MAT 504: Algèbre appliquée

Chapitre I: Congruence et le code ISBN

Le but de ce chapitre est d'appliquer la congruence sur les entiers pour étudier le code ISBN (c'est-à-dire, International Standard Book Number), un système international de numérotation des livres, qui permet d'identifier chaque livre publié par un même éditeur. On verra que l'étude de la relation de la congruence sur les entiers exige une application de la théorie des nombres et la théorie des anneaux.

Partout dans ce cours, $\mathbb{N}$ désigne l'ensemble des nombres naturels; $\mathbb{Z}$, l'ensemble des nombres entiers; $\mathbb{Q}$, l'ensemble des nombres rationnels; $\mathbb{R}$, l'ensemble des nombres réels; et $\mathbb{C}$, l'ensemble des nombres complexes.

1.1 Entiers

Le but de cette section est d'étudier les propritétés des entiers.

1.1.1. Définition. Pour tout $\alpha \in \mathbb{R}$, la *partie entière* de α, notée $[\alpha]$, est le plus grand entier qui est plus petit ou égal à α. C'est-à-dire, $[\alpha] \in \mathbb{Z}$ tel que $[\alpha] \leq \alpha < [\alpha] + 1$.

1.1.2. Lemme. Si $\alpha, \beta \in \mathbb{R}$, alors $[\alpha] + [\beta] \leq [\alpha + \beta] \leq [\alpha] + [\beta] + 1$.

Démonstration. Comme $[\alpha] \leq \alpha < [\alpha] + 1$ et $[\beta] \leq \beta < [\beta] + 1$, on a

$$[\alpha] + [\beta] \leq \alpha + \beta < [\alpha] + [\beta] + 2.$$

Comme $[\alpha] + [\beta]$ est un entier, on a $[\alpha] + [\beta] \leq [\alpha + \beta] \leq \alpha + \beta < [\alpha] + [\beta] + 2$. Étant un entier, $[\alpha + \beta] \leq [\alpha] + [\beta] + 1$. La preuve du lemme s'achève.

1.1.3. Théorème de la division. Soient $a, b \in \mathbb{Z}$. Si $b > 0$, alors il existe deux entiers uniques q et r tels que $a = qb + r,\ 0 \leq r < b$.

Démonstration. On montrera premièrement l'existence de q et r. D'abord, supposons que $a \geq 0$. Posons $q = [\frac{a}{b}]$ et $r = bq - a$. Alors $q \leq \frac{a}{b} < q + 1$. Comme $b > 0$, on a $qb \leq a < bq + b$. D'où, $0 \leq r < b$. Supposons maintenant que $a < 0$. Comme $-a > 0$, on a que $-a = qb + r$ avec $0 \leq r < b$. Donc $a = -qb - r$. Si $r = 0$, alors $a = (-q)b + r$. Sinon, $a = (-q - 1)b + (b - r)$ avec $0 < b - r < b$.

On montrera maintenant l'unicité de q et r. Supposons que q_1 et r_1 sont deux entiers tels que $a = q_1 b + r_1,\ 0 \leq r_1 < b$. On peut supposer que $r_1 \leq r$. Alors $0 \leq r - r_1 = (q_1 - q)b < b$.

Comme $b > 0$, on a $q_1 - q \geq 0$. Si $q_1 - q \neq 0$, alors $q_1 - q \geq 1$. Ceci implique que $b > r - r_1 = (q_1 - q)b \geq b$, une contradiction. Ainsi $q_1 - q = 0$ et donc $r_1 - r = 0$. C'est-à-dire, $q = q_1$ et $r = r_1$. Ceci achève la démonstration du théorème.

Remarque. (1) Les entiers q et r dans l'algorithme s'appellent le *quotient* et le *reste* de a divisé par b, respectivement. On note $q = q_b(a)$ et $r = r_b(a)$.

(2) Si $r_b(a) = 0$, on dit alors que b est un *diviseur* de a, noté $b \mid a$.

Exemple. Trouver le quotient et le rest de -22 par 6.

Soient $a, b \in \mathbb{Z}$ non tous nuls. Un entier n s'appelle *commun diviseur* de a et b si $n \mid a$ et $n \mid b$; et dans ce cas, $|n| \leq |a| + |b|$. Ainsi le nombre de commun diviseurs de a, b est fini. Par conséquent, il existe un plus grand commun diviseur de a, b, noté $\text{pgcd}(a, b)$. Comme 1 est toujours un commun diviseur de a et b, on voit que $\text{pgcd}(a, b) \geq 1$.

1.1.4. Théorème de Bachet-Bézout. Soient a, b deux entiers avec $a \geq b > 0$. Posons $r_0 = a$ et $r_1 = b$. Alors il existe une suite finie de divisions suivante:

$$\begin{array}{lcllll}
r_0 & = & q_1 r_1 & + & r_2, & 0 < r_2 < r_1; \\
r_1 & = & q_2 r_2 & + & r_3, & 0 < r_3 < r_2; \\
 & \vdots & & & & \\
r_{i-2} & = & q_{i-1} r_{i-1} & + & r_i, & 0 < r_i < r_{i-1}; \\
 & \vdots & & & & \\
r_{t-2} & = & q_{t-1} r_{t-1} & + & r_t, & 0 < r_t < r_{t-1}; \\
r_{t-1} & = & q_t r_t & + & r_{t+1}, & 0 = r_{t+1}.
\end{array}$$

Dans ce cas, $\text{pgcd}(a, b) = r_t$ et il existe des entiers x, y tels que

$$ax + by = \text{pgcd}(a, b).$$

Démonstration. L'existence de la suite est une conséquence du théorème 1.1.3. Posons $d = \text{pgcd}(a, b)$. D'abord, on prétend que $r_t \mid r_i$, pour $i = t + 1, t, \ldots, 1, 0$. En effet, c'est évident pour $i = t + 1, t$. Supposons que $t \geq i > 0$ et $r_t \mid r_j$ pour $j = t + 1, t, \ldots, i + 1, i$. Comme $r_{i-1} = q_i r_i + r_{i+1}$, on voit que $r_t \mid r_{i-1}$. Ceci montre l'énoncé. En particulier, r_t est un commun diviseur de a et b. D'où, $r_t \leq d$.

Ensuite, on prétend que $r_i = ax_i + by_i$, où $x_i, y_i \in \mathbb{Z}$, pour $i = 0, 1, \ldots, t$. C'est évident pour $i = 0, 1$. Supposons que $1 \leq i < t$ et que l'énoncé est vrai pour $j = 0, 1, \ldots, i - 1, i$. Maintenant,

$$r_{i+1} = r_{i-1} - r_i q_i = a(x_{i-1} + x_i) + b(y_{i-1} - y_i q_i).$$

Ceci montre l'énoncé. En particulier, $r_t = ax_t + by_t$. D'où, $d \mid r_t$; et donc, $d \leq r_t$. Par conséquent, $d = r_t = a\,x_t + b\,y_t$. Ceci achève la démonstration du théorème.

Remarque. La suite de divisions dans le théorme 1.1.4 s'appelle *algorithme d'Euclide.*

Exemple. Trouver x, y tels que

$$196x + 60y = \text{pgcd}(196, 60).$$

MAPLE. Pour trouver $x, y \in \mathbb{Z}$ tels que $ax + by = \text{pgcd}(a, b)$, on tape la commande

$$\text{igcdex}(a, b, x, y); x; y;$$

Deux entiers non nuls a, b sont dits *co-premiers* si $\text{pgcd}(a, b) = 1$.

1.1.5. Proposition. Soient a, b, c des entiers non tous nuls.
(1) Si $c \mid a$ et $c \mid b$, alors $c \mid \text{pgcd}(a, b)$.
(2) Les entiers a, b sont co-premiers si, et seulement si, $ax + by = 1$ avec $x, y \in \mathbb{Z}$.
(3) Si $\text{pgcd}(a, b) = \text{pgcd}(a, c) = 1$, alors $\text{pgcd}(a, bc) = 1$.
(4) Si $a \mid bc$ avec $\text{pgcd}(a, b) = 1$, alors $a \mid c$.
(5) Si $\text{pgcd}(a, b) = 1$, alors $a \mid c$ et $b \mid c$ si et seulement si $ab \mid c$.

Démonstration. Posons $d = \text{pgcd}(a, b)$. D'après le théorème de Bachet-Bézout, il existe $x, y \in \mathbb{Z}$ tels que $d = ax + by$.

(1) Si $c \mid a$ et $c \mid b$, alors $c \mid ax$ et $c \mid by$. Par conséquent, $c \mid d$.

(2) Supposons que $ax + by = 1$ avec $x, y \in \mathbb{Z}$. Alors $d \mid 1$, et donc $d = 1$. C'est-à-dire, a, b sont co-premiers.

(3) D'après la nécissité de la partie (2), $ar + bs = 1$ et $ax + cy = 1$ avec $r, s, x, y \in \mathbb{Z}$. Ceci donne $a(arx + rcy + bsx) + (bc)(sy) = 1$. D'après la suffisance de la partie (2), a est co-premier à bc.

(4) Supposons que $a \mid bc$ avec $\text{pgcd}(a, b) = 1$. Alors $ar + bs = 1$ avec $r, s \in \mathbb{Z}$, et donc, $acr + bcs = c$. D'où, $a \mid c$.

(5) Supposons que $\text{pgcd}(a, b) = 1$. Il suffit de montrer la nécessité. Pour ce faire, on suppose que $a \mid c$ et $b \mid c$. Écrivant $c = aa_1$ avec $a_1 \in \mathbb{Z}$, on voit que $b \mid aa_1$. D'après la partie (4), on a $b \mid a_1$. D'où, $ab \mid c$. La preuve de la proposition s'achève.

Un entier n est dit *premier* si $n > 1$ et n n'a que deux diviseurs positifs 1 et p.

Voici des propriétés de nombres premiers.

1.1.6. Lemme. Soient $p, a, b \in \mathbb{Z}$ avec p premier.

(1) Si $p \nmid a$, alors $\text{pgcd}(p, a) = 1$.

(2) Si $p \mid ab$, alors $p \mid a$ ou $p \mid b$.

Démonstration. (1) Posons $d = \text{pgcd}(p, a)$. Si $p \nmid a$, alors $d \neq p$. Comme p est premier, on voit que $d = 1$.

(2) Supposons que $p \nmid a$ et $p \nmid b$. D'après l'énoncé (1), $\text{pgcd}(p, a) = \text{pgcd}(p, b) = 1$. D'après la proposition 1.1.5(3), $\text{pgcd}(p, ab) = 1$. D'où, $p \nmid ab$. la preuve du lemme s'achève.

On a un critère pour qu'un entier soit premier.

1.1.7. Lemme. Un entier $n(> 1)$ est premier si et seulement si n n'est divisible par aucun nombre premier p qui est plus petit ou égal à $\sqrt{n}$.

Démonstration. La necessité est trivial. Supposons que n n'est pas premier. Alors, il existe un entier p avec $1 < p < n$ tel que $n = pq$ avec q un entier. On peut supposer p est le plus petit entier pour cette proprété. Alors p est premier et $p \leq q$. Or $p^2 \leq pq = n$, d'où $p \leq \sqrt{n}$. La preuve du lemme s'achève.

Exemple. Le nombre 97 est premier.

MAPLE. Pour vérifier si un entier a est premier ou non, on tape la commande

$$\text{isprime}(a);$$

En appliquant le lemme 1.1.7, on obtient une méthode pour chercher les nombres premiers plus petits ou égaux à un entier donné. Pour un entier a, on note $a\mathbb{N} = \{an \mid n \in \mathbb{N}\}$.

1.1.8. Crible d'Ératosthènes. Soit $N > 1$ un entier.

(1) Posons $\mathcal{E}_1 = \{n \mid 2 \leq n \leq N\}$, dont le plus petit entier est $p_1 = 2$.

(2) Posons $\mathcal{E}_2 = \mathcal{E}_1 \backslash p_1\mathbb{N}$, dont le plus petit entier est $p_2 = 3$.

(3) Posons $\mathcal{E}_3 = \mathcal{E}_2 \backslash p_2\mathbb{N}$, dont le plus petit entier est $p_3 = 5$.

$\vdots$

(n) Posons $\mathcal{E}_n = \mathcal{E}_{n-1} \backslash p_{n-1}\mathbb{N}$, dont le plus petit entier est noté p_n.

Si $p_n^2 \leq N$, on continue par posant $\mathcal{E}_{n+1} = \mathcal{E}_n \backslash p_n\mathbb{N}$.

Si $p_n^2 > N$, alors $\{p_1, \ldots, p_{n-1}\} \cup \mathcal{E}_n$ est l'ensemble des nombres premiers $\leq N$.

Exemple. Trouver les nombres premiers ≤ 60.

1.1.9. Théorème d'Euclide. Il y a une infinité de nombres premiers.

Démonstration. Supposons, au contraire, qu'il n'y a qu'un nombre fini de nombres premiers, disons $p_1, \ldots, p_r$. Posons $n = p_1 \cdots p_r + 1$. Comme $n > p_i$, pour tout $1 \leq i \leq r$,

n n'est pas premier. D'après le lemme 1.1.6, il existe au moins un p_i avec $1 \leq i \leq r$ tel que $p_i \mid n$. Comme $p_i \mid p_1 \cdots p_r$, on obtient $p_i|1$, c'est absurde. La preuve du théorème s'achève.

Remarque. Jusqu'à février 2013, le plus grand nombre premier connu a 17,425,170 chiffres décimales.

MAPLE. Pour trouver le plus petit nombre premier $\geq a$, on tape la commande

$$\text{nextprime}(a);$$

1.1.10. Théorème. Tout entier $n(> 1)$ admet une factorisation unique, appelée la *factorisation canonique*, comme suit :

$$n = p_1^{e_1} \cdots p_r^{e_r}, \quad p_1 < \cdots < p_r;\ e_1, \ldots, e_r > 0,$$

où $p_1, \ldots, p_r$ sont des nombres premiers.

Démonstration. Il suffit de montrer que n admet une décomposition unique:

$$(*) \qquad n = p_1 p_2 \cdots p_s; \ \text{ avec } \ p_1 \leq p_2 \leq \cdots \leq p_s,$$

où les p_i sont premiers. On procède par récurrence. Si $n = 2$, l'énoncé est évident. Supposons que $n > 2$ et l'énoncé est valide pour tout entier m avec $1 < m < n$. Si n est premier, l'énoncé est valide. Sinon, $n = ab$ avec $1 < a, b < n$. Par l'hypothèse de récurrence, $a = a_1 \cdots a_s$ et $b = b_1 \cdots b_t$, où les a_i, b_j sont premiers. Ceci montre l'existence de la décomposition $(*)$. Supposons que n a une autre décomposition

$$(**) \quad n = q_1 q_2 \cdots q_t; \ \text{ avec } \ q_1 \leq q_2 \leq \cdots \leq q_t,$$

où les q_j sont premiers. Soit q le plus grand diviseur premier de n. En vue de la décomposition (*), on déduit de la proposition 1.1.6(2) que $q = p_s$. De même, on a $q = q_t$. Ceci donne

$$p_1 \cdots p_{s-1} = q_1 \cdots q_{t-1}.$$

Par h'hypothèse de récurence, on a $t - 1 = s - 1$ et $p_i = q_i$ pour $i = 1, \ldots, s - 1$. Ceci montre l'unicité de la décomposition $(*)$. La preuve du théorème s'achève.

Remarque. (1) Dans la factorisation canonique, e_i est le plus grand exposant tel que $p_i^{e_i} \mid n$, pour tout $i = 1, \ldots, r$.

(2) Si p est premier avec $p \neq p_i$ pour tout $1 \leq i \leq r$, alors 0 est le plus grand exposant tel que $p^0 \mid n$.

Étant donné un ensemble X, on désigne par $|X|$ la cardinalité de X.

1.1.11. Lemme. Soient m, n des entiers avec $m \geq 0$ et $n \geq 1$. Alors

$$|\{x \in \mathbb{Z} \mid 1 \leq x \leq m \text{ et } n \mid x\}| = \left[\frac{m}{n}\right].$$

Démonstration. Si $m < n$, alors $[\frac{m}{n}] = 0$. De l'autre côté, il n'y a aucun multiple x de n avec $1 \leq x \leq m$. L'énoncé est valide dans ce cas.

Supposons maintenant que $m \geq n$. Posons $[\frac{m}{n}] = q \geq 1$. Comme $q \leq \frac{m}{n} < q + 1$, on a $qn \leq m < (q + 1)n$. Si $x \in \{1, \ldots, m\}$, alors $n \mid x$ si et seulement si $x = ny$ avec $1 \leq y \leq q$. Par conséquent,

$$\{x \in \mathbb{Z} \mid 1 \leq x \leq m \text{ et } n|x\} = \{n, \ldots, (q-1)n, qn\}.$$

D'où, on a l'énoncé. Ceci achève la démonstration du lemme.

Le résultat suivant nous permet de trouver la factorisation canonique de $n!$, pour un entier positif n.

1.1.12. Formule de de Polignac. Soient p un nombre premier et $n \geq 1$ un entier. Si e est le plus grand exposant tel que $p^e \mid n!$, alors

$$e = \sum\nolimits_{i=1}^{\infty} \left[\frac{n}{p^i}\right].$$

Démonstration. L résultat est évident pour $n = 1$. Supposons que $n > 1$ et le résultat est valide pour $n-1$. Alors $n! = (n-1)!\, n$. Supposons que r, s sont les plus grands exposants tels que $p^r \mid (n-1)!$ et $p^s \mid n$. Alors $e = r + s$ et

$$r = \sum\nolimits_{i=1}^{\infty} \left[\frac{n-1}{p^i}\right].$$

On se fixe un entier $i \geq 1$ et on pose

$$\mathcal{E}_{n-1} = \{x \in \mathbb{Z} \mid 1 \leq x \leq n-1 \text{ et } p^i|x\} \text{ et } \mathcal{E}_n = \{x \in \mathbb{Z} \mid 1 \leq x \leq n \text{ et } p^i|x\}.$$

D'après le lemme 1.1.10, $[\frac{n-1}{p^i}] = |\mathcal{E}_{n-1}|$ et $[\frac{n}{p^i}] = |\mathcal{E}_n|$. Maintenant, on voit aisément que $\mathcal{E}_{n-1} \subseteq \mathcal{E}_n$; et $\mathcal{E}_{n-1} \neq \mathcal{E}_n$ si et seulement si $n \notin \mathcal{E}_{n-1}$ si et seulement si $p^i \nmid n$. Par conséquent,

$$\left[\frac{n}{p^i}\right] - \left[\frac{n-1}{p^i}\right] = \begin{cases} 1, \text{ si } p^i \mid n; \\ 0, \text{ sinon.} \end{cases}$$

Comme $p^s \mid n$ et $p^{s+1} \nmid n$, on a

$$\sum_{i=1}^{\infty} \left[\frac{n}{p^i}\right] - r = \sum_{i=1}^{\infty} \left(\left[\frac{n}{p^i}\right] - \left[\frac{n-1}{p^i}\right]\right) = \sum_{i=1}^{s} \left(\left[\frac{n}{p^i}\right] - \left[\frac{n-1}{p^i}\right]\right) = s.$$

Ceci donne

$$e = r + s = \sum_{i=1}^{\infty} \left[\frac{n}{p^i} \right].$$

La preuve du théorème s'achève.

Exemple. Factoriser 10! en produit de puissances de nombres premiers.

1.2 Anneaux

1.2.1. Définition. Un *anneau* est un ensemble A muni d'une addition

$$+ : A \times A \to A : (a, b) \mapsto a + b$$

et d'une multiplication

$$\cdot : A \times A \to A : (a, b) \mapsto a \cdot b$$

telles que, pour tous $a, b, c \in A$, on a

(1) $a + b = b + a$;

(2) $a + (b + c) = (a + b) + c$;

(3) il existe $0_A \in A$, appelé *zéro*, tel que $a + 0_A = a$;

(4) Tout a a un *opposé* $-a \in A$ tel que $a + (-a) = 0_A$;

(5) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$;

(6) il existe $1_A \in A$, appelé *identité*, tel que $1_A \cdot a = a \cdot 1_A = a$;

(7) $a \cdot (b + c) = a \cdot b + a \cdot c$;

(8) $(a + b) \cdot c = a \cdot c + b \cdot c$.

En outre, A est dit *nul* si $A = \{0_A\}$; et *commutatif* si $a \cdot b = b \cdot a$, pour tous $a, b \in A$.

Remarque. Soit A un anneau.

(1) A a un seul zéro 0_A et un seul identité 1_A.

(2) On définit la *soustraction* dans A par $a - b = a + (-b)$.

Exemple. (1) Les ensembles $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont des anneauxs commutatifs pour l'addition et la multiplication habituelles.

(2) L'ensemble $M_n(\mathbb{R})$ des matrices carrées réelles d'ordre n est un anneau, qui est non commutatif lorsque $n > 1$.

(3) L'ensemble $\mathbb{R}[x]$ des polynômes réels est un anneau pour l'addition et la multiplication habituelles.

(4) L'ensemble $\mathbb{N}$ des entiers naturels n'est pas un anneau pour l'addition et la multiplication habituelles.

Soit A un anneau. Un élément $a \in A$ est dit *inversible* s'il existe $b \in A$ tel que

$$a \cdot b = b \cdot a = 1_A;$$

et dans ce cas, b s'appelle *inverse* de a et noté $b = a^{-1}$. En outre, A s'appelle un *corps* si A est commutatif, non nul, et tous les éléments non nuls sont inversibles. Par exemple, $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont des corps, mais $\mathbb{Z}$ ne l'est pas.

Le résultat suivant est évident.

1.2.2. Proposition. Soit A un anneau avec $a, b, c \in A$.
(1) $0_A \cdot a = a \cdot 0_A = 0_A$.
(2) $(-1_A) \cdot a = -a$.
(3) $-(-a) = a$.
(4) $a(b - c) = ab - ac$.
(5) $(a - b)c = ac - bc$.

1.2.3. Proposition. Si A est un anneau non nul, alors les éléments inversibles de A forment un groupe, appelé le *groupe multiplicatif* de A et noté $U(A)$.

Démonstration. Comme A est non nul, $1_A \neq 0_A$, et donc $1_A \in U(A)$. Si $a, b \in U(A)$, alors $(a^{-1})^{-1} = a$ et $b^{-1}a^{-1} = (ab)^{-1}$, et donc $a^{-1}, ab \in U(A)$. Par conséquent, $U(A)$ est un groupe. La preuve de la proposition s'achève.

Exemple. (1) Si F est un corps, alors $U(F) = F^* := F\backslash\{0\}$.
(2) $U(\mathbb{R}[x]) = \mathbb{R}^* := \mathbb{R}\backslash\{0\}$.

1.2.4. Définition. Soient A, B deux anneaux. Une application $\phi : A \to B$ s'appelle un *homomorphisme* si les conditions suivantes sont vérifiées.
(1) $\phi(1_A) = 1_B$.
(2) $\phi(a + b) = \phi(a) + \phi(b)$, pour tous $a, b \in A$.
(3) $\phi(ab) = \phi(a)\phi(b)$, pour tous $a, b \in A$.
En outre, un homomorphisme bijectif s'appelle un *isomorphisme*.

Exemple. Soit $a \in \mathbb{R}$. L'application d'évaluation

$$\rho_a : \mathbb{R}[x] \to \mathbb{R} : f(x) \mapsto f(a)$$

est un homomorphisme surjectif d'anneaux.

1.2.5. Lemme. Soit $\phi : A \to B$ un homomorphisme d'anneaux avec $a, b \in A$.
(1) $\phi(0_A) = 0_B$.

(2) $\phi(-a) = -\phi(a)$.

(3) $\phi(a-b) = \phi(a) - \phi(b)$.

Démonstration. (1) On a $\phi(0_A) = \phi(0_A + 0_A) = \phi(0_A) + \phi(0_A)$. Donc $\phi(0_A) = \phi(0_A) - \phi(0_A) = 0_B$.

(2) $\phi(a) + \phi(-a) = \phi((a + (-a)) = \phi(0_A) = 0_B$. Donc $\phi(-a) = -\phi(a)$.

(3) $\phi(a-b) = \phi(a + (-b)) = \phi(a) + \phi(-b) = \phi(a) + (-\phi(b)) = \phi(a) - \phi(b)$. Ceci achève la preuve de la proposition.

1.2.6. Lemme. Soient A, B des anneaux. Si $\phi : A \to B$ est un isomorphisme, alors $U(A) \cong U(B)$.

Démonstration. Si $a \in U(A)$, alors $aa^{-1} = a^{-1}a = 1_A$. D'où,

$$1_B = \phi(1_A) = \phi(a)\phi(a^{-1}) = \phi(a^{-1})\phi(a).$$

C'est-à-dire, $\phi(a) \in U(B)$. Ainsi ϕ induit une application

$$\psi : U(A) \to U(B) : a \mapsto \phi(a).$$

Pour tous $x, y \in U(A)$, on a $\psi(xy) = \phi(xy) = \phi(x)\phi(y) = \psi(x)\psi(y)$. Donc, ψ est un homorphisme de groupes. Comme ϕ est injective, ψ l'est aussi. Supposons maintenant que $b \in U(B)$. Comme ϕ est surjective, $b = \phi(a)$ et $b^{-1} = \phi(c)$, avec $a, c \in A$. Donc, $\phi(ac) = \phi(a)\phi(c) = bb^{-1} = 1_B = \phi(1_A)$. Comme ϕ est injective, $ac = 1_A$. De même, on voit que $ca = 1$. C'est-à-dire, $a \in U(A)$ tel que $\psi(a) = b$. Ainsi, ψ est bijective. Ceci montre que ψ est un isomorphisme de groupes. La preuve du lemme s'achève.

1.2.7. Proposition. Si A, B sont des anneaux, alors le produit cartésien

$$A \times B = \{(a, b) \mid a \in A, b \in B\}$$

est un anneau avec

$$U(A \times B) = U(A) \times U(B).$$

Démonstration. Il s'agit d'une vérification de routine que $A \times B$ est un anneau si l'on définit, pour tous $(a, b), (c, d) \in A \times B$, que

$$(a, b) + (c, d) = (a + b, b + d),\ (a, b)(c, d) = (ac, bd).$$

Évidemment, $0_{A\times B} = (0_A, 0_B)$ et $1_{A\times B} = (1_A, 1_B)$.

En outre, pour tout $(a, b) \in A \times B$, on voit que $(a, b) \in U(A \times B)$ si et seulemengt s'il existe $(c, d) \in A \times B$ tel que $(a, b)(c, d) = (c, d)(a, b) = 1_{A\times B}$ si et seulement si $ac = ca = 1_A$ et $bd = db = 1_B$, si et seulement si $a \in U(A)$ et $b \in U(B)$. Par conséquent, on voit que $U(A \times B) = U(A) \times U(B)$. La preuve de la proposition s'achève.

Pour construire des nouveaux anneaux à partir d'un anneau donné, on a besoin de la notion d'une relation d'équivalence.

1.2.8. Définition. Soit E un ensemble.

(1) Une *relation binaire* sur E est un sous-ensemble $\mathcal{R}$ du produit cartésien $E \times E$. Dans ce cas, si $(x, y) \in \mathcal{R}$, on dit alors que x est *en relation avec* y, noté $x\mathcal{R}y$.

(2) Une relation binaire $\mathcal{R}$ sur E est dite

(i) *réflexive* si $x\mathcal{R}x$, pour tout $x \in E$;

(ii) *symétrique* si $x\mathcal{R}y$ entraîne que $y\mathcal{R}x$, pour tous $x, y \in E$;

(iii) *transitive* si $x\mathcal{R}y$ et $y\mathcal{R}z$ entraîne que $x\mathcal{R}z$, pour tous $x, y, z \in E$.

(3) Une relation binaire sur E s'appelle *relation d'équivalence* si elle est réflexive, symétrique et transitive.

Exemple. (1) L'ensemble $\mathcal{S} = \{(m, n) \in \mathbb{Z} \times \mathbb{Z} \mid m \mid n\}$ définit une relation binaire sur $\mathbb{Z}$, qui est réflexive et transitive, mais non symétrique.

(2) L'ensemble $\mathcal{R} = \{(m, n) \in \mathbb{Z} \times \mathbb{Z} \mid (-1)^m = (-1)^n\}$ définit une relation d'équivalence sur $\mathbb{Z}$.

1.2.9. Définition. Soit $\sim$ une relation d'équivalence sur un ensemble E.

(1) Si $x \in E$, alors $\bar{x} = \{y \in E \mid y \sim x\}$ s'appelle *classe d'équivalence par* $\sim$ de x.

(2) L'*ensemble quotient par* $\sim$ de E est l'ensemble des classes d'équivalence par $\sim$ suivant:

$$E/\sim := \{\bar{x} \mid x \in E\}.$$

Remarque. Pour tous $x, y \in E$, on voit que $\bar{x} = \bar{y}$ si, et seulement si, $x \sim y$.

Exemple. Considérons la relation d'équivalence sur $\mathbb{Z}$ suivante:

$$\mathcal{R} = \{(m, n) \in \mathbb{Z} \times \mathbb{Z} \mid (-1)^m = (-1)^n\}.$$

On a

$$\mathbb{Z}/\mathcal{R} = \{\bar{x} \mid x \in \mathbb{Z}\} = \{\bar{0}, \bar{1}\}.$$

1.2.10. Définition. Soit $\sim$ une relation d'équivalence sur un ensemble E.

(1) Si X est une classe d'équivalence par $\sim$, alors tout $x \in X$ est dit *représentant* de X.

(2) Un sous-ensemble C de E s'appelle *ensemble complet des représentants des classes d'équivalence par* $\sim$ si tout $x \in E$ est en relation avec un unique $c \in C$. Dans ce cas,

$$E/\sim = \{\bar{c} \mid c \in C\}.$$

Exemple. Considérons la relation d'équivalence $\mathcal{R} = \{(m,n) \in \mathbb{Z}\times\mathbb{Z} \mid (-1)^m = (-1)^n\}$. On voit que $\{0,1\}$ est un ensemble complet des représentants des classes d'équivalence par $\mathcal{R}$. Remarquons que $\{3,6\}$ l'est aussi.

On revient à étudier des propriétés des anneaux.

1.2.11. Définition. Soit A un anneau. Un sous ensemble non vide I de A s'appelle *idéal* si les conditions suivantes sont vérifiées.

(1) Si $r, s \in I$, alors $r + s \in I$;

(2) Si $r \in I$ et $a \in A$, alors $ar, ra \in I$.

Remarque. Si I est un idéal d'un anneau A, alors

(1) $0_A \in I$; et

(2) $r - s \in I$ pour tous $r, s \in I$.

Exemple. (1) Pour tout $m \in \mathbb{Z}$, l'anneau $\mathbb{Z}$ a un idéal $m\mathbb{Z} := \{mx \mid x \in \mathbb{Z}\}$.

(2) Pour tout $p(x) \in \mathbb{R}[x]$, l'anneau $\mathbb{R}[x]$ a un idéal

$$< p(x) >:= \{p(x)f(x) \mid f(x) \in \mathbb{R}[x]\}\,.$$

(3) Le sous-ensemble $\mathbb{Z}$ de $\mathbb{Q}$ n'est pas un idéal.

