terme $|h(z)|$ sera plus petit que $|b_m z^m|$. Il suffira, donc, de choisir l'argument de z de telle manière pour que l'on ait $b_m z^m \in \mathbf{R}$ et $b_m z^m < 0$.

Plus précisement, si $|z| < 1$ et $0 < |z| < r_1 := |b_m|/(|b_{m+1}| + \cdots + |b_n|)$, alors

$$|h(z)| < |z^{m+1}|(|b_{m+1}| + \cdots + |b_n||z^{n-m-1}|) < |z^{m+1}|(|b_{m+1}| + \cdots + |b_n|) < |b_m z^m|.$$

De plus, si $|z| < r_2 := 1/|b_m|^{1/m}$, alors $|b_m z^m| < 1$. Par conséquent, on a $|h(z)| < |b_m z^m| < 1$ si $0 < |z| < r_0 := \min(1, r_1, r_2)$.

Il faut trouver z tel que $b_m z^m < 0$, ce qui équivaut à $(-b_m/|b_m|)z^m > 0$. On sait qu'il existe $w \in \mathbf{C}$ tel que $w^m = -|b_m|/b_m$; on pose $z = tw$, où $0 < t < \min(r, r_0)$. On a $b_m z^m = -|b_m| t^m < 0$ et $|h(z)| < |b_m z^m| < 1$, d'où

$$g(z) = 1 + b_m z^m + h(z) = 1 - |b_m z^m| + h(z), \qquad |g(z)| \leq |1 - |b_m z^m|| + |h(z)| = 1 - |b_m z^m| + |h(z)| < 1.$$

□

10.3.6 Une autre preuve du lemme d'Argand Pour démontrer l'existence d'une racine m-ième d'un nombre complexe de valeur absolue $|z| = 1$ il faut utiliser des formules trigonométriques : il faut savoir que z s'écrit $z = \cos(\alpha) + i\sin(\alpha)$, où $\alpha \in \mathbf{R}$, et que $z = (\cos(\alpha/m) + i\sin(\alpha/m))^m$.

Voici une autre preuve du lemme 10.3.5 qui n'utilise que l'existence d'une racine carré des nombres complexes :

— si $z = a + bi \in \mathbf{C}$, alors $w := \sqrt{(a + \sqrt{a^2 + b^2})/2} + i\sqrt{(-a + \sqrt{a^2 + b^2})/2} \in \mathbf{C}$ vérifie $w^2 = z$.

Si l'on écrit $g(z) = 1 + g_0(z)$, $g_0(z) = z^m(b_m + z(b_{m+1} + \cdots + b_n z^{n-m-1}))$ $(b_m \neq 0)$, alors on a $|g(z)|^2 = (1 + g_0(z))(1 + \overline{g_0(z)}) = 1 + 2\,\mathrm{Re}(g_0(z)) + |g_0(z)|^2$. On fixe $w \in \mathbf{C} \smallsetminus \{0\}$ et on prend $z = tw$, où $t > 0$. L'égalité $\lim_{z \to 0} g_0(z)/z^m = b_m$ implique que

$$\lim_{t \to 0+} \frac{|g(tw)|^2 - 1}{t^m} = 2\,\mathrm{Re}(b_m w^m).$$

Il suffit, donc, de montrer qu'il existe $w \in \mathbf{C}$ tel que $\mathrm{Re}(b_m w^m) < 0$. On écrit $m = 2^k n$, où $2 \nmid n$.

— Si $\mathrm{Re}(b_m) < 0$, on prend $w = 1$.

— Si $\mathrm{Re}(b_m) > 0$, on prend w tel que $w^{2^k} = -1$, d'où $w^m = -1$.

— Si $\mathrm{Re}(b_m) = 0$ et $\mathrm{Re}(i^n b_m) < 0$, on prend w tel que $w^{2^k} = i$, d'où $w^m = i^n$.

— Si $\mathrm{Re}(b_m) = 0$ et $\mathrm{Re}(i^n b_m) > 0$, on prend w tel que $w^{2^k} = -i$, d'où $w^m = -i^n$.

10.3.7 Exercice. Supposons que $z_0 \in \mathbf{C}$, $R > 0$, $a_0, a_1, a_2, \ldots \in \mathbf{C}$, il existe $m > 0$ tel que $a_m \neq 0$, et $\sup_{n \in \mathbf{N}} |a_n| R^n < +\infty$.
(1) La série $f(z) := \sum_{n=0}^{\infty} a_n (z - z_0)^n$ converge absolument si $z \in \mathbf{C}$ et $|z - z_0| < R$.
(2) Il existe $z \in \mathbf{C}$ tel que $|z - z_0| < R$ et $|f(z)| > |f(z_0)| = |a_0|$.
(3) Si $f(z_0) = a_0 \neq 0$, alors il existe $z \in \mathbf{C}$ tel que $|z - z_0| < R$ et $|f(z)| < |f(z_0)| = |a_0|$.

10.3.8 Proposition. *(1) Si le corps K est algébriquement clos (par exemple, $K = \mathbf{C}$), alors l'ensemble $\mathcal{P}_K$ de tous les polynômes irréductibles unitaires (non constants) dans $K[X]$ est égal à $\{X - \alpha \mid \alpha \in K\}$. (2) L'ensemble $\mathcal{P}_{\mathbf{R}}$ est égal à $\{X - \alpha \mid \alpha \in \mathbf{R}\} \cup \{(X - \beta)(X - \overline{\beta}) = X^2 - 2\,\mathrm{Re}(\beta)X + |\beta|^2 \mid \beta \in \mathbf{C} \smallsetminus \mathbf{R}\}$.*

Démonstration. (1) Soit $f \in \mathcal{P}_K$. Il existe $\alpha \in K$ tel que $f(\alpha) = 0$, ce qui signifie que f est divisible par $X - \alpha$ dans $K[X]$. Les polynômes f et $X - \alpha$ sont irréductibles (et non constants), ce qui implique qu'il existe $b \in K[X]^* = K^* = K \smallsetminus \{0\}$ tel que $f = b(X - \alpha)$. Les deux polynômes étant unitaires, on a $b = 1$.

(2) Soit $f \in \mathcal{P}_{\mathbf{R}}$. D'après le théorème 10.3.4 il existe $\alpha \in \mathbf{C}$ tel que $f(\alpha) = 0$. Si $\alpha \in \mathbf{R}$, alors le raisonnement dans (1) implique que $f = X - \alpha$. Si $\alpha \notin \mathbf{R}$, alors $0 = \overline{f(\alpha)} = \overline{f}(\overline{\alpha}) = f(\overline{\alpha})$. Par conséquent, f est divisible dans $\mathbf{C}[X]$ par $X - \alpha$ et $X - \overline{\alpha}$, donc par $g := \mathrm{ppcm}(X - \alpha, X - \overline{\alpha}) = (X - \alpha)(X - \overline{\alpha}) \in \mathbf{R}[X]$ (on a utilisé le fait que $\alpha \neq \overline{\alpha}$). Le corollaire 9.3.5 implique alors que $g \mid f$ dans $\mathbf{R}[X]$, car $f = gh$ avec $h \in \mathbf{C}[X]$ et $f, g \in \mathbf{R}[X]$. Le polynôme $g = X^2 - 2\,\mathrm{Re}(\alpha)X + |\alpha|^2 \in \mathbf{R}[X]$ est unitaire et irréductible dans $\mathbf{R}[X]$, car $\deg(g) = 2$ et g n'a pas de racines dans $\mathbf{R}$. Le raisonnement de (1) montre alors que $f = g$. □

10.4 Anneau quotient $K[X]/(b)$

10.4.1 Dimension de $K[X]/(b)$ Soit $b \in K[X] \smallsetminus \{0\}$ un polynôme de degré $\deg(b) = n \geq 0$. D'après (9.3.6.1), l'application

$$K[X]_{\deg < n} \hookrightarrow K[X] \longrightarrow K[X]/(b) \tag{10.4.1.1}$$

est K-linéaire et bijective. Autrement dit, c'est un isomorphisme de K-espaces vectoriels, ce qui implique que l'anneau quotient $K[X]/(b)$ est un espace vectoriel de dimension n sur K.

Si $n = 1$, alors $b = a_1(X - \alpha)$, où $\alpha \in K$ et $a_1 \in K \smallsetminus \{0\}$. L'aplication (10.4.1.1) est alors un isomomorphisme d'anneaux

$$K \xrightarrow{\sim} K[X]/(X - \alpha).$$

Son inverse est l'isomorphisme d'évaluation en α

$$\overline{\mathrm{ev}}_\alpha : K[X]/(X - \alpha) \xrightarrow{\sim} K, \qquad a \pmod{(X - \alpha)} \mapsto a(\alpha). \tag{10.4.1.2}$$

10.4.2 Le théorème chinois dans $K[X]$ Le théorème 3.3.2 (la version arithmétique du théorème chinois) a été déduit de la version forte du théorème de Bézout. Pour démontrer le théorème 10.4.3 ci-dessous on peut utiliser la relation (10.2.5.2) de la même manière, ou on peut raisonner directement (cf. la Remarque 2 dans le paragraphe 3.3.3).