1.2.12. Définition. Soit I un idéal d'un anneau A. Deux éléments $a, b \in A$ sont dits *congrus modulo* I, noté $a \equiv b\,(\bmod I)$, si $b - a \in I$. Cette relation sur A s'appelle *congruence modulo* I.

1.2.13. Proposition. Soit I un idéal d'un anneau A. La *congruence modulo* I est une relation d'équivalence sur A telle que, pour tout $a \in A$, on a

$$\bar{a} = \{a + r \mid r \in I\} := a + I,$$

appelée *classe de congruence modulo* I de a.

Démonstration. Soient $a, b, c \in A$.

(1) Comme $a - a = 0_A \in I$, on voit que $a \equiv a(\bmod I)$.

(2) Si $a \equiv b\,(\bmod I)$, alors $b - a \in I$ et donc, $a - b = -(b - a) \in I$. Ainsi $b \equiv a\,(\bmod I)$.

(3) Supposons que $a \equiv b\,(\bmod I)$ et $b \equiv c\,(\bmod I)$. Alors $b - a, c - b \in I$. D'où, $c - a = (c - b) + (b - a) \in I$. C'est-à-dire, $a \equiv c\,(\bmod I)$.

Enfin, $a \equiv b\,(\bmod I)$ si et seulement si $b - a = r \in I$ si et seulement si $b = a + r$ avec $r \in I$, si et seulement si $b \in a + I$. D'où, $\bar{a} = a + I$. La preuve de la proposition s'achève.

Remarque. Si I est un idéal d'un anneau A, alors l'ensemble des classes de congruence modulo I sera noté

$$A/I := \{a + I \mid a \in A\}.$$

1.2.14. Proposition. Soit A un anneau. Si I est un idéal de A, alors A/I est un anneau, appelé l'*anneau quotient* de A *modulo* I, pour les opérations suivantes:

$$(a+I)+(b+I)=(a+b)+I \text{ et } (a+I)(b+I)=(ab)+I.$$

Démonstration. Si $a+I=c+I$ et $b+I=d+I$, alors $a-c\in I$ et $b-d\in I$. Comme I est un idéal de A, on a $(a+b)-(c+d)\in I$ et $(ac)-(bd)=(a-b)c+b(c-d)\in I$. C'est-à-dire, $(a+b)+I=(c+d)+I$ et $ab+I=cd+I$. Cela veut dire que l'addition et la multiplication sont correctement définies. Pour tout $\bar{a}\in\bar{A}$, on a

$$\bar{a}+\overline{0_A}=\overline{a+0_A}=\bar{a}; \qquad \overline{1_A}\cdot\bar{a}=\overline{1_A\cdot a}=\bar{a}.$$

D'où $\overline{0_A}=I$ est le zéro et $\overline{1_A}=1_A+I$ est l'identié de $\bar{A}$. On peut vérifier les autres axiomes énoncés dans la définition 1.2.1. La preuve de la proposition s'achève.

Remarque. Si A est un commutatif, alors A/I l'est aussi.

1.2.15. Proposition. Soit A un anneau avec un idéal I. Pour tout $a\in A$, on a
(1) $\bar{a}=\overline{0_A}$ si et seulement si $a\in I$;
(2) $\bar{a}$ est inversible si et seulement s'il existe $b\in A$ et $r\in I$ tel que $ab+r=1_A$.
Démonstration. D'après la proposition 1.2.13, $\overline{0_A}=0_A+I=I$ et $\overline{1_A}=\{1_A+r\mid r\in I\}$.
(1) On a $\bar{a}=\overline{0_A}$ si et seulement si $a\in\overline{0_A}=I$.
(2) $\bar{a}$ est inversible si et seulement s'il existe $b\in A$ tel que $\bar{a}\cdot\bar{b}=\overline{ab}=\overline{1_A}$ si et seulement si $ab\in\overline{1_A}$ si et seulement si $ab=1_A+s$ avec $s\in I$ si et seulement si $ab+r=1_A$ avec $r\in I$. La preuve du lemme s'achève.

Remarque. Si A un anneau et I est un idéal de A, alors A/I est non nul si et seulement si $A\neq I$.

Exemple. Considérons l'anneau $\mathbb{R}[x]$ et son idéal $<x-1>=(x-1)\mathbb{R}[x]$.
(1) Vérifier que $\mathbb{R}[x]/<x-1>=\{\bar{a}\mid a\in\mathbb{R}\}$, et il est un corps.
(2) Trouver l'inverse de $\overline{g(x)}$, où $g(x)=2-x+3x^3$.

1.2.16. Théorème. Soit $\phi:A\to B$ un homomorphisme d'anneaux.
(1) $\mathrm{Ker}(\phi)=\{a\in A\mid\phi(a)=0_B\}$ est un idéal de A.
(2) ϕ est injective si et seulement si $\mathrm{Ker}(\phi)=\{0_A\}$.
(3) Si ϕ est surjectif, alors $A/\mathrm{Ker}(\phi)\cong B$.
Démonstration. (1) Si $a,b\in\mathrm{Ker}(\phi)$ et $c\in A$, alors $\phi(a+b)=\phi(a)+\phi(b)=0_B$ et $\phi(ac)=\phi(a)\phi(c)=0_B\phi(c)=0_B$. D'où, $a+b, ac\in\mathrm{Ker}(\phi)$.
(2) Supposons que ψ est injective. Si $a\in\mathrm{Ker}(\phi)$, alors $\phi(a)=0_B=\phi(0_A)$. Comme ϕ est injective, $a=0_A$. Donc $\mathrm{Ker}(\phi)=\{0_A\}$. Supposons réciproquement que $\mathrm{Ker}(\phi)=\{0_A\}$.

Si $a, b \in A$ sont tels que $\phi(a) = \phi(b)$, alors $\phi(a-b) = 0_B$, et donc $a - b \in \mathrm{Ker}(\phi) = \{0_A\}$. D'où, $a = b$. Ceci montre que ϕ est injective.

(3) Pour tous $a + \mathrm{Ker}(\phi)$, $b + \mathrm{Ker}(\phi) \in A/\mathrm{Ker}(f)$, on a $a + \mathrm{Ker}(\phi) = b + \mathrm{Ker}(\phi)$ si et seulement si $a - b \in \mathrm{Ker}(\phi)$, si et seulement si, $\phi(a) = \phi(b)$. D'où, l'application

$$\bar{\phi} : A/\mathrm{Ker}(\phi) \to B : a + \mathrm{Ker}(\phi) \mapsto \phi(a)$$

est correctement définie et injective. Il est facile de vérifier que $\bar{\phi}$ est un homomorphisme. Supposons maintenant que ϕ est surjectif. Alors, pour tout $b \in B$, il existe $a \in A$ tel que $b = \phi(a) = \bar{\phi}(a + \mathrm{Ker}(\phi))$. C'est-à-dire, $\bar{\phi}$ est surjectif, et donc un isomorphisme. La démonstration du théorème s'achève.

Remarque. Si I est un idéal d'un anneau A, alors la projection

$$p : A \to A/I : a \mapsto \bar{a}$$

est un homomorphisme surjectif.

Exemple. Considérons l'application d'évaluation

$$\rho_1 : \mathbb{R}[x] \to \mathbb{R} : f(x) \mapsto f(1).$$

Il est evident que ρ_1 est surjectif. Comme $\mathrm{Ker}(\rho_1) =< x - 1 >$, on a un isomorphisme

$$\overline{\rho_1} : \mathbb{R}[x]/ < x - 1 > \longrightarrow \mathbb{R} : \overline{f(x)} \mapsto f(1).$$

1.3 Congruence sur les entiers

Dans cette section, on appliquera les résulats obtenus dans la section 1.2 à l'anneau $\mathbb{Z}$. On se fixe un entier $m \geq 2$. Alors $\mathbb{Z}$ a un idéal $m\mathbb{Z} = \{mn \mid n \in \mathbb{Z}\}$. Pour tous $a, b \in \mathbb{Z}$, on voit que $a \equiv b \pmod{m\mathbb{Z}}$ si et seulement si $b - a \in m\mathbb{Z}$ si et seulement si $m \mid b - a$. Dans ce cas, on dit que a, b sont *congrus modulo* m (ou bien, a est *congru à* b *modulo* m), et on écrit $a \equiv b (\mathrm{mod} m)$. En outre, on note

$$\mathbb{Z}_m := \mathbb{Z}/m\mathbb{Z} = \{a + m\mathbb{Z} \mid a \in \mathbb{Z}\}.$$

1.3.1. Lemme. Soient m, a, b, c, d des entiers avec $m \geq 2$.

(1) Si $r \in \mathbb{Z}$, alors $r = r_m(a)$ si et seulement si $a \equiv r (\mathrm{mod} m)$ et $0 \leq r < m$.

(2) Si $a \equiv b (\mathrm{mod} m)$ et $c \equiv d (\mathrm{mod} m)$, alors

$$a + c \equiv b + d (\mathrm{mod} m) \quad \text{et} \quad ac \equiv bd (\mathrm{mod} m).$$

Démonstration. (1) Par définition, $r = r_m(a)$ si et seulement si, $a = mq + r$ avec $q \in \mathbb{Z}$ et $0 \leq r < m$, si et seulement si, $a \equiv r \,(\mathrm{mod} m)$ et $0 \leq r < m$.

(2) Si $a \equiv b \,(\mathrm{mod} m)$ et $c \equiv d \,(\mathrm{mod} m)$, alors $\bar{a} = \bar{b}$ et $\bar{c} = \bar{d}$ dans $\mathbb{Z}_m$. Ceci donne

$$\overline{a+c} = \bar{a} + \bar{c} = \bar{b} + \bar{d} = \overline{b+d}$$

et

$$\overline{ac} = \bar{a} \cdot \bar{c} = \bar{b} \cdot \bar{d} = \overline{bd}$$

D'où, $a + c \equiv b + d \,(\mathrm{mod} m)$ et $ab \equiv cd \,(\mathrm{mod} m)$. La preuve du lemme s'achève.

Remarque. Si $a \equiv b \,(\mathrm{mod} m)$, alors $a^i \equiv b^i \,(\mathrm{mod} m)$, pour tout entier $i \geq 0$.

MAPLE. Pour calculer le reste de a divisé par m, on utilise la commande suivante:

$$a \bmod m;$$

1.3.2. Corollaire. Si $m \geq 2$ est un entier, alors $\{0, 1, \ldots, m-1\}$ est un ensemble complet des représentants des classes de congruence modulo m. En particulier,

$$\mathbb{Z}_m = \{\bar{0}, \bar{1}, \ldots, \overline{m-1}\}.$$

Démonstration. Pour tout $a \in \mathbb{Z}$, on voit que $r_m(a) \in \{0, 1, \ldots, m-1\}$ est tel que $a \equiv r_m(a) \,(\mathrm{mod} m)$. En outre, si $s \in \{0, 1, \ldots, m-1\}$ est tel que $a \equiv s (\mathrm{mod} m)$ alors, d'après le lemme 1.3.1, $s = r_m(a)$. La preuve du corollaire s'achève.

1.3.3. Proposition. Soient m, a, b des entiers avec $m \geq 2$. La congruence

$$ax \equiv b \,(\mathrm{mod} m)$$

a des solutions si et seulement si b est divisible par $\mathrm{pgcd}(a, m)$.

Démonstration. Posons $\mathrm{pgcd}(a, m) = d$. D'après le théorème de Bachet-Bézout, il existe $x_0, y_0 \in \mathbb{Z}$ tels que

$$ax_0 + my_0 = d.$$

Si $b = db_0$ avec $b_0 \in \mathbb{Z}$, alors $a(x_0 b_0) + m(y_0 b_0) = db_0 = b$. D'où, $a(x_0 b_0) \equiv b \,(\mathrm{mod} m)$.

Réciproquement, si $ax_1 \equiv b \,(\mathrm{mod} m)$ avec $x_1 \in \mathbb{Z}$, alors $ax_1 + my_1 = b$ avec $y_1 \in \mathbb{Z}$. Comme $d \mid a$ et $d \mid m$, on a $d \mid b$. La preuve de la proposition s'achève.

Exemple. (1) La congruence $25x \equiv 34 (\mathrm{mod}\, 85)$ n'a pas de solution.

(2) La congruence $4x \equiv 10 \,(\mathrm{mod}\, 18)$ a des solutions.

1.3.4. Corollaire. Soit un entier $m \geq 2$. Si $a \in \mathbb{Z}$, alors $\bar{a} \in U(\mathbb{Z}_m)$ si et seulement si a, m sont co-premiers.

Démonstration. Pour tout $a \in \mathbb{Z}$, par définition, $\bar{a} \in U(\mathbb{Z}_m)$ si et seulement si $\bar{a}\bar{b} = \bar{1}$ pour un $b \in \mathbb{Z}$, si et seulement si, la congruence $ax \equiv 1 \pmod{m}$ a une solution b si et seulement si $\text{pgcd}(a, m) \mid 1$ si et seulement si a, m sont co-premiers. La preuve du corollaire s'achève.

Exemple. Considérons $\mathbb{Z}_{171}$. Vérifier que $\bar{5} \in U(\mathbb{Z}_{171})$ et trouver son inverse.

1.3.5. Théorème. Si $m \geq 2$ est un entier, alors $\mathbb{Z}_m$ est un corps si et seulement si m est premier.

Démonstration. Si m n'est pas premier, alors $m = ab$ with $1 < a, b < m$. Donc, $\bar{a} \in \mathbb{Z}_m$ est non nul. Comme $\text{pgcd}(a, m) = a > 1$, d'après le corollaire 1.3.4, $\bar{a}$ n'est pas inversible dans $\mathbb{Z}_m$. Par conséquent, $\mathbb{Z}_m$ n'est pas un corps.

Supposons maintenant que m est premier. Si $\bar{a} \in \mathbb{Z}_m$ est non nul, alors $m \nmid a$. Comme m est premier, $\text{pgcd}(m, a) = 1$. D'après le corollaire 1.3.4, $\bar{a}$ est inversible. Ceci montre que $\mathbb{Z}_m$ est un corps. La preuve du théorème s'achève.

Remarque. Soit p un entier premier. Comme $\{0, 1, \ldots, p-1\}$ est un ensemble complet des représentants des classes de congruence modulo p, par abus de notation, on identifiera $r \in \{0, 1, \ldots, p-1\}$ avec $\bar{r}$, la classe de congruence modulo p de r. De cette façon, on a que $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$ muni des oppérations suivantes:

$$a \oplus b = r_p(a + b) \quad \text{et} \quad a \odot b = r_p(ab).$$

En particulier, si $ax + py = 1$ avec $0 < a < p$, alors $a^{-1} = r_p(x)$.

On conclut cette section par la résolution d'un système de congruences.

1.3.6. Théorème des restes chinois. Soit un système de congruences

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_r \pmod{m_r}. \end{aligned}$$

Si $m_1, m_2, \ldots, m_r$ sont deux à deux co-premiers, alors

(1) le système admet une solution a; et

(2) un entier b est une autre solution si et seulement si $b \equiv a \pmod{m_1 \cdots m_r}$.

Démonstration. Supposons que $m_1, m_2, \ldots, m_r$ sont deux à deux co-premiers. Posons $\hat{m}_i = m_1 \cdots m_r / m_i$, pour $i = 1, \ldots, r$. Si $i \neq j$, alors $m_i \mid \hat{m}_j$, et d'après la proposition

1.1.5(3), $\text{pgcd}(m_i, \hat{m}_i) = 1$, D'après le théorème de Bachet-Bézout, il existe $x_i, y_i \in \mathbb{Z}$ tels que $\hat{m}_i x_i + m_i y_i = 1$, et donc, $\hat{m}_i x_i a_i + m_i y_i a_i = a_i,\ i = 1, \ldots, n$. Alors $\hat{m}_i(a_i x_i) \equiv a_i \,(\text{mod}\, m_i)$ et $\hat{m}_j \equiv 0 \,(\text{mod}\, m_i)$ pour $j \neq i$. Posant $a = \sum_{j=1}^{r} \hat{m}_j x_j a_j$, on obtient

$$a \equiv \hat{m}_i a_i x_i \equiv a_i \,(\text{mod}\, m_i), \quad \text{pour} \ \ i = 1, \ldots, r.$$

Si $b \in \mathbb{Z}$, alors $b \equiv a_i \,(\text{mod}\, m_i)$, $i = 1, \ldots, r$, si et seulement si, $b \equiv a \,(\text{mod}\, m_i)$, $i = 1, \ldots, r$, si et seulement si, $m_i \mid b - a$, $i = 1, \ldots, r$. D'après la proposition 1.1.5(5), cette dernière condition est équivalente à $m_1 \cdots m_r \mid b - a$, c'est-à-dire,

$$b \equiv a \,(\text{mod}\, m_1 \cdots m_r).$$

La preuve du théorème s'achève.

L'exemple suivant a apparu la première fois dans un livre chinois datant d'environ le 5-ième siècle.

Exemple. Soient des objets en un nombre < 100. Si l'on les range par 3 il en reste 2; si l'on les range par 5, il en reste 3; et si l'on les range par 7, il en reste 2. Combien d'objets a-t-on?

Le résultat suivant sera très utile pour le calcul.

1.3.7. Proposition. Soient deux entiers $m, n \geq 2$. Si $\text{pgcd}(m, n) = 1$, alors

$$\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n.$$

Démonstration. D'abord, considérons l'application suivante:

$$\phi : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n : \bar{x} \mapsto (\hat{x}, \tilde{x}),$$

où $\bar{x} = x + (mn)\mathbb{Z}$, et $\hat{x} = x + m\mathbb{Z}$, et $\tilde{x} = x + n\mathbb{Z}$.

Si $\bar{x} = \bar{y}$, alors $mn \mid x - y$, et donc $m \mid x - y$ et $n \mid x - y$. C'est-à-dire, $(\hat{x}, \tilde{x}) = (\hat{y}, \tilde{y})$. Ceci montre que ϕ est bien défini. Il est évident que ϕ est un homorphisme d'anneaux.

Supposons maintenant que $\text{pgcd}(m, n) = 1$. Fixons $(\hat{a}, \tilde{b}) \in \mathbb{Z}_m \times \mathbb{Z}_n$. En vertu du théorème des restes chinois, il existe $x \in \mathbb{Z}$ tel que $x \equiv a \,(\text{mod}\, m)$ et $x \equiv b \,(\text{mod}\, n)$. D'où, $\phi(\bar{x}) = (\hat{x}, \tilde{x}) = (\hat{a}, \tilde{b})$. En outre si $\phi(\bar{y}) = (\hat{a}, \tilde{b})$, c'est-à-dire, $(\hat{y}, \tilde{y}) = (\hat{a}, \tilde{b})$. Alors $y \equiv a \,(\text{mod}\, m)$ et $y \equiv b \,(\text{mod}\, n)$. D'après le théorème 1.3.6(2), $y \equiv x \,(\text{mod}\, mn)$, c'est-à-dire, $\bar{y} = \bar{x}$. Ceci montre que ϕ est bijective, et donc un isomorphisme. La preuve de la proposition s'achève.

1.4 Code ISBN

Comme 11 est un nombre premier, on a un corps $\mathbb{Z}_{11} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, X\}$, où X représente 10. Les éléments de $\mathbb{Z}_{11}$ s'appellent *caractères*.

1.4.1. Définition. Le code ISBN d'un livre (avant l'an 2007) est une suite

$$a_1a_2a_3a_4a_5a_6a_7a_8a_9a_{10}$$

de 10 caractères de $\mathbb{Z}_{11}$ qui sont regroupés en quatre segments:

$$\mathbf{A} - \mathbf{B} - \mathbf{C} - \mathbf{D}$$

où **A**, **B**, **C** se composent des chiffres de $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Plus précisément,

(1) **A**, de un à cinq chiffres, est le code de la zone linguistique ou la zone géographique: plus la production dans la zone est abondante, plus le segment est court.

(2) **B**, de un à sept chiffres, est le code de l'éditeur: plus la production chez l'éditeur est abondante, plus le segment est court.

(3) **C** est le numéro d'ordre du livre chez l'éditeur; sa longueur est déterminée telle que la longueur totale de $\mathbf{A} - \mathbf{B} - \mathbf{C}$ est 9.

(4) $\mathbf{D} = \{a_{10}\}$, où a_{10} est la clé de contrôle définie par $a_{10} = \sum_{n=1}^{9} n \cdot a_n$ dans $\mathbb{Z}_{11}$.

Remarque. (1) À titre d'exemple, le code pour la zone anglophone est 0 ou 1; pour la zone francophone, c'est 2; pour la zone germanophone c'est 3; et pour le Japon, c'est 4; et pour le Cambodge, c'est 99950. Enfin, le code 92 est réservé pour les organisations internationales.

(2) Un livre publié en France porte un code ISBN se commençant par 2, mais peut être rédigé en anglais.

(3) Le segment **C** est normalement attribué séquentiellement et complété par des zéros à l'avant.

Exemple. Le code ISBN du livre *Algèbre linéaire* par Joseph Grifone (Cépaduès Éditions, Toulouse, 1990) est 2-85428-239-6. Ceci signifie que ce livre est publié dans la zone francophone, et la production chez l'éditeur est peu abondante.

1.4.2. Proposition. Soit $a_1a_2a_3a_4a_5a_6a_7a_8a_9a_{10}$ un code ISBN.

(1) $\sum_{n=1}^{10} n \cdot a_n = 0$ dans $\mathbb{Z}_{11}$.

(2) $a_i = (11 - i)^{-1} \cdot \sum_{1 \leq n \leq 10;\, n \neq i} n \cdot a_n$, pour tout $1 \leq i \leq 10$.

Démonstration. (1) Par définition, $a_{10} = \sum_{n=1}^{9} n \cdot a_n$, et donc $\sum_{n=1}^{9} n \cdot a_n - a_{10} = 0$. Comme $-1 = 10$, on obtient $\sum_{n=1}^{10} n \cdot a_n = 0$.

(2) D'après l'énoncé (1), $(-i) \cdot a_i = \sum_{1 \leq n \leq 10;\, n \neq i} n \cdot a_n$. Comme $-i = (11 - i) \neq 0$, on obtient $a_i = (11 - i)^{-1} \cdot \sum_{1 \leq n \leq 10;\, n \neq i} n \cdot a_n$. La preuve de la proposition s'achève.

Remarque. La proposition 1.4.2(2) dit que chaque caractère d'un code ISBN est uniquement déterminé par les autres catractères.

Exemple. Est-ce que $023456712X$ est un code ISBN?

On étudiera des propriétés des codes ISBN par rapport à la transmission de l'information.

1.4.3. Proposition. Lors de la transmission d'un code ISBN,

(1) si un seul caractère du code a été mal transcrit, alors cette erreur peut être détectée;

(2) si un caractère du code reçu est illisible et les autres caractères du code sont correctement transcrits, alors ce caractère peut être corrigé.

(3) si deux caractères voisins distincts du code ont été intervertis, alors cette erreur peut être détectée.

Démonstration. Soit $a_1a_2a_3a_4a_5a_6a_7a_8a_9a_{10}$ le code transmis.

(1) Supposons que le caractère a_i a été mal transcrit comme b_i, pour un certain $1 \leq i \leq 10$. Comme $b_i \neq a_i = (-i)^{-1} \cdot \sum_{1\leq n\leq 10;\, n\neq i} n \cdot a_n$, on voit que

$$i \cdot b_i + \sum\nolimits_{1\leq n\leq 10;\, n\neq i} n \cdot a_n \neq 0,$$

c'est-à-dire, le code reçu n'est pas un code ISBN.

(2) Supposons que le j-ième caractère du code reçu est illisible et les caractères a_n avec $n \neq j$ sont correctement transcripts. D'après la proposition 1.4.2(2), le j-ième caractère du code reçu est donné par $(11-j)^{-1} \cdot \sum_{1\leq n\leq 10;\, n\neq j} n \cdot a_n$. Ceci achève la démontrsation de la proposition.

(3) Supposons que le i-ième et le $(i+1)$-ième caractères du code original sont distincts et ont été intervertis et les autres sont correctement transcrits. Alors

$$\begin{aligned} i \cdot a_{i+1} + (i+1) \cdot a_i + \sum\nolimits_{1\leq n\leq 10;\, n\neq i,i+1} n \cdot a_n &= a_i - a_{i+1} + \sum\nolimits_{n=1}^{10} n \cdot a_n \\ &= a_i - a_{i+1} \neq 0. \end{aligned}$$

Ainsi le code reçu n'est pas un code ISBN. La preuve de la proposition s'achève.

1.5 Exercices

1. Si $n \in \mathbb{Z}$ et $\alpha \in \mathbb{R}$, montrer que $[n+\alpha] = n + [\alpha]$.

2. (**MAPLE**) Donner un nombre premier de 9 chiffres décimales.

3. Soient p, a, b des entiers positifs avec p premier. Si r, s sont les plus grands exposants tels que $p^r \mid a$ et $p^s \mid b$, montrer que $r+s$ est le plus grand exposant tel que $p^{r+s} \mid ab$.

4. Vérifier que 103 est un nombre premier.

5. (**MAPLE**) Vérifier les quels des nombres suivants sont premiers:

$$1234577; \quad 1789017237; \quad 1789017271; \quad 19912017.$$

6. Trouver le quotient et le reste de -2363 par 215.

7. Si $a, b \in \mathbb{Z}$ avec $b > 0$, montrer qu'il existe $r, s \in \mathbb{Z}$ avec $0 \leq r < b$ tels que

$$ar + bs = \text{pgcd}(a, b).$$

8. Trouver $r, s \in \mathbb{Z}$ avec $0 \leq r < 75$ tels que $(-365)r + 75s = \text{pgcd}(-365, 75)$.

9. (**MAPLE**) Soient $a = 120365821$ et $b = 237894103$. Trouver des entiers x, y tels que

$$ax + by = \text{pgcd}(a, b).$$

10. Donner la décomposition canonique de 30!.

11. Si p est un nombre premier, montrer que $\binom{p}{k} \equiv 0 \,(\text{mod}\, p)$ pour tout k avec $0 < k < p$.

12. Soit $n = n_1 + \cdots + n_r$ avec $n_i > 0$ des entiers.

    (1) Si $e, e_1, \ldots, e_r$ sont les plus grands exposants tels que p^e, $p^{e_1}, \ldots, p^{e_r}$ sont diviseurs de $n!, n_1!, \ldots, n_r!$, respectivement, montrer que $e_1 + \cdots + e_r \leq e$.

    (2) En déduire que le nombre rationnel suivant est un entier:

$$\frac{n\,!}{n_1!\cdots n_r!}$$

    (3) En déduire, pour tout entier k avec $0 \leq k \leq n$, que le coefficient binomial suivant est un entier:

$$\binom{n}{k} = \frac{n\,!}{k\,!\,(n-k)\,!}.$$

13. Considérer l'anneau $M_2(\mathbb{Z})$ des matrices carrées d'ordre 2 sur $\mathbb{Z}$. Montrer que son groupe multiplicative se compose des matrices de déterminant 1 ou -1.

    Indice: Observer que le déterminant de toute matrice de $M_2(\mathbb{Z})$ est un entier, et calculer l'inverse d'une matrice inversible en utilisant sa matrice adjointe.

14. Dans chacun des cas suivants, déterminer si la relation binaire $\mathcal{R}$ est une relation d'équivalence or non; et si oui, trouver un ensemble complet de représantants des classes d'équivalences.

    (1) Si $m, n \in \mathbb{Z}$, alors $m\mathcal{R}n$ si et seulement si $nm > 0$.

    (2) Si $x, y \in \mathbb{R}$, alors $x\mathcal{R}y$ si et seulement si $x \geq y$.

(3) Si $x, y \in \mathbb{R}$, alors $x\mathcal{R}y$ si et seulement si $|x - y| \leq 3$.

15. Considérer $\mathbb{Z} \times \mathbb{Z}^* = \{(m, n) \in \mathbb{Z}^2 \mid n \neq 0\}$. Pour tous $(m, n), (r, s) \in \mathbb{Z} \times \mathbb{Z}^*$, définir

$$(m, n) \sim (r, s) \text{ si et seulenet si } ms = rn.$$

(1) Vérifier que $\sim$ est une relation d'équivalence sur $\mathbb{Z} \times \mathbb{Z}^*$.

(2) Désignant par $\dfrac{m}{n}$ la classe d'équivalence par $\sim$ de (m, n), vérifier que les opérations suivantes sont correctement définies:

$$\frac{m}{n} + \frac{r}{s} = \frac{ms + rn}{ns} \text{ et } \frac{m}{n} \times \frac{r}{s} = \frac{mr}{ns}.$$

(3) Vérifier que muni des opérations définies ci-dessus, l'ensemble quotient de $\mathbb{Z} \times \mathbb{Z}^*$ par $\sim$ est un corps, appelé *corps de nombres rationnels* et noté $\mathbb{Q}$.

Remarque. Pour vérifier que $\mathbb{Q}$ est un corps, il suffit de vérifier les axiomes (3), (4), (6), (7) de la définition 1.2.1, ainsi que la commutativité de la multiplication et que tout élément non nul est inversible.

16. Soit ℓ une droite du plan définie par l'équation $y = ax + b$. Soit $\mathcal{R}$ la relation binaire définie, pour tous $x, y \in \mathbb{R}$, par $x\mathcal{R}y$ si et seulement si le point (x, y) se trouve sur ℓ. Si $\mathcal{R}$ est une relation d'équivalence, trouver a et b.

17. Soit $a \in \mathbb{Q}$. Considérer l'anneau quotient

$$\mathbb{Q}[x]/ < x - a >:= \left\{ \overline{f(x)} \mid f(x) \in \mathbb{Q}[x] \right\}.$$

Montrer, pour tout $f(x) \in \mathbb{Q}[x]$, que $\overline{f(x)} = \overline{f(a)}$.

Indice: En divisant $f(x)$ par $x - a$, on a $f(x) = (x - a)q(x) + r$, où $q(x) \in \mathbb{Q}[x]$ et $r \in \mathbb{Q}$.

18. Considérer l'anneau quotient $\mathbb{Q}[x]/ < x + 1 >$ et les polynômes suivants:

$$f(x) = x^{100} - 3x^{12} + 1; \quad g(x) = 2x^{200} + x - 1.$$

À l'aide du numéro précédant, calculer

(1) $\overline{f(x)} + \overline{g(x)}$; (2) $\overline{f(x)} \cdot \overline{g(x)}$; (3) $\overline{f(x)}^{-1}$.

Attention: Les résultats finaux doivent être des classes de congruence de constants.

19. Calculer dans l'anneau quotient $\mathbb{Z}_{20} = \{\bar{a} \mid a \in \mathbb{Z}\}$:

(1) $\overline{57} - \overline{125}$; (2) $\overline{35} \times \overline{27}$.

Attention: Les résultats finaux doivent être des classes de congruence d'entiers non négatifs et inférieurs que 20.

20. Soit $n = a_r \cdots a_1 a_0$, avec $0 \leq a_i \leq 9$, un entier en notation décimale.
    (1) Montrer que $5 \mid n$ si et seulement si $a_0 = 0$ ou 5.
    (2) Montrer que $3 \mid n$ si et seulement si $3 \mid \sum_{i=0}^{r} a_i$.
    (3) Montrer que $11 \mid n$ si et seulement si $11 \mid a - b$, où a est la somme des a_i avec i paire et b est la somme des a_i avec i impaire.

21. Soit $m \geq 2$ un entier. Montrer, pour tous $a, b \in \mathbb{Z}$, que $a \equiv b (\mathrm{mod} m)$ si et seulement si $r_m(a) = r_m(b)$.

22. (**MAPLE**) Trouver le reste de 7868965346533765 divisé par 8971232.

23. Dans chacun des cas suivants, déterminer si la congruence a des solutions ou non; si oui, donner une solution.
    (1) $145x \equiv 15 (\mathrm{mod} 85)$; (2) $123x \equiv 217 (\mathrm{mod} 195)$;
    (3) $209x \equiv 22 (\mathrm{mod} 77)$; (4) $142x \equiv 67 (\mathrm{mod} 792)$.

24. Soient des objets en un nombre < 210. Si l'on les range par 5 il en reste 2; si l'on les range par 6, il en reste 1; et si l'on les range par 7, il en reste 3. Combien d'objets a-t-on?

25. Considérer l'anneau commutatif $\mathbb{Z}_{174}$. Dans chacun des cas suivants, déterminer si la classe de congruence $\bar{a}$ est inversible ou non; et si oui, trouver son inverse.
    (1) $a = 669$; (2) $a = 131$.

26. Trouver les éléments inversibles de l'anneau commutatif $\mathbb{Z}_{12}$.

27. (**MAPLE**) Soient $a = 1234567$ et $m = 8974251$. Vérifier que $\bar{a}$ est inversible dans $\mathbb{Z}_m$ et trouver un entier b avec $0 < b < m$ tel que $\bar{a}^{-1} = \bar{b}$.

28. Trouver le groupe multiplicatif de $\mathbb{Z}_{30}$.

29. (**MAPLE**) Déterminer lequel de $\mathbb{Z}_{2345678901}$ et $\mathbb{Z}_{2345678917}$ est un corps.

30. Les Éditions Québec Amérique est une maison d'édition québécoise du code 7644. Fabriquer un code ISBN du 203-ième livre publié chez Les Éditions Québec Amérique.

31. America Press est un éditeur aux États-Unis du code 12. Il a publié un livre dont le numéro d'ordre chez America Press est 599250. Trouver le code ISBN de ce livre, en sachant que le dernier caractère est un chiffre impaire.

Chapitre II: Cryptographie

La cryptographie est la pratique et l'étude des techniques de communication sécurisée en présence de tiers, appelés *adversaires*. Plus généralement, il s'agit de la construction et de l'analyse des protocoles qui permettent de surmonter l'influence des adversaires et qui sont liés à divers aspects de la sécurité de l'information tels que la confidentialité des données, l'intégrité des données et l'authentification. Les applications de la cryptographie incluent des cartes ATM, mots de passe informatiques et le commerce électronique.

2.1 Indicatrice d'Euler

2.1.1. Définition. Soit un entier $m \geq 1$. Le nombre d'entiers $a \in \{1, \ldots, m\}$ avec $\text{pgcd}(a, m) = 1$ s'appelle l'*indicatrice d'Euler de* m, noté $\varphi(m)$.

Remarque. Comme $\text{pgcd}(1, m) = 1$, on a $\varphi(m) \geq 1$.

On donnera une autre intépretation de $\varphi(m)$.

2.1.2. Proposition. Soit un entier $m \geq 2$. Alors $\varphi(m)$ est égal à l'ordre du groupe multiplicative de l'anneau $\mathbb{Z}_m$.

Démonstration. D'abord, $\mathbb{Z}_m = \{\bar{1}, \bar{2}, \ldots, \bar{m}\}$. Pour tout $1 \leq a \leq m$, d'après la proposition 1.3.4, la classe $\bar{a}$ appartient à $U(\mathbb{Z}_m)$ si et seulement $\text{pgcd}(a, m) = 1$. Par conséquent, l'ordre de $U(\mathbb{Z}_m)$ est égal à $\varphi(m)$. La preuve de la proposition s'achève.

2.1.3. Corollaire. Si p est un nombre premier, alors $\varphi(p) = p - 1$.

Démonstration. D'après le théorème 2.3.5, $\mathbb{Z}_p = \{\bar{0}, \bar{1}, \ldots, \overline{p-1}\}$ est un corps de p éléments. Ainsi $U(\mathbb{Z}_p) = \{\bar{1}, \ldots, \overline{p-1}\}$ est un groupe d'ordre $p - 1$. D'après la proposition 2.1.2, on a $\varphi(p) = p - 1$. La preuve du corollaire s'achève.

Le résultat précédant nous permet d'évaluer l'indicatrice d'Euler.

2.1.4. Lemme. Soient $m, n \geq 2$ des entiers. Si $\text{pgcd}(m, n) = 1$, alors

$$\varphi(mn) = \varphi(m)\varphi(n).$$

Démonstration. Supposons que $\text{pgcd}(m, n) = 1$. En vertu de la proposition 1.3.7, $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$, et d'après la proposition 1.2.5, $U(\mathbb{Z}_{mn}) \cong U(\mathbb{Z}_m) \times U(\mathbb{Z}_n)$. Par conséquent,

$$\varphi(mn) = |U(\mathbb{Z}_{mn})| = |U(\mathbb{Z}_m \times \mathbb{Z}_n)| = |U(\mathbb{Z}_m)||U(\mathbb{Z}_n)| = \varphi(m)\varphi(n).$$

La preuve du lemme s'achève.

2.1.5. Théorème. Soit un entier $m \geq 2$. Si $m = p_1^{e_1} \cdots p_r^{e_r}$ est la factorisation canonique, alors

$$\varphi(m) = (p_1^{e_1} - p_1^{e_1-1}) \cdots (p_r^{e_r} - p^{\,e_r-1}) = m\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right).$$

Démonstration. D'abord, supposons que $m = p^e$ avec $e > 0$ et p un premier. Si $x \in \{1, 2, \ldots, m\}$, alors $\text{pgcd}(x, m) > 1$ si et seulement si $p \mid m$ si et seulement si $x = py$ avec $1 \leq y \leq p^{e-1}$ si et seulement si $x \in \{p, 2p, \cdots, (p^{e-1} - 1)p, p^{e-1}p\}$. Cela nous donne $\varphi(p^e) = p^e - p^{e-1}$. Supposons que $r > 1$ et le résultat est valide pour $r - 1$. Comme $p_1^{e_1} \cdots p_{r-1}^{e_{r-1}}$ et $p_r^{e_r}$ sont co-premiers, en vertu du lemme 2.1.4, on voit que

$$\varphi(m) = \varphi(p_1^{e_1} \cdots p_{r-1}^{e_{r-1}})\varphi(p_r^{e_r}) = (p_1^{e_1} - p_1^{e_1-1}) \cdots (p_{r-1}^{e_{r-1}} - p_{r-1}^{e_{r-1}-1})(p_r^{e_r} - p^{e_r-1}).$$

La preuve du théorème s'achève.

2.1.6. Théorème d'Euler. Soit un entier $m \geq 2$. Si a est un entier co-premier à m, alors

$$a^{\varphi(m)} \equiv 1 \,(\text{mod}m).$$

Démonstration. Considérons $\bar{a} \in \mathbb{Z}_m$. Si $\text{pgcd}(a, m) = 1$, alors $\bar{a} \in U(\mathbb{Z}_m)$. Comme l'ordre de $U(\mathbb{Z}_m)$ est $\varphi(m)$, d'après le théorème de Lagrange, l'ordre de $\bar{a}$ est un diviseur de $\varphi(m)$. En particulier, $\overline{a^{\varphi(m)}} = \bar{a}^{\,\varphi(m)} = \bar{1}$. C'est-à-dire, $a^{\varphi(m)} \equiv 1 \,(\text{mod}m)$. Ceci achève la preuve du théorème.

Exemple. Donner le dernier chiffre décimal de 2013^4.

Le résultat célèbre suivant est un cas particulier du théorème d'Euler, mais il est apparu beaucoup plus avant.

2.1.7. Petit théorème de Fermat. Soit p un nombre premier. Si a est un entier non divisible par p, alors $a^{p-1} \equiv 1(\text{mod}p)$.

Démonstration. D'après le corollaire 2.1.3, $\varphi(p) = p - 1$. Si $p \nmid a$, alors $\text{pgcd}(a, p) = 1$. D'après le théorème d'Euler, $a^{p-1} \equiv 1(\text{mod}p)$. La preuve du théorème s'achève.

2.1.8. Corollaire. Soit p un nombre premier. Si a est un entier, alors

$$a^p \equiv a \,(\text{mod}p).$$

Démonstration. Si $p \mid a$, alors $a^p \equiv 0$ et $a \equiv 0 \,(\text{mod}p)$, et donc, $a^p \equiv a \,(\text{mod}p)$. Sinon, $a^{p-1} \equiv 1$, et donc $a^p \equiv a \,(\text{mod}p)$. La preuve du corollaire s'achève.

En généralisant le corollaire 2.1.8, on obtient le résultat suivant, qui est la base du chiffrement RSA.

2.1.9 Théorème. Soit $m = p\,q$, avec p, q deux nombres premiers distincts. Soit n un entier avec $n \equiv 1(\mathrm{mod}\,\varphi(m))$. Pour tout entier a, on a

$$a^n \equiv a\,(\mathrm{mod} m).$$

Démonstration. Par l'hypothèse, on a $n = \varphi(m)\,s + 1$, pour un certain $s \in \mathbb{Z}$.

(1) Si $p \mid a$ et $q \mid a$, alors $m \mid a$, et donc, $a^n \equiv 0 \equiv a\,(\mathrm{mod} m)$.

(2) Si $p \nmid a$ et $q \nmid a$, alors $\mathrm{pgcd}(a, m) = 1$. D'après le théorème d'Euler, $a^{\varphi(m)} \equiv 1\,(\mathrm{mod} m)$, et donc, $a^{\varphi(m)s} \equiv 1\,(\mathrm{mod} m)$. Par conséquent, $a^n = a(a^{\varphi(m)})^s \equiv a\,(\mathrm{mod} m)$.

(3) Supposons que $p \mid a$ et $q \nmid a$. Alors $a = p^t b$, avec $t > 0$ et $p \nmid b$. Comme $q \nmid b$, d'après le cas (2), $b^n \equiv b\,(\mathrm{mod} m)$. Or, d'après le théorème 2.1.5, $\varphi(m) = (p-1)(q-1)$. Comme $p \neq q$, d'après le petit théorème de Fermat, $p^{\,q-1} \equiv 1(\mathrm{mod}\,q)$, et donc,

$$p^{\,\varphi(m)st} = (p^{\,q-1})^{(p-1)st} \equiv 1(\mathrm{mod}\,q).$$

C'est-à-dire, $p^{\,\varphi(m)st} = qc + 1$ avec $c \in \mathbb{Z}$. Comme $qa = qp^t b = mp^{t-1}b \equiv 0\,(\mathrm{mod} m)$, on obtient

$$a^n = p^{\,tn} b^n \equiv (p^{\,t})^{\,\varphi(m)s+1} b = p^{\,\varphi(m)st}(p^{\,t}b) = (qc+1)a = (qa)c + a \equiv a\,(\mathrm{mod} m).$$

De même, si $q \mid a$ et $p \nmid a$, alors $a^n \equiv a\,(\mathrm{mod} m)$. Ceci achève la preuve du théorème.

Dans l'application, on doit calculer le reste de a^n divisé par m. On étudiera comment effectuer ce calcul lorsque n est très grand.

2.1.10. Lemme. Si $n \geq 0$ est un entier, alors n s'écrit d'une façon unique

$$n = n_s \times 2^{\,s} + \cdots + n_1 \times 2^1 + n_0 \times 2^0, \text{ où } n_0, n_1, \ldots, n_s \in \{0, 1\}.$$

Dans ce cas, on écrit $n = n_s \cdots n_1 n_0$, appelée *notation binaire* de n.

Démonstration. Le lemme est evident si $n = 0$ ou 1. Supposons que $n > 1$ et le lemme est valide pour tout entier $< n$. Soit $s \geq 0$ le plus grand exposant tel que $2^{\,s} \leq n$. Alors $m = n - 2^s \geq 0$. Si $m = 0$, alors $n = 2^s$, et le lemme est valide. Sinon, $m = n_t \times 2^t + \cdots + n_1 \times 2 + n_0$ avec $0 \leq t < s$ et $n_0, \ldots, n_t \in \{0, 1\}$. Ceci donne

$$n = 2^s + n_t \times 2^t + \cdots + n_1 \times 2^1 + n_0 \times 2^0.$$

La preuve du lemme s'achève.

Exemple. La notation binaire de zero est 0; et celle-ci de 1 est 1.

Exemple. Donner la notation binaire d'onze

2.1.11. Proposition. Soient a, n, m des entiers strictement positifs. Soit $n = n_s \cdots n_1 n_0$ la notation binaire de n. Posons $a_0 = r_m(a)$ et $r_0 = r_m(a_0^{n_0})$. Si $a_i = r_m(a_{i-1}^2)$ et $r_i = r_m(a_i^{n_i} r_{i-1})$, pour $i = 1, \ldots, s$, alors $r_m(a^n) = r_s$.

Démonstration. On prétend, pour tout $0 \leq i \leq s$, que $a_i \equiv a^{2^i} \pmod{m}$ et

$$r_i \equiv a^{n_i \times 2^i + n_{i-1} \times 2^{i-1} + \cdots + n_0} \pmod{m}.$$

En effet, $a_0 \equiv a = a^{2^0} \pmod{m}$ et $r_0 \equiv a_0^{n_0} \equiv a^{n_0} \pmod{m}$. Supposons que l'énoncé est valide pour s avec $0 \leq i < s$. Alors, $a_{i+1} \equiv a_i^2 \equiv (a^{2^i})^2 = a^{2^{i+1}} \pmod{m}$ et

$$r_{i+1} \equiv a_{i+1}^{n_{i+1}} r_i \equiv (a^{2^{i+1}})^{n_{i+1}} a^{n_i \times 2^i + n_{i-1} \times 2^{i-1} + \cdots + n_0} \equiv a^{n_{i+1} \times 2^{i+1} + n_i \times 2^i + \cdots + n_0} \pmod{m}.$$

Ceci montre lénoncé. En particulier, $r_s \equiv a^n \pmod{m}$. Comme $0 \leq r_s < m$, on a $r_m(a^n) = r_s$. La preuve de la proposition s'achève.

MAPLE. Pour calculer le reste de a^n divisé par m, on tape la commande

$$\text{power}(a, n) \bmod m;$$

Exemple. On veut trouver les deux derniers chiffres décimaux de 27^{1234}, c'est-à-dire, le reste de 27^{1234} par 100. D'abord, à l'aide du MAPLE, on trouve

$1234 = 1 \times 2^{10} + 0 \times 2^9 + 0 \times 2^8 + 1 \times 2^7 + 1 \times 2^6 + 0 \times 2^5 + 1 \times 2^4 + 0 \times 2^3 + 0 \times 2^2 + 1 \times 2^1 + 0 \times 2^0$.

D'où, $1234 = 10011010010$. Or, on calcule des congruences modulo 100 suivantes:

i	a_i	n_i	r_i
0	27	0	$27^0 = 1$
1	$27^2 \equiv 29$	1	$29^1 \times 1 = 29$
2	$29^2 \equiv 41$	0	$41^0 \times 29 = 29$
3	$41^2 \equiv 81$	0	$81^0 \times 29 = 29$
4	$81^2 \equiv 61$	1	$61^1 \times 29 \equiv 69$
5	$61^2 \equiv 21$	0	$21^0 \times 69 = 69$
6	$21^2 \equiv 41$	1	$41^1 \times 69 \equiv 29$
7	$41^2 \equiv 81$	1	$81^1 \times 29 \equiv 49$
8	$81^2 \equiv 61$	0	$61^0 \times 49 = 49$
9	$61^2 \equiv 21$	0	$21^0 \times 49 \equiv 49$
10	$21^2 \equiv 41$	1	$41^1 \times 49 \equiv 09$

D'où, les deux derniers chiffres décimaux de 27^{1234} sont 0 et 9.

2.2 Chiffrement RSA

Le chiffrement d'un message a besoin deux clés: une pour le chiffrer et une pour le déchiffrer. Voici la schéma du chiffrement:

$$\text{texte claire} \xrightarrow{\text{chiffrer}} \text{texte illisible} \xrightarrow{\text{transmission}} \text{texte illisible} \xrightarrow{\text{déchiffrer}} \text{texte original.}$$

Pendant très longtemps, on a utilisé une même clé pour chiffrer et déchiffrer. L'un des problèmes de cette technique est que la clé doit rester totalement confidentielle. Et la mise en oeuvre peut s'avérer difficile, surtout avec un grand nombre de correspondants car il faut autant de clés que de correspondants. En 1976, Diffie et Hellman ont imaginé un modèle théorique de chiffrement, appelé *chiffrement à clé publique*, dans lequel la clé pour chiffrer est publique, et la clé pour déchiffrer est privée. En 1978, Rivest, Shamir et Adelmann ont réalisé ce modèle par la création du chiffrement RSA.

2.2.1. Définition. Un code RSA se compose d'une clé publique (m, e) et d'une clé privée (m, d), où

(1) $m = p\,q$ avec p, q deux nombres premiers distincts, appelé *module de chiffrement*;

(2) e est tel que $1 < e < \varphi(m)$ et $\text{pgcd}(e, \varphi(m)) = 1$, appelé *exposant de chiffrement*;

(3) d est tel que $0 < d < \varphi(m)$ et $ed \equiv 1(\text{mod}\,\varphi(m))$, appelé *exposant de déchiffrement*.

Remarque. (1) Dans la pratique, p, q doivent être de grande taille, par exemple, de 100 à 200 chiffres décimales. Dans ce cas, en utilisant le meilleur algorithme et des ordinateurs les plus rapides, il faudrait des siècles pour trouver p, q à partir de m. Par conséquent, il sera impossible de trouver $\varphi(m)$.

(2) L'exposant de chiffrement e doit être très grand. On applique l'algorithme d'Euclide pour assurer que $(e, \varphi(m)) = 1$ et trouver des entiers x, y tels que $ex + \varphi(m)y = 1$.

(3) L'exposant de déchiffrement d est l'inverse de e modulo $\varphi(m)$, ce qui est $r_{\varphi(m)}(x)$. Sans connaître p, q, il sera impossible de trouver d à partir de m et e.

Le résultat suivant est le principe du code RSA.

2.2.2. Théorème. Soient un code RSA dont la clé publique est (m, e) et la clé privée est (m, d). Soit n un entier avec $0 < n < m$. Si $x = r_m(n^e)$, alors $r_m(x^d) = n$.

Démonstration. Supposons que $x = r_m(n^e)$ et $y = r_m(x^d)$. Alors $n^e \equiv x\,(\text{mod}m)$ et $x^d \equiv y\,(\text{mod}m)$. Comme $ed \equiv 1(\text{mod}\,\varphi(m))$, d'après le théorème 2.1.9, on a

$$n \equiv n^{e\,d} = (n^e)^d \equiv x^d \equiv y\,(\text{mod}m).$$

Comme $0 < n, y < m$, on a $n = y$. La preuve du théorème s'achève.

Exemple. Donner un code RSA avec $p = 100000000019$ et $q = 1000000000039$.

Solution. On tape les commandes du MAPLE suivantes:

$p := 100000000019;$

$$100000000019$$

$q := 1000000000039;$

$$1000000000039$$

$m := p * q;$

$$100000000022900000000741$$

$a := (p-1) * (q-1);$

$$100000000021800000000684$$

Ainsi on obtient le module de chiffrement $m = 100000000022900000000741$. En outre, on a $\varphi(m) = 100000000021800000000684$. On choisit l'exposant de chiffrement $e = 1234567$. On continue avec les commandes suivants:

$e := 1234567;$

$$1234567$$

$\text{igcdex}(e, a, x, y); x; y;$

$$1$$
$$-3658651171616129406504717$$
$$451685$$

$d := -3658651171616129406504717 \bmod a;$

$$6341348830567059349596 7$$

Donc, l'exposant de déchiffrement est $d = 6341348830567059349596 7$. Ceci nous donne un code RSA dont la clé publique est

$$(m, e) = (100000000022900000000741, 1234567)$$

et la clé privée est

$$(m, d) = (100000000022900000000741, 6341348830567059349596 7).$$

Pour appliquer le chiffrement RSA, on doit convertir les textes en nombres naturels inférieurs que le module de chiffrement: chaque caractère est remplacé par un nombre naturel, et une phrase est remplacée par la concatenation de nombres naturels correspondants. Par exemple, le code ASCII (American Standard Code for Information Interchange) remplace chaque caractère non accentué par un 3-chiffre nombre, qui permet de convertir toutes les

phrases en anglais. Pour ce cours, on va écrire les textes en majuscules et les convertir en nombres naturels selon le tableau suivant.

$A(01)$	$B(02)$	$C(03)$	$D(04)$	$E(05)$	$F(06)$	$G(07)$	$H(08)$	$I(09)$	$J(10)$
$K(11)$	$L(12)$	$M(13)$	$N(14)$	$O(15)$	$P(16)$	$Q(17)$	$R(18)$	$S(19)$	$T(20)$
$U(21)$	$V(22)$	$W(23)$	$X(24)$	$Y(25)$	$Z(26)$	À(27)	Â(28)	Ç(29)	É(30)
È(31)	Ê(32)	Î(33)	Ï(34)	Ô(35)	Ù(36)	Û(37)	!(38)	$'$(39)	.(40)
”(41)	: (42)	, (43)	?(44)	; (45)	#(46)	&(47)	$(48)	˜(49)	espace(50)

Exemple. Avec le tableau ci-dessus, la phrase

DEMAIN, J'IRAI À QUÉBEC.

est converti en le nombre suivant:

$$405130109144310390918010950275017213002040 3$$

2.2.3. Fonctionnement du chiffrement RSA. Étant donné un code RSA dont la clé publique est (m, e) et la clé privée est (m, d).

(1) L'expéditeur convertit un texte en un nombre n avec $0 < n < m$ (le texte doit être séparé en plusieurs blocs s'il est trop long);

(2) L'expéditeur calcule $x = r_m(n^e)$, et l'expédie au destinataire;

(3) Quand le nombre x est reçu, le destinataire calcule $r_m(x^d)$, qui est égal à n;

(4) Le destinataire retrouve le texte original à partir de n.

Exemple. Considérons le code RSA dont la clé publique et la clé privée sont données respectivement par

$$(m, e) = (100000000022900000000741, 1234567)$$

et

$$(m, d) = (100000000022900000000741, 63413488305670593495967).$$

Bob veut envoyer à Alice le message suivant

J'AI FAIM.

D'abord, à l'aide du tableau ci-dessus, Bob convertit ce message en le nombre naturel

$$n = 10390109500601091340.$$

Selon la clé publique, il calcule $x := r_m(n^e)$ en tapant la commande du MAPLE suivant:

$m := 100000000022900000000741;$

100000000022900000000741

$e := 1234567;$

$$1234567$$

$n := 10390109500601091340;$

$$10390109500601091340$$

$x := \text{power}(n, e) \bmod m;$

$$7257226681447992490 2350$$

Enfin, Bob envoie à Alice ce nombre $x = 7257226681447992490 2350$. Après reçu le nombre x, à l'aide de la clé privée, Alice retrouve le nombre n en tape les commandes suivantes:

$m := 100000000022900000000741;$

$$100000000022900000000741$$

$d := 63413488305670593495967;$

$$63413488305670593495967$$

$x := 7257226681447992490 2350;$

$$7257226681447992490 2350$$

$y :=\ \text{power}(x, d) \bmod m;$

$$10390109500601091340$$

En utilisant le tableau ci-dessus, Alice trouve le message de Bob.

2.3 Exercices

1. Evaluer $\varphi(38115)$. *Indice*: Factoriser le nombre à l'aide du numéro 18 des Exercices 1.5.

2. Trouver tous les entiers n tels que $\varphi(n) = 24$.

3. Si $n > 2$ est un entier, monter que $\varphi(n)$ est un nombre pair. *Indice*: Appliquer le théorème 2.1.5.

4. Soient deux entiers $m, n > 1$. Si $m \mid n$, montrer que $\varphi(m) \mid \varphi(n)$.

5. Soit $m = pq$ avec p, q deux nombres premiers distincts. Vérifier que p, q sont les racines de l'equation quadratique suivante:

$$x^2 + (\varphi(m) - m - 1)x + m = 0.$$

6. Factoriser 9991, en sachant que 9991 est un produit de deux nombre premiers distincts tels que $\varphi(9991) = 9792$. *Indice*: Utiliser le numéro précédant.

7. Montrer, pour tout entier naturel a, que le dernièr chiffre décimal de a^5 coincide avec celui-ci de a. *Indice*: Appliquer le théorème 2.1.9 au cas où $m = 10$ et $n = 5$.

8. Soient p, a, b des entiers avec p premier. Si $a^p \equiv b^p (\mathrm{mod}\, p)$, montrer que $a^p \equiv b^p (\mathrm{mod}\, p^2)$.

9. Soient a, b des entiers tels que $\mathrm{pgcd}(a, 91) = 1$ et $b \equiv a^{67} (\mathrm{mod}\, 91)$.
   (1) Trouver un entier $n > 0$ tel que $b^n \equiv a (\mathrm{mod}\, 91)$.
   (2) Si $b = 53$, trouver $r_{91}(a)$, le reste de a par 91.

10. (1) Trouver la notation binaire de 1386.
    (2) Vérifier que $2^{1386} \equiv 1 (\mathrm{mod}\, 1387)$.
    (3) Vérifier que $3^{1386} \not\equiv 1 (\mathrm{mod}\, 1387)$, et en déduire si 1387 est un premier ou non.

11. (1) Trouver la notation binaire de 1762.
    (2) Vérifier que 1763 n'est pas premier. *Indice*: Appliquer la proposition 2.1.11 pour $a = 2$ ou 3.

12. Donner le reste de 999^{179} par 63.

13. (**MAPLE**) Calculer 125678912^{234567} et son reste divisé par 3456921.

14. (**MAPLE**) Bob envoie un message à Alice en utilisant le code RSA dont la clé privée est

$$(m, d) = (100000000022900000000741, 63413488305670593495967).$$

    Si Alice récoit le nombre

$$x = 4204879488553950340505,$$

    quel est le message de Bob?

15. Bob envoie des informations à Alice par un code RSA dont la clé publique est $(143, 97)$.
    (1) Trouver, à l'aide de l'algorithme d'Euclide, la clé privée de ce code RSA.
    (2) Si Alice reçoit le nombre 3, quel est le message de Bob?
    (3) Si Bob veut envoyer le mot AU à Alice, quel nombre doit-il expédier dans le canal de transmission?

    Remarque. Pour les parties (2) et (3), utiliser la proposition 2.1.11 au lieu d'une calculatrice ou du MAPLE.

16. Bob envoie des informations à Alice en utilisant un code RSA dont la clé publique est $(323, 169)$.
    (1) Trouver la clé privée de ce code RSA.
    (2) Si Bob veut envoyer le mot UN, quel nombre doit-il expédier dans le canal de transmission?
    (3) Si Alice reçoit le nombre 126, quel est le message de Bob?

Chapitre III: Codes correcteurs

La théorie des codes correcteurs est une technique de codage basée sur la redondance. Elle est destinée à corriger des erreurs de transmission d'une information (ou bien un message) sur un canal de transmission peu fiable. Dans ce chapitre, on verra comment l'algèbre linéaire est appliquée dans ce domaine du transport de l'information.

3.1 Rappel de l'algèbre linéaire

Partout dans cette section, on se fixe K un corps.

3.1.1. Définition. Soit E un K-espace vectoriel.

(1) Un sous-ensemble non-vide E' de E s'appelle *sous-espace* si, pour tous $u, v \in E'$ et $\alpha \in K$, on a $u + v \in E'$ et $\alpha u \in E'$.

(2) Si $\mathcal{U}$ est une famille non-vide de vecteurs de E, alors le sous-espace de E engendré par $\mathcal{U}$, noté $< \mathcal{U} >$, est le plus petit sous-espace de E contenant $\mathcal{U}$, qui se compose des combinaisons linéaires de vecteurs de $\mathcal{U}$.

Remarque. Si E' est un sous-espace de E, alors $0_E \in E'$.

Maintenant, considérons les K-espaces vectoriels $K^n = \{(a_1, \ldots, a_n) \mid a_i \in K\}$ et

$$K^{(n)} = \left\{ \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \mid a_i \in K \right\}.$$

Soit M une matrice de type $m \times n$ sur K. Rappelons que l'*espace-ligne* $\mathscr{L}(M)$ de M est le sous-espace vectoriel de K^n engendré par les lignes de M; l'*espace-colonne* $\mathscr{C}(M)$ de M est le sous-espace vectoriel de $K^{(m)}$ engendré par les colonnes de M; et le *noyau* $\mathscr{N}(M)$ de M est le sous-espace vectoriel de $K^{(n)}$ composé des vecteurs v tel que $Mv = 0$.

Le résultat suivant est vu dans le cours MAT153.

3.1.2. Théorème. Soit M une matrice de type $m \times n$ sur K.

(1) $\dim \mathscr{L}(M) = \dim \mathscr{C}(M) = \mathrm{rg}(M)$.

(2) $\dim \mathscr{N}(M) = n - \mathrm{rg}(M)$.

(3) $\mathrm{rg}(M) = m$ si et seulement si les lignes de M sont linéairement indépendantes.

(4) Si $m = n$, alors M est inversible si et seulement si les colonnes de M sont linéairement indépendantes.

D'après le cours MAT153, on a le résultat suivant.

3.1.3. Lemme. Soit M une matrice sur K ayant m lignes $L_1, \ldots, L_m$ et n colonnes $C_1, \ldots, C_n$. Si $a_1, \ldots, a_n; b_1, \ldots, b_m \in K$, alors

(1) $(b_1 \cdots b_m)A = b_1L_1 + \cdots + b_mL_m \in \mathscr{L}(M)$;

(2) $$M \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = a_1C_1 + \cdots + a_nC_n \in \mathscr{C}(M).$$

Plus généralement, on a le résultat suivant.

3.1.4. Lemme. Soient M, N des matrices sur K telles que MN est défini.

(1) Si $N_1, \ldots, N_q$ sont les colonnes de N, alors $MN = (MN_1, \ldots, MN_n)$.

(2) Si $M_1, \ldots, M_p$ sont les lignes de M, alors

$$MN = \begin{pmatrix} M_1N \\ \vdots \\ M_pN \end{pmatrix}.$$

On dit qu'une matrice M *s'échelonne* à une matrice N si N est obtenue à partir de M par une suite finie d'opérations élémentaires sur les lignes. Le résultat suivant est vu dans le cours MAT153.