10.4.3 Théorème (Le théorème chinois dans $K[X]$)**.** *Si $a, b \in K[X] \smallsetminus \{0\}$ et si $\mathrm{pgcd}(a, b) = 1$, alors l'application*

$$\begin{aligned} f : K[X]/(ab) &\longrightarrow K[X]/(a) \times K[X]/(b) \\ c \pmod{ab} &\mapsto (c \pmod{a}, c \pmod{b}) \end{aligned}$$

est bijective (il s'agit, donc, d'un isomorphisme d'anneaux).

Démonstration. L'application f est un morphisme d'anneaux. Si $c \pmod{ab} \in \mathrm{Ker}(f)$, alors c est divisible dans $K[X]$ par a et b, donc aussi par $\mathrm{ppcm}(a, b) = \lambda ab/\mathrm{pgcd}(a, b) = \lambda ab$ ($\lambda \in K^*$), d'où $c \equiv 0 \pmod{ab}$. Cela montre que $\mathrm{Ker}(f) = \{0\}$ et que l'application f est injective. On en déduit que f est bijective, car f est K-linéaire et les K-espaces vectoriels $K[X]/(ab)$ et $K[X]/(a) \times K[X]/(b)$ ont la même dimension $\deg(ab) = \deg(a) + \deg(b)$. □

10.4.4 Exemple : $\mathbf{R}[X]/(X^2-1)$ Si l'on met ensemble l'isomorphisme d'anneaux

$$\begin{array}{rcl} \mathbf{R}[X]/(X^2-1) & \xrightarrow{\sim} & \mathbf{R}[X]/(X-1)\times\mathbf{R}[X]/(X+1) \\ f \pmod{(X^2-1)} & \mapsto & (f \pmod{(X-1)}, f \pmod{(X+1)}) \end{array}$$

du théorème chinois et les isomorphismes d'évaluation (10.4.1.2)

$$\overline{\mathrm{ev}}_{\pm 1} : \mathbf{R}[X]/(X\mp 1) \xrightarrow{\sim} \mathbf{R}, \qquad f \pmod{(X\mp 1)} \mapsto f(\pm 1),$$

on obtient un isomorphisme d'anneaux

$$(\overline{\mathrm{ev}}_1, \overline{\mathrm{ev}}_{-1}) : \mathbf{R}[X]/(X^2-1) \xrightarrow{\sim} \mathbf{R}\times\mathbf{R}, \qquad f \pmod{(X^2-1)} \mapsto (f(1), f(-1)). \tag{10.4.4.1}$$

Explicitement,

$$\mathbf{R}[X]/(X^2-1) = \{u+vX \pmod{(X^2-1)} \mid u,v\in\mathbf{R}\}, \ \ (\overline{\mathrm{ev}}_1, \overline{\mathrm{ev}}_{-1}) : u+vX \pmod{(X^2-1)} \mapsto (u+v, u-v).$$

L'inverse à (10.4.4.1) est défini par

$$\mathbf{R}\times\mathbf{R} \xrightarrow{\sim} \mathbf{R}[X]/(X^2-1), \qquad (s,t) \mapsto \tfrac{(s+t)+(s-t)X}{2} \pmod{(X^2-1)}. \tag{10.4.4.2}$$

Autrement dit, $f(X) = \frac{(s+t)+(s-t)X}{2}$ est l'unique polynôme dans $\mathbf{R}[X]$ de degré $\deg < 2$ tel que $f(1) = s$ et $f(-1) = t$.

10.4.5 Exemple : $\mathbf{R}[X]/(X^2+1)$ Le polynôme X^2+1 est irréductible dans $\mathbf{R}[X]$. Il se factorise dans $\mathbf{C}[X]$ comme $(X-i)(X+i)$ (ces racines étant $\pm i$). L'évaluation

$$\mathrm{ev}_i : \mathbf{R}[X] \longrightarrow \mathbf{C}, \qquad f \mapsto f(i)$$

est un morphisme d'anneaux tel que $\mathrm{Im}(\mathrm{ev}_i) = \mathbf{C}$ (car $\mathrm{ev}_i(u+vX) = u+vi$) et $\mathrm{Ker}(\mathrm{ev}_i) = (X^2+1) = (X^2+1)\mathbf{R}[X]$.

En effet, si $f\in\mathbf{R}[X]$ vérifie $f(i)=0$, alors $0 = \overline{f(i)} = \overline{f}(\bar{i}) = f(-i)$, ce qui implique que f est divisible dans $\mathbf{C}[X]$ par $X-i$ et $X+i$, donc aussi par $\mathrm{ppcm}(X-i, X+i) = X^2+1$. Le corollaire 9.3.5 implique alors que f est divisible par X^2+1 dans $\mathbf{R}[X]$ (voir le raisonnement dans la preuve de la proposition 10.3.8).

Le théorème de l'homomorphisme 8.5.12 implique alors que l'application

$$\overline{\mathrm{ev}}_i : \mathbf{R}[X]/(X^2+1) \xrightarrow{\sim} \mathbf{C}, \qquad f \pmod{(X^2+1)} \mapsto f(i)$$

est un isomorphisme d'anneaux (son inverse étant $u+vi \mapsto u+vX \pmod{(X^2+1)}$).

On peut remplacer partout i par $-i$. L'isomorphisme d'anneaux ainsi obtenu

$$\overline{\mathrm{ev}}_{-i} : \mathbf{R}[X]/(X^2+1) \xrightarrow{\sim} \mathbf{C}, \qquad f \pmod{(X^2+1)} \mapsto f(-i)$$

est égal à la composition de $\overline{\mathrm{ev}}_i$ avec la conjugaison complexe sur on $\mathbf{C}$, car $\mathrm{ev}_{\pm i}(u+vX) = u\pm vi$.

10.4.6 Exercice. Décrire l'anneau quotient $\mathbf{R}[X]/(X^2+X+1)$ de la même manière.

10.4.7 Théorème. *Soient $a,b\in K[X]$, $b\neq 0$. La classe de congruence $a \pmod b \in K[X]/(b)$ est inversible dans $K[X]/(b)$ si et seulement si* $\mathrm{pgcd}(a,b) = 1$.

Démonstration. On s'est appercu dans (8.5.11.2) et (9.3.2.1) que $a \pmod b$ est inversible dans $K[X]/(b)$ si et seulement si $1 \in aK[X] + bK[X] = \mathrm{pgcd}(a,b)K[X]$, ce qui équivaut à $\mathrm{pgcd}(a,b) = 1$. □

10.4.8 Calcul de l'inverse de $a \pmod b$ On calcule d'abord $\operatorname{pgcd}(a,b)$ en utilisant l'algorithme d'Euclide. Si $\operatorname{pgcd}(a,b) \neq 1$, alors $a \pmod b$ n'est pas inversible dans $K[X]/(b)$. Si $\operatorname{pgcd}(a,b) = 1$, l'algorithme d'Euclide fournit aussi une relation de Bézout explicite $au + bv = 1$, où $u, v \in K[X]$, ce qui implique que $au \equiv 1 \pmod b$ et que $u \pmod b$ est égal à l'inverse de $a \pmod b$ dans $K[X]/(b)$.

10.4.9 Exercice. (1) Calculer l'inverse de $X^2 - 2X + 3 \pmod{(X^3 - 2)}$ dans $\mathbf{Q}[X]/(X^3 - 2)$.
(2) Ecrire $(3 - 2\sqrt[3]{2} + \sqrt[3]{4})^{-1}$ sous la forme $a + b\sqrt[3]{2} + c\sqrt[3]{4}$, où $a, b, c \in \mathbf{Q}$.
(3) Y a-t-il un lien entre (1) et (2) ?

10.4.10 Théorème. *Soient $b \in K[X]$, $b \neq 0$. Les propriétés suivantes sont équivalentes.*
(1) $K[X]/(b)$ est un corps.
(2) $K[X]/(b)$ est un anneau intègre.
(3) Le polynôme b est non constant et irréductible dans $K[X]$.

Démonstration. L'implication (1) $\implies$ (2) est automatique.
(2) $\implies$ (3) : Si b est constant, alors $(b) = (1) = K[X]$ et $K[X]/(b) = \{0\}$ n'est pas un anneau intègre. Si $b = fh$ est non constant mais réductible ($f, h \in K[X]$, f, h non constants), alors $\deg(f), \deg(h) < \deg(b)$, ce qui implique que $b \nmid f$ et $b \nmid h$. Par conséquent, les classes $f \pmod b$ et $h \pmod b$ sont des éléments non nuls de $K[X]/(b)$, mais leur produit est égal à zéro, car $fh \equiv 0 \pmod b$.
(3) $\implies$ (1) : on peut supposer que b est irréducible et unitaire. Il faut montrer que toute classe de congruence non nulle $a \pmod b \neq 0 \in K[X]/(b)$ est inversible dans $K[X]/(b)$. Le plus grand commun diviseur $d := \operatorname{pgcd}(a,b)$ divise b ; il est donc égal soit à 1, soit à b, grâce à l'irréductibilité de b. Si $d = b$, alors $b \mid a$, ce qui implique que $a \pmod b = 0$. La contradiction montre que $d = 1$, et donc $a \pmod b$ est inversible dans $K[X]/(b)$, d'après le théorème 10.4.7. □

10.4.11 Remarque On peut aussi démontrer l'implication non triviale (2) $\implies$ (1) d'une façon plus abstraite (voir la proposition 8.3.7 et l'exercise 8.3.9).

10.5 Applications de $K[X]/(b)$ (exemples)

10.5.1 Introduction Les exemples ci-dessous sont inclus ici pour illustrer la théorie générale qu'on a vue dans le paragraphe 10.4. Le lecteur peut passer directement au paragraphe 10.6.

10.5.2 Interpolation de Lagrange Etant donnés

- un corps K
- n éléments distincts $\alpha_1, \ldots, \alpha_n \in K$
- n éléments $t_1, \ldots, t_n \in K$

on cherche à trouver un polynôme $g \in K[X]$ tel que

$$\deg(g) < n, \qquad \forall i = 1, \ldots, n \quad g(\alpha_i) = t_i. \tag{10.5.2.1}$$

On a résolu un cas très particulier de ce problème ($n = 2$, $\alpha_1 = 1$, $\alpha_2 = -1$) dans le paragraphe 10.4.4.

Unicité : si $g, h \in K[X]$ sont des solutions de (10.5.2.1), alors $g - h \in K[X]$ est un polynôme de degré $\deg(g - h) < n$ ayant au moins n racines distinctes dans K, à savoir $\alpha_1, \ldots, \alpha_n \in K$. On en déduit que $g - h = 0$, grâce au théorème 9.2.7.

Construction : on peut exprimer g en termes des polynômes suivants :

$$f(X) = \prod_{i=1}^{n} (X - \alpha_i), \qquad f_i(X) = \prod_{\substack{j=1 \\ j \neq i}}^{n} (X - \alpha_j) = f(X)/(X - \alpha_i).$$

En effet, on a

$$(X-\alpha_i)f_i(X)=f(X),\qquad \deg(f_i)=n-1,\qquad f_i(\alpha_j)=\begin{cases}f_i(\alpha_i)\neq 0, & j=i\\ 0, & j\neq i,\end{cases} \tag{10.5.2.2}$$

ce qui implique que les polynômes $p_i(X)=f_i(X)/f_i(\alpha_i)$ vérifient $p_i(\alpha_j)=\delta_{ij}$ (le symbole de Kronecker) et que

$$g=\sum_{i=1}^{n} t_i\, p_i(X)$$

est une solution de (10.5.2.1). On a

$$(X-\alpha_i)(f_i(X)-f'(\alpha_i))=f(X)-f(\alpha_i)-(X-\alpha_i)f'(\alpha_i)\equiv 0 \pmod{(X-\alpha_i)^2}$$

d'après (9.2.5.2), ce qui implique que $f_i(\alpha_i)=f'(\alpha_i)$. Par conséquent,

$$p_i(X)=\frac{1}{f'(\alpha_i)}\frac{f(X)}{X-\alpha_i},\qquad g=\sum_{i=1}^{n} t_i\,\frac{1}{f'(\alpha_i)}\frac{f(X)}{X-\alpha_i}$$

est une solution de (10.5.2.1).

Le polynôme constant 1 est une solution de (10.5.2.1) pour $t_1=\cdots=t_n$, ce qui implique que

$$\sum_{i=1}^{n} p_i(X)=1.$$

10.5.3 Reformulation algébrique La condition $g(\alpha_i)=t_i$ équivaut à $g\equiv t_i \pmod{(X-\alpha_i)}$, ce qui signifie que pour résoudre (10.5.2.1) il faut invertir l'isomorphisme d'anneaux

$$\begin{aligned} &K[X]/(f)\xrightarrow{\sim}\prod_{i=1}^{n}K[X]/(X-\alpha_i)\xrightarrow{\sim}\prod_{i=1}^{n}K\\ &g \pmod f \;\mapsto\; (g \pmod{(X-\alpha_i)})\mapsto (g(\alpha_1),\dots,g(\alpha_n)),\end{aligned} \tag{10.5.3.1}$$

car $K[X]/(f)=\{g \pmod f \mid \deg(g)<n\}$. Sous cet isomorphisme, les classes de congruence $p_i(X) \pmod f$ correspondent aux éléments $e_i=(0,\dots,1,\dots,0)\in K\times\cdots\times K$.

10.5.4 Exercice. Définir un isomorphisme d'anneaux $\mathbf{R}[X]/(X^2+X-2)\xrightarrow{\sim}\mathbf{R}\times\mathbf{R}$. Expliciter son inverse.

10.5.5 Déterminants d'interpolation Si la valeur de n est petite on peut résoudre (10.5.2.1) à la main. Si $n=1$, alors $g(X)=t_1$.

Si $n=2$, alors $g(X)=u+vX$ et $u+v\alpha_i=t_i$ $(i=1,2)$, ce qui implique que $v(\alpha_2-\alpha_1)=t_2-t_1$ et

$$v=\tfrac{t_2-t_1}{\alpha_2-\alpha_1},\qquad u=t_1-v\alpha_1=\tfrac{t_1(\alpha_2-\alpha_1)-(t_2-t_1)\alpha_1}{\alpha_2-\alpha_1}=-\tfrac{\alpha_1t_2-\alpha_2t_2}{\alpha_2-\alpha_1},\qquad g(X)=\tfrac{(t_2-t_1)X-(\alpha_1t_2-\alpha_2t_2)}{\alpha_2-\alpha_1}$$

Ces formules s'écrivent comme suit :

$$v=\frac{\begin{vmatrix}1&1\\ t_1&t_2\end{vmatrix}}{\begin{vmatrix}1&1\\ \alpha_1&\alpha_2\end{vmatrix}},\qquad u=-\frac{\begin{vmatrix}\alpha_1&\alpha_2\\ t_1&t_2\end{vmatrix}}{\begin{vmatrix}1&1\\ \alpha_1&\alpha_2\end{vmatrix}},\qquad Y-g(X)=\frac{\begin{vmatrix}1&1&1\\ \alpha_1&\alpha_2&X\\ t_1&t_2&Y\end{vmatrix}}{\begin{vmatrix}1&1\\ \alpha_1&\alpha_2\end{vmatrix}}$$

10.5.6 Exercice. Trouver une formule analogue pour $Y - g(X)$ qui soit valable pour tout $n \geq 1$.

10.5.7 Diagonalisabilité de matrices Soit $A \in M_n(K)$ une matrice carré à coefficients dans un corps K. On note $P_A(X) := \det(X \cdot I_n - A) \in K[X]$ le polynôme caractéristique de A.

La matrice A définit une application linéaire

$$K^n \longrightarrow K^n, \qquad X \mapsto AX.$$

L'image de cette application est le sous-espace vectoriel de K^n engendré par les images Ae_i des vecteurs $e_i = {}^t(0, \ldots, 1, \ldots 0)$ de la base canonique de K^n. Remarquons que le vecteur Ae_i n'est rien d'autre que la i-ième colonne de A, ce qui signifie que $\mathrm{Im}(A)$ est engendré par les colonnes de A.

Pour tout scalaire $\alpha \in K$ on note

$$V(\alpha) := \mathrm{Ker}(A - \alpha \cdot I_n) = \{v \in V = K^n \mid Av = \alpha v\} \subset V = K^n$$

l'espace propre de A qui correspond à α. Le sous-espace $V(\alpha)$ est non nul si et seulement si $P_A(\alpha) = 0$. Un élément non nul de $V(\alpha)$ est un **vecteur propre** de A, et $\alpha \in K$ est la **valeur propre** correspondante.

Si $v \in V(\alpha)$, alors $A^2v = A(\alpha v) = \alpha^2 v$, $A^3v = A(\alpha^2 v) = \alpha^3 v$, etc. On en déduit que l'on a $g(A)v = g(\alpha)v$ pour tout $g \in K[X]$.

La matrice A est **diagonalisable sur** K s'il existe une base de $V = K^n$ dont les éléments sont des vecteurs propres de A. Si c'est le cas, on peut mettre les éléments d'une telle base comme les colonnes d'une matrice $P \in M_n(K)$. Cette matrice sera inversible ($P \in GL_n(K)$) et la matrice $P^{-1}AP$ sera diagonale (les termes diagonaux étant les valeurs propres de A).

On va étudier les vecteurs propres et la diagonalisabilité de A en utilisant interpolation de Lagrange, i.e., une version explicite du théorème chinois

$$K[X]/\prod_{i=1}^{m}(X - \alpha_i) \xrightarrow{\sim} \prod_{i=1}^{m} K[X]/(X - \alpha_i) \xrightarrow{\sim} \prod_{i=1}^{m} K \tag{10.5.7.1}$$

(avec $\alpha_1, \ldots, \alpha_m \in K$ distincts).