3.1.5. Théorème. Soient M, N des matrices de même type sur K. Alors M s'échelonne à N si et seulement si $N = PM$ avec P inversible. Dans ce cas,

(1) $\mathscr{L}(M) = \mathscr{L}(N)$ et $\mathrm{rg}(M) = \mathrm{rg}(N)$; et

(2) si N est échelonnée, alors les lignes non nulles de N forment une base de $\mathscr{L}(M)$.

Exemple. Donner une base du sous-espace E' de $\mathbb{R}^5$ engendré par les vecteurs

$$(0, 2, 3, 2, 5),\ (0, 1, 2, 2, 7),\ (0, 1, 2, 1, 5).$$

3.1.6. Proposition. Soient $M, N \in M_{m\times n}(K)$. Si $\mathrm{rg}(M) = \mathrm{rg}(N) = m$, alors $\mathscr{L}(M) = \mathscr{L}(N)$ si et seulement si M s'échelonne à N.

Démonstration. Supposons que $\mathrm{rg}(M) = \mathrm{rg}(N) = m$. Il suffit de montrer la nécessité. Supposons que $\mathscr{L}(M) = \mathscr{L}(N)$. D'après la proposition 3.1.5, les lignes $M_1, \ldots, M_m$ de M forment une base de $\mathscr{L}(M)$, et les lignes $N_1, \ldots, N_m$ forment une base de $\mathscr{L}(N)$. Donc $\{N_1, \ldots, N_m\}$ et $\{M_1, \ldots, M_m\}$ sont deux bases de $\mathscr{L}(N)$. Supposons que $P = (a_{ij})_{m\times m}$ est

la matrice de passage de $\{N_1, \ldots, N_m\}$ vers $\{M_1, \ldots, M_m\}$. Posant P_j la j-ième colonne de P, on obtient

$$M_j = a_{1j}N_1 + \cdots + a_{mj}N_m = (a_{1j}, \cdots, a_{mj})N = P_j^T N,\ j = 1, \ldots, m.$$

Ceci donne

$$P^T N = \begin{pmatrix} P_1^T N \\ \vdots \\ P_m^T N \end{pmatrix} = \begin{pmatrix} M_1 \\ \vdots \\ M_m \end{pmatrix} = M.$$

Comme P est inversible, P^T l'est aussi. Donc, M s'échelonne à N. La preuve de la proposition s'achève.

3.1.7. Définition. Une matrice échelonnée $M \in M_{m\times n}(K)$ est dite *echelonnée réduite* si les conditions suivante sont vérifiées.

(1) Tous les pivots de M sont 1.

(2) Toute colonne de M contenant un pivot admet un seul terme non nul.

Dans ce cas, si a_{i,j_i} est le pivot de la i-ième ligne de M, alors la j_i-ième colonne de M est e_i, la i-ième colonne de I_m.

Remarque. Une matrice de la forme $(I_k \mid A)$ avec $k \geq 1$ est échelonnée réduite, appelée *échelonnée normée*.

Exemple. (1) Une matrice nulle est échelonnée réduite.

(2) Une matrice identité I_n est échelonnée normée.

3.1.8. Lemme. Soient $M = (a_{ij})_{m\times n}$ et $N = (b_{ij})_{m\times n}$ des matrices échelonnées réduites sur K. Si M s'échelonne à N, alors $M = N$.

Démonstration. Supposons que M s'échelonne à N. Alors, $N = PM$ avec P une matrice inversible. Écrivons $P = (P_1, \cdots, P_m)$, $M = (M_1, \ldots, M_n)$, $N = (N_1, \ldots, N_n)$, et $I_m = (e_1, \ldots, e_m)$ en colonnes. D'après le lemme 3.1.4(1), on a $N = (N_1, \ldots, N_n) = (PM_1, \ldots, PM_n)$; et donc, $N_j = PM_j$, pour $j = 1, 2, \ldots, n$.

Comme $\mathrm{rg}(N) = \mathrm{rg}(M)$, on peut supposer que $\mathrm{rg}(M) = m$. Supposons que les pivots de M sont $a_{1,j_1}, \ldots, a_{m,j_m}$ et ceux de N sont $b_{1,p_1}, \ldots, b_{m,p_m}$. Comme M et N sont échelonnées réduites, $M_{j_i} = N_{p_i} = e_i$, $i = 1, \ldots, m$.

Si $j_1 < p_1$, alors $0 = N_{j_1} = PM_{j_1} = Pe_1 = P_1$, une contradiction. Ainsi $p_1 \leq j_1$. Comme N s'échelonne à M, on a aussi $j_1 \leq p_1$, et donc $p_1 = j_1$. En particulier,

$$P_1 = Pe_1 = PM_{j_1} = N_{j_1} = e_1.$$

Supposons que $1 \leq s < m$ et $P_j = e_j$, pour $j = 1, \ldots, s$. Si $j_{s+1} < p_{s+1}$, alors

$$N_{j_{s+1}} = \begin{pmatrix} b_{1,j_{s+1}} \\ \vdots \\ b_{s,j_{s+1}} \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Maintenant,

$$P_{s+1} = Pe_{s+1} = PM_{j_{s+1}} = N_{j_{s+1}} = \sum\nolimits_{i=1}^{s} b_{i,j_{s+1}} P_i,$$

ce qui contredit que P est inversible. Donc $p_{s+1} \leq j_{s+1}$, et par la symétrie, $j_{s+1} \leq p_{s+1}$, et donc $p_{s+1} = j_{s+1}$. Ainsi $P_{s+1} = Pe_{s+1} = PM_{j_{s+1}} = N_{j_{s+1}} = e_{s+1}$. Ceci montre que $P_i = e_i$, $i = 1, \ldots, m$. C'est-à-dire, $P = I_m$, et donc $M = N$. La preuve de la démonstration du lemme s'achève.

3.1.9. Théorème. Toute matrice sur K s'échelonne à une seule matrice échelonnée réduite.

Démonstration. Soit M une matrice de type $m \times n$ sur K. On peut supposer que $\mathrm{rg}(M) = r > 0$. Supposons que $N = (a_{ij})_{m \times n}$ est une forme échelonnée de M dont les pivots sont $a_{1,j_1}, a_{2,j_2}, \ldots, a_{r,j_r}$, où $1 \leq j_1 < j_2 < \cdots < j_r \leq m$. En effectuant les opérations $a_{i,j_i}^{-1} L_i, i = 1, \ldots, r$, on obtient une forme échelonnée N' de M dont tous les pivots sont 1. À partir du dernier pivot de N', on peut éliminer tous les termes au-dessus des pivots de N'. Ceci donne une forme échelonnée réduite de M.

Si N_1, N_2 sont deux formes échelonnées réduites de M, alors N_1 s'échelonne à N_2. D'après le lemme 3.1.8, $N_1 = N_2$. La preuve du théorème s'achève.

Dès maintenant, on se fixe E, F des K-espaces vectoriels.

3.1.10. Définition. (1) Une application $T : E \to F$ est dite *linéaire* si, pour tous $u, v \in E$ et $\alpha \in K$, on a $T(\alpha u) = \alpha T(u)$ et $T(u + v) = T(u) + T(v)$.

(2) Une application linéaire bijective s'appelle un *isomorphisme*.

Remarque. Si $T : E \to F$ est linéaire, alors $T(0_E) = 0_F$, et

$$T(\alpha_1 u_1 + \cdots + \alpha_n u_n) = \alpha_1 T(u_1) + \cdots + \alpha_n T(u_n),$$

pour tous $\alpha_1, \ldots, \alpha_n \in K$ et $u_1, \ldots, u_n \in E$.

Exemple. On voit aisément la projection suivante est linéaire:

$$p_x : \mathbb{R}^2 \to \mathbb{R}^2 : (x, y) \mapsto (x, 0).$$

3.1.11. Proposition. Soit $\{u_1, \ldots, u_n\}$ une base de E. Si $v_1, \ldots, v_n \in F$, alors il existe une seule application linéaire $T : E \to F$ telle que $T(u_i) = v_i$, $i = 1, \ldots, n$; et dans ce cas, T est injective si, et seulement si, $\{v_1, \ldots, v_n\}$ est libre.

Démonstration. Tout $u \in E$ s'écrit uniquement $u = \alpha_1 u_1 + \cdots + \alpha_n u_n$, $\alpha_i \in K$. Définissons une application

$$T : E \to F : \alpha_1 u_1 + \cdots + \alpha_n u_n \mapsto \alpha_1 v_1 + \cdots + \alpha_n v_n.$$

Il est facile que T est linéaire. Par définition, $T(u_i) = T(1 \cdot u_i) = 1 \cdot v_i = v_i$, pour $i = 1, \ldots, n$.

Supposons que $\{v_1, \ldots, v_n\}$ est libre. Si $u = \alpha_1 u_1 + \cdots + \alpha_n u_n$ et $v = \beta_1 u_1 + \cdots + \beta_n u_n \in E$ sont tels que $T(u) = T(v)$, alors

$$\alpha_1 v_1 + \cdots + \alpha_n v_n = \beta_1 v_1 + \cdots + \beta_n v_n.$$

Ceci donne $(\alpha_1 - \beta_1)v_1 + \cdots + (\alpha_n - \beta_n)v_n = 0_F$. Comme $\{v_1, \ldots, v_n\}$ est libre, $\alpha_i - \beta_i = 0$, $i = 1, \ldots, n$, et donc $u = v$. Ceci montre que T est injective.

Supposons maintenant que T est injective. Supposons que $\gamma_1 v_1 + \cdots + \gamma_n v_n = 0_F$, où $\gamma_1, \ldots, \gamma_n \in K$. Alors $T(\gamma_1 u_1 + \cdots + \gamma_n u_n) = 0_F = T(0_E)$. Comme T est injective, on a $\gamma_1 u_1 + \cdots + \gamma_n u_n = 0_E$. Comme $\{u_1, \ldots, u_n\}$ est libre, on a $\gamma_1 = \cdots = \gamma_n = 0_K$. La démonstration de la proposition s'achève.

Exemple. Considérons les espaces vectoriels réels $\mathbb{R}_3[x] = \{a + bx + cx^2 \mid a, b, c \in \mathbb{R}\}$ et $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$. Trouver une application linéaire $T : \mathbb{R}_3[x] \to {}_{\mathbb{R}}\mathbb{C}$ telle que

$$T(1 - x) = T(x + x^2) = 1 + i,\ T(1 - x^2) = 1 - i.$$

3.1.12. Proposition. Soit $T : E \to F$ une application linéaire. Soit E' un sous-espace vectoriel de E.

(1) L'ensemble $T(E') = \{T(u) \mid u \in E'\}$ est un sous-espace de F.

(2) Si $E' =< u_1, \ldots, u_r >$, alors $T(E') =< T(u_1), \ldots, T(u_r) >$.

Démonstration. (1) Si $v_1, v_2 \in T(E')$ et $\alpha_1, \alpha_2 \in K$, alors $v_i = T(u_i)$ avec $u_i \in E'$, $i = 1, 2$. Comme T est linéaire, $\alpha_1 v_1 + \alpha_2 v_2 = T(\alpha_1 u_1 + \alpha_2 u_2)$. Comme E' est un sous-espace de E, on a $\alpha_1 u_1 + \alpha_2 u_2 \in E'$. Ainsi, $\alpha_1 v_1 + \alpha_2 v_2 \in T(E')$. Cela montre que $\mathrm{Im}(T)$ est un sous-espace de F.

(2) Par définition, $\{T(u_1), \ldots, T(u_r)\} \subseteq T(E')$. Comme $T(E')$ est un sous-espace de F, on a $< T(u_1), \ldots, T(u_r) > \subseteq T(E')$. D'autre part, si $v \in T(E')$, alors $v = T(w)$ avec $w \in E'$. Or w s'écrit $w = \alpha_1 u_1 + \cdots + \alpha_r u_r, \alpha_i \in K$. Donc

$$v = T(w) = \alpha_1 T(u_1) + \cdots + \alpha_r T(u_r) \in < T(u_1), \ldots, T(u_r) > .$$

Ceci montre $T(E') \subseteq < T(u_1), \ldots, T(u_r) >$, et donc $T(E') = < T(u_1), \ldots, T(u_r) >$. La dḿonstration de la proposition s'achève.

Remarque. Si $T : E \to F$ est linéaire, alors $T(E)$ est un sous-espace de F, appelé *image* de T.

Exemple. Trouver l'image de l'application linéaire suivante:

$$T : \mathbb{R}^2 \to \mathbb{R}^3 : (x, y) \mapsto (x - y, 2x - 2y, 3x - 3y).$$

3.1.13. Proposition. Soient des entiers $m, n > 0$. Une application $T : K^m \to K^n$ est linéaire si et seulement s'il existe une matrice $M \in M_{m\times n}(K)$ telle que T est de la forme suivante:

$$T : K^m \to K^n : u \mapsto uM.$$

Dans ce cas, $\mathrm{Im}(T) = \mathscr{L}(M)$; et par conséquent, $\dim(\mathrm{Im}(T)) = \mathrm{rg}(M)$.

Démonstration. Considérons la base canonique de K^m suivante:

$$\{e_1 = (1, 0, \cdots, 0), e_2 = (0, 1, \cdots, 0), \ldots, e_m = (0, \cdots, 0, 1)\}.$$

D'abord, supposons que T est de la forme énoncée dans la proposition. Il est facile de voir que T est linéaire. En outre, $T(e_i) = e_i M$, ceci est la i-ième ligne de M d'après le lemme 3.1.4(2), pour $i = 1, \ldots, m$. D'après la proposition 3.1.12, on a

$$\mathrm{Im}(T) = < e_1 M, \ldots, e_m M > = \mathscr{L}(M).$$

Supposons maintenant que T est linéaire. Comme $w_i = T(e_i) \in K^n$, $i = 1, \ldots, m$,

$$M = \begin{pmatrix} w_1 \\ \vdots \\ w_m \end{pmatrix} \in M_{m\times n}(K).$$

Pour tout $u = (a_1, \cdots, a_m) \in K^m$, on a

$$T(u) = T(a_1 e_1 + \cdots + a_m e_m) = a_1 T(e_1) + \cdots + a_m T(e_m) = a_1 w_1 + \cdots + a_m w_m = uM.$$

Ceci achève la démonstration de la proposition.

Exemple. Trouver l'image de l'application linéaire suivante:

$$T : \mathbb{R}^3 \to \mathbb{R}^5 : (x, y, z) \mapsto (x, y, z) \begin{pmatrix} 1 & 1 & 0 & 1 & 2 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 2 & 1 & 1 & 3 \end{pmatrix}.$$

Démonstration. Par définition, T est définie par

$$M = \begin{pmatrix} 1 & 1 & 0 & 1 & 2 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 2 & 1 & 1 & 3 \end{pmatrix}.$$

D'après la proposition 3.1.13, on a

$$\mathrm{Im}(T) = \mathscr{L}(M) =< (1,1,0,1,2), (0,1,1,0,1), (1,2,1,1,3) >=< (1,1,0,1,2), (0,1,1,0,1) > .$$

3.1.14. Proposition. Soit $T : E \to F$ une application linéaire injective. Si $\{u_1, \ldots, u_n\}$ est une base de E, alors $\{T(u_1), \ldots, T(u_n)\}$ est une base de $\mathrm{Im}(T)$. Par conséquent, $\dim(\mathrm{Im}(T)) = \dim(E)$.

Démonstration. Comme T est injective, d'après la proposition 3.1.11, $\{T(u_1), \ldots, T(u_n)\}$ est libre. En outre, comme $E =< u_1, \ldots, u_n >$, on a $\mathrm{Im}(T) =< T(u_1), \ldots, T(u_n) >$, d'après la proposition 3.1.12(2). Ainsi, $\{T(u_1), \ldots, T(u_n)\}$ est une base de $\mathrm{Im}(T)$. La démonstration de la proposition s'achève.

Soit $n \geq 1$ un entier. Rappelons qu'une *n-permutation* est une bijection

$$\sigma : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\} : i \mapsto \sigma(i),$$

notée

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}.$$

3.1.15. Définition. Soit σ une n-permutation avec $n \geq 1$ un entier.
(1) Pour tout $u = (a_1, \cdots, a_n) \in K^n$, on pose $\sigma \cdot u = (a_{\sigma(1)}, \cdots, a_{\sigma(n)})$.
(2) Pour tout sous-ensemble $\mathcal{S}$ de K^n, on pose $\sigma \cdot \mathcal{S} = \{\sigma \cdot u \mid u \in \mathcal{S}\}$.
(3) Pour une matrice M sur K de lignes $L_1, \ldots, L_m$ et de colonnes $C_1, \ldots, C_n$, on définit

$$\sigma \cdot M = \begin{pmatrix} \sigma \cdot L_1 \\ \vdots \\ \sigma \cdot L_m \end{pmatrix} = (C_{\sigma(1)}, \ldots, C_{\sigma(n)}).$$

Remarque. (1) Si σ, τ sont des n-permutations alors, pour tout $u \in K^n$, on a

$$\tau \cdot (\sigma \cdot u) = (\tau\sigma) \cdot u.$$

(2) Si $M \in M_{m\times n}(K)$ est échelonnée réduite de rang m, alors il existe des n-permutations σ, τ telles que $M = \sigma \cdot (I_m \mid A) = \tau \cdot (B \mid I_m)$.

Exemple. Considérant la 5-permutation $\sigma = (23)$, on a

(1) $\sigma \cdot (0, 1, 0, 1, 0) = (0, 0, 1, 1, 0)$.

(2) $\sigma \cdot \{(0, 0, 0, 0, 0), (1, 2, 3, 0, 1), (0, 1, 1, 0, 1)\} = \{(0, 0, 0, 0, 0), (1, 3, 2, 0, 1), (0, 1, 1, 0, 1)\}$.

(3)

$$\sigma \cdot \begin{pmatrix} 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 2 & 3 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 1 & 3 & 2 & 4 & 1 \end{pmatrix}.$$

3.1.16. Lemme. Soit σ une n-permutation. Si $M \in M_{m\times n}(K)$, alors

(1) $\mathrm{rg}(M) = \mathrm{rg}(\sigma \cdot M)$;

(2) $\mathscr{L}(\sigma \cdot M) = \sigma \cdot \mathscr{L}(M)$.

Démonstration. (1) Écrivons $M = (C_1 \cdots C_n)$ en colonnes. Par définition, on a

$$\sigma \cdot M = (C_{\sigma(1)} \cdots C_{\sigma(n)}).$$

Comme $\{C_1, \ldots, C_n\} = \{C_{\sigma(1)}, \ldots C_{\sigma(n)}\}$, on a

$$\mathscr{C}(M) =< C_1, \ldots, C_n >=< C_{\sigma(1)}, \ldots C_{\sigma(n)} >= \mathscr{C}(\sigma \cdot M).$$

Par conséquent, $\mathrm{rg}(M) = \dim\mathscr{C}(M) = \dim\mathscr{C}(\sigma \cdot M) = \mathrm{rg}(\sigma \cdot M)$.

(2) Il est évident qu'on a une application linéaire

$$\sigma : K^n \to K^n : u \mapsto \sigma \cdot u.$$

Par définition, $\sigma \cdot \mathscr{L}(M) = \sigma(\mathscr{L}(M))$. Soient $M_1, \ldots, M_n$ les lignes de M. Alors $\sigma \cdot M_1, \ldots, \sigma \cdot M_m$ sont les lignes de $\sigma \cdot M$. Comme $\mathscr{L}(M) =< M_1, \ldots, M_n >$, d'après la proposition 3.1.12, $\sigma(\mathscr{L}(M)) =< \sigma \cdot M_1, \ldots, \sigma \cdot M_m >= \mathscr{L}(\sigma \cdot M)$. Ceci nous donne $\sigma \cdot \mathscr{L}(M) = \mathscr{L}(\sigma \cdot M)$. La preuve du lemme s'achève.

Exemple. Considérons la matrice sur $\mathbb{Z}_2$ suivante:

$$M = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

avec $\mathscr{L}(M) = \{(0,0,0,0,0), (1,1,0,1,0), (0,0,1,0,1), (1,1,1,1,1)\}$. Si $\sigma = (23)$, alors

$$\sigma \cdot M = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

avec

$$\mathscr{L}(\sigma \cdot M) = \{(0,0,0,0,0), (1,0,1,1,0), (0,1,0,0,1), (1,1,1,1,1)\}.$$

En particulier, $\mathscr{L}(M) \neq \mathscr{L}(\sigma \cdot M)$.

3.1.17. Lemme. Si $M \in M_{m\times n}(K)$ est échelonnée réduite de rang m, alors il existe des n-permutations σ et τ telles que

$$\sigma \cdot M = (I_m \mid A) \text{ et } \tau \cdot M = (B \mid I_m).$$

Démonstation. Écrivons $M = (M_1\, M_2 \cdots M_n)$ en colonnes. Posons $M = (a_{ij})_{m\times n}$, où les pivots sont $a_{1,j_1}, a_{2,j_2}, \ldots, a_{m,j_m}$ avec $j_1 < j_2 < \cdots < j_m$. Comme M est échelonnée réduite, $M_{j_i} = e_i$, la i-ième colonne de I_m. Posons $\{1,\ldots,n\}\backslash\{j_1,\ldots,j_m\} = \{j_{m+1},\ldots,j_n\}$ avec $j_{m+1} < \cdots < j_n$. Posant

$$\sigma = \begin{pmatrix} 1 & \cdots & m & m+1 & \cdots & n \\ j_1 & \cdots & j_m & j_{m+1} & \cdots & j_n \end{pmatrix} \text{ et } \sigma = \begin{pmatrix} 1 & \cdots & n-m & n-m+1 & \cdots & n \\ j_{m+1} & \cdots & j_n & j_1 & \cdots & j_m \end{pmatrix},$$

on voit que $\sigma \cdot M = (I_m \mid A)$ et $\tau \cdot M = (B \mid I_m)$. La preuve s'achève.

Exemple. Considérons la matrice échelonnée réduite

$$A = \begin{pmatrix} 1 & 2 & 0 & 6 & 0 & 1 & 0 \\ 0 & 0 & 1 & 3 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 1 & 5 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Trouver deux 7-permutations σ et τ telles que $\sigma \cdot A = (I_5 \mid B)$ et $\tau \cdot A = (C \mid I_5)$.

Étant donnée $M \in M_{m\times n}(K)$, on pose $\mathscr{N}^T(M) = \{u \in K^n \mid Mu^T = 0\}$.

3.1.18. Lemme. Soit M une matrice de type $m \times n$ sur K.

(1) Si M s'échelonne à L, alors $\mathscr{N}^T(M) = \mathscr{N}^T(L)$.

(2) Si σ est une n-permutation, alors $\mathscr{N}^T(\sigma \cdot M) = \sigma \cdot \mathscr{N}^T(M)$.

(3) Si N est une matrice de n colonnes, alors $\mathscr{L}(N) \subseteq \mathscr{N}^T(M)$ si et seulement si $MN^T = 0$.

Démonstration. (1) Supposons que M s'échelonnant à N. Alors, le système homogène $MX = 0$ est équivalent au système homogène $LX = 0$. D'où, $\mathscr{N}(M) = \mathscr{N}(L)$. Par conséquent, $\mathscr{N}^T(M) = \mathscr{N}^T(L)$.

(2) Soit σ une n-permutation. Si $u = (a_1, \cdots, a_n), v = (b_1, \ldots, b_n) \in K^n$, alors

$$uv^T = \sum\nolimits_{i=1}^{n} a_i b_i = \sum\nolimits_{i=1}^{n} a_{\sigma(i)} b_{\sigma(i)} = (\sigma \cdot u)(\sigma \cdot v)^T.$$

Posons $M_1, \ldots, M_m$ les lignes de M. Alors, $\sigma \cdot M_1, \ldots, \sigma \cdot M_m$ sont les lignes de $\sigma \cdot M$. Pour tout $u \in K^n$, en vue de l'équation ci-dessus, on a

$$\begin{aligned}
u \in \mathscr{N}^T(\sigma \cdot M) &\Leftrightarrow (\sigma \cdot M)u^T = 0 \\
&\Leftrightarrow (\sigma \cdot M_i)\,(\sigma \cdot (\sigma^{-1} \cdot u))^T = 0,\ i = 1, \ldots, m \\
&\Leftrightarrow M_i\,(\sigma^{-1} \cdot u)^T = 0,\ i = 1, \ldots, m \\
&\Leftrightarrow M\,(\sigma^{-1} \cdot u)^T = 0 \\
&\Leftrightarrow \sigma^{-1} \cdot u \in \mathscr{N}^T(M) \\
&\Leftrightarrow u \in \sigma \cdot \mathscr{N}^T(M).
\end{aligned}$$

Ceci donne $\mathscr{N}^T(\sigma \cdot M) = \sigma \cdot \mathscr{N}^T(M)$.

(3) Supposons que les lignes de N sont $N_1, \ldots, N_p$. D'après le lemme 3.1.4(1), on a

$$MN^T = M(N_1^T \cdots N_p^T) = (MN_1^T \cdots MN_p^T).$$

Comme $\mathscr{L}(N) =< N_1, \ldots, N_p >$, on voit que $\mathscr{L}(N) \subseteq \mathscr{N}^T(M)$ si et seulement si $N_j \in \mathscr{N}^T(M),\ j = 1, \ldots, p$, si et seulement si $MN_j^T = 0,\ j = 1, \ldots, p$, si et seulement si $(MN_1^T \cdots MN_p^T) = 0$ si et seulement si $MN^T = 0$. La preuve du lemme s'achève.

3.2 Codes correcteurs

Partout dans cette section, considérons le corps $\mathbb{Z}_2 = \{0, 1\}$, dont les éléments s'appellent *bits*. Rappelons que l'addition et la multiplication sont données par les tableaux suivants :

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Un *mot binaire*, ou simplement *mot*, de longueur n est une suite de n bits $b_1 \cdots b_n$, qui peut être considéré comme un vecteur du $\mathbb{Z}_2$-espace vectoriel $\mathbb{Z}_2^n$. On désignera par $\mathbb{Z}_2^*$ l'ensemble des mots binaires.

3.2.1. Définition. La *concaténation* de mots binaires

$$\cdot : \quad \mathbb{Z}_2^* \times \mathbb{Z}_2^* \to \mathbb{Z}_2^* : (\mathbf{x}, \mathbf{y}) \mapsto \mathbf{x} \cdot \mathbf{y}$$

est définie de la façon que si $\mathbf{x} = x_1 \cdots x_r$ et $\mathbf{y} = y_1 \cdots y_s$, alors

$$\mathbf{x} \cdot \mathbf{y} = x_1 \cdots x_r y_1 \cdots y_s.$$

3.2.2. Définition. Soit un entier $n \geq 2$. Un *code binaire*, ou simplement *code*, de longueur n est un ensemble non-vide de mots binaires de longueur n, c'est-à-dire, un sous-ensemble non vide de $\mathbb{Z}_2^n$.

Remarque. Un code binaire est dit *trivial* s'il ne contient qu'un mot.

Exemple. (1) $\mathcal{C}_1 = \{000000, 010101, 101010, 111111\}$ est un code de longueur 6.
(2) $\mathcal{C}_2 = \{00000, 01101, 10110, 11011\}$ est un code de longueur 5.

Dans le transport d'information, on représente premièrement l'information par une succession de mots binaires d'une longueur fixe, et ensuite, on l'envoie mot par mot. Malheureusement, les canaux de transmission souvent subissent des interférences, appelé *bruit*. On doit prendre certaines précautions afin de détecter, ou mieux, corriger des erreurs dues au bruit. Cela sera fait par un codeur défini comme ci-dessous.

3.2.3. Définition. Soient k, n des entiers avec $n > k > 0$. Un (n, k)-*codeur binaire*, ou simplement *codeur*, est une application injective

$$\varphi : \mathbb{Z}_2^k \to \mathbb{Z}_2^n : \mathbf{x} \mapsto \mathbf{x} \cdot \mathbf{r}_\mathbf{x}.$$

On appelle $\mathbf{x}$ *mot d'information*; et $\mathbf{r}_\mathbf{x}$, *mot de redondance*. En outre, $\mathrm{Im}(\varphi)$ s'appelle le *code* défini par φ.

Exemple. (1) *Codeur de répétition.* En répétant deux fois chaque mot de $\mathbb{Z}_2^2$, on obtient un codeur comme suit:

$$\begin{array}{rccc} \varphi_1 : & \mathbb{Z}_2^2 & \to & \mathbb{Z}_2^6 : \\ & 00 & \mapsto & 000000 \\ & 01 & \mapsto & 010101 \\ & 10 & \mapsto & 101010 \\ & 11 & \mapsto & 111111 \end{array}$$

Le code défini par ce codeur est $\mathcal{C}_1 = \{000000, 010101, 101010, 111111\}$.

(2) *Codeur de somme de contrôle.* En ajoutant la somme des bits de chacun des mots de $\mathbb{Z}_2^2$, on obtient un codeur comme suit:

$$\begin{array}{rccc} \varphi : & \mathbb{Z}_2^2 & \to & \mathbb{Z}_2^3 : \\ & 00 & \mapsto & 000 \\ & 01 & \mapsto & 011 \\ & 10 & \mapsto & 101 \\ & 11 & \mapsto & 110 \end{array}$$

Le code défini par ce codeur est $\{000, 011, 101, 110\}$.

(3) Pour chaque mot de $\mathbb{Z}_2^2$, en ajoutant premièrement la somme des bits et ensuite répétant une fois le mot original, on obtient un codeur comme suit:

$$\begin{array}{rccc} \varphi_2: & \mathbb{Z}_2^2 & \to & \mathbb{Z}_2^5: \\ & 00 & \mapsto & 00000 \\ & 01 & \mapsto & 01101 \\ & 10 & \mapsto & 10110 \\ & 11 & \mapsto & 11011 \end{array}$$

Le code défini par ce codeur est $\mathcal{C}_2 = \{00000, 01101, 10110, 11011\}$.

Dès qu'un mot est arrivé au destinataire, il sera traîté par le décodeur. On discutera comment le dćodeur détectera, ou mieux, corrigera des erreurs dues au bruit.

3.2.4. Définition. Étant donnés deux mots $\mathbf{x} = x_1 \cdots x_n$ et $\mathbf{y} = y_1 \cdots y_n$ de longueur n, la *distance* entre $\mathbf{x}$ et $\mathbf{y}$ est définie par

$$d(\mathbf{x}, \mathbf{y}) = |\{i \mid 1 \leq i \leq n; x_i \neq y_i\}|.$$

3.2.5. Lemme. Soient $\mathbf{x}, \mathbf{y}, \mathbf{z}$ des mots de même longueur.

(1) $d(\mathbf{x}, \mathbf{y}) = 0$ si et seulement si $\mathbf{x} = \mathbf{y}$.

(2) $d(\mathbf{x}, \mathbf{y}) = d(\mathbf{y}, \mathbf{x})$.

(3) $d(\mathbf{x}, \mathbf{y}) \leq d(\mathbf{x}, \mathbf{z}) + d(\mathbf{z}, \mathbf{y})$.