10.5.8 Proposition. *Soient $\alpha_1, \ldots, \alpha_m \in K$ distincts. On définit des polynômes*

$$f(X) = \prod_{i=1}^{m}(X - \alpha_i), \qquad f_i(X) = \prod_{\substack{j=1 \\ j \neq i}}^{m}(X - \alpha_j) = f(X)/(X - \alpha_i), \qquad p_i(X) = f_i(X)/f_i(\alpha_i)$$

comme dans (10.5.2.2).
(1) Si $v = v_1 + \cdots v_m$ et $v_j \in V(\alpha_j)$ pour tout j, alors on a $v_i = p_i(A)v$ pour tout i.
(2) Si $0 \neq v_i \in V(\alpha_i)$ pour tout i, alors $v_1, \ldots, v_m$ sont linéairement indépendants dans $V = K^n$.
*(3) Le sous-espace $W := V(\alpha_1) + \cdots + V(\alpha_m) = \{v_1 + \cdots + v_m \mid v_i \in V(\alpha_i)\} \subset V$ est une somme **directe** des sous-espaces $V(\alpha_1), \ldots, V(\alpha_m)$.*
(4) La projection de $W = V(\alpha_1) \oplus \cdots \oplus V(\alpha_m)$ sur le i-ième facteur est définie par $v \mapsto p_i(A)v$. En particulier, $p_i(A)W = V(\alpha_i)$.
(5) $W = \mathrm{Ker}(f(A)) := \{v \in V \mid f(A)v = 0\}$.

Démonstration. (1) C'est une conséquence des formules

$$p_i(\alpha_j) = \begin{cases} 1, & i = j \\ 0, & i \neq j, \end{cases} \qquad p_i(A)v_j = p_i(\alpha_j)v_j = \begin{cases} v_i, & i = j \\ 0, & i \neq j, \end{cases} \qquad p_i(A)\big(\sum_{j=1}^{m} v_j\big) = v_i.$$

(2) Si $t_j \in K$ et $\sum t_j v_j = 0$, alors $0 = p_i(A)\sum t_j v_j = t_i v_i$, d'où $t_i = 0$.
(3), (4) C'est une reformulation abstraite de (1).

(5) Si $(A-\alpha_i\cdot I)v=0$, alors $f(A)v=f_i(A)(A-\alpha_i\cdot I)v=0$. On en déduit que $\mathrm{Ker}(f)$ contient chaque $V(\alpha_i)$, donc aussi leur somme W. Réciproquement, si $v\in\mathrm{Ker}(f(A))$, alors $(A-\alpha_i\cdot I)p_i(A)v=\frac{f(A)}{f_i(\alpha_i)}\,v=0$, ce qui implique que $p_i(A)v\in V(\alpha_i)$ et $v=(\sum_i p_i(A))v\in\sum V(\alpha_i)=W$. □

10.5.9 Proposition. *Supposons que le polynôme caractéristique de A s'écrit $P_A(X)=\prod_{i=1}^n(X-\alpha_i)$, où $\alpha_1,\dots,\alpha_n\in K$ appartiennent à K et sont distincts.*
(1) Chaque espace propre $V(\alpha_i)=Kv_i$ est de dimension un et les vecteurs propres $v_1,\dots,v_n$ forment une base de $V=K^n$.
(2) La matrice A est diagonalisable sur K.
(3) $P_A(A)=0$ (le théorème de Cayley–Hamilton pour A).
(4) La projection de $V=Kv_1\oplus\cdots\oplus Kv_n$ sur Kv_i est définie par $v\mapsto p_i(A)$, où $p_i(X)\in K[X]$ est comme dans la proposition 10.5.8, avec $f(X)=P_A(X)$.

Démonstration. (1) D'après la proposition 10.5.8, le sous-espace $W:=V(\alpha_1)+\cdots+V(\alpha_n)\subset V=K^n$ est une somme directe $W=V(\alpha_1)\oplus\cdots\oplus V(\alpha_n)$ de n sous-espaces non nuls. Leurs dimensions vérifient

$$n=\dim(V)\geq\dim(W)=\sum_{i=1}^n\dim(V(\alpha_i))\geq\sum_{i=1}^n 1=n,$$

ce qui implique qu'il y a des égalités partout : $V=W$, $\dim(V(\alpha_i))=1$, $V(\alpha_i)=Kv_i$ et $K^n=V=Kv_1\oplus\cdots\oplus Kv_n$. La dernière égalité nous dit que les vecteurs $v_1,\dots,v_n$ forment une base de K^n, ce qui montre (2). Le point (3) est une conséquence du fait que $P_A(A)v_i=f_i(A)(A-\alpha_i\cdot I)v_i=0$, pour tout i. Le point (4) est un cas particulier de la proposition 10.5.8(4). □

10.5.10 Exemples (1) La matrice $A=\begin{pmatrix}4&-2\\1&1\end{pmatrix}\in M_2(\mathbf{R})$ vérifie $\mathrm{Tr}(A)=5$, $\det(A)=6$, $P_A(X)=X^2-5X+6=(X-2)(X-3)$ et

$$A-2I=\begin{pmatrix}2&-2\\1&-1\end{pmatrix},\qquad A-3I=\begin{pmatrix}1&-2\\1&-2\end{pmatrix},\qquad (A-2I)(A-3I)=0,$$
$$\mathrm{Im}(A-2I)=\mathbf{R}\begin{pmatrix}2\\1\end{pmatrix}=\mathrm{Ker}(A-3I),\qquad \mathrm{Im}(A-3I)=\mathbf{R}\begin{pmatrix}1\\1\end{pmatrix}=\mathrm{Ker}(A-2I).$$

On a $\alpha_1=2$, $\alpha_2=3$, $f_1=X-3$, $f_2=X-2$, $p_1=3-X$, $p_2=X-2$.
(2) Considérons la matrice

$$A=\begin{pmatrix}-7&18&27\\0&5&6\\-2&2&4\end{pmatrix}\in M_3(\mathbf{R}),\qquad P_A(X)=X^3-2X^2-X+2=(X-1)(X-2)(X+1).$$

On a $\alpha_1=1$, $\alpha_2=2$, $\alpha_3=-1$, $f_1=(X-2)(X+1)$, $f_2=(X-1)(X+1)$, $f_3=(X-1)(X-2)$, $p_1=-f_1/2$, $p_2=f_2/3$, $p_3=f_3/6$ et

$$\mathrm{Ker}(A-\alpha_iI)=\mathbf{R}v_i,\qquad v_1=\begin{pmatrix}0\\-3\\2\end{pmatrix},\qquad v_2=\begin{pmatrix}1\\2\\-1\end{pmatrix},\qquad v_3=\begin{pmatrix}3\\-2\\2\end{pmatrix},$$
$$f_1(A)=\big(4v_1\big|-10v_1\big|-16v_1\big),\qquad f_2(A)=\big(-6v_2\big|18v_2\big|27v_2\big),\qquad f_3(A)=\big(6v_3\big|-12v_3\big|-18v_3\big).$$

10.5.11 Proposition (Caractérisation des matrices diagonalisables)**.** *Les propriétés suivantes sont équivalentes :*

(1) $A \in M_n(K)$ est diagonalisable sur K.
(2) Il existe $f = \prod_{i=1}^m (X - \alpha_i) \in K[X]$ tel que $\alpha_1, \dots, \alpha_m \in K$ sont distincts et $f(A) = 0$.
(3) Il existe f vérifiant (2) tel que $P_A(\alpha_i) = 0$ pour tout $i = 1, \dots, m$.

Démonstration. (3) $\Longrightarrow$ (2) est automatique.
(2) $\Longrightarrow$ (3) : On écrit

$$f = \prod_{P_A(\alpha_i)=0} (X - \alpha_i) \prod_{P_A(\alpha_i)\neq 0} (X - \alpha_i) = f_1 f_2.$$

Si $P_A(\alpha_i) \neq 0$, alors $A - \alpha_i \cdot I$ est inversible ; on en déduit l'invertibilité de $f_2(A)$. Par conséquent, $f(A) = 0$ implique que $f_1(A) = f(A) f_2(A)^{-1} = 0$.
(1) $\Longrightarrow$ (3) : D'après (1), on a $V = Ku_1 \oplus \cdots \oplus Ku_n$, $Au_j = \lambda_j u_j$. On écrit $P_A(A) = \prod_{j=1}^n (X - \lambda_j) = \prod_{i=1}^m (X - \alpha_i)^{k_i}$, où $\alpha_1, \dots, \alpha_m \in K$ sont distincts et $k_i \geq 1$. Pour tout $j = 1, \dots, n$ il existe $i \in \{1, \dots, m\}$ tel que $\lambda_j = \alpha_i$, ce qui implique que $f(A)u_j = \prod_{i=1}^m (A - \alpha_i \cdot I)u_j = 0$.
(2) $\Longrightarrow$ (1) : D'après la proposition 10.5.8, on a $\mathrm{Ker}(f(A)) = V(\alpha_1) \oplus \cdots \oplus V(\alpha_m)$, mais $\mathrm{Ker}(f(A)) = V$, car $f(A) = 0$. Si l'on choisit une base quelconque de chacun de $V(\alpha_i)$, on obtient une base de V dont tous les éléments sont des vecteurs propres de A. □

10.5.12 Remarques (1) L'ensemble $J := \{g \in K[X] \mid g(A) = 0\} \subset K[X]$ est un idéal de $K[X]$. Il est non nul, car les $n^2 + 1 > n^2 = \dim_K(M_n(K))$ matrices $I, A, A^2, \dots, A^{n^2} \in M_n(K)$ satisfont à une relation linéaire non triviale à coefficients dans K. On a $J = (f_A) = f_A K[X]$, où $f_A \in K[X]$ est un polynôme unitaire (unique) ; on l'appelle le **polynôme minimal** de A.

(2) La proposition 10.5.11 implique que $A \in M_n(K)$ est diagonalisable sur K si et seulement si son polynôme minimal f_A s'écrit $f_A(X) = \prod_{i=1}^m (X - \alpha_i)$, où $\alpha_1, \dots, \alpha_m \in K$ appartiennent à K et sont distincts.

(3) Selon le théorème de Cayley–Hamilton, on a $P_A(A) = 0$. En particulier, le polynôme minimal f_A divise le polynôme caractéristique P_A dans $K[X]$.

Exemples :

$$A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad P_A(X) = f_A(X) = X^2; \quad B = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \quad P_B(X) = X^2, \quad f_B(X) = X.$$

(4) L'évaluation

$$\mathrm{ev}_A : K[X] \longrightarrow M_n(K) = \mathrm{End}_K(V), \qquad g(X) \mapsto g(A)$$

est un morphisme d'anneaux tel que $\mathrm{Ker}(\mathrm{ev}_A) = (f_A) = f_A K[X]$. Il induit, donc, un isomorphisme d'anneaux

$$\overline{\mathrm{ev}}_A : K[X]/(f_A) \xrightarrow{\sim} \mathrm{Im}(\mathrm{ev}_A), \qquad g \pmod{f_A} \mapsto g(A).$$

Dans un cas particulier lorsque $f_A(X) = \prod_{i=1}^m (X - \alpha_i)$, où $\alpha_1, \dots, \alpha_m \in K$ appartiennent à K et sont distincts, on a un autre isomorphisme d'anneaux (10.5.7.1)

$$(\overline{\mathrm{ev}}_{\alpha_1}, \dots, \overline{\mathrm{ev}}_{\alpha_m}) : K[X]/(f_A) \xrightarrow{\sim} \prod_{i=1}^m K[X]/(X - \alpha_i) \xrightarrow{\sim} \prod_{i=1}^m K.$$

Sous cet isomorphisme la classe $p_i \pmod{f_A}$ correspond à $e_i = (0, \dots, 1, \dots, 0) \in K \times \cdots \times K$. La matrice $\mathrm{ev}_A(p_i)$ définit la projection de $V = K^n$ sur $V(\alpha_i)$.

10.6 Construction de corps

10.6.1 Théorème. *Si $f \in K[X]$ est un polynôme irréductible de degré $\deg(f) = n \geq 1$, alors l'anneau $L := K[X]/(f)$ est un corps contenant K. L'élément $\alpha := \overline{X} = X \pmod f \in L$ vérifie $f(\alpha) = 0$. Tout élément $\beta \in L$ s'écrit d'une façon unique*

$$\beta = r_0 + r_1\alpha + \cdots + r_{n-1}\alpha^{n-1} = r(\alpha) \qquad (r = r_0 + r_1X + \cdots + r_{n-1}X^{n-1} \in K[X],\ \deg(r) < n).$$

Autrement dit, L est un K-espace vectoriel de dimension n ; les éléments $1, \alpha, \ldots, \alpha^{n-1}$ forment une base de L sur K.

Démonstration. D'après le théorème 10.4.10, l'anneau L est un corps. Les autres énoncés ont été démontrés dans le paragraphe 9.3.6. □

10.6.2 Corollaire. *Si $g \in K[X]$ est un polynôme de degré $\deg(g) = m \geq 1$, alors il existe un corps $L \supset K$ dans lequel g a une racine, et un corps $M \supset K$ tel que $g = a_m(X - \alpha_1)\cdots(X - \alpha_m)$, où $a_m \in K^*$ et $\alpha_1, \ldots, \alpha_m \in M$ (pas forcément distincts).*

Démonstration. Il existe un polynôme irréductible $f \in K[X]$ (non constant) qui divise g dans $K[X]$. On pose $L := K[X]/(f)$ et $\alpha_1 := X \pmod f \in L$. L'anneau $L \supset K$ est un corps et on a $f(\alpha_1) = 0$, d'où $g = (X - \alpha_1)h$ avec $h \in L[X]$, $\deg(h) = m - 1$. On peut conclure par récurrence sur m. □

10.6.3 Exercice. Sous les hypothèse du corollaire 10.6.2, il est équivalent : $\alpha_1, \ldots, \alpha_m$ sont distincts $\iff \operatorname{pgcd}(g, g') = 1$ dans $K[X]$.

10.6.4 Construction réciproque Le lecteur peut aller directement au paragraphe 10.7 et ne pas tenir compte du reste de la discussion dans 10.6.

La construction dans le théorème 10.6.1 marche aussi dans l'autre sens (cf. le paragraphe 10.4.5).

Supposons que $K \subset M$ sont des corps et que $\alpha \in M$ est une racine d'un polynôme non constant à coefficients dans K (on dit que α est **algébrique sur** K). Le cas le plus simple est celui qu'on a considéré dans le paragraphe 10.4.5 : $K = \mathbf{R}$, $M = \mathbf{C}$ et $\alpha = i$.

- Il existe un polynôme unitaire (non constant) $f \in K[X]$ de degré minimum tel que $f(\alpha) = 0$. Il est unique, car la différence de deux polynômes ayant cette propriété est un polynôme de degré plus petit qui s'annule en α. On dit que f est le **polynôme minimal de α sur K**.
- Le polynôme f est irréductible dans $K[X]$ (si $f = gh$, alors $g(\alpha) = 0$ ou $h(\alpha) = 0$).
- Si $g \in K[X]$ vérifie $g(\alpha) = 0$, la division euclidienne dans $K[X]$ nous dit que $g = qf + r$, où $q, r \in K[X]$ et $\deg(r) < \deg(f)$. Comme $r(\alpha) = g(\alpha) - q(\alpha)f(\alpha) = 0$, minimalité de $\deg(f)$ implique que $r = 0$ et que f divise g dans $K[X]$.
- En particulier, si $g \in K[X]$ est unitaire, irréductible et $g(\alpha) = 0$, alors $g = f$.
- Réciproquement, si $g \in K[X]$ est divisible par f, alors $g(\alpha) = 0$.
- Autrement dit, le noyau du morphisme d'évaluation $\mathrm{ev}_\alpha : K[X] \longrightarrow M$ est égal à $\operatorname{Ker}(\mathrm{ev}_\alpha) = fK[X] = (f)$. Selon le théorème de l'homomorphisme 8.5.12, ev_α induit un isomorphisme d'anneaux (qui envoie chaque élément de K sur lui même) $\overline{\mathrm{ev}}_\alpha : K[X]/(f) \xrightarrow{\sim} \operatorname{Im}(\mathrm{ev}_\alpha)$ entre l'anneau abstrait $K[X]/(f)$ et le plus petit sous-anneau $K[\alpha] \subset M$ de M contenant K et α.
- Le théorème 10.6.1 affirme que $K[X]/(f)$ est un corps (donc $K[\alpha]$ est égal au plus petit sous-corps $K(\alpha) \subset M$ de M contenant K et α). On en déduit que $K(\alpha) = \operatorname{Im}(\mathrm{ev}_\alpha) = K + K\alpha + \cdots + K\alpha^{n-1} \subset M$ est un K-espace vectoriel de dimension $n = \deg(f)$ et base $1, \alpha, \ldots, \alpha^{n-1}$.
- Si $K = \mathbf{R}$, $M = \mathbf{C}$ et $\alpha = i$, alors $f = X^2 + 1$ et $\mathbf{R}(i) = \mathbf{R}[i] = \mathbf{R} + \mathbf{R}i = \mathbf{C}$.

— Voici une version abstraite du raisonnement ci-dessus : par l'hypothèse, le noyau du morphisme d'évaluation $\mathrm{ev}_\alpha : K[X] \longrightarrow M$ $(\mathrm{ev}_\alpha(h) = h(\alpha))$, qui est un idéal de $K[X]$, n'est pas nul. Par conséquent, $\mathrm{Ker}(\mathrm{ev}_\alpha) = fK[X]$, ou $f \in K[X]$ est un polynôme non constant. L'anneau quotient $K[X]/(f)$ est isomorphe à l'anneau intègre $\mathrm{Im}(\mathrm{ev}_\alpha) \subset M$, ce qui implique que f est irréductible dans $K[X]$.