Démonstratin. Les premiers deux énoncés sont évidents. Pour montrer l'énoncé (3), posons $\mathbf{x} = x_1 \cdots x_n$, $\mathbf{y} = y_1 \cdots y_n$ et $\mathbf{z} = z_1 \cdots z_n$. Considérons $\Sigma = \{i \mid 1 \leq i \leq n;\ x_i \neq y_i\}$, $\Sigma_1 = \{i \mid 1 \leq i \leq n;\ x_i \neq z_i\}$, et $\Sigma_2 = \{i \mid 1 \leq i \leq n;\ z_i \neq y_i\}$. Il est évident que $\Sigma \subseteq \Sigma_1 \cup \Sigma_2$. Ceci donne

$$d(\mathbf{x}, \mathbf{y}) = |\Sigma| \leq |\Sigma_1 \cup \Sigma_2| \leq |\Sigma_1| + |\Sigma_2| = d(\mathbf{x}, \mathbf{z}) + d(\mathbf{z}, \mathbf{y}).$$

La preuve du lemme s'achève.

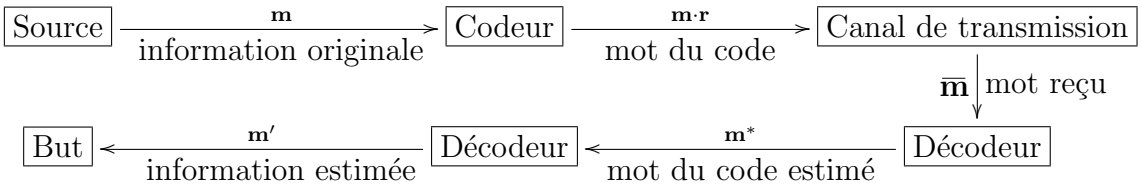
3.2.6. Règle de codes correcteurs. Soit un codeur $\varphi : \mathbb{Z}_2^k \to \mathbb{Z}_2^n$. Soit $\mathbf{m} \in \mathbb{Z}_2^k$ un mot à transmettre.

(1) Le mot expédié dans le canal de transmission est $\varphi(\mathbf{m}) = \mathbf{m} \cdot \mathbf{r}$.

(2) Si le décodeur reçoit un mot $\overline{\mathbf{m}}$, il cherche $\mathbf{m}^* \in \mathrm{Im}(\varphi)$ avec $d(\overline{\mathbf{m}}, \mathbf{m}^*)$ minimal.

(3) L'estimé de $\mathbf{m}$ par le décodeur sera le mot $\mathbf{m}'$ formé des k premiers bits de $\mathbf{m}^*$.

Voici une schéma du transport de l'information par un code correcteur:



Exemple. Considérons le codeur de répétition $\varphi_1 : \mathbb{Z}_2^2 \to \mathbb{Z}_2^6$, qui définit le code

$$\mathcal{C}_1 = \{000000, 010101, 101010, 111111\}.$$

On veut transmettre l'information 00. Le mot expédié dans le canal de transmission est 000000.

(1) Supposons que le décodeur reçoit $000000 \in \mathcal{C}_1$. Éviemment, parmi les mots de $\mathcal{C}_1$, le mot 00000 est le plus près de 000000, ce qui est l'estimé du mot du code par le décodeur. Par conséquent, l'estimé de l'information originale par le décodeur est 00. C'est correcte.

(2) Supposons que le mot reçu est $001000 \notin \mathcal{C}_1$. Parmi les mots de $\mathcal{C}_1$, le mot 000000 est le plus près de 001000, ce qui est l'estimé du mot du code par le décodeur. Par conséquent, l'estimé de l'information originale par le décodeur sera 00. C'est correcte.

(3) Supposons que le mot reçu est $010100 \notin \mathcal{C}_1$. Parmi les mots de $\mathcal{C}_1$, le mot 010101 est le plus près de 010100, ce qui est l'estimé du mot du code par le décodeur. Par conséquent, l'estimé de l'information originale par le décodeur sera 01. Et c'est faux.

On a vu que le code $\mathcal{C}_1$ est incapable de corriger 2 erreurs. On étudiera la capacité correctrice d'un code. Pour ce faire, on introduira la notion suivante.

3.2.7. Définition. Soit $\mathbf{x}$ un mot binaire de longueur n. Si $\varepsilon \in \mathbb{R}^+$, alors

$$B(\mathbf{x}, \varepsilon) = \{\mathbf{y} \in \mathbb{Z}_2^n \mid d(\mathbf{x}, \mathbf{y}) \leq \varepsilon\}$$

s'appelle *boule de Hamming* de centre $\mathbf{x}$ et de rayon ε.

Remarque. On voit que $\mathbf{y} \in \mathbf{B}(\mathbf{x}, \varepsilon)$ si et seulement si $\mathbf{x} \in \mathbf{B}(\mathbf{y}, \varepsilon)$.

Exemple. Pour tout mot binaire $\mathbf{x}$, on voit que $B(\mathbf{x}, \mathbf{0}) = \{\mathbf{x}\}$.

3.2.8. Définition. Soit $\mathcal{C}$ un code de longueur n. Soit un entier $t \geq 0$. On dit que $\mathcal{C}$ est *capable de corriger t erreurs* si $|\mathcal{C} \cap B(\mathbf{x}, t)| \leq 1$, pour tout $\mathbf{x} \in \mathbb{Z}_2^n$. Dans ce cas, si $\mathbf{x}_0 \in \mathcal{C}$ est expédié dans le canal de transmission et le décodeur reçoit un mot $\mathbf{x}$ avec $d(\mathbf{x}_0, \mathbf{x}) \leq t$, alors l'estimé de $\mathbf{x}_0$ par le décodeur sera bien $\mathbf{x}_0$.

Remarque. (1) Tout code est capable de corriger 0 erreur.

(2) Si $\mathcal{C}$ est capable de corriger t erreurs, alors il est capable de corriger s erreurs, pour tout $0 \leq s \leq t$.

Exemple. Considérons le code $\mathcal{C}_1 = \{000000, 010101, 101010, 111111\}$. On voit que $\mathcal{C}_1$ est incapable de corriger 2 erreurs.

3.2.9. Proposition. Un code $\mathcal{C}$ de longueur n est capable de corriger t erreurs si et seulement si les boules $B(\mathbf{x}, t)$ de $\mathbb{Z}_2^n$, avec $\mathbf{x} \in \mathcal{C}$, sont deux à deux disjointes.

Démonstration. Supposons que les boules $B(\mathbf{x}, t)$ avec $\mathbf{x} \in \mathcal{C}$ sont deux à deux disjointes. Soit $\mathbf{y} \in \mathbb{Z}_2^n$. Si $\mathbf{x}_1, \mathbf{x}_2 \in \mathcal{C} \cap B(\mathbf{y}, \mathbf{t})$, alors $\mathbf{y} \in B(t, \mathbf{x}_1) \cap B(t, \mathbf{x}_2)$. Par hypothèse, $\mathbf{x}_1 = \mathbf{x}_2$. Ainsi $\mathcal{C}$ est capable de corriger t erreurs.

Supposons qu'il existe deux mots distincts $\mathbf{x}_1, \mathbf{x}_2$ de $\mathcal{C}$ tels que $B(t, \mathbf{x}_1) \cap B(t, \mathbf{x}_2)$ contient un mot $\mathbf{y}$. Alors $\mathbf{x_1}, \mathbf{x_2} \in \mathcal{C} \cap \mathbf{B}(\mathbf{y}, \mathbf{t})$. Ainsi $\mathcal{C}$ est incapable de corriger t erreurs. Ceci achève la démonstration de la proposition.

3.2.10. Définition. La *capacité correctrice* d'un code $\mathcal{C}$ est définie par

$$\delta(\mathcal{C}) = \sup\{t \in \mathbb{N} \mid \mathcal{C} \text{ est capable de corriger } t \text{ erreurs}\}.$$

Remarque. Plus la capacité correctrice est grande, plus le code est fiable.

La notion suivante sera utile pour calculer la capacité correctrice d'un code.

3.2.11. Définition. Soit $\mathcal{C}$ un code non trivial. La *distance minimum* de $\mathcal{C}$ est définie par

$$d(\mathcal{C}) = \min\{d(\mathbf{x}, \mathbf{y}) > 0 \mid \mathbf{x}, \mathbf{y} \in \mathcal{C}\}.$$

Remarque. (1) Si $\mathcal{C}$ est non trivial de longueur n, alors $1 \leq d(\mathcal{C}) \leq n$.

(2) Plus $d(\mathcal{C})$ est grand, plus les mots de $\mathcal{C}$ sont éloingnés les uns des autres.

Exemple. (1) Si $\mathcal{C} = \mathbb{Z}_2^n$, alors $d(\mathcal{C}) = 1$.

(2) On a $d(\mathcal{C}_1) = d(\mathcal{C}_2) = 3$, où

$$\mathcal{C}_1 = \{000000, 010101, 101010, 111111\};\ \mathcal{C}_2 = \{00000, 01101, 10110, 11011\}.$$

3.2.12. Théorème. Soit $\mathcal{C}$ un code de longueur n. Si $\mathcal{C}$ est trivial, alors $\delta(\mathcal{C}) = \infty$; et sinon,

$$\delta(\mathcal{C}) = \left[\frac{d(\mathcal{C}) - 1}{2}\right].$$

Démonstration. D'abord, supposons que $\mathcal{C}$ est trivial. Pour tous $t \geq 0$ et $\mathbf{x} \in \mathbb{Z}_2^n$, on a $|\mathcal{C} \cap B(\mathbf{x}, t)| \leq |\mathcal{C}| = 1$. C'est-à-dire, $\mathcal{C}$ est capable de corriger t erreurs. D'où, $\delta(\mathcal{C}) = \infty$.

Supposons que $\mathcal{C}$ est non trivial. Écrivons $d = d(\mathcal{C})$ et $s = [\frac{d(\mathcal{C})-1}{2}]$. Alors

$$\left[\frac{d}{2}\right] = \left[\frac{d-1}{2} + \frac{1}{2}\right] \leq \left[\frac{d-1}{2} + 1\right] = \left[\frac{d-1}{2}\right] + 1 = s + 1.$$

Maintenant, on prétend que

$$d - \left[\frac{d}{2}\right] = s + 1.$$

En effet, si $d = 2m$, alors $s = \left[m - \frac{1}{2}\right] = m - 1$, et donc $d - \left[\frac{d}{2}\right] = m = s + 1$. Si $d = 2m + 1$, alors $s = m$. Donc,

$$d - \left[\frac{d}{2}\right] = 2m + 1 - m = m + 1 = s + 1.$$

Or, par définition, $d = d(\mathbf{x}, \mathbf{y})$, pour certains $\mathbf{x}, \mathbf{y} \in \mathcal{C}$. Écrivons $\mathbf{x} = x_1 \cdots x_n$ et $\mathbf{y} = y_1 \cdots y_n$. Il existe des indices $i_1, \ldots, i_d$ tels que $x_i \neq y_i$ si et seulement si $i \in \{i_1, \ldots, i_d\}$, pour tout $1 \leq i \leq n$. Posons $\mathbf{z} = z_1, \ldots, z_n$, où $z_i = x_i$ pour tout $i \notin \{i_1, \ldots, i_d\}$; et

$$z_{i_j} = \begin{cases} x_{i_j},\ 1 \leq j \leq [\frac{d}{2}]; \\ y_{i_j},\ [\frac{d}{2}] < j \leq d. \end{cases}$$

Alors $d(\mathbf{z}, \mathbf{y}) \leq [\frac{d}{2}] \leq s + 1$ et $d(\mathbf{z}, \mathbf{x}) \leq d - [\frac{d}{2}] = s + 1$. C'est-à-dire, $\mathbf{z} \in B(\mathbf{x}, s + 1)$ et $\mathbf{z} \in B(\mathbf{y}, s + 1)$. D'après la proposition 3.2.9, $\mathcal{C}$ est incapable de corriger $s + 1$ erreurs.

Supposons que $\mathcal{C}$ est incapable de corriger s erreurs. D'après la proposition 3.2.9, il existe deux mots distincts $\mathbf{m}_1, \mathbf{m}_2$ de $\mathcal{C}$ tels que l'intersection de $B(\mathbf{m}_1, s)$ et $B(\mathbf{m}_2, s)$ contient au moins un mot $\mathbf{m}$. Or

$$0 < d(\mathbf{m}_1, \mathbf{m}_2) \leq d(\mathbf{m}_1, \mathbf{m}) + d(\mathbf{m}_2, \mathbf{m}) \leq 2s \leq d(\mathcal{C}) - 1 < d(\mathcal{C}),$$

une contradiction. Donc $\mathcal{C}$ est capable de corriger s erreurs. Par définition, $\delta(\mathcal{C}) = s$. La preuve du théorème s'achève.

Remarque. Soit $\mathcal{C}$ un code. Plus $d(\mathcal{C})$ est grande, plus $\delta(\mathcal{C})$ est grande, et plus $\mathcal{C}$ est fiable.

Appliquant le théorème 3.2.12, on obtient immédiatement le résulat suivant.

3.2.13. Corollaire. Soit $\mathcal{C}$ un code non trivial de longueur n. Si $\mathcal{C}$ est capable de corriger t erreurs, alors $2t \leq d(\mathcal{C}) - 1 < n$.

La cardinalité d'un code s'appelle *capacité expressive*. Plus la capacité expressive est grande, plus le code est capable d'exprimer. En vertu du théorème 3.2.12, pour qu'un code

soit fiable, il faut que ses mots soient éloingnés les uns des autres. Mais cela a un prix: pour une longueur donnée (souvent 16, 32 ou 64 bits), plus les mots du code sont éloingnés les uns des autres, plus la capacité expressive est petite.

3.2.14. Proposition. Soit $\mathcal{C}$ un code non trivial de longueur n. Si δ est la capacité correctrice de $\mathcal{C}$, alors $|\mathcal{C}| \leq 2^{n-2\delta}$.

Démonstration. D'après le théorème 3.2.12, $2\,\delta \leq d(\mathcal{C})-1$. Posant $m = n-(d(\mathcal{C})-1)$, on obtient $m \leq n-2\,\delta$. Pour tout $\mathbf{x} \in \mathcal{C}$, posons $\mathbf{x}'$ le mot formé des premiers m bits de $\mathbf{x}$. Si $\mathbf{x}, \mathbf{y} \in \mathcal{C}$ sont tels que $\mathbf{x}' = \mathbf{y}'$, alors $d(\mathbf{x}, \mathbf{y}) \leq n-m = d(\mathcal{C})-1 < d(\mathcal{C})$. D'après la minimalité de $d(\mathcal{C})$, on voit que $d(\mathbf{x}, \mathbf{y}) = 0$, c'est-à-dire, $\mathbf{x} = \mathbf{y}$. Ceci montre que l'application

$$\varphi : \mathcal{C} \to \mathbb{Z}_2^m : \mathbf{x} \mapsto \mathbf{x}'$$

est injective. Par conséquent, $|\mathcal{C}| \leq |\mathbb{Z}_2^m| = 2^m \leq 2^{n-2\delta}$. Cela s'achève la démonstration de la proposition.

3.3 Codes linéaires

Dans l'industrie, on utilise souvent les codes linéaires dont la détection d'erreurs est la plus simple.

3.3.1. Définition. Un code $\mathcal{C}$ de longueur n est dit *linéaire* si $\mathcal{C}$ est un sous-espace vectoriel de $\mathbb{Z}_2^n$.

Le résultat suivant sera pratique.

3.3.2. Lemme. Un code binaire $\mathcal{C}$ est linéaire si, et seulement si, les deux conditions suivantes sont vérifiées:

(1) $\mathbf{0} \in \mathcal{C}$.

(2) Si $\mathbf{x}, \mathbf{y} \in \mathcal{C}$ sont distincts et tous non nuls, alors $\mathbf{x}+\mathbf{y} \in \mathcal{C}$.

Démonstration. La nécessité est évidente. Supposons que les conditions sont vérifiées. Soient $\mathbf{x}, \mathbf{y} \in \mathcal{C}$. Pour tout $\lambda \in \mathbb{Z}_2 = \{0, 1\}$, on voit que $\lambda\mathbf{x} = \mathbf{0}$ ou $\lambda\mathbf{x} = \mathbf{x}$. D'où, $\lambda\mathbf{x} \in \mathcal{C}$. En plus, si $\mathbf{x} = \mathbf{y}$, alors $\mathbf{x}+\mathbf{y} = \mathbf{0} \in \mathcal{C}$. Supposons que $\mathbf{x} \neq \mathbf{y}$. Si $\mathbf{x} = \mathbf{0}$ ou $\mathbf{y} = \mathbf{0}$, alors $\mathbf{x}+\mathbf{y} = \mathbf{x}$ ou $\mathbf{y}$, et donc $\mathbf{x}+\mathbf{y} \in \mathcal{C}$. Si $\mathbf{x}, \mathbf{y}$ sont tous non nuls, d'après l'énoncé (2), $\mathbf{x}+\mathbf{y} \in \mathcal{C}$. Ceci achève la démonstration du lemme.

Exemple. Le code $\mathcal{C} = \{00000, 11001, 11100, 00101\}$ est linéaire.

On verra qu'un code linéaire est uniquement déterminé par sa dimension. En bref, un code linéaire de longueur n et de dimension k s'appelle un (n, k)-*code linéaire*. Si $0 < k < n$, on dit alors que $\mathcal{C}$ est *propre*.

3.3.3. Proposition. Si $\mathcal{C}$ est un (n,k)-code linéaire avec $0 < k \leq n$, alors $\mathcal{C} = \mathscr{L}(G)$ avec $G \in M_{k\times n}(\mathbb{Z}_2)$ de rang k. Dans ce cas, G s'appelle *matrice génératrice* de $\mathcal{C}$.

Démonstration. Supposons que $\mathcal{C}$ est un sous-espace de $\mathbb{Z}_2^n$ de dimension $k > 0$. Alors $\mathcal{C}$ admet une base $\{u_1, \ldots, u_k\}$. En particulier, $\mathcal{C} = \mathscr{L}(M)$, où M est la matrice dont les lignes sont $u_1, \ldots, u_k$. Comme les lignes de M sont linéairement indépendantes, $\mathrm{rg}(M) = k$. La preuve de la proposition s'achève.

3.3.4. Lemme. Soit $\mathcal{C}$ un code linéaire non trivial. Si G est une matrice binaire, alors les conditions suivantes sont équivalentes.

(1) G est une matrice génératrice de $\mathcal{C}$.

(2) $\mathcal{C} = \mathscr{L}(G)$ et les lignes de G sont linéairement indépendantes.

(3) Les lignes de G forment une base de $\mathcal{C}$.

(4) G s'échelonne à une matrice génératrice de $\mathcal{C}$.

Démonstration. Supposons que G est de type $k \times n$ dont les lignes sont $G_1, \ldots, G_k$.

Supposons que (1) est valide. C'est-à-dire, $\mathcal{C} = \mathscr{L}(G)$, et G est de rang k. D'après le théorème 3.1.2(3), $G_1, \ldots, G_k$ sont linéairement indépendantes.

Supposons que (2) est valide. C'est-à-dire, $\mathcal{C} =< G_1, \ldots, G_k >$, et $G_1, \ldots, G_k$ sont linéairement indépendantes. Ainsi, $\{G_1, \ldots, G_k\}$ est une base de $\mathcal{C}$.

Supposons que (3) est valide. C'est-à-dire, $\{G_1, \ldots, G_k\}$ est une base de $\mathcal{C}$. En particulier, $\mathcal{C} = \mathscr{L}(G) =< G_1, \ldots, G_k >= \mathscr{L}(G)$ est un (n,k)-code linéiare. Comme $\{G_1, \ldots, G_k\}$ est libre, d'après le théorème 3.1.2(3), G est de rang k. Ainsi, G est une matrice génératrice de $\mathcal{C}$. En particulier, G s'échelonne à une matrice génératrice de $\mathcal{C}$.

Supposons enfin que G s'échelonne à une matrice génératrice G' de $\mathcal{C}$. En particulier, $\mathcal{C} = \mathscr{L}(G')$ et G' est de type $k \times n$ et de rang k. D'après le théorème 3.1.5, $\mathcal{C} = \mathscr{L}(G') = \mathscr{L}(G)$ et $\mathrm{rg}(G) = \mathrm{rg}(G') = k$. Donc, G est aussi une matrice génératrice de $\mathcal{C}$. La preuve du lemme s'achève.

Exemple. Trouver une matrice de génératrice du code linéaire

$$\mathcal{C} = \{00000, 11001, 11100, 00101\}.$$

Le résultat suivant nous dit comment trouver tous les mots d'un code linéaire en utilisant une matrice génératrice.

3.3.5. Théorème. Soit $\mathcal{C}$ un (n,k)-code linéaire non trivial, dont G est une matrice génératrice. Si M est une matrice de type $2^k \times k$ formée de tous éléments de $\mathbb{Z}_2^k$, alors les lignes de MG sont deux à deux distinctes et forment l'ensemble des mots de $\mathcal{C}$. En particulier, la capacité expressive de $\mathcal{C}$ est égale à 2^k.

Démonstration. Les éléments de $\mathbb{Z}_2^k$ s'écrivent $u_i = (a_{i1}, \ldots, a_{ik})$, avec $a_{ij} \in \mathbb{Z}_2$, $i = 1, \ldots, 2^k$. Posons

$$M = \begin{pmatrix} u_1 \\ \vdots \\ u_{2^k} \end{pmatrix} \in M_{2^k \times k}(\mathbb{Z}_2).$$

Alors

$$MG = \begin{pmatrix} u_1 G \\ \vdots \\ u_{2^k} G \end{pmatrix}.$$

D'après le lemme 3.3.4,

$$G = \begin{pmatrix} G_1 \\ \vdots \\ G_k \end{pmatrix},$$

où $G_1, \ldots, G_k$ forment une base de $\mathcal{C}$. Pour tout $1 \leq i \leq 2^k$, d'après le lemme 3.1.3(2), on a

$$u_i G = (a_{i1}, \ldots, a_{ik})G = a_{i1}G_1 + \cdots + a_{ik}G_k \in \mathcal{C}.$$

Comme $\{G_1, \ldots, G_k\}$ est libre, les $u_i G$ avec $1 \leq i \leq 2^k$ sont deux à deux distincts. En outre, pour tout $u \in \mathcal{C}$, il existe $a_1, \ldots, a_k \in \mathbb{Z}_2$ tels que

$$u = a_1 G_1 + \cdots + a_k G_k = (a_1, \ldots, a_k)G.$$

Or $(a_1, \ldots, a_k) = u_j$, pur un unique indice j avec $1 \leq j \leq k$. Cela dit que u est la j-ième ligne de MG. La preuve du théorème s'achève.

Exemple. Trouver les mots du code $\mathcal{C}$ ayant pour matrice génératrice

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

3.3.6. Théorème. Tout code linéaire non trivial admet une seule matrice génératrice qui est échelonnée réduite, appelée *matrice génératrice canonique.*

Démonstration. Soit $\mathcal{C}$ un (n, k)-code linéaire avec $0 < k \leq n$, dont G est une matrice génératrice. Alors $\mathcal{C} = \mathscr{L}(G)$ avec G de type $k \times n$ et de rang k. D'après le théorème 3.1.9, G s'échelonne à une matrice échelonnée réduite M. D'après la proposition 3.1.5(1), $\mathcal{C} = \mathscr{L}(M)$. Étant de type $k \times n$ et de rang k, la matrice M est une matrice génératrice de $\mathcal{C}$.

Supposons que N est aussi une matrice génératrice de $\mathcal{C}$ qui est échelonnée réduite. En particulier, $\mathscr{L}(N) = \mathcal{C} = \mathscr{L}(M)$. En vertu de la proposition 3.1.6, M s'échelonne à N, et d'après le lemme 3.1.8, $M = N$. La preuve du théorème s'achève.

Exemple. Trouver la matrice génératrice canonique du code linéaire

$$\mathcal{C} = \{00000, 11001, 11100, 00101\}.$$

3.3.7. Définition. Un (n, k)-code linéaire non trivial s'appelle un (n, k)-*code standard* si sa matrice génératrice canonique est échelonnée normée.

Exemple. Vérifier que $\mathcal{C} = \{000, 101, 011, 110\}$ est un code standard.

Deux codes $\mathcal{C}, \mathcal{D}$ de longueur n sont dits *équivalents* s'il existe une n-permutation σ telle que $\mathcal{D} = \sigma \cdot \mathcal{C}$.

3.3.8. Lemme. Soient $\mathcal{C}, \mathcal{D}$ deux codes linéaires non triviaux de longueur n. Si $\mathcal{D} = \sigma \cdot \mathcal{C}$ avec σ une n-permutation, alors G est une matrice génératrice de $\mathcal{C}$ si et seulement si $\sigma \cdot G$ est une matrice génératrice de $\mathcal{D}$.

Démonstration. Supposons que $\mathcal{C}$ est un sous-espace de $\mathbb{Z}_2^n$ de dimension $k > 0$. Alors $\mathcal{D} = \sigma \cdot \mathcal{C}$ est l'image de l'application linéaire injective

$$\sigma' : \mathcal{C} \to \mathbb{Z}_2^n : \mathbf{x} \mapsto \sigma \cdot \mathbf{x}.$$

Supposons que G est une matrice génératrice de $\mathcal{C}$. D'après le lemme 3.3.4, les lignes $G_1, \ldots, G_k$ de G forment une base de $\mathcal{C}$. D'après la proposition 3.1.14, $\{\sigma \cdot G_1, \ldots, \sigma \cdot G_k\}$ est une base de $\mathcal{D}$. D'après le lemme 3.3.4,

$$\sigma \cdot G = \begin{pmatrix} \sigma \cdot G_1 \\ \vdots \\ \sigma \cdot G_k \end{pmatrix}$$

est une matrice génératrice de $\mathcal{D}$. Réciproquement, si $\sigma \cdot G$ est une matrice génératrice de $\mathcal{D}$, alors $G = \sigma^{-1}(\cdot\sigma \cdot G)$ est une matrice génératrice de $\sigma^{-1} \cdot \mathcal{D} = \mathcal{C}$. La preuve du lemme s'achève.

Remarque. Deux codes linéaires équivalents sont de même dimension.

3.3.9. Théorème. Tout (n, k)-code linéaire non trivial est équivalent à un (n, k)-code standard.

Démonstration. Supposons que $\mathcal{C}$ est un (n,k)-code linéaire non trivial dont G est une matrice génératrice canonique. Comme $\mathrm{rg}(G) = k$, d'après le lemme 3.1.17, il existe une n-permutation σ telle que $M = \sigma \cdot G$ est une matrice échelonnée normée. Posons $\mathcal{D} = \mathscr{L}(M)$. Comme les lignes de M sont linéairement indépendantes, d'après le lemme 3.3.4(2), M est une matrice génératrice de $\mathcal{D}$. Par définition, $\mathcal{D}$ est un (n,k)-code standard. D'après le lemme 3.1.16(2), $\mathcal{D} = \mathscr{L}(M) = \sigma \cdot \mathscr{L}(G) = \sigma \cdot \mathcal{C}$. C'est-à-dire, $\mathcal{C}, \mathcal{D}$ sont équivalents. La preuve du théorème s'achève.

Exemple. Trouver un code standard qui est équivalent au $(5,2)$-code linéaire

$$\mathcal{C} = \{00000, 11001, 11100, 00101\}.$$

Le résultat suivant donne une autre méthode pour trouver des codes linéaires.

3.3.10. Lemme. Si M est une matrice binaire de type $m \times n$, alors $\mathscr{N}^T(M)$ est un (n,s)-code linéaire, où $s = n - \mathrm{rg}(M)$.

Démonstration. Pour tout $\mathbf{x} \in \mathbb{Z}_2^n$, d'après la définition, $\mathbf{x} \in \mathscr{N}^T(M)$ si et seulement si $\mathbf{x}^T \in \mathscr{N}(M)$. Or, d'après le théorème 3.1.2(2), $\mathscr{N}(M)$ est un sous-espace de $\mathbb{Z}_2^{(n)}$ de dimension $n - \mathrm{rg}(M)$. Il est évident que

$$\mathbb{Z}_2^{(n)} \to \mathbb{Z}_2^n : u \mapsto u^T$$

est un isomorphisme d'espaces vectoriels, qui envoie $\mathscr{N}(M)$ sur $\mathscr{N}^T(M)$. Par conséquent, $\mathscr{N}^T(M)$ est un sous-espace de $\mathbb{Z}_2^n$ de dimension $n - \mathrm{rg}(M)$. La preuve du lemme s'achève.

3.3.11. Définition. Soit $\mathcal{C}$ un (n,k)-code linéaire avec $k < n$. Une matrice binaire H de type $(n-k) \times n$ s'appelle *matrice de contrôle* de $\mathcal{C}$ si $\mathcal{C} = \mathscr{N}^T(H)$; et *matrice de contrôle canonique* de $\mathcal{C}$ si H est, de surcroît, échelonnée réduite.

Remarque. Si H est une matrice de contrôle de $\mathcal{C}$ alors, pour tout $\mathbf{x} \in \mathbb{Z}_2^n$, on a

$$\mathbf{x} \in \mathcal{C} \text{ si et seulement si } H\mathbf{x}^T = \mathbf{0}.$$

3.3.12. Lemme. Soit $\mathcal{C}$ un (n,k)-code linéaire avec $0 \leq k < n$. Si H est une matrice binaire, alors les conditions suivantes sont équivalentes:

(1) H est une matrice de contrôle de $\mathcal{C}$;

(2) $\mathcal{C} = \mathscr{N}^T(H)$ et les lignes de H sont linéairement indépendantes.

(3) H s'échelonne à une matrice de contrôle de $\mathcal{C}$.

Démonstration. Supposons que H est une matrice de contrôle de $\mathcal{C}$. Alors $\mathcal{C} = \mathscr{N}^T(H)$ avec H de type $(n-k) \times n$. $k = \dim \mathscr{N}^T(H) = n - \mathrm{rg}(H)$, et donc $\mathrm{rg}(H) = n - k$. D'après le théorème 3.1.2(3), les lignes de H sont linéairement indépendantes.

Supposons que $\mathcal{C} = \mathscr{N}^T(H)$ et les lignes de H sont linéairement indépendantes. Alors H est de type $s \times n$ et de rang s. D'après le lemme 3.3.10, $n - s = \dim(\mathcal{C}) = k$. D'où, $s = n - k$. D'après la définition, H est une matrice de contôle de $\mathcal{C}$.

Supposons enfin que H s'échelonne à H', une matrice de contrôle de $\mathcal{C}$. Alors $\mathcal{C} = \mathscr{N}^T(H')$ et H' est de type $(n-k) \times n$. D'après le lemme 3.1.18(1), $\mathcal{C} = \mathscr{N}^T(H)$. Comme H est de type $(n-k) \times n$, elle est aussi une matrice de contrôle de $\mathcal{C}$. La preuve du lemme s'achève.