— Si $K = \mathbf{Q}$, $M = \mathbf{C}$ et $\alpha = \sqrt{3}$, alors $g = X^2 - 3$ est unitaire, irréductible dans $\mathbf{Q}[X]$ (g n'a aucune racine dans $\mathbf{Q}$ et $\deg(g) \leq 3$) et $g(\sqrt{3}) = 0$, ce qui implique que $g = f$ est le polynôme minimal de $\sqrt{3}$ sur $\mathbf{Q}$ et l'application $\mathrm{ev}_{\sqrt{3}} : \mathbf{Q}[X]/(X^2 - 3) \xrightarrow{\sim} \mathbf{Q} + \mathbf{Q}\sqrt{3}$ $(h \pmod{X^2 - 3}) \mapsto h(\sqrt{3}))$ est un isomorphisme de corps.

— Si $K = \mathbf{Q}$, $M = \mathbf{C}$ et $\alpha = \sqrt[3]{2}$, alors $g = X^3 - 2$ est unitaire, irréductible dans $\mathbf{Q}[X]$ (g n'a aucune racine dans $\mathbf{Q}$ et $\deg(g) \leq 3$) et $g(\sqrt[3]{2}) = 0$, ce qui implique que $g = f$ est le polynôme minimal de $\sqrt[3]{2}$ sur $\mathbf{Q}$ et l'application $\mathrm{ev}_{\sqrt[3]{2}} : \mathbf{Q}[X]/(X^3 - 2) \xrightarrow{\sim} \mathbf{Q} + \mathbf{Q}\sqrt[3]{2} + \mathbf{Q}\sqrt[3]{4}$ $(h \pmod{X^3 - 2}) \mapsto h(\sqrt[3]{2}))$ est un isomorphisme de corps. Voir aussi l'exercise 10.4.9.

10.6.5 Irréductibilité dans $\mathbf{Q}[X]$ Les exemples ci-dessus montrent qu'il est important de décider si un polynôme $g \in \mathbf{Q}[X]$ est irréductible ou pas dans $\mathbf{Q}[X]$. Voici quelques critères d'irréductibilité.

10.6.6 Théorème (Gauss)**.** *(1) Si $g, h \in \mathbf{Z}[X]$ et s'il existe un nombre premier p tel que $p \mid gh$ dans $\mathbf{Z}[X]$, alors $p \mid g$ ou $p \mid h$ dans $\mathbf{Z}[X]$.*
*(2) (Lemme de Gauss) On a $ct(gh) = ct(g)ct(h)$ pour tous $g, h \in \mathbf{Z}[X] \smallsetminus \{0\}$, où le **contenu** $ct(g)$ d'un polynôme non nul $g \in \mathbf{Z}[X]$ est le* pgcd *de ses coefficients.*
(3) Si $f \in \mathbf{Z}[X] \smallsetminus \mathbf{Z}$ et si l'on a $f = gh$, où $g, h \in \mathbf{Q}[X] \smallsetminus \mathbf{Q}$, alors il existe $u \in \mathbf{Q}^*$ tel que $f = (ug)(u^{-1}h)$, où $ug, u^{-1}h \in \mathbf{Z}[X] \smallsetminus \mathbf{Z}$. ["Si f est réductible dans $\mathbf{Q}[X]$, il est réductible dans $\mathbf{Z}[X]$."]

Démonstration. (1) L'anneau quotient $\mathbf{Z}[X]/p\mathbf{Z}[X] = (\mathbf{Z}/p\mathbf{Z})[X]$ est un anneau intègre, car $\mathbf{Z}/p\mathbf{Z}$ l'est. Le produit des classes $g \pmod p), h \pmod p) \in \mathbf{Z}[X]/p\mathbf{Z}[X]$ est égal à zéro, car $gh \in p\mathbf{Z}[X]$. Par conséquent, $g \pmod p)$ ou $h \pmod p)$ est aussi égal à zéro dans $\mathbf{Z}[X]/p\mathbf{Z}[X]$.
(2) Quitte à diviser g (resp. h) par son contenu, on peut supposer que $ct(g) = ct(h) = 1$. Si $ct(gh) \neq 1$, alors il existe un nombre premier p qui divise $cd(gh)$. Le point (1) implique que $p \mid ct(g)$ ou $p \mid ct(h)$, ce qui est une contradiction.
(3) Il existe des entiers $c, d \geq 1$ tels que $cg, dh \in \mathbf{Z}[X]$. Les polynômes $G := cg/ct(cg) = ug$ ($u := c/ct(cg) \in \mathbf{Q}^*$) et $H := dh/ct(dh)$ appartiennent à $\mathbf{Z}[X]$. Le point (2) nous dit que $cdf/(GH) = ct(cg)ct(dh) = ct((cg)(dh)) = ct(cdf) = cd\,ct(f)$, ce qui implique que $GHct(f) = f$ et $u^{-1}h = Hct(f) \in \mathbf{Z}[X]$. □

10.6.7 Exercice. (1) Supposons que $f = a_nX^n + \cdots + a_0 \in \mathbf{Z}[X]$, $n = \deg(f) \geq 1$, et qu'il existe un nombre premier $p \nmid a_n$ tel que $f \pmod p$ est irréductible dans $(\mathbf{Z}/p\mathbf{Z})[X]$. Alors f est irréductible dans $\mathbf{Q}[X]$.
(2) Le polynôme $a(X) = X^3 - 2X^2 - 7X + 3$ est irréductible dans $\mathbf{Q}[X]$. [Indication : on prend $p = 2$.]

10.6.8 Théorème (Critère d'irréductibilité d'Eisenstein)**.** *Si $f = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in \mathbf{Z}[X]$ est un polynôme pour lequel il existe un nombre premier p tel que $p \mid a_i$ pour tout $i = 0, \ldots, n-1$ et $p^2 \nmid a_0$, alors f est irréductible dans $\mathbf{Q}[X]$.*

Démonstration. Exercice. □

10.6.9 Corollaire. *Pour tout $n \geq 1$, les polynômes $X^n - 2$ et $X^n - 6$ sont irréductibles dans $\mathbf{Q}[X]$.*

10.7 Construction des corps finis

10.7.1 Introduction Soit p un nombre premier. On sait que l'anneau $\mathbf{Z}/p\mathbf{Z} = \mathbf{F}_p$ est un corps à p éléments. L'objectif du paragraphe 10.7 est de construire des corps finis plus généraux F comme des

anneaux quotient $F = \mathbf{F}_p[X]/(f)$, où $f \in \mathbf{F}_p[X]$ est un polynôme irréductible.

Rappelons qu'on a montré dans la proposition 8.5.18 que tout corps F contient d'une manière canonique soit $\mathbf{Q}$ ("F est de caractéristique nulle"), soit $\mathbf{F}_p$ ("F est de caractéristique p" ; le nombre premier p étant unique).

10.7.2 Proposition. *Soit F un corps.*
(1) F est fini $\iff$ F est de caractéristique p et F est de dimension finie en tant qu'un espace vectoriel sur son sous-corps $\mathbf{F}_p$.
(2) Si $\dim_{\mathbf{F}_p}(F) = n$, alors $|F| = p^n = q$, $|F^*| = p^n - 1 = q - 1$ and

$$\forall a \in F^* \quad a^{q-1} = 1, \qquad \forall a \in F \quad a^q = a.$$

Démonstration. (1) Finitude de F implique que F ne peut pas contenir $\mathbf{Q}$, d'où $F \supset \mathbf{F}_p$ pour un certain nombre premier p. Si $\dim_{\mathbf{F}_p}(F) = n < \infty$, alors $F \xrightarrow{\sim} \mathbf{F}_p^n$ un tant qu'un espace vectoriel, ce qui implique que $|F| = |\mathbf{F}_p|^n = p^n$. Si $\dim_{\mathbf{F}_p}(F) = \infty$, alors F contient des sous-espaces vectoriels isomorphes à $\mathbf{F}_p^n$ pour tout $n \geq 1$, d'où $|F| = \infty$.
(2) Le groupe multiplicatif $F^* = (F \smallsetminus \{0\}, \cdot)$ a $|F^*| = p^n - 1 = q - 1$ éléments. Le théorème de Lagrange sous la forme du corollaire 7.5.9 nous dit que l'on a $\forall a \in F^* \quad a^{q-1} = 1$ (ce qui implique que $a^q = a$). Si $a \in F \smallsetminus F^*$, alors $a = 0$, d'où $a^q = 0 = a$. □

10.7.3 Construction des corps finis On applique le théorème 10.6.1 dans le cas particulier $K = \mathbf{F}_p$.

Pour tout polynôme irréductible unitaire $f \in \mathbf{F}_p[X]$ de degré $\deg(f) = n \geq 1$, l'anneau quotient $F = \mathbf{F}_p[X]/(f)$ est un corps contenant $\mathbf{F}_p$. L'élément $\alpha = \overline{X} = X \pmod f \in F$ vérifie $f(\alpha) = 0$. Tout élément $\beta \in F$ s'écrit d'une façon unique

$$\beta = r_0 + r_1\alpha + \cdots + r_{n-1}\alpha^{n-1} = r(\alpha) = r(X) \pmod f \qquad (r = r_0 + r_1 X + \cdots + r_{n-1}X^{n-1} \in \mathbf{F}_p[X],\ \deg(r) < n).$$

Autrement dit, F est un $\mathbf{F}_p$-espace vectoriel de dimension n et de base $1, \alpha, \ldots, \alpha^{n-1}$. En particulier, $|F| = p^n$.

Si f est réductible dans $\mathbf{F}_p[X]$, alors l'anneau quotient $\mathbf{F}_p[X]/(f)$ n'est pas un corps, mais les autres propriétés ci-dessus sont satisfaites, d'après la discussion dans le paragraphe 9.3.6.

10.7.4 Calcul dans un corps fini On exprime chaque élément du corps $F = \mathbf{F}_p[X]/(f)$ comme la classe de congruence $r \pmod f = r(\alpha)$, où $r \in \mathbf{F}_p[X]$ est un polynôme (unique) de degré $\deg(r) < n$. L'addition dans F correspond alors à l'addition de polynômes. Pour calculer le produit il faut prendre le reste de la division euclidienne par f du produit de polynômes (voir la discussion dans le paragraphe 9.3.6).

Si $r \neq 0$ et $\deg(r) < n$, alors $\beta = r \pmod f = r(\alpha)$ est inversible dans F. L'algorithme d'Euclide fournit une relation de Bézout explicite $ru + vf = 1$, où $u, v \in \mathbf{F}_p[X]$. On a $ru \pmod f = 1 \pmod f$ et $u \pmod f = u(\alpha)$ est l'inverse de β dans F.

10.7.5 Exemples (1) $p = 2$, $n = 2$. On écrit $\mathbf{F}_2 = \mathbf{Z}/2\mathbf{Z} = \{0, 1\}$, $1 + 1 = 0$ (d'où $-1 = 1$ dans $\mathbf{F}_2$). Le polynôme $f = X^2 + X + 1 \in \mathbf{F}_2[X]$ est irréductible dans $\mathbf{F}_2[X]$, car $\deg(f) \leq 3$ et f n'a pas de racines dans $\mathbf{F}_2$ ($f(0) = f(1) = 1 \in \mathbf{F}_2$).

L'anneau quotient $F = \mathbf{F}_2[X]/(X^2 + X + 1)$ est un corps à $p^n = 2^2 = 4$ éléments. Explicitement, $F = \{0, 1, \overline{X}, \overline{X} + 1\} = \{0, 1, \alpha, \alpha + 1\}$, où $\alpha = \overline{X} = X \pmod{(X^2 + X + 1)}$ vérifie $\alpha^2 + \alpha + 1 = 0$.

Par exemple,

$$\alpha^2 = -\alpha - 1 = \alpha + 1, \qquad \alpha^3 = \alpha(\alpha + 1) = \alpha^2 + \alpha = -1 = 1, \qquad (\alpha + 1)^2 = \alpha^2 + 2\alpha + 1 = \alpha^2 + 1 = \alpha.$$

Remarquons qu'on a

$$X^2 - X = X(X-1), \qquad \frac{X^4 - X}{X^2 - X} = X^2 + X + 1 \in \mathbf{F}_2[X].$$

(2) $p = 3$, $n = 2$. On a $\mathbf{F}_3 = \mathbf{Z}/3\mathbf{Z} = \{0, 1, 2\}$, où $2 = 1 + 1$ et $1 + 1 + 1 = 0$. En particulier, $2 = -1 \in \mathbf{F}_3$. Le polynôme $f = X^2 + 1 \in \mathbf{F}_3[X]$ est irréductible dans $\mathbf{F}_3[X]$, car $\deg(f) \leq 3$ et f n'a pas de racines dans $\mathbf{F}_3$ ($f(0) = 1$ et $f(\pm 1) = 2 = -1 \in \mathbf{F}_3$).

L'anneau quotient $F = \mathbf{F}_3[X]/(X^2 + 1)$ est un corps à $p^n = 3^2 = 9$ éléments. Explicitement, $F = \{0, \pm 1, \pm\overline{X}, \overline{X} \pm 1, -\overline{X} \pm 1\} = \{0, \pm 1, \pm\alpha, \alpha \pm 1, -\alpha \pm 1\}$, où $\alpha = \overline{X} = X \pmod{(X^2+1)}$ vérifie $\alpha^2 + 1 = 0$.

Par exemple,

$$0 = \alpha^2 + 1 = (\alpha + 1)(\alpha - 1) - 1, \qquad (\alpha + 1)^{-1} = \alpha - 1, \qquad (\alpha + 1)^2 = \alpha^2 + 2\alpha + 1 = 2\alpha = -\alpha,$$
$$(\alpha + 1)^4 = (-\alpha)^2 = \alpha^2 = -1, \qquad (\alpha + 1)^3 = -(\alpha + 1)^{-1} = 1 - \alpha,$$
$$\alpha^6 + \alpha^5 - \alpha^3 - \alpha + 1 = (\alpha^2 + 1)(\alpha^4 + \alpha^3 - \alpha^2 + \alpha + 1) + \alpha = \alpha.$$

On peut construire d'autres polynômes irréductibles à partir de f par un changement de variables. On obtient les deux polynômes suivants :

$$f_\pm(Y) := f(Y \pm 1) = (Y \pm 1)^2 + 1 = Y^2 \pm 2Y + 2 = Y^2 \mp X - 1 \in \mathbf{F}_3[X].$$

Le même changement de variables $X = Y \pm 1$ définit un isomorphisme entre F et le corps $F_\pm := \mathbf{F}_3[Y]/(f_\pm(Y))$:

$$F_\pm = \mathbf{F}_3[Y]/(f_\pm(Y)) \xrightarrow{\sim} \mathbf{F}_3[X]/(f(X)) = F, \qquad r(Y \pm 1) \pmod{f_\pm(Y)} \mapsto r(X) \pmod{f(X)}.$$

Remarquons qu'on a

$$\frac{X^9 - X}{X^3 - X} = X^6 + X^4 + X^2 + 1 = (X^2 + 1)(X^4 + 1) = f(X) f_+(X) f_-(X) \in \mathbf{F}_3[X].$$

10.7.6 Résultats généraux sur les corps finis Voici une liste des propriétés fondamentales des corps finis. On ne donne que l'idée principale des preuves, sans rentrant dans les détails.

(1) Le groupe multiplicatif F^* d'un corps fini F est cyclique (d'ordre $q - 1 = |F| - 1$).

On a démontré ce résultat pour $F = \mathbf{F}_p$ dans le théorème 5.5.2. Le même raisonnement montre que tout sous-groupe fini A du groupe multiplicatif K^* d'un corps quelconque K est cyclique (l'énoncé ci-dessus correspond au cas $K = F$ et $A = K^* = F^*$).

(2) La construction dans le paragraphe 10.7.3 fournit tous les corps finis. Plus précisement, tout corps fini F est isomorphe au corps $\mathbf{F}_p[X]/(f)$, où $f \in \mathbf{F}_p[X]$ est un polynôme irréductible unitaire.

C'est une conséquence de la discussion dans le paragraphe 10.6.4 pour $K = \mathbf{F}_p$, $M = F$ et $\alpha \in F$ un générateur quelconque du groupe cyclique F^* (cette condition implique que $\mathbf{F}_p(\alpha) = F$).

(3) Un corps F à $|F| = q < \infty$ éléments existe $\iff$ $q = p^n$, où p est un nombre premier et $n \geq 1$. Un tel corps est unique à un isomorphisme près ; on le note $\mathbf{F}_q$.

On sait que $|F| = q = p^n$ si le corps F existe. Si c'est le cas, la proposition 10.7.2(2) implique que les éléments de F sont précisement les racines du polynôme $X^q - X \in \mathbf{F}_p[X]$. Ce polynôme a q racines $\alpha_1, \ldots, \alpha_q \in L$ appartenant à un certain corps $L \supset \mathbf{F}_p$, d'après le corollaire 10.6.2, et ces racines sont distinctes, d'après l'exercise 10.6.3 (car la dérivée de $X^q - X \in \mathbf{F}_p[X]$ est égale à $-1 \in \mathbf{F}_p[X]$).

L'unicité de F est alors assez évidente et facile à démontrer. L'existence est une conséquence du fait que $F := \{\alpha \in L \mid \alpha^q = \alpha\}$ est un sous-corps de L, car l'application de Frobenius itérée $\varphi_q : \alpha \mapsto \alpha^q$ est

un morphisme d'anneaux $L \longrightarrow L$. Le corps F contient toutes les q racines α_i de $X^q - X \in \mathbf{F}_p[X]$, mais il a au plus $\deg(X^q - X) = q$ éléments, d'où $|F| = q$.

(4) $\mathbf{F}_q$ est un sous-corps de $\mathbf{F}_{q'} \iff$ il existe un entier $m \geq 1$ tel que $q' = q^m$.