Exemple. Donner une matrice de contrôle du code $\mathcal{C}$ défini par le codeur suivant:

$$\phi : \mathbb{Z}_2^2 \to \mathbb{Z}_2^3 : b_1b_2 \mapsto b_1b_2b; \quad \text{où } b = b_1 + b_2.$$

Le résultat suivant nous donne une méthode pour trouver une matrice de contrôle d'un code linéaire.

3.3.13. Lemme. Soit $\mathcal{C} = \mathscr{N}^T(M)$ avec M une matrice binaire non nulle. Si L est une forme échelonnée de M, alors les lignes non nulles de L forment une matrice de contrôle de $\mathcal{C}$.

Démonstration. Supposons que L est une forme échelonnée de M. D'après le lemme 3.1.18(1), $\mathscr{N}^T(L) = \mathscr{N}^T(M) = \mathcal{C}$. Soit H la matrice formée des lignes non nulles de L. D'après le théorème 3.1.5(2), les lignes de H sont linéairement indépendantes. En outre, le système homogène $HX = 0$ est obtenu à partir du système homogène $LX = 0$ en enlevant des équations $0 = 0$. Donc, ces deux systèmes homogènes sont équivalents. Par conséquent, $\mathscr{N}(H) = \mathscr{N}(L)$; et donc, $\mathscr{N}^T(H) = \mathscr{N}^T(L) = \mathcal{C}$. D'après le lemme 3.3.12, H est une matrice de contrôle de $\mathcal{C}$. La preuve du lemme s'achève.

Exemple. Donner la matrice de contrôle canonique de $\mathcal{C} = \mathscr{N}^T(M)$, où

$$M = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \end{pmatrix}.$$

3.3.14. Lemme. Soit $\mathcal{C}$ un (n,k)-code linéaire avec $0 \leq k < n$. Si $\mathcal{D} = \sigma \cdot \mathcal{C}$ avec σ une n-permutation, alors une matrice binaire H est une matrice de contrôle de $\mathcal{C}$ si et seulement si $\sigma \cdot H$ est une matrice de contrôle de $\mathcal{D}$.

Démonstration. Si H est une matrice de contrôle de $\mathcal{C}$, alors H est de type $(n-k) \times n$ telle que $\mathcal{C} = \mathscr{N}^T(H)$. D'après le lemme 3.1.18(2), $\mathcal{D} = \sigma \cdot \mathscr{N}^T(H) = \mathscr{N}^T(\sigma \cdot H)$. Comme $\mathcal{D}$ est un (n,k)-code linéaire et $\sigma \cdot H$ est de type $(n-k) \times n$, d'après la définition, $\sigma \cdot H$ est une matrice de contrôle de $\mathcal{D}$.

Réciproquement, si $\sigma \cdot H$ est une matrice de contrôle de $\mathcal{D}$, alors $H = \sigma^{-1} \cdot (\sigma \cdot H)$ est une matrice de contrôle de $\sigma^{-1} \cdot \mathcal{D} = \mathcal{C}$. La preuve du lemme s'achève.

Le résultat suivant nous comment trouver une matrice de contrôle d'un code linéaire propre à partir de sa matrice génératrice canonique.

3.3.15. Théorème. Soit $\mathcal{C}$ un (n, k)-code linéaire avec $0 < k < n$, dont G est une matrice génératrice canonique. Si $\sigma \cdot G = (I_k \mid A)$ avec σ une n-permutation, alors

$$H = \sigma^{-1} \cdot (A^T \mid I_{n-k})$$

est une matrice de contrôle de $\mathcal{C}$.

Démonstration. Posons $\mathscr{D} = \mathscr{L}(I_k \mid A)$. Comme $\mathrm{rg}(I_k \mid A) = k$, on voit que $\mathscr{D}$ est un (n, k)-code linéaire. D'après le numéro 2 des exercices 3.5, $\mathrm{rg}(A^T \mid I_{n-k}) = n - k$. D'après le lemme 3.3.10, $\mathscr{N}^T(A^T \mid I_{n-k})$ est de dimension k. À l'aide de la multiplication par blocs, on trouve

$$(A^T \mid I_{n-k})(I_k \mid A)^T = (A^T \mid I_{n-k}) \begin{pmatrix} I_k \\ A^T \end{pmatrix} = A^T I_k + I_{n-k} A^T = A^T + A^T = 0_{(n-k)\times k}.$$

Ainsi, d'après le lemme 3.1.18(3), $\mathcal{D} = \mathscr{L}(I_k \mid A) \subseteq \mathscr{N}^T(A^T \mid I_{n-k})$. Par conséquent, $\mathcal{D} = \mathscr{N}^T(A^T \mid I_{n-k})$. Ceci montre que $(A^T \mid I_{n-k})$ est une matrice de contrôle de $\mathcal{D}$. Remarquons que

$$\sigma^{-1} \cdot \mathcal{D} = \sigma^{-1} \cdot \mathscr{L}(I_k \mid A) = \mathscr{L}(\sigma^{-1} \cdot (I_k \mid A)) = \mathscr{L}(G) = \mathcal{C},$$

d'après le lemme 3.3.14, $H = \sigma^{-1} \cdot (A^T \mid I_{n-k})$ est une matrice de contrôle de $\mathcal{C}$. Ceci achève la démonstration du théorème.

Remarque. Si $\mathcal{C}$ est un (n, k)-code standard dont $(I_k|A)$ est la matrice génératrice canonique, alors $(A^T \mid I_{n-k})$ est une matrice de contrôle de $\mathcal{C}$.

Exemple. Donner une matrice de contrôle du $(5, 2)$-code

$$\mathcal{C} = \{00000, 11001, 11100, 00101\}.$$

Réciproquement, le résultat suivant nous dit en particulier qu'on peut trouver une matrice génératrice d'un code linéaire à partir de sa matrice de contrôle canonique.

3.3.16. Théorème. Soit $\mathcal{C}$ un (n, k)-code linéaire avec $0 < k < n$, dont H est une matrice de contrôle. Si $\sigma \cdot H = (A \mid I_{n-k})$ avec σ une n-permutation, alors

$$G = \sigma^{-1} \cdot (I_k \mid A^T)$$

est une matrice de génératrice de $\mathcal{C}$.

Démonstration. Posons $\mathcal{D} = \mathscr{L}(I_k \mid A^T)$. Alors $\mathcal{D}$ est un (n,k)-code linéaire dont $(I_k \mid A^T)$ est la matrice génératrice canonique. D'après le théorème 3.3.15, $(A \mid I_{n-k})$ est une matrice de contrôle de $\mathcal{D}$. En vertu des lemmes 3.1.18(2) et 3.1.14(2),

$$\mathcal{C} = \mathscr{N}^T(\sigma^{-1} \cdot (A \mid I_{n-k})) = \sigma^{-1} \cdot \mathscr{N}^T(A \mid I_{n-k}) = \sigma^{-1} \cdot \mathscr{L}(I_k \mid A^T) = \mathscr{L}(\sigma^{-1} \cdot (I_k \mid A^T)).$$

Étant de rang k, la matrice $\sigma^{-1} \cdot (I_k \mid A^T)$ est une matrice génératrice de $\mathcal{C}$. La preuve du théorème s'achève.

Remarque. Soit $\mathcal{C}$ un (n,k)-code linéaire, dont H est une matrice de contrôle. Si H s'échelonne à $(A \mid I_{n-k})$, alors $(I_k \mid A^T)$ est la matrice génératrice canonique de $\mathcal{C}$.

Exemple. Donner une matrice génératrice du code linéaire $\mathcal{C} = \mathscr{N}^T(M)$, où

$$M = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

On étudiera le relation entre les codes linéaires et les codeurs.

3.3.17. Définition. Un (n,k)-codeur avec $0 < k < n$

$$\varphi : \mathbb{Z}_2^k \to \mathbb{Z}_2^n : \mathbf{x} \mapsto \mathbf{x} \cdot \mathbf{r}_\mathbf{x}$$

est dit *linéaire* si φ est une application linéaire d'espaces vectoriels.

3.3.18. Lemme. Soit un (n,k)-codeur avec $0 < k < n$

$$\varphi : \mathbb{Z}_2^k \to \mathbb{Z}_2^n : \mathbf{x} \mapsto \mathbf{x} \cdot \mathbf{r}_\mathbf{x}.$$

Alors φ est linéaire si et seulement si, il existe une matrice $A \in M_{k\times(n-k)}(\mathbb{Z}_2)$ telle que $\mathbf{r}_\mathbf{x} = \mathbf{x}A$, pour tout $\mathbf{x} \in \mathbb{Z}_2^k$.

Démonstration. Supposons que $\mathbf{r}_\mathbf{x} = \mathbf{x}A$, pour tout $\mathbf{x} \in \mathbb{Z}_2^k$. Posant $M = (I_k \mid A)$, on obtient $\mathbf{x} \cdot \mathbf{r}_\mathbf{x} = \mathbf{x}M$, pour tout $\mathbf{x} \in \mathbb{Z}_2^k$. C'est-à-dire, φ est de la forme

$$\varphi : \mathbb{Z}_2^k \to \mathbb{Z}_2^n : \mathbf{x} \mapsto \mathbf{x}M,$$

qui est évidemment linéaire.

Supposons, réciproquement, que φ est linéaire. En vertu de la proposition 3.1.11, il existe une matrice $G = (B \mid A) \in M_{k\times n}(\mathbb{Z}_2)$, où $B \in M_{k\times k}(\mathbb{Z}_2)$ et $A \in M_{k\times(n-k)}(\mathbb{Z}_2)$, telle que

$$\mathbf{x} \cdot \mathbf{r}_\mathbf{x} = \varphi(\mathbf{x}) = \mathbf{x}G = (\mathbf{x}B \mid \mathbf{x}A),$$

et donc, $\mathbf{r}_{\mathbf{x}} = \mathbf{x}A$, pour tout $\mathbf{x} \in \mathbb{Z}_2^k$. Ceci achève la démonstration du lemme.

Exemple. (1) Le codeur de répétition suivant est linéaire:

$$\varphi_1 : \quad \mathbb{Z}_2^2 \quad \to \quad \mathbb{Z}_2^6 : \mathbf{x} \mapsto \mathbf{x} \cdot \mathbf{x} \cdot \mathbf{x}$$

(2) Le codeur de la somme de contrôle suivant est linéaire:

$$\varphi : \mathbb{Z}_2^2 \to \mathbb{Z}_2^3 : b_1 b_2 \mapsto b_1 b_2 b_3, \text{ où } b_3 = b_1 + b_2.$$

3.3.19. Théorème. Un code linéaire $\mathcal{C}$ est standard propre si, et seulement si, $\mathcal{C}$ est défini par un codeur linéaire φ; et dans ce cas, si G est la matrice génératrice canonique de $\mathcal{C}$, alors $\varphi(\mathbf{x}) = \mathbf{x}G$, pour tout $\mathbf{x} \in \mathbb{Z}_2^k$.

Démonstration. Supposons que $\mathcal{C} = \mathrm{Im}(\varphi)$, où

$$\varphi : \mathbb{Z}_2^k \to \mathbb{Z}_2^n : \mathbf{x} \mapsto \mathbf{x} \cdot \mathbf{r}_{\mathbf{x}}$$

est un (n, k)-codeur linéaire. Par définition, $0 < k < n$. Comme φ est injective, d'après la proposition 3.1.14, $\mathcal{C}$ est de dimension k. En vertu du lemme 3.3.16, φ est de la forme

$$\varphi : \mathbb{Z}_2^k \to \mathbb{Z}_2^n : \mathbf{x} \mapsto \mathbf{x}M,$$

avec $M = (I_k \mid A) \in M_{k \times n}(\mathbb{Z}_2)$. D'après la proposition 3.1.13, $\mathcal{C} = \mathscr{L}(M)$. Étant échelonnée normée, M est une matrice génératrice canonique de $\mathcal{C}$. D'où, $\mathcal{C}$ est standard propre.

Réciproquement, supposons que $\mathcal{C}$ est un (n, k)-code standard avec $0 < k < n$. Alors sa matrice génératrice canonique est de la forme $G = (I_k \mid A)$, où $A \in M_{k \times (n-k)}(\mathbb{Z}_2)$. Considérons l'application linéaire

$$\varphi : \mathbb{Z}_2^k \to \mathbb{Z}_2^n : \mathbf{x} \mapsto \mathbf{x}G.$$

D'après la proposition 3.1.13, $\mathrm{Im}(\varphi) = \mathscr{L}(G) = \mathcal{C}$. Si $\{e_1, \ldots, e_k\}$ est la base canonique de $\mathbb{Z}_2^k$, alors $\varphi(e_i) = e_i G = G_i$, la i-ième ligne de G, $i = 1, \ldots, k$. Comme $\{G_1, \ldots, G_k\}$ est libre, d'après la proposition 3.1.11, φ est injective. Ainsi, φ est un (n, k)-code linéaire. La preuve du théorème s'achève.

Exemple. Trouver le codeur linéaire qui définit le code standard $\mathcal{C} = \{000, 101, 011, 110\}$.

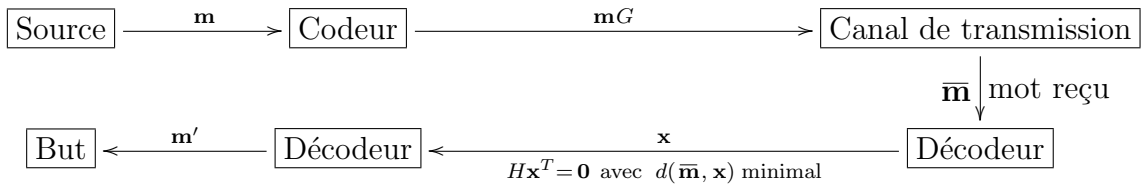
Exemple. Soit $\mathcal{C}$ le code défini par le codeur

$$\begin{array}{rccl} \varphi : & \mathbb{Z}_2^2 & \to & \mathbb{Z}_2^5 : \\ & 00 & \mapsto & 00000 \\ & 01 & \mapsto & 01101 \\ & 10 & \mapsto & 10110 \\ & 11 & \mapsto & 11011 \end{array}$$

(1) Vérifier que $\mathcal{C}$ est un code standard.

(2) Trouver la matrice génératrice canonique et une matrice de contrôle de $\mathcal{C}$.

On termine cette section par la schéma du transport de l'information par un code standard propre, dont G est la matrice génératrice canonique et H est une matrice de contrôle :



où $\mathbf{m}'$ est le mot formé des k premiers bits de $\mathbf{x}$.

3.4 Capacité correctrice de codes linéaires

Le but de cette section est d'étudier la capacité correctrice de codes linéaires. Pour ce faire, on a besoin de la notion suivante.

3.4.1. Définition. Le *poids* d'un mot $\mathbf{x}$, noté $w(\mathbf{x})$, est le nombre de bits non nuls de $\mathbf{x}$.

Exemple. Pour tout mot $\mathbf{x}$, on voit que $w(\mathbf{x}) = 0$ si, et seulement si, $\mathbf{x} = \mathbf{0}$.

3.4.2. Définition. Soit $\mathcal{C}$ un code linéaire non trivial. On définit *poids minimum* de $\mathcal{C}$ comme étant

$$w(\mathcal{C}) = \min\{w(\mathbf{x}) \mid \mathbf{0} \neq \mathbf{x} \in \mathcal{C}\}.$$

3.4.3. Proposition. Soit $\mathcal{C}$ un code linéaire non trivial. Alors $d(\mathcal{C}) = w(\mathcal{C})$, et donc, la capacité correctrice de $\mathcal{C}$ est donnée par

$$\delta(\mathcal{C}) = \left[\frac{w(\mathcal{C}) - 1}{2}\right].$$

Démonstration. Si $\mathbf{0} \neq \mathbf{x} \in \mathcal{C}$, alors $w(\mathbf{x}) = d(\mathbf{x}, \mathbf{0}) \geq d(\mathcal{C})$. D'où, $w(\mathcal{C}) \geq d(\mathcal{C})$. De l'autre côté, il existe $\mathbf{x}, \mathbf{y} \in \mathcal{C}$ tels que $d(\mathbf{x}, \mathbf{y}) = d(\mathcal{C}) > 0$. Comme $\mathcal{C}$ est un sous-espace de $\mathbb{Z}_2^n$, on voit que $\mathbf{0} \neq \mathbf{x} - \mathbf{y} \in \mathcal{C}$. Posons $\mathbf{x} = x_1 \cdots x_n$ et $\mathbf{y} = y_1 \cdots y_n$. Alors $\mathbf{x} - \mathbf{y} = z_1 \cdots z_n$ avec $z_i = x_i - y_i$, et donc,

$$d(\mathcal{C}) = d(\mathbf{x}, \mathbf{y}) = |\{i \in \{i \mid x_i \neq y_i\}| = |\{i \in \{i \mid z_i \neq 0\}| = w(\mathbf{x} - \mathbf{y}) \geq w(\mathcal{C}).$$

D'où, $d(\mathcal{C}) = w(\mathcal{C})$. La preuve du lemme s'achève.

Voici une autre interprétation du poids minimum de $\mathcal{C}$.

3.4.4. Lemme. Soit $\mathcal{C}$ un code linéaire non trivial, dont H est une matrice de contrôle. Alors $w(\mathcal{C})$ est le plus petit entier s tel que H admet s colonnes linéairement dépendantes.

Démonstration. Comme $\mathcal{C} = \mathscr{N}^T(H)$ est non nul, $\mathscr{N}(H)$ est non nul. Ainsi, les colonnes $H_1, \ldots, H_n$ de H sont linéairement dépendantes. Supposons que $s\,(\geq 1)$ est minimal tel qu'il existe une famille liée $\{H_{i_1}, \ldots, H_{i_s}\}$, où $1 \leq i_1 < \cdots < i_s \leq n$. Alors il existe $a_{i_1}, \ldots, a_{i_s} \in \mathbb{Z}_2$, non tous nuls, tels que

$$a_{i_1}H_{i_1} + \cdots + a_{i_s}H_{i_s} = \mathbf{0}.$$

Posons $\mathbf{x} = x_1 \cdots x_n$, où

$$x_j = \begin{cases} a_j, & \text{si } j \in \{i_1, \ldots, i_s\}; \\ 0, & \text{sinon.} \end{cases}$$

Alors

$$H\mathbf{x}^T = (H_1 \cdots H_n)\mathbf{x}^T = \sum\nolimits_{i=1}^{n} x_j H_j = \sum\nolimits_{j=1}^{s} a_{i_j} H_{i_j} = \mathbf{0}.$$

Ainsi $\mathbf{x} \in \mathcal{C}$ avec $0 < w(\mathbf{x}) \leq s$. D'où, $w(\mathcal{C}) \leq s$.

De l'autre côté, posant $d = w(\mathcal{C})$, on obtient un mot $\mathbf{y} = b_1 \cdots b_n \in \mathcal{C}$ avec $w(\mathbf{y}) = d$. Soient les indices $i_1, \ldots, i_d$ avec $1 \leq i_1 < \cdots < i_d \leq n$ tels que, pour tout $1 \leq j \leq n$, on a $b_j \neq 0$ si et seulement si $j \in \{i_1, \ldots, i_d\}$. Ceci donne

$$\mathbf{0} = H\,\mathbf{y}^T = \sum\nolimits_{j=1}^{n} b_j H_j = \sum\nolimits_{j=1}^{d} b_{i_j} H_{i_j}.$$

C'est-à-dire, $\{H_{i_1}, \ldots, H_{i_d}\}$ est liée. D'après la minimalité de s, on obtient $s \leq d = w(\mathcal{C})$. La preuve du lemme s'achève.

3.4.5. Théorème. Soit $\mathcal{C}$ un (n, k)-code linéaire linéaire non trivial, dont H est une matrice de contrôle. Si $m\,(\geq 0)$ est maximal tel que toute famille de m colonnes de H est libre, alors la capacité correctrice de $\mathcal{C}$ est donnée par

$$\delta(\mathcal{C}) = \left\lfloor \frac{m}{2} \right\rfloor.$$

Démonstration. Soient $H_1, \ldots, H_n$ les colonnes de H. Par convention, toute famille de 0 colonne de H est libre. Comme $\mathcal{C}$ est non nul, la famille $\{H_1, \ldots, H_n\}$ est liée. Ainsi il existe un entier maximal m avec $0 \leq m < n$ tel que toute famille de m colonnes de H est libre. Alors il existe une famille liée de $m + 1$ colonnes de H.

En outre, soit $\{H_{i_1}, \cdots, H_{i_s}\}$ avec $i_1 < \cdots < i_s$ une famille liée de colonnes de H. Si $s \leq m$, elle est contenue dans une famille liée de m colonnes de H, une contradiction. Ainsi

$s \geq m+1$. D'après le lemme 3.4.4, $w(\mathcal{C}) = m+1$. En vertu de la proposition 3.4.3, $\delta(\mathcal{C}) = [\frac{w(\mathcal{C})-1}{2}] = [\frac{m}{2}]$. La preuve du théorème s'achève.

3.4.6. Lemme. Soit E un espace vectoriel sur $\mathbb{Z}_2 = \{0,1\}$. Si $u, v \in E$, alors $\{u, v\}$ est libre si et seulement si u, v sont distincts et tous non nuls.

Démonstration. La nécessité est évidente. Supposons que $\{u, v\}$ est liée. Alors l'un de u, v est un multiple de l'autre, disons $v = \lambda u$ avec $\lambda \in \mathbb{Z}_2$. Si $\lambda = 0$, alors $v = 0_E$; et sinon, on a $v = u$. Ceci montre ls suffisance. La preuve du lemme s'achève.

Exemple. Calculer la capacité correctrice d'un code linaire $\mathcal{C}$, dont une matrice de contrôle est

$$H = \begin{pmatrix} 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

3.4.7. Corollaire. Soit $\mathcal{C}$ un code linéaire non trivial, dont H est une matrice de contrôle. Alors $\delta(\mathcal{C}) > 0$ si et seulement si les colonnes de H sont toutes non nulles et deux à deux distinctes.

Démonstration. D'après le théorème 3.4.5, $\delta(\mathcal{C}) = [\frac{m}{2}]$, où $m\,(\geq 0)$ est maximal tel que toute famille de m colonnes de H est libre. Donc, $\delta(\mathcal{C}) > 0$ si, et seulement si, $m \geq 2$ si, et seulement si, toute famille de deux colonnes de H est libre. D'après le lemme 3.4.6, cette dernière est valide si, et seulement si, toute colonne de H est non nulle et toutes les deux colonnes sont distinctes. La preuve du corollaire s'achève.

3.4.8. Définition. Soit $m > 1$ un entier. Un *code de Hamming de co-rang* m est un code linéaire dont une matrice de contrôle se compose de tous les vecteurs non nuls de $\mathbb{Z}_2^{(m)}$.

Remarque. En vue le lemme 3.3.10(2), les codes de Hamming de co-rang m sont deux à deux équivalents.

Le résultat suivant explique le terminologie de co-rang m.

3.4.9. Proposition. Un code de Hamming de co-rang m est un $(2^m-1, 2^m-1-m)$-code linéaire, qui est capable de corriger au moins une erreur.

Démonstration. Soit $\mathcal{H}_m$ un code de Hamming de co-rang m, dont H est une matrice de contrôle. D'après le corollaire 3.4.7, $\delta(\mathcal{H}_m) > 0$. Donc, $\mathcal{H}_m$ est capable de corriger au moins une erreur.

En outre, par définition, H est de type $m \times (2^m - 1)$. Ainsi $\mathrm{rg}(H) \leq m$. Comme H contient m colonnes linéairement indépendantes, $\mathrm{rg}(H) \geq m$, et donc, $\mathrm{rg}(H) = m$. Ainsi la dimension de $\mathcal{H}_m$ est $2^m - 1 - m$. La preuve de la proposition s'achève.

Exemple. Donner un code standard de Hamming de corang 2.

3.5 Exercices

1. Soit $A = (A_1 A_2 \cdots A_n)$ une matrice partagée en colonnes sur un corps K, s'échelonnant à $B = (B_1 B_2 \cdots B_n)$. Si $j_1, j_2, \ldots, j_r \in \{1, 2, \ldots, n\}$, montrer que $A' = (A_{j_1} A_{j_2} \cdots A_{j_r})$ s'échelonne à $B' = (B_{j_1} B_{j_2} \cdots B_{j_r})$.

2. Soit $A = (B \mid I_m)$ une matrice partagée sur un corps K. Montrer que $\mathrm{rg}(A) = m$.

3. Soit E un $\mathbb{Z}_2$-espace vectoriel. Si $u, v \in E$ sont tous non nuls, montrer que u, v sont linéairement indépendants si et seulement si $u \neq v$. Donner un exemple où cet énoncé n'est pas valide.

4. Considérer la matrice sur $\mathbb{Z}_3$ suivante:

$$M = \begin{pmatrix} 1 & 2 & 0 & 2 \\ 1 & 0 & 1 & 1 \\ 2 & 2 & 1 & 0 \\ 1 & 1 & 2 & 0 \end{pmatrix}.$$

   Donner les vecteurs de $\mathscr{L}(M)$ et ceux de $\mathscr{N}(M)$.

5. Trouver la forme échelonnée réduite de la matrice sur $\mathbb{Z}_5$ suivante:

$$M = \begin{pmatrix} 2 & 1 & 3 & 1 & 0 \\ 1 & 1 & 3 & 1 & 2 \\ 4 & 2 & 1 & 2 & 1 \\ 2 & 4 & 2 & 4 & 3 \end{pmatrix}.$$

6. Considérer la forme échelonnée réduite sur $\mathbb{Z}_7$ suivante:

$$M = \begin{pmatrix} 1 & 1 & 0 & 5 & 0 \\ 0 & 0 & 1 & 4 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

   qui se réduit, par des permutations de colonnes, à la matrice échelonnée normée suivante:

$$N = \begin{pmatrix} 1 & 0 & 0 & 1 & 5 \\ 0 & 1 & 0 & 0 & 4 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}.$$

   Vérifier que $\mathscr{L}(M) \neq \mathscr{L}(N)$.

7. Considérer l'espaces vectoriels réels $\mathbb{R}^3$ et $\mathbb{R}^4$.
   (1) Trouver une application linéaire $T : \mathbb{R}^3 \to \mathbb{R}^4$ satisfait à la condition suivante:
   $$T(u_1) = T(u_2) = (1, 0, 2, 1),\ T(u_3) = (0, 1, -1, 2),$$
   où $u_1 = (-1, 1, 1)$, $u_2 = (1, 2, 1)$, $u_3 = (0, 1, 2)$.
   (2) Décrire l'image de l'application linéaire T trouvée ci-dessus.
   (3) Déterminer s'il existe ou non une application linéaire $S : \mathbb{R}^3 \to \mathbb{R}^4$ telle que
   $$S(u_1) = S(u_2) = (1, 2, 0, 1),\ S(u_3) = (1, 0, 1, 1), S(-1, 0, 1) = (1, 0, 1, 0).$$

8. Soit $T : E \to F$ une applications linéaires de K-espace vectoriels. Si $u_1, \ldots, u_n \in E$ sont tels que $\{T(u_1), \ldots, T(u_n)\}$ est libre, montrer que $\{u_1, \ldots, u_n\}$ est libre.

9. Soit K un corps. Si σ est une permutation de $\{1, 2, \ldots, n\}$, montrer que
   $$\sigma : K^n \to K^n : (x_1, x_2, \cdots, x_n) \mapsto (x_{\sigma(1)}, x_{\sigma(2)}, \cdots, x_{\sigma(n)})$$
   est un isomorphisme.

10. Trouver des permutations σ et τ telle que $\sigma \cdot A = (I_4 \mid B)$ et $\tau \cdot A = (C \mid I_4)$, où
$$A = \begin{pmatrix} 1 & 3 & 0 & 5 & 0 & 2 & 0 & 2 \\ 0 & 0 & 1 & 2 & 0 & 3 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 7 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

11. Considérer le codeur de répétition suivant:
$$\varphi : \mathbb{Z}_2^2 \to \mathbb{Z}_2^{10} : \mathbf{m} \mapsto \mathbf{m} \cdot \mathbf{m} \cdot \mathbf{m} \cdot \mathbf{m} \cdot \mathbf{m}$$
   (1) Donner le code $\mathcal{C}$ défini par φ.
   (2) Si $\mathbf{x}, \mathbf{y} \in \mathcal{C}$ sont distincts, montrer que $d(\mathbf{x}, \mathbf{y}) \geq 5$.
   (3) Supposer qu'on veut transmettre l'information $\mathbf{m} \in \mathbb{Z}_2^2$ et le décodeur reçoit $\mathbf{x} \in \mathbb{Z}_2^{10}$. Si $d(\mathbf{x}, \varphi(\mathbf{m})) \leq 2$, montrer que l'estimé de $\mathbf{m}$ par le décodeur est bien $\mathbf{m}$.
   (4) Supposer qu'on veut transmettre l'information 10 et le décodeur reçoit 1011111110. Quel est l'estimé de l'information originale 10 par le décodeur?

12. Soit $\mathcal{C}$ un code de longueur n contenant les mots $\mathbf{0} = 00\cdots0$ et $\mathbf{1} = 11\cdots1$. Si la capacité expressive de $\mathcal{C}$ est au moins 3, montrer que la capacité correctrice $\delta(\mathcal{C})$ de $\mathcal{C}$ est inférieure que $\dfrac{n}{4}$. *Indice*: Estimer $d(\mathcal{C})$ à l'aide de $d(\mathbf{0}, \mathbf{x})$ et $d(\mathbf{1}, \mathbf{x})$, où $\mathbf{x} \neq \mathbf{0}, \mathbf{1}$.

13. Soit $\mathbf{x}_0 \in \mathbb{Z}_2^n$ avec $n \geq 2$. Pour un entier k avec $1 \leq k \leq n$, exprimer la cardinalité de $B(\mathbf{x}_0, k)$ en termes de coefficients binomiaux.

14. Soient $\mathbf{x} = 011011101$ et $\mathbf{y} = 100001011 \in \mathbb{Z}_2^9$.
    (1) Calculer la distance $d(\mathbf{x}, \mathbf{y})$.
    (2) Donner la boule $B(\mathbf{x}, 1)$.
    (3) Donner le nombre de mots $\mathbf{m}$ avec $d(\mathbf{x}, \mathbf{m}) = 3$.
    (4) Calculer la cardinalité de la boule $B(\mathbf{y}, 3)$.

15. Soit $\mathcal{C}$ le code défini par le codeur de la somme de contrôle

$$\phi : \mathbb{Z}_2^7 \to \mathbb{Z}_2^8 : b_1b_2b_3b_4b_5b_6b_7 \mapsto b_1b_2b_3b_4b_5b_6b_7b_8, \text{ où } b_8 = \sum_{i=1}^{7} b_i.$$

    (1) Montrer que $\mathcal{C}$ est capable de déceler la présence d'une seule erreur.
    (2) Montrer que $\mathcal{C}$ est incapable de corriger une erreur.

16. Considérer le code $\mathcal{C}$ défini par le codeur de répétition suivant:

$$\phi : \mathbb{Z}_2^2 \to \mathbb{Z}_2^8 : \mathbf{m} \mapsto \mathbf{m} \cdot \mathbf{m} \cdot \mathbf{m} \cdot \mathbf{m}$$

    (1) Donner la distance minimum $d(\mathcal{C})$.
    (2) Donner la capacité correctrice $\delta(\mathcal{C})$.

17. Considérer le code suivant:

$$\mathcal{C} = \{000000, 011110, 101101, 110011, 001011, 010101, 100110, 111000\}.$$

    (1) Vérifier, à l'aide du lemme 2.4.2, que $\mathcal{C}$ est linéaire.
    (2) Trouver la matrice génératrice canonique de $\mathcal{C}$.
    (3) Trouver la matrice de contrôle canonique de $\mathcal{C}$.

18. Considérer le code suivant:

$$\mathcal{C} = \{000000, 000111, 111000, 111111, 110001, 110110, 011001, 001110, 010111, 101000\}.$$

    Déterminer s'il s'agit d'un code linéaire ou non.

19. Soit $\mathcal{C}$ un (n, k)-code linéaire avec $0 < k \leq n$.

    (1) Donner la capacité expressive de $\mathcal{C}$.
    (2) Montrer que $\delta(\mathcal{C}) \leq \frac{n-k}{2}$. *Indice*: À l'aide de la proposition 3.2.14, comparer la capacité expressive et la capacité correctrice.

20. Soit $\mathcal{C}$ un (n,k)-code avec $0 < k \leq n$, dont G est une matrice génératrice. Si M est une matrice binaire de type $k \times n$, montrer que les conditions suivantes sont équivalentes.
    (1) M est une matrice génératrice de $\mathcal{C}$.
    (2) G s'échelonne à M.
    (3) $G = PM$ avec P une matrice binaire carrée d'ordre k.

21. Soit $\mathcal{C}$ un code linéaire dont H est une matrice de contrôle. Montrer que $\mathcal{C}$ est trivial si et seulement si les colonnes de H sont linéairement indépendantes.

22. Considérer le code linéaire $\mathcal{C} = \mathscr{L}(M)$, où

$$M = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}.$$

    (1) Trouver la matrice génératrice canonique de $\mathcal{C}$.
    (2) Trouver une matrice de contrôle de $\mathcal{C}$.
    (3) Donner tous les mots de $\mathcal{C}$.
    (4) Donner un code standard qui est équivalent à $\mathcal{C}$.

23. Si n, k sont des entiers avec $0 < k < n$, trouver le nombre de (n,k)-codes standards.

24. Considérer le code linéaire $\mathcal{C} = \mathscr{L}(N)$, où

$$N = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

    (1) Vérifier que $\mathcal{C}$ est standard de dimension 3.
    (2) Trouver le codeur linéaire φ qui définit $\mathcal{C}$.
    (3) Donner une matrice de contrôle de $\mathcal{C}$.
    (4) Supposons que $\mathbf{m} = 111$ est le mot à transmettre, et $\mathbf{x} = 11011$ est le mot reçu par le décodeur.
        (a) À l'aide de la matrice génératrice canonique, trouver le mot qui sera expédié au canal de transmission.
        (b) À l'aide de la matrice de contrôle, déterminer si $\mathbf{x}$ est un mot du code ou non.
        (c) Quel est l'estimé du décodeur pour le mot original $\mathbf{m}$?

25. Considérer le code linéaire $\mathcal{C} = \mathscr{N}^T(M)$, où

$$M = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

(1) Trouver la matrice de contrôle canonique de $\mathcal{C}$.
(2) Trouver la matrice génératrice canonique de $\mathcal{C}$.
(3) Déterminer si $\mathcal{C}$ est capable de corriger au moins une erreur ou non.

26. Donner un $(6, 3)$-code standard $\mathcal{C}$ contenant le mot 111111, en spécifiant ses mots et une matrice de contrôle.

27. Soit $\mathcal{C}$ un code linéaire de longueur n. Soient G, H des matrices binaire de types $k \times n$ et $(n-k) \times n$, respectivement, dont les lignes sont linéairement indépendantes. Montrer que les énoncés suivants sont équivalents.

(1) G est une matrice génératrice et H est une matrice de contrôle de $\mathcal{C}$.
(2) G est une matrice génératrice de $\mathcal{C}$ avec $HG^T = 0$.
(3) H est une matrice de contrôle de $\mathcal{C}$ avec $HG^T = 0$.

28. Soit $\mathcal{C}$ un (n, k)-code linéaire avec $0 < k < n$, dont G est une matrice génératrice et H est une matrice de contrôle. Si $\mathcal{D} = \mathscr{L}(H)$, montrer que $\mathcal{D}$ est un $(n, n-k)$-code dont H est une matrice génératrice et G est une matrice de contrôle.

29. Soit $\mathcal{C}$ un (n, k)-code linéaire avec $0 < k < n$. Montrer que les énoncés suivants sont équivalents:

(1) $\mathcal{C}$ est standard.
(2) $\mathcal{C}$ a une matrice de contrôle de la forme $(A \mid I_{n-k})$.
(3) Les $n-k$ dernières colonnes de toute matrice de contrôle de $\mathcal{C}$ sont linéairement indépendantes.
(4) Les $n-k$ dernières colonnes d'une matrice de contrôle de $\mathcal{C}$ sont linéairement indépendantes.

30. Considérer le code linéaire $\mathcal{C} = \mathscr{L}(M)$, où

$$M = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

(1) Trouver la matrice génératrice canonique de $\mathcal{C}$.
(2) Trouver la matrice de contrôle canonique de $\mathcal{C}$.
(3) Trouver le poids minimum $w(\mathcal{C})$ de $\mathcal{C}$.
(4) Trouver la capacité correctrice $\delta(\mathcal{C})$ de $\mathcal{C}$.

31. Soit $\mathcal{C}$ un (n, k)-code avec $0 < k < n$. Si $\delta(\mathcal{C}) = \frac{n-k}{2}$, montrer que $\mathcal{C}$ est standard.

Indice: Vérifier que les dernières $n-k$ colonnes d'une matrice de contrôle sont linéairement indépendantes.

32. Donner un code standard de Hamming de co-rang 3, en spécifiant
(1) une matrice de contrôle;
(2) sa matrice génératrice canonique;
(3) sa capacité correctrice.

Chapitre IV: Construction géométrique à la règle et au compas

Le but principal de ce chapitre est d'appliquer la théorie des corps à répondre les questions géométriques de très longtemps suivantes.

La quadrature du cercle. Étant donné un cercle quelconque, est-ce qu'on peut toujours construire à la règle et au compas un carré ayant le même aire que le cercle donné ?

La duplication du cube. Étant donné un cube quelconque, est-ce qu'on peut toujours construire à la règle et au compas un cube qui double le volume du cube donné ?

La trisection de l'angle. Étant donné un angle quelconque, est-ce qu'on peut toujours construire à la règle et au compas deux demi-droites qui partagent l'angle donné en trois angles égaux ?

4.1 Polynômes irréductibles

Partout dans cette section, on se fixe F un corps.

4.1.1. Définition. Soit un polynôme sur F comme suit:

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n; a_i \in F,$$

où $a_n \neq 0$ lorsque f est non nul. Le *degré* de f, noté $\partial(f)$, est défini par

$$\partial(f) = \begin{cases} n, & \text{si } f \neq 0; \\ -\infty, & \text{si } f = 0. \end{cases}$$

En outre, si f est non nul, alors a_n s'appelle le *coefficient directeur* de f. On dit que $f(x)$ est *monique* si $a_n = 1_F$.

4.1.2. Proposition. L'ensemble $F[x]$ des polynômes sur F est un anneau commutatif pour l'addition et la multiplication de polynômes.

Remarque. En identifiant $a \in F$ avec le polynôme constant a, on voit que F est un sous-anneau de $F[x]$.

Le résultat suivant sur le degré du produit et celui de la somme est évident.

4.1.3. Lemme. Si $f(x), g(x)$ sont deux polynômes sur F, alors
(1) $\partial(f(x)g(x)) = \partial(f(x)) + \partial(g(x))$;

(2) $\partial(f(x)+g(x)) \leq \max\{\partial(f(x)),\ \partial(g(x))\}$.

Le résultat suivant est l'algorithme de division de polynômes.

4.1.4. Théorème. Soient $f(x), g(x) \in F[x]$. Si $g(x)$ est non nul, alors il existe des polynômes uniques $q(x), r(x) \in F[x]$ avec $\partial(r(x)) < \partial(g(x))$ tels que

$$f(x) = g(x)q(x) + r(x).$$

Démonstration. Posons $g = b_0 + \cdots + b_{m-1}x^{m-1} + b_m x^m$, où $m \geq 0$ et $b_m \neq 0$. Si $\partial(f(x)) < m$, alors $f(x) = g(x) \cdot 0 + f(x)$ avec $\partial(f(x)) < \partial(g(x))$.

Supposons maintenant que $\partial(f(x)) = n \geq m$ et le résultat est valide pour les polynômes de degré $< n$. Écrivons $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ avec $a_n \neq 0$. Remarquons que

$$a_n b_m^{-1} x^{n-m} g(x) = c_0 + \cdots + c_{n-1}x^{n-1} + a_n x^n.$$

D'où, $h(x) = f(x) - a_n b_m^{-1} x^{n-m} g(x)$ est de degré $< n$. D'après l'hypothèse de récurrence, $h(x) = g(x)q_1(x) + r(x)$ avec $\partial(r(x)) < \partial(g(x))$. Ceci nous donne

$$f(x) = (a_n b_m^{-1} x^{n-1} + q_1(x))g(x) + r(x).$$

Pour montrer l'unicité, supposons que $f(x) = q_0(x)g(x) + r_0(x)$ avec $\partial(r_0(x)) < \partial(g(x))$. Alors $(q(x) - q_0(x))g(x) = r(x) - r_0(x)$. Si $q(x) - q_0(x) \neq 0$, alors $\partial(q(x) - q_0(x)) \geq 0$ et $\partial(g(x)) > 0$. D'après le lemme 4.1.3,

$$\max\{\partial(r(x)),\ \partial(r_0(x))\} \geq \partial(r(x) - r_0(x)) = \partial(q(x) - q_0(x)) + \partial(g(x)) \geq \partial(g(x)),$$

une contradiction. Ainsi $q(x) = q_0(x)$, et donc $r(x) = r_0(x)$. Ceci achève la démonstration du théorème.

Remarque. (1) Les polynômes $q(x)$ et $r(x)$ dans le théorème s'appellent le *quotient* et le *reste* de $f(x)$ divisé par $g(x)$, respectivement.

(2) Si $r(x) = 0$, on dit alors que $g(x)$ *divise* $f(x)$, noté $g(x) \mid f(x)$.

Exemple. Considérons deux polynômes rationnels $f(x) = 1 + x^7$ et $g(x) = 2 + 3x - x^4$. Trouver le quotient et le reste de $f(x)$ divisé par $g(x)$.

Soit $f(x) = \sum_{i=0}^{n} a_i x^i \in F[x]$. Pour $a \in F$, on pose $f(a) = \sum_{i=0}^{n} a_i a^i \in F$.

4.1.5. Proposition. Soit $a \in F$. L'application

$$\rho_a : F[x] \to F : f(x) \mapsto f(a)$$

est un homomorphisme d'anneaux, appelée *l'évaluation* en a.

Démonstration. D'abord, $\rho_a(1_F) = 1_F$. Soient $f(x), g(x) \in F[x]$. On peut écrire $f(x) = \sum_{i=0}^{n} a_i x^i$ et $g(x) = \sum_{i=0}^{n} b_i x^i$. Alors

$$f(x) + g(x) = \sum_{i=0}^{n} (a_i + b_i)x^i; f(x)g(x) = \sum_{k=0}^{2n} (\sum_{i+j=k} a_i b_j)x^k.$$

Donc

$$\rho_a(f(x) + g(x)) = \sum_{i=0}^{n} (a_i + b_i)a^i = \sum_{i=0}^{n} a_i a^i + \sum_{i=0}^{n} b_i a^i = \rho_a(f(x)) + \rho_a(g(x))$$

et

$$\rho_a(f(x)g(x)) = \sum_{k=0}^{2n} (\sum_{i+j=k} a_i b_j)a^k = (\sum_{i=0}^{n} a_i a^i)(\sum_{j=0}^{n} b_j a^j) = \rho_a(f(x))\rho_a(g(x)).$$

Ceci montre que ρ_a est un homomorphisme. La preuve de la proposition s'achève.

4.1.6. Définition. Soit $f(x) \in F[x]$ non constant. On dit que $a \in F$ est une *racine* de f si $f(a) = 0_F$.

Remarque. Tout polynôme de degré 1 sur F admet une racine dans F.

4.1.7. Proposition. Si $f(x) \in F[x]$ est non constant, alors $a \in F$ est une racine de $f(x)$ si, et seulement si, $f(x) = (x - a)q(x)$ avec $q(x) \in F[x]$.

Démonstration. D'après le théorème 4.1.4, $f(x) = (x - a)q(x) + r$, où $q(x) \in F[x]$ et $r \in F$. En vertu de la proposition 4.1.5, $f(a) = (a - a)q(a) + r = r$. Donc $f(a) = 0_F$ si, et seulement si, $r = 0_F$ si, et seulement si, $f(x) = (x - a)q(x)$. Ceci achève la démonstration de la proposition.

4.1.8. Définition. Soit $f(x) \in F[x]$ non constant. On dit que f est *réductible sur* F si $f(x) = g(x)h(x)$ avec $g(x), h(x) \in F[x]$ non constants; et *irréductible* sinon.

Remarque. Si $f(x) = g(x)h(x)$ avec $g(x), h(x)$ non constants, alors $\partial(g(x)), \partial(h(x)) < \partial(f(x))$.

4.1.9. Lemme. Soit $f(x) \in F[x]$ non constant.

(1) Si $\partial(f(x)) = 1$, alors $f(x)$ est irréductible sur F.

(2) Si $\partial(f(x)) \geq 2$ et $f(x)$ a une racine dans F, alors $f(x)$ est réductible.

Démonstration. (1) Supposons que $\partial(f) = 1$. Si $f(x) = g(x)h(x)$ avec $g(x), h(x) \in F[x]$, alors $\partial(g(x)) + \partial(h(x)) = 1$. D'où, $\partial(g(x)) = 0$ ou $\partial(h(x)) = 0$. Ceci montre que $f(x)$ est irréductible sur F.

(2) Supposons que $\partial(f(x)) \geq 2$ et $f(a) = 0$ pour un certain $a \in F$. D'après la proposition 4.1.7, $f(x) = (x-a)q(x)$ avec $q(x) \in F[x]$. Comme $2 \geq \partial(f(x)) = \partial(q(x)) + 1$, on a $\partial(q(x)) > 0$. C'est-à-dire, $f(x)$ est réductible sur F. Ceci achève la démonstration du lemme.

Exemple. Le polynôme $x^2 - 2$ est réductible sur $\mathbb{R}$.

4.1.10. Proposition. Soit $f(x) \in F[x]$ avec $2 \leq \partial(f(x)) \leq 3$. Alors $f(x)$ est irréductible sur F si, et seulement si, $f(x)$ n'a aucune racine dans F.

Démonstration. Si $f(x)$ a au moins une racine dans F, d'après le lemme 4.1.9, il est réductible.

Supposons réciproquement que $f(x)$ est réductible sur F. Alors $f(x) = g(x)h(x)$ avec $g(x), h(x) \in F[x]$ non constants. Comme $0 < \partial(g(x)) + \partial(h(x)) = \partial(f(x)) \leq 3$, on a $\partial(g(x)) = 1$ ou $\partial(h(x)) = 1$. D'où, $g(x)$ ou $h(x)$ admet une racine dans F, et donc $f(x)$ en a une. Ceci achève la démonstration de la proposition.

Exemple. (1) Le polynôme $x^2 - 2$ est irréductible sur $\mathbb{Q}$.

(2) Le polynôme $x^4 + 2x^2 + 1$ est réductible sur $\mathbb{R}$, même s'il n'a aucune racine réelle.

Tout $p(x) \in F[x]$ engendre a un idéal de l'anneau $F[x]$ comme suit:

$$< p(x) >= \{p(x)q(x) \mid q(x) \in F[x]\}.$$

4.1.11. Théorème. Soit $p(x) \in F[x]$. L'anneau quotient

$$\bar{F} := F[x]/ < p(x) >= \{\overline{f(x)} \mid f(x) \in F[x]\}$$

est un corps si, et seulement si, $p(x)$ est irréductible sur F. Dans ce cas, en identifiant $a \in F$ avec $\bar{a} \in \bar{F}$, on voit que F est un sous-corps de $\bar{F}$.

Démonstration. Si $p(x)$ est réductible sur F, alors $p(x) = g(x)h(x)$, où $g(x), h(x) \in F[x]$ avec $0 < \partial(g(x)), \partial(h(x)) < \partial(p(x))$. Donc $\overline{g(x)}, \overline{h(x)} \in \bar{F}$ sont tous non nuls tels que

$$\overline{g(x)} \cdot \overline{h(x)} = \overline{g(x)h(x)} = \overline{p(x)} = \bar{0}.$$

D'où, $\bar{F}$ n'est pas un corps.

Supposons maintenant que $p(x)$ est irrédutctible sur F. Comme $p(x)$ est non constant, $F[x] \neq < p(x) >$. Ainsi, $\bar{F}$ est non nul. Si $\overline{f(x)} \in \bar{F}$ est non nul, alors $p(x) \not| f(x)$. Donc, $f(x)$ est co-premier à $p(x)$. D'après le théorème de Bézout-Bachet, il existe $g(x), h(x) \in F[x]$ tels que

$$f(x)g(x) + p(x)h(x) = 1.$$

D'où, $\overline{f(x)} \cdot \overline{g(x)} = \overline{f(x)g(x)} = \bar{1}$, c'est-à-dire, $\overline{f(x)}$ est inversible. Ceci montre que $\bar{F}$ est un corps. La preuve du théorème s'achève.

Exemple. On a vu que $p(x) = x^2 - 2$ est irréductible sur $\mathbb{Q}$. Ainsi

$$\bar{\mathbb{Q}} := \mathbb{Q}[x]/ < p >= \{\overline{f(x)} \mid f(x) \in \mathbb{Q}[x]\}$$

est un corps. Trouver l'inverse de $\overline{x^3}$.

On étudiera l'irréductibité de polynômes rationnels. On commence par la notion suivante.

4.1.12. Définition. Un polynôme non nul sur $\mathbb{Z}$ est dit *primitif* si le plus grand commun facteur de ses coefficients est 1.

Remarque. Si $f(x) \in \mathbb{Q}[x]$, alors il existe $\alpha \in \mathbb{Q}$ et un polynôme primitif $g(x) \in \mathbb{Z}[x]$ tels que $f(x) = \alpha g(x)$.

4.1.13. Lemme. Si $f(x), g(x) \in \mathbb{Z}[x]$ sont primitifs, alors $f(x)g(x)$ est primitif.
Démonstration. Posons $f(x) = \sum_{i=0}^{n} a_i x^i$ et $g(x) = \sum_{j=0}^{m} b_j x^j$. Alors

$$f(x)g(x) = \sum_{k=0}^{n+m} c_k x^k; \text{ où } c_k = \sum_{i+j=k} a_i b_j.$$

Si $f(x)g(x)$ n'est pas primitif, alors il existe un nombre premier p tel que $p \,|\, c_k$, pour tout $0 \leq k \leq n+m$. Comme $f(x), g(x)$ sont primitifs, il existe un indice minimal $r \geq 0$ tel que $p \nmid a_r$ et un indice minimal $s \geq 0$ tel que $p \nmid b_s$. En particulier, $p \,|\, \not{a}_r b_s$. Si $r + s = 0$, alors $r = s = 0$. Donc $p \nmid a_0 b_0 = c_0$, une contradiction. Si $r + s > 0$, alors

$$c_{r+s} = \sum_{i+j=r+s} a_i b_j = a_r b_s + \sum_{i+j=r+s,\ (i,j)\neq(r,s)} a_i b_j.$$

Remarquons que si $i + j = r + s$ et $(i, j) \neq (r, s)$, alors $i < r$ ou $j < s$, et donc $p \,|\, a_i b_j$. On en déduit que $p \nmid c_{r+s}$, une contradiction. Donc $f(x)g(x)$ est primitif. Ceci achève la démonstration du lemme.

4.1.14. Théorème de Gauss. Si $f(x) \in \mathbb{Z}[x]$ est non constant, alors $f(x)$ est irréductible sur $\mathbb{Q}$ si, et seulement si, $f(x)$ est irréductible sur $\mathbb{Z}$.

Démonstration. Il suffit de montrer la suffisance. Supposons que $f(x)$ est réductible sur $\mathbb{Q}$. Alors $f(x) = g(x)h(x)$, où $g(x), h(x) \in \mathbb{Q}[x]$ non constants. Écrivons $g(x) = \alpha g_1(x)$ et $h(x) = \beta h_1(x)$, où $\alpha, \beta \in \mathbb{Q}$ et $g_1(x), h_1(x) \in \mathbb{Z}[x]$ sont primitifs. Donc $f(x) = \gamma g_1(x)h_1(x)$, où $\gamma = \alpha\beta \in \mathbb{Q}$ et $g_1(x)h_1(x) \in \mathbb{Z}[x]$ est primitif d'après le lemme 4.1.13. Posons

$$g_1(x)h_1(x) = a_1 + a_1 x + \cdots + a_n x^n;\ a_i \in \mathbb{Z}.$$

Alors $\gamma a_i \in \mathbb{Z}$, pour tout $0 \leq i \leq n$, car $f(x) \in \mathbb{Z}[x]$. En outre, comme le plus grand commun facteur de $a_0, a_1, \ldots, a_n$ est 1, il existe $s_i \in \mathbb{Z}$ tels $\sum_{i=0}^{n} a_i s_i = 1$. Ceci nous donne

$$\gamma = \gamma \left(\sum_{i=0}^{n} a_i s_i \right) = \sum_{i=0}^{n} (\gamma a_i) s_i \in \mathbb{Z}.$$

Par conséquent, $f(x) = (\gamma g_1(x))h_1(x)$ est réductible sur $\mathbb{Z}$. Ceci achève la démonstration du théorème.

Le résultat suivant est un critère très pratique pour qu'un polynôme rationnel soit irréductible sur $\mathbb{Q}$.

4.1.15. Critère d'Eisenstein. Soit un polynôme non constant

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x].$$

Alors $f(x)$ est irréductible sur $\mathbb{Q}$ s'il existe un nombre premier p tel que

(1) $p \mid a_i$, $i = 0, 1, \ldots, n-1$, et $p \nmid a_n$;

(2) $p^2 \nmid a_0$.

Démonstration. Supposons que les deux conditions sont vérifiées et que f est réductible sur $\mathbb{Q}$. D'après le théorème de Gauss,

$$f(x) = (b_0 + b_1 x + \cdots + b_r x^r)(c_0 + c_1 x + \cdots + c_s x^s),\ b_i, c_j \in \mathbb{Z}; b_r \neq 0, c_s \neq 0,\ r, s > 0.$$

Comme $b_r c_s \neq 0$, on a $0 < r, s < n$. Comme $p \,|\, a_0 = b_0 c_0$, on a $p \,|\, b_0$ ou $p \,|\, c_0$. On peut supposer $p \,|\, b_0$. Comme $p \nmid a_n = b_r c_s$, on a $p \nmid b_r$. Ainsi il existe un $0 < t \leq r$ tel que $p \,|\, b_i$, pour tout $0 \leq i < t$ et $p \nmid b_t$. Remarquons

$$a_t = \sum_{i+j=t} b_i c_j = b_t c_0 + \sum_{i+j=t,\, i<t} b_i c_j.$$

Comme $t \leq r < n$, on a $p | a_t$ par l'hypothèse et $p | b_i c_j$ pour tout $0 \leq i < t$. Ceci implique $p \,|\, b_t c_0$. Comme $p \nmid b_t$, on a $p \,|\, c_0$. Ainsi $p^2 | b_0 c_0 = a_0$, une contradiction. Donc f est irréductible sur $\mathbb{Q}$. Ceci achève la démonstration du théorème.

Exemple. (1) Si p est un nombre premier et $n > 1$, vérifier que $\sqrt[n]{p}$ est irrationnel.

(2) Vérifier que $f(x) = \frac{2}{9}x^5 + \frac{5}{3}x^4 + x^3 + \frac{1}{3}$ est irréductible sur $\mathbb{Q}$.

4.1.16. Proposition. Soit $f(x) \in \mathbb{Q}[x]$ non constant. Si $a, b \in \mathbb{Q}$ avec a non nul, alors $f(x)$ est irréductible sur $\mathbb{Q}$ si, et seulement si, $g(x) = f(ax + b)$ est irréductible sur $\mathbb{Q}$.

Démonstration. Si $f(x) = f_1(x) f_2(x)$, où $f_1(x), f_2(x) \in \mathbb{Q}[x]$ avec $\partial(f_1(x)),\ \partial(f_2(x)) > 0$, alors

$$g(x) = f(ax + b) = f_2(ax + b) f_2(ax + b) = g_1(x) g_2(x),$$

où $g_i(x) = f_i(ax+b) \in \mathbb{Q}[x]$. Comme $a \neq 0$, on a $\partial(g_i(x)) = \partial(f_i(x)) > 0$. Ainsi $g(x)$ est réductible sur $\mathbb{Q}$. D'autre part, si $g(x)$ est réductible sur $\mathbb{Q}$, alors $f(x) = g(\frac{1}{a}x - \frac{b}{a})$ est réductible sur $\mathbb{Q}$. Ceci achève la démonstration de la proposition.

Exemple. Vérifier que $f(x) = x^3 - \frac{3}{4}x - \frac{1}{8}$ est irréductible sur $\mathbb{Q}$.

4.2 Extensions de corps

4.2.1. Définition. Soit E un corps. Un sous-ensemble F de E s'appelle *sous-corps* de E si les conditions suivantes sont vérifiées:

(1) $1_E \in F$, et

(2) $a - b, ab^{-1}(b \neq 0) \in F$ pour tous $a, b \in F$.

Dans ce cas, F est un corps et on appelle $E : F$ une *extension de corps*.

Exemple. (1) Si F est un sous-corps de $\mathbb{C}$, alors $\mathbb{Q} \subseteq F$.

(2) $\mathbb{R} : \mathbb{Q}$ et $\mathbb{C} : \mathbb{R}$ sont des extensions de corps.

Si $E : F$ est une extension de corps, on voit aisément que E est un espace vectoriel sur F, noté ${}_FE$, pour l'addition de E et la multiplication externe

$$\bullet : F \times E \to E : (a, \alpha) \mapsto a\alpha$$

induite de la multiplication de E.

4.2.2. Définition. Le *degré* d'une extension de corps $E : F$, notée $[E : F]$, est défini comme étant la dimension de l'espace vectoriel ${}_FE$.

Exemple. L'extension de corps $\mathbb{C} : \mathbb{R}$ est de degré deux.

4.2.3. Lemme. Soit $E : F$ une extension de corps. Alors $[E : F] = 1$ si, et seulement si, $E = F$.

Démonstration. Si $E = F$, alors $\{1_F\}$ est une base de ${}_FE$, et donc, $[E : F] = 1$. Supposons réciproquement $[E : F] = 1$. Prenons $\{\alpha\}$ une base de E sur F. Alors il existe $a \in F$ tel que $1 = a\alpha$. Donc a est non nul et $\alpha = a^{-1} \in F$ car F est un sous-corps de E. Or, pour tout $\beta \in E$, il existe $b \in F$ tel que $\beta = b\alpha$. Ainsi $\beta \in F$. Ceci donne $E \subseteq F$, et donc $E = F$. La preuve du lemme s'achève.

4.2.4. Définition. Une extension de corps $E : F$ est dite *finie* ou *infinie* si $[E : F]$ est fini ou infini, respectivement. On dit aussi que E est *fini* ou *infini* sur F, respectivement.

Exemple. $\mathbb{C}$ est fini sur $\mathbb{R}$.

4.2.5. Théorème. Soient $F \subseteq L \subseteq E$ des corps. Alors $E : F$ est finie si, et seulement si, $E : L$ et $L : F$ sont toutes finies; et dans ce cas, $[E : F] = [E : L][L : F]$.

Démonstration. Supposons premièrement que $[E : F] = n$, c'est-à-dire, $\dim_F E = n$. Comme L est un sous-espace de E, on a $[L : F] = \dim_F L \leq n$. En outre, prenons une base $\{\alpha_1, \ldots, \alpha_n\}$ de E sur F. Pour tout $\alpha \in E, \alpha = a_1\alpha_1 + \cdots + a_n\alpha_n$ avec $a_i \in F \subseteq L$. Donc le L-espace vectoriel E est engendré par $\alpha_1, \ldots, \alpha_n$. Par conséquent, $[E : L] = \dim_L E \leq n$.

Supposons maintenant que $[E : L] = r$ et $[L : F] = s$, c'est-à-dire, $\dim_L E = r$ et $\dim_F L = s$. Prenons une base $\{\beta_1, \ldots, \beta_r\}$ de E sur L et une base $\{\gamma_1, \ldots, \gamma_s\}$ de L sur F. On prétend que $\mathcal{B} = \{\beta_i\gamma_j \,|\, 1 \leq i \leq r, 1 \leq j \leq s\}$ est une F-base de E.

D'abord, soit $\alpha \in E$. Alors $\alpha = \sum_{i=1}^{r} b_i\beta_i$ avec $b_i \in L$. Or $b_i = \sum_{j=1}^{s} c_{ij}\gamma_j$ avec $c_{ij} \in F$, pour $i = 1, \ldots, r$. Ainsi $\alpha = \sum_{i,j} c_{ij}\beta_i\gamma_j, c_{ij} \in F$. Ainsi le F-espace E est engendré par $\mathcal{B}$.

Enfin, supposons que $\sum_{i,j} a_{ij}\beta_i\gamma_j = 0$, où $a_{ij} \in F$. Alors $\sum_{i=1}^{r}(\sum_{j=1}^{s} a_{ij}\gamma_j)\beta_i = 0$ avec $\sum_{j=1}^{s} a_{ij}\gamma_j \in L$. Comme les β_i sont linéairement indépendants sur L, on a $\sum_{j=1}^{s} a_{ij}\gamma_j = 0$, pour $i = 1, \ldots, r$. Comme les γ_j sont linéairement indépendants sur F, on a $a_{ij} = 0$, pour tous $1 \leq j \leq s; 1 \leq i \leq r$. Donc $\mathcal{B}$ est F-libre, et donc, $\mathcal{B}$ est une F-base de E. Par conséquent, $[E : F] = rs = [E : L][L : F]$. Ceci achève la démonstration du théorème.

4.2.6. Définition. Soit $E : F$ une extension de corps. On dit $\alpha \in E$ *algébrique sur* F s'il est une racine d'un polynôme non nul sur F; et *transcendant sur* F sinon.

En outre, l'extension $E : F$ est dite *algébrique* (ou bien, E est dit *algébrique sur* F) si tout élément de E est algébrique sur F.

Exemple. (1) Tout $a \in F$ est algébrique sur F. Par conséquent, $F : F$ est algébrique.

(2) L'extension $\mathbb{C} : \mathbb{R}$ est algébrique.