L'implication "$\Longrightarrow$" est automatique, car $\mathbf{F}_{q'}$ est un espace vectoriel sur son sous-corps $\mathbf{F}_q$. Réciproquement, si $q' = q^m$, alors $X^{q'} - X$ est divisible par $X^q - X$ dans $\mathbf{F}_p[X]$, ce qui implique que l'ensemble des racines de $X^q - X \in \mathbf{F}_p[X]$ est un sous-ensemble de l'ensemble des racines de $X^{q'} - X \in \mathbf{F}_p[X]$.

(5) Si $q = p^n$ et $m \geq 1$, alors le polynôme $X^{q^m} - X \in \mathbf{F}_q[X]$ se factorise de la façon suivante :

$$X^{q^m} - X = \prod_{\substack{f \in \mathcal{P}_{\mathbf{F}_q} \\ \deg(f) | m}} f$$

(rappelons que l'on a noté $\mathcal{P}_K$ l'ensemble de tous le polynômes irréductibles unitaires dans $K[X]$).

En effet, si $f \in \mathcal{P}_{\mathbf{F}_q}$ et $\deg(f) = d$, alors le corps $F = \mathbf{F}_q[X]/(f)$ a q^d éléments. Comme $a^{q^d} - a = 0$ pour tout $a \in F$, on a $f \mid (X^{q^d} - X)$ dans $\mathbf{F}_q[X]$. Si $d \mid m$, alors $(q^d - 1) \mid (q^m - 1)$, d'où $(X^{q^d} - X) \mid (x^{q^m} - X)$ dans $\mathbf{F}_q[X]$. Réciproquement, si $f \mid (x^{q^m} - X)$ dans $\mathbf{F}_q[X]$, alors $\alpha^{q^m} = \alpha$ pour tout $\alpha \in F$, d'où $\alpha^{q^m - 1} = 1$ pour tout $\alpha \in F^*$. Si α est un génerateur du groupe cyclique F^*, l'égalité précédente implique que $q^m - 1$ est divisible par $q^d - 1$ (l'ordre de α). On écrit $m = da + b$, où $a, b \in \mathbf{N}$, $0 \leq b < d$. On a $q^m = (q^d)^a q^b \equiv q^b \pmod{(q^d - 1)}$, d'où $(q^d - 1) \mid (q^b - 1)$. Cela n'est possible que si $b = 0$, car $0 \leq q^b - 1 < q^d - 1$, d'où $d \mid m$. Il reste a remarquer que $f^2 \nmid (X^{q^m} - X)$ dans $\mathbf{F}_q[X]$, car les racines du polynôme $X^{q^m} - X \in \mathbf{F}_q[X]$ sont distinctes (voir (3) ci-dessus).

11 Appendice : Quotients

11.1 Quotients abstraits

11.1.1 Quotients et partitions On se donne les données suivantes :

— un ensemble X ;

— une partition $X = \coprod_{s\in S} X_s$ de X en une réunion disjointe de sous-ensembles non vides (des "classes") X_s. Autrement dit, tout élément de X appartient à précisement une classe X_s.

On dit que des éléments $x, y \in X$ (pas forcément distincts) sont **equivalents** s'ils appartiennent à la même classe X_s (**notation :** $x \sim y$). On appelle l'ensemble $\{X_s\}_{s\in S}$ des classes d'équivalence (qui s'identifie naturellement à S) **le quotient de X par la relation d'équivalence** $\sim$; on le note $X/\sim$.

On a une application de projection (surjective) $\mathrm{pr} : X \longrightarrow X/\sim$ qui associe à chaque élément $x \in X$ l'unique classe à laquelle il appartient.

Il y a plusieures reformulations équivalentes de la construction du quotient.

11.1.2 Quotients et projections Si $p : X \longrightarrow S$ est une application surjective entre deux ensembles, alors les fibres de p

$$X_s := p^{-1}(s) = \{x \in X \mid p(x) = s\} \qquad (s \in S)$$

forment une partition de X. Des éléments $x, y \in X$ appartiennent à la même fibre $p^{-1}(s)$ si et seulement si $p(x) = p(y) = s$. On retrouve la situation que l'on a considéré dans le paragraphe 11.1.1 avec $X/\sim = S$ et $\mathrm{pr} = p$.

11.1.3 Relations Une **relation** sur un ensemble X est un sous-ensemble $\mathcal{R} \subset X \times X$. Si $x, y \in X$ satisfont $(x, y) \in \mathcal{R}$, on dit que x et y sont en relation $\mathcal{R}$ (notation : $x\mathcal{R}y$).

Exemples : $X = \mathbf{Z}$ et (1) $x\mathcal{R}_1 y$ si $x = y$;
(2) $x\mathcal{R}_2 y$ si $x \neq y$;
(3) $x\mathcal{R}_3 y$ si $x \leq y$;
(4) $x\mathcal{R}_4 y$ si $x < y$;
(5) $x\mathcal{R}_5 y$ si $x \equiv y \pmod 5$.

On dit qu'une relation $\mathcal{R}$ sur X est

— **reflexive** si $\quad \forall x \in X \quad x\mathcal{R}x$;

— **symétrique** si $\quad \forall x, y \in X \quad [x\mathcal{R}y \Longrightarrow y\mathcal{R}x]$;

— **transitive** si $\quad \forall x, y, z \in X \quad [x\mathcal{R}y,\ y\mathcal{R}z \Longrightarrow x\mathcal{R}z]$;

— **une relation d'équivalence** si $\mathcal{R}$ est reflexive, symétrique et transitive.

Dans les exemples ci-dessus, $\mathcal{R}_1, \mathcal{R}_3$ et $\mathcal{R}_5$ sont reflexives, $\mathcal{R}_1, \mathcal{R}_2$ et $\mathcal{R}_5$ sont symétriques, et $\mathcal{R}_1, \mathcal{R}_3, \mathcal{R}_4$ et $\mathcal{R}_5$ sont transitives. En particulier, $\mathcal{R}_1$ et $\mathcal{R}_5$ sont des relations d'équivalence (mais $\mathcal{R}_2, \mathcal{R}_3, \mathcal{R}_4$ ne le sont pas).

11.1.4 Quotients et relations d'équivalence Soit $X = \coprod_{s\in S} X_s$ comme dans le paragraphe 11.1.1. Si l'on définit $x \sim y$ comme ci-dessus, alors $\sim$ est bien une relation d'équivalence sur X.

Réciproquement, supposons que $\mathcal{R}$ est une relation d'équivalence sur un ensemble X. Pour tout $x \in X$ on considère le sous-ensemble

$$C_x := \{y \in X \mid x\mathcal{R}y\} \subset X$$

(dans l'exemple 5 du paragraphe 11.1.3 on a $C_x = x \pmod 5$). La reflexivité de $\mathcal{R}$ implique que $x \in C_x$, d'où $\bigcup_{x\in X} = X$. Si $y \in C_x$ et $z \in C_y$, alors $z \in C_x$ (d'après la transitivité de $\mathcal{R}$), d'où $C_y \subset C_x$. D'autre

part, la symétrie de $\mathcal{R}$ implique que $x \in C_y$, d'où $C_x \subset C_y$. En résumé, $C_y = C_x$ dès que $y \in C_x$ (ce qui implique que $C_x \cap C_{x'} = \emptyset$ si $x' \notin C_x$).

Par conséquent, on obtient une partition $X = \coprod_{s \in S} X_s$ en des classes $X_s = C_x$ (pour tout $x \in X_s$). La relation $x \sim y$ que l'on a définie dans le paragraphe 11.1.1 est alors égale à $x\mathcal{R}y$. On note $X/\mathcal{R}$ le quotient correspondant et on dit que $X/\mathcal{R}$ est **le quotient de X par la relation d'équivalence $\mathcal{R}$**.

11.1.5 Propriété universelle de $X/\mathcal{R}$ Soit $\mathcal{R}$ une relation d'équivalence sur un ensemble X. Le quotient $X/\mathcal{R}$ a la propriété universelle suivante.

Si Y est un ensemble et si $f : X \longrightarrow Y$ est une application tel que $f(x) = f(x')$ dès que $x\mathcal{R}x'$, alors il existe une unique application $f' : X/\mathcal{R} \longrightarrow Y$ vérifiant

$$f = f' \circ \mathrm{pr} : X \longrightarrow X/\mathcal{R} \longrightarrow Y.$$

En effet, f' est déterminé par cette condition : on a $f'(\mathrm{pr}(x)) = f(x)$, et cette définition a un sens, car $f(x) = f(x')$ dès que $\mathrm{pr}(x) = \mathrm{pr}(x')$, par l'hypothèse.

11.1.6 Relation à G/H Si H est un sous-groupe d'un groupe abélien G, alors la relation de congruence $x \equiv y \pmod H$ sur G est une relation d'équivalence (voir la proposition 7.6.7) et le quotient abstrait $G/\equiv \pmod H$ s'identifie au quotient G/H que l'on a défini dans le corollaire 7.6.5.