(3) Le nombre réel $\alpha = \sqrt[3]{2 + 3\sqrt{5}}$ est algébrique sur $\mathbb{Q}$.

On accepte le résultat célèbre suivant sans preuve.

4.2.7. Théorème de Lindemann. Le nombre réel π est transcendant sur $\mathbb{Q}$.

Exemple. L'extension $\mathbb{R} : \mathbb{Q}$ n'est pas algébrique.

4.2.8. Lemme. Soit $E : F$ une extension de corps. Si $\alpha \in E$, alors α est algébrique sur F si, et seulement si, il existe $n > 0$ tel que $\{1, \alpha, \ldots, \alpha^n\}$ est liée sur F.

Démonstration. Par définition, α est algébrique sur F si et seulement si, il existe $f(x) = a_0 + a_1x + \cdots + a_nx^n \in F[x]$ non nul (c'est-à-dire, $a_0, a_1, \ldots, a_n \in F$ non tous nuls) tel que

$$0 = f(\alpha) = a_0 + a_1\alpha + \cdots + a_n\alpha^n = a_0 \cdot 1 + a_1 \cdot \alpha + \cdots + a_n \cdot \alpha_n,$$

c'est-à-dire, $\{1, \alpha, \ldots, \alpha^n\}$ est liée sur F. Ceci achève la démonstration du lemme.

Exemple. $\mathbb{R} : \mathbb{Q}$ est une extension infinie de corps.

4.2.9. Proposition. Toute extension finie de corps est algébrique.

Démonstration. Soit $[E : F] = n < \infty$, c'est-à-dire, le F-espace vectoriel E est de dimension n. Donc, pour tout $\alpha \in E$, la famille $\{1, \alpha, \ldots, \alpha^n\}$ est liée sur F. D'après le lemme 4.2.8, α est algébrique sur F. Ceci achève la démonstration.

4.3 Extensions simples

Partout dans cette section, on se fixe $E : F$ une extension de corps.

4.3.1. Définition. Si $S \subseteq E$, alors le plus petit sous-corps de E contenant F et S, noté $F(S)$, s'appelle le sous-corps de E *engendré par* S *sur* F.

Remarque. Si $S \subseteq F$, alors $F(S) = F$.

Exemple. Montrer que $\mathbb{R}(\sqrt{-1}) = \mathbb{C}$.

4.3.2. Lemme. Si S_1, S_2 sont des sous-ensembles de E, alors

$$F(S_1 \cup S_2) = F(S_1)(S_2) = F(S_2)(S_1).$$

Démonstration. Comme $S_1 \subseteq S_1 \cup S_2$, on a $F(S_1) \subseteq F(S_1 \cup S_2)$. Comme $S_2 \subseteq F(S_1 \cup S_2)$, on a $F(S_1)(S_2) \subseteq F(S_1 \cup S_2)$. D'autre part, $F(S_1)(S_2)$ contient F et $S_1 \cup S_2$. Cela implique $F(S_1 \cup S_2) \subseteq F(S_1)(S_2)$. Par conséquent, $F(S_1 \cup S_2) = F(S_1)(S_2)$. La preuve du lemme s'achève.

Remarque. Si $\alpha_1, \alpha_2, \ldots, \alpha_n \in E$, alors $F(\alpha_1, \alpha_2, \ldots, \alpha_n) = F(\alpha_1)(\alpha_2) \cdots (\alpha_n)$.

4.3.3. Définition. On dit que $E : F$ est une *extension simple*, ou bien E est simple sur F, si $E = F(\alpha)$, pour un certain $\alpha \in E$.

Exemple. Comme $\mathbb{C} = \mathbb{R}(\sqrt{-1})$, on voit que $\mathbb{C} : \mathbb{R}$ est une extension simple.

Exemple. Montrer que l'extension $\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}$ est simple.

4.3.4. Définition. Soit $\alpha \in E$ algébrique sur F. Un polynôme non-constant $m(x) \in F[x]$ s'appelle *polynôme minimal* de α sur F si les conditions suivantes sont vérifiées:

(1) $m(x)$ est monique.

(2) $m(\alpha) = 0$.

(3) Si $f(x) \in F[x]$ est non-constant avec $f(\alpha) = 0$, alors $\partial(m(x)) \leq \partial(f(x))$.

Exemple. Si $a \in F$, alors $x - a$ est un polynôme minimal de a sur F.

Exemple. Vérifier que $\sqrt{2} \in \mathbb{R}$ est algébrique sur $\mathbb{Q}$, et donner son polynôme minimal sur $\mathbb{Q}$.

4.3.5. Lemme. Soit $\alpha \in E$ algébrique sur F dont $m(x)$ est un polynôme minimal.

(1) $m(x)$ est irréductible sur F.

(2) Si $f(x) \in F[x]$, alors $f(\alpha) = 0$ si, et seulement si, $m(x) \mid f(x)$.

Démonstratio. (1) Supposons au contraire que $m(x) = m_1(x)m_2(x)$ avec $m_i(x) \in F[x]$ et $0 < \partial(m_i(x)) < \partial(m(x))$. Comme $0 = m(\alpha) = m_1(\alpha)m_2(\alpha)$, on a $m_1(\alpha) = 0$ ou $m_2(\alpha) = 0$. Ceci contredit la minimalité de $\partial(m(x))$. Donc $m(x)$ est irréductible sur F.

(2) Pour tout $f(x) \in F[x]$, on a $f(x) = m(x)q(x) + r(x)$, où $q(x), r(x) \in F[x]$ avec $\partial(r(x)) < \partial(m(x))$. Si $m(x) \mid f(x)$, alors $r(x) = 0$, et donc, $f(x) = m(x)q(x)$. Ainsi $f(\alpha) = m(\alpha)q(\alpha) = 0$. Supposons réciproquement que $f(\alpha) = 0$. Comme $m(\alpha) = 0$, on a $r(\alpha) = 0$. Il suit de la minimalité de $\partial(m(x))$ que $r(x) = 0$, et donc $m(x) \mid f(x)$. Ceci achève la démonstration.

4.3.6. Corollaire. Soit $\alpha \in E$ algébrique sur F.

(1) α admet un seul polynôme minimal sur F, noté $m_F^\alpha(x)$.

(2) Si $p(x) \in F[x]$ est irréductible monique tel que $p(\alpha) = 0$, alors $m_F^\alpha(x) = p(x)$.

Démonstration. (1) Soient $m_1(x), m_2(x)$ des polynômes minimaux de α sur F. D'après le lemme 4.3.5(2), $m_1(x) | m_2(x)$ et $m_2(x) | m_1(x)$. D'où, $m_1(x) = am_2(x)$ avec $a \in F$. Comme $m_1(x), m_2(x)$ sont tous moniques, on a $a = 1$, c'est-à-dire, $m_1(x) = m_2(x)$.

(2) Supposons que $p(\alpha) = 0$. D'après le lemme 4.3.5(2), $m_F^\alpha(x) | p(x)$. Comme $p(x)$ est irréductible sur F, on a $p(x) = b\, m_F^\alpha(x)$ avec $b \in F$. Comme $p(x), m_F^\alpha(x)$ sont moniques, $b = 1$, et donc $m_F^\alpha(x) = p(x)$. Ceci achève la démonstration du corollaire.

Exemple. Considérons $\alpha = \sqrt{1 - \sqrt{2}} \in \mathbb{C}$. Trouver le polynôme minimal de α sur $\mathbb{Q}$.

4.3.7. Définition. Soit $\alpha \in E$ algébrique sur F. On définit le *degré* de α sur F par

$$\partial_F(\alpha) = \partial(m_F^\alpha(x)).$$

Exemple. Si p est un entier premier et $n > 0$, alors $\partial_{\mathbb{Q}}(\sqrt[n]{p}) = n$. En effet, d'après le critère d'Eisenstein, $x^n - p$ est irréductible sur $\mathbb{Q}$, dont $\sqrt[n]{p}$ est une racine. D'après le corollaire 4.3.6(2), $m_{\mathbb{Q}}^{\sqrt[n]{p}}(x) = x^n - p$. D'où, $\partial_{\mathbb{Q}}(\sqrt[n]{p}) = n$.

Exemple. Soit $\alpha = \sqrt{1-\sqrt{2}} \in \mathbb{C}$. Vérifier que α est algébrique de degré 4 sur $\mathbb{Q}$.

4.3.8. Théorème. Soit $E = F(\alpha)$ une extension simple de F. Si α est algébrique de degré n sur F, alors $\{1, \alpha, \ldots, \alpha^{n-1}\}$ est une base de ${}_FE$. En particulier,

(1) $[F(\alpha) : F] = \partial_F(\alpha)$; et

(2) $E = \{r(\alpha) \mid r(x) \in F[x] \text{ avec } \partial(r(x)) < n\}$.

Démonstration. Supposons que $\alpha \in E$ est algébrique sur F avec $\partial(m_F^\alpha(x)) = n$. On voit aisément que l'ensemble

$$F[\alpha] = \{f(\alpha) \mid f \in F[x]\}$$

est un sous-anneau de E contenant F et α. Comme $F(\alpha)$ est un sous-corps de E contenant F et α, on voit que $F[\alpha] \subseteq F(\alpha)$. Considérons le homomorphisme d'anneaux suivant:

$$\rho : F[x] \to F[\alpha] : f(x) \mapsto f(\alpha).$$

Pour tout $f(x) \in F[x]$, on a $f(x) \in \mathrm{Ker}(\rho)$ si, et seulement si, $f(\alpha) = 0$ si, et seulement si, $m_F^\alpha(x) \mid f(x)$. Par conséquent, $\mathrm{Ker}(\rho) =< m_F^\alpha(x) >$. Comme ρ est surjectif, d'après le théorème 1.2.11(3), $F[\alpha] \cong F[x]/ < m_\alpha^F(x) >$. Comme $m_\alpha^F(x)$ est irréductible sur F, d'après le lemme 4.3.5(1), $F[x]/ < m_F^\alpha(x) >$ est un corps. Par conséquent, $F[\alpha]$ est un sous-corps de E contenant F et α. Par définition, $E = F(\alpha) \subseteq F[\alpha]$. D'où, $E = F[\alpha]$.

Si $\beta \in E$ alors, $\beta = f(\alpha)$ avec $f(x) \in F[x]$. Maintenant, $f(x) = m_F^\alpha(x)q(x) + r(x)$, où $q(x), r(x) \in F[x]$ avec $\partial(r(x)) < n$. Écrivant $r(x) = b_0 + b_1x + \cdots + b_{n-1}x^{n-1}$, où $b_i \in F$, on obtient

$$\beta = f(\alpha) = m_F^\alpha(\alpha)q(\alpha) + r(\alpha) = b_0 \cdot 1 + b_1 \cdot \alpha + \cdots + b_{n-1} \cdot \alpha^{n-1}.$$

Donc, le F-espace vectoriel E est engendré par $1, \alpha, \ldots, \alpha^{n-1}$. Si $a_0, a_1, \ldots, a_{n-1} \in F$ sont non tous nuls alors, d'après la minimalité de $\partial(m_F^\alpha(x))$, on voit que α n'est pas racine de $a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$, c'est-à-dire,

$$a_0 \cdot 1 + a_1 \cdot \alpha + \cdots + a_{n-1} \cdot \alpha^{n-1} \neq 0.$$

Donc $\{1, \alpha, \ldots, \alpha^{n-1}\}$ est libre sur F, et donc, une F-base de E. La preuve du théorème s'achève.

Exemple. Considérons $\alpha = -\frac{1}{2} + \frac{\sqrt{-3}}{2} \in \mathbb{C}$. Vérifier que $\mathbb{Q}(\alpha) = \{a + b\alpha \mid a, b \in \mathbb{Q}\}$, et calculer $(\alpha + 4)^{-1}$.

Exemple. Soit $\alpha = \sqrt{1-\sqrt{2}} \in \mathbb{C}$. Trouver le polynôme minimal de α sur $\mathbb{Q}(\sqrt{2})$.

En appliquant le théorème 4.3.8 et la proposition 4.2.9, on obtient le résultat suivant.

4.3.9. Corollaire. Si $\alpha \in E$, alors les conditions suivantes sont équivalentes.

(1) α est algébrique sur F.

(2) $[F(\alpha) : F]$ est fini.

(3) $F(\alpha)$ est algébrique sur F.

Démonstration. En vertu du théorème 4.3.8, l'énoncé (1) implique l'énoncé (2); et d'après la proposition 4.2.9, l'énoncé (2) implique l'énoncé (3). Enfin, il est trivial que l'énoncé (3) implique l'énoncé (1). Ceci achève la preuve du corollaire.

4.3.10. Théorème. L'extension $E : F$ est finie si, et seulement si, $E = F(\alpha_1, \ldots, \alpha_s)$ avec $\alpha_1, \ldots, \alpha_s$ algébriques sur F. Dans ce cas,

$$E = \{f(\alpha_1, \cdots, \alpha_s) \mid f \in F[x_1, \ldots, x_s], \partial_{x_i}(f) < \partial_F(\alpha_i)\}.$$

Démonstration. Supposons que $[E : F] = n$. Prenons une base $\{\alpha_1, \ldots, \alpha_n\}$ de E sur F. Alors tout $\beta \in E$ s'écrit comme $\beta = a_1\alpha_1 + \cdots + a_n\alpha_n$ avec $a_i \in F$. En particulier, $\beta \in F(\alpha_1, \ldots, \alpha_n)$. Ceci montre que $E = F(\alpha_1, \ldots, \alpha_n)$. D'après la proposition 4.2.9, les α_i sont algébriques sur F.

Supposons récipquement que $E = F(\alpha_1, \ldots, \alpha_s)$ avec $\alpha_1, \ldots, \alpha_s$ algébriques sur F. Si $s = 1$, d'après le théorème 4.3.8, le résultat est valide. Supposons que $s > 1$ et le résultat est valide pour $F(\alpha_1, \ldots, \alpha_{s-1})$. En particulier, $[F(\alpha_1, \ldots, \alpha_{s-1}) : F]$ est finie. Or, étant algébrique sur F, l'élément α_s est algérique sur $F(\alpha_1, \ldots, \alpha_{s-1})$ de degré $t \leq \partial_F(\alpha_s)$. Donc $E = F(\alpha_1, \ldots, \alpha_{s-1})(\alpha_s)$ est fini sur $F(\alpha_1, \ldots, \alpha_{s-1})$. En vertu du théorème 4.2.5, E est fini sur F.

En outre, d'après le théorème 4.3.8, tout $\beta \in E$ s'écrit $\beta = \beta_0 + \beta_1\alpha_s + \cdots + \beta_{t-1}\alpha_s^{t-1}$, où $\beta_0, \beta_1, \ldots, \beta_{t-1} \in F(\alpha_1, \ldots, \alpha_{s-1})$. Pour tout $1 \leq i \leq t-1$, par l'hypothèse de récurrence, $\beta_i = g_i(\alpha_1, \ldots, \alpha_{s-1})$, où $g_i \in F[x_1, \ldots, x_{s-1}]$ avec $\partial_{x_j}(g_i) < \partial_F(\alpha_j)$, pour $j = 0, \ldots, s-1$. Maintenant

$$f(x_1, \ldots, x_{s-1}, x_s) = g_0 + g_1x_s + \cdots + g_{t-1}x_s^{t-1} \in F[x_1, \ldots, x_{s-1}, x_s]$$

est tel que $\beta = f(\alpha_1, \ldots, \alpha_s)$ et $\partial_{x_j}(\alpha_j) < \partial_F(\alpha_j)$, pour $j = 1, \ldots, s$. Ceci achève la démonstration du théorème.

Exemple. Donner une $\mathbb{Q}$-base de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

4.4 Construction géométrique

Posons $\mathcal{P}_0 = \{(0,0), (1,0)\}$, un ensemble de deux points du plan $\mathbb{R}^2$. Supposons que l'ensemble $\mathcal{P}_n$ de points du plan est défini pour un certain entier $n \geq 0$. Désignons par $\mathcal{D}_n$ l'ensemble des droites passant par deux points distincts de $\mathcal{P}_n$; et par $\mathcal{C}_n$ l'ensemble des

cercles de centre d'un point de $\mathcal{P}_n$ et de rayon la distance entre deux points de $\mathcal{P}_n$. On définit alors $\mathcal{P}_{n+1}$ comme étant la réunion de $\mathcal{P}_n$ et l'ensemble des points p, qui est le point

(1) d'intersection de deux droites distinctes de $\mathcal{D}_n$; ou

(2) d'intersection de deux cercles distincts de $\mathcal{C}_n$; ou

(3) d'intersection d'une droite de $\mathcal{D}_n$ et d'un cercle de $\mathcal{C}_n$.

Ceci donne une suite infinie croissante d'ensembles de points de $\mathbb{R}^2$ suivante:

$$\mathcal{P}_0 \subseteq \mathcal{P}_1 \subseteq \cdots \subseteq \mathcal{P}_n \subseteq \cdots$$

Exemple. Trouver les ponts de $\mathcal{P}_1$.

Démonstration. Comme $\mathcal{P}_0 = \{(0,0),(1,0)\}$, on voit que $\mathcal{P}_0$ se compose d'une seule droite D_x, l'axe des x; et $\mathcal{C}_0$ se compose de deux cercles C_1, C_2 de rayon 1 dont les centers sont $(0,0)$ et $(1,0)$ respectivement. On voit aisément que $D_x \cap C_1 = \{(-1,0),(1,0)\}$ et $D_x \cap C_2 = \{(0,0),(2,0)\}$. Enfin, si $(x,y) \in C_1 \cap C_2$, alors $x^2+y^2 = 1$ et $(x-1)^2+y^2 = 1$. D'où, $x = \frac{1}{2}$, et par conséquent, $y = \pm\frac{\sqrt{3}}{2}$. Donc $C_1 \cap C_2 = \{(\frac{1}{2}, \frac{\sqrt{3}}{2}), (\frac{1}{2}, -\frac{\sqrt{3}}{2})\}$. Par conséquent,

$$\mathcal{P}_1 = \mathcal{P}_1 \cup (D_x \cap C_1) \cup (D_x \cap C_2) \cup (C_1 \cap C_2) = \{(0,0),(1,0),(-1,0),(2,0),(\tfrac{1}{2}, \tfrac{\sqrt{3}}{2}),(\tfrac{1}{2}, -\tfrac{\sqrt{3}}{2})\}.$$

4.4.1. Définition. (1) Un point du plan est dit *constructible* s'il appartient à $\cup_{n=0}^{\infty} \mathcal{P}_n$.

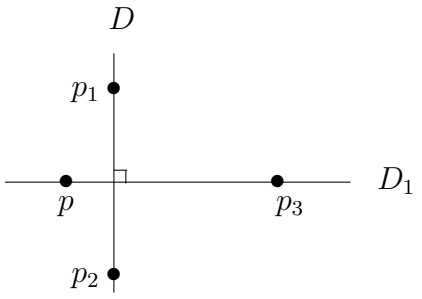
(2) Une droite du plan est dite *constructible* si elle appartient à $\cup_{n=0}^{\infty} \mathcal{D}_n$.

(3) Un cercle du plan est dit *constructible* s'il appartient à $\cup_{n=0}^{\infty} \mathcal{C}_n$.

Remarque. Un point d'intersection de deux droites constructibles distinctes (respectivement, de deux cercles constructibles distincts, ou d'une droite constructible et d'un cercle constructible) est constructible.

4.4.2. Lemme. Soit p un point constructible. Si D est une droite constructible, alors la perpendiculaire, ainsi que la parallèle, à D passant par p est constructible.

Démonstration. Par définition, D contient un point constructible p_1 avec $p_1 \neq p$. Or $p, p_1 \in \mathcal{P}_n$, pour un certain $n \geq 1$. Désignons par p_2 le point d'intersection de D et le cercle de centre p et de rayon $\overline{pp_1}$, qui est différent de p_1. Remarquons que $p_2 \in \mathcal{P}_{n+1}$. Prenons p_3 un point d'intersection des cercles de rayon $\overline{p_1p_2}$ et de centre p_1 et de centre p_2, respectivement. Alors $p_3 \in \mathcal{P}_{n+2}$. Soit D_1 la droite passant par p et p_3.



Alors D_1 est perpendiculaire à D et appartient à $\mathcal{D}_{n+2}$. Enfin, si D_2 est la droite passant par p et parallèlle à D, alors D_2 est perpendiculaire à D_1. Comme D_1 est constructible, D_2 est constructible. La preuve du lemme s'achève.

4.4.3. Définition. Un nombre complexe $z = a + bi$ est dit *constructible* si le point (a, b) est constructible.

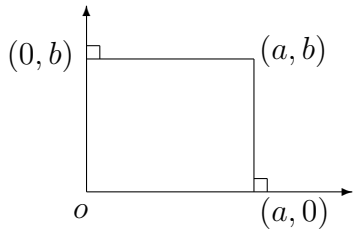
Remarque. Un nombre réel a est constructible si, et seulement si, le point $(a, 0)$ est constructible.

Exemple. Les nombres suivants sont tous constructibles:

$$0, 1, i, \frac{1}{2} + \frac{\sqrt{3}}{2}i, \frac{1}{2} - \frac{\sqrt{3}}{2}i.$$

4.4.4. Lemme. Un nombre complexe $z = a + bi$ est constructible si, et seulement si, a et b sont tous constructibles.

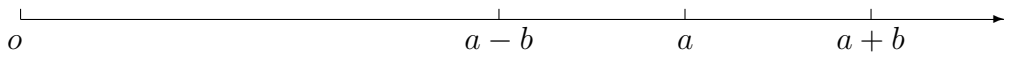
Démonstration. L'énoncé suit immédiatement du diagramme suivant:



La preuve du lemme s'achève.

4.4.5. Lemme. Si $a, b \in \mathbb{R}$ sont constructibles, alors $a \pm b$ sont aussi constructibles.

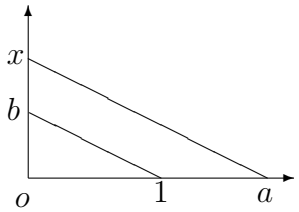
Démonstration. L'énoncé suit immédiatement du diagramme suivant:



La preuve du lemme s'achève.

4.4.6. Lemme. Si $a, b \in \mathbb{R}$ sont constructibles, alors ab est constructible.

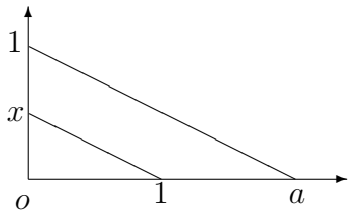
Démonstration. Considérons le diagramme suivant:



où $b1//xa$. Donc $\triangle bo1 \sim \triangle xoa$. Par conséquent, $\frac{x}{b} = \frac{a}{1}$, c'est-à-dire, $x = ab$. La preuve du lemme s'achève.

4.4.7. Lemme. Si $0 \neq a \in \mathbb{R}$ est constructible, alors a^{-1} est constructible.

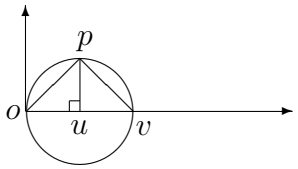
Démonstration. Considérons le diagramme suivant:



où $x1//1a$. Donc $\triangle xo1 \sim \triangle 1oa$. Par conséquent, $\frac{1}{a} = \frac{x}{1} = x$. La preuve du lemme s'achève.

4.4.8. Lemme. Si $a \in \mathbb{R}^+$ est constructible, alors $\sqrt{a}$ est constructible.

Démonstration. Considérons le diagramme suivant:



où $u = (1, 0)$, $v = (1 + a, 0)$, et $p = (1, x)$. Comme $\triangle oup \sim \triangle puv$, on a $\frac{x}{a} = \frac{1}{x}$, c'est-à-dire, $x = \sqrt{a}$. Ceci achève la démonstration du lemme.

Remarque. En vue des lemmes 4.4.5, 4.4.6 et 4.4.8, on voit que la distance entre deux points constructibles est un nombre constructible.

4.4.9. Théorème. L'ensemble des nombres complexes constructibles est le plus petit sous-corps de $\mathbb{C}$, qui est stable pour l'extraction de racines carrées et pour la conjugaison.

Démonstration. En vertu des lemmes 4.4.4, 4.4.5, 4.4.6, 4.4.7 et 4.4.8, les nombres complexes constructibles forment un sous-corps de $\mathbb{C}$ qui est stable pour l'extraction de racines carrées et pour la conjugaison.

Supposons que E est un sous-corps de $\mathbb{C}$ qui est stable pour l'extraction de racines carrées et pour la conjugaison. Alors $\mathbb{Q} \subseteq E$, et donc $i = \sqrt{-1} \in E$. Si $a + bi \in E$ avec $a, b \in \mathbb{R}$, comme $a - bi \in E$, on a $a \in E$, et donc $b \in E$. Ceci montre que $a + bi \in E$ si et seulement si $a, b \in E$. En outre, si $\alpha, \beta, \gamma \in E$ avec $\alpha \neq 0$, comme E est stable pour l'extraction de racines carrées, on voit que les racines du polynôme $\alpha x^2 + \beta x + \gamma = 0$ appartiennent à E.

On se fixe un nombre constructible $z = a + bi$, où $a, b \in \mathbb{R}$. Alors $(a, b) \in \cup_{n \geq 0} \mathcal{P}_n$. Il est évident que si $(a, b) \in \mathcal{P}_0$, alors $z \in E$. Supposons, pour un entier $n > 0$, que si $(a, b) \in \cup_{0 \leq i < n} \mathcal{P}_i$, alors $z \in E$. Remarquons que si $(c_1, d_1), (c_2, d_2) \in \mathcal{P}_{n-1}$, alors la distance

entre (c_1, d_1) et (c_2, d_2) appartient à E, puisque $c_1, c_2, d_1, d_2 \in E$ par l'hypothèse de récurence. Supposons que $(a, b) \notin \mathcal{P}_{n-1}$. Considérons les cas suivants.

(1) Le point (a, b) est le point d'intersection de deux droites L_1 et L_2 de $\mathcal{D}_{n-1}$. Par définition, L_i passe par deux points distincts (a_i, b_i) et (c_i, d_i) de $\mathcal{P}_{n-1}$, et donc,

$$(*) \qquad (a - a_i)(d_i - b_i) = (c_i - a_i)(b - b_i),\ i = 1, 2.$$

En résolvant le système $(*)$ d'équations linéaires, on voit que $a, b \in E$ puisque $a_i, b_i, c_i, d_i \in E$, $i = 1, 2$. Ainsi $z = a + bi \in E$.

(2) Le point (a, b) est le point d'intersection d'une droite L passant par deux points distincts (a_1, b_1) et (a_2, b_2) de $\mathcal{P}_{n-1}$ et d'un cercle de centre $(c_0, d_0) \in \mathcal{P}_{n-1}$ et de rayon r_0, qui est la distance entre deux points de $\mathcal{P}_{n-1}$. Donc

$$\begin{aligned} (a - a_1)(b_2 - b_1) &= (a_2 - a_1)(b - b_1); \\ (a - c_0)^2 + (b - d_0)^2 &= r_0^2. \end{aligned}$$

Comme $a_2 - a_1 \neq 0$ ou $b_2 - b_1 \neq 0$ et $a_i, b_i, c_0, d_0, r_0 \in E$, $i = 1, 2$, on voit que $a, b \in E$. Donc $z = a + bi \in E$.

(3) Le point (a, b) est le point d'intersection deux cercles distincts C_1, C_2 de $\mathcal{C}_n$. Alors C_i est de centre $(a_i, b_i) \in \mathcal{P}_{n-1}$ et de rayons $r_i \in E$, $i = 1, 2$, avec $(a_1, b_1) \neq (a_2, b_2)$. Par définition, $(a - a_i)^2 + (b - b_i)^2 = r_i^2$, $i = 1, 2$. Ceci donne

$$(a_2 - a_1)(2a - (a_1 + a_2)) + (b_2 - b_1)(2b - (b_1 + b_2)) = r_1^2 - r_2^2.$$

Comme $a_2 - a_1 \neq 0$ ou $b_2 - b_1 \neq 0$ et $a_i, b_i, r_i \in E$, $i = 1, 2$, on voit que $a, b \in E$. Par conséquent, $z = a + bi \in E$. Ceci achève la démontsration du théorème.

Remarque. Tous les nombres rationnels sont constructibles.

4.4.10. Théorème. Un nombre complexe z est constructible si, et seulement si, z appartient à un sous-corps $\mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_r)$ de $\mathbb{C}$, où $\alpha_1^2 \in \mathbb{Q}$ et $\alpha_i^2 \in \mathbb{Q}(\alpha_1, \ldots, \alpha_{i-1})$, pour $i = 2, \ldots, r$.

Démonstration. Soit F le corps des nombres constructibles. Posons E l'ensemble des complexes satisfaisant à la condition énoncée dans le théorème. On se fixe $z \in E$, qui appartient à $\mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_r)$, où $\alpha_1^2 \in \mathbb{Q}$ et $\alpha_i^2 \in \mathbb{Q}(\alpha_1, \ldots, \alpha_{i-1})$, pour $i = 2, \ldots, r$.

(1) On prétend que $z \in F$. En effet, d'après le théorème 4.4.9, $\mathbb{Q} \subseteq F$. Comme $\alpha_1^2 = a_1 \in \mathbb{Q}$, on a $\alpha_1 = \sqrt{a_0}$ avec $a_0 \in F$. D'après le théorème 4.4.9, $\alpha_1 \in F$, et donc $\mathbb{Q}(\alpha_1) \in F$. Supposons que $\mathbb{Q}(\alpha_1, \ldots, \alpha_{i-1}) \subseteq F$ avec $1 < i \leq r$. Alors $\alpha_i^2 = a_i \in F$, et en vertu du théorème 4.4.9, $\alpha_i \in F$. Par conséquent, $\mathbb{Q}(\alpha_1, \ldots, \alpha_i) \subseteq F$. Par récurrence, $\mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_r) \subseteq F$. En particulier, $z \in F$.

(2) On prétend que $\bar{z} \in E$. En effet, d'après le théorème 4.3.10, on voit que $\bar{z} \in \mathbb{Q}(\bar{\alpha_1}, \ldots, \bar{\alpha_r})$, où $\bar{\alpha_1}^2 = \alpha_1^2 \in \mathbb{Q}$ et $\bar{\alpha_i}^2 = \overline{\alpha_i^2} \in \mathbb{Q}(\bar{\alpha_1}, \ldots, \bar{\alpha}_{i-1})$, pour $i = 2, \ldots, r$.

(3) On prétend que toute racine carrée β de z appartient à E. En effet, posant $\alpha_{r+1} = \beta$, on voit que $\beta \in \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_r, \alpha_{r+1})$, où $\alpha_1^2 \in \mathbb{Q}$, et $\alpha_i^2 \in \mathbb{Q}(\alpha_1, \ldots, \alpha_{i-1})$, pour $i = 2, \ldots, r, r+1$.

(4) Soit $y \in E$, qui appartient à $\mathbb{Q}(\beta_1, \beta_2, \ldots, \beta_s)$, où $\beta_1^2 \in Q$, et $\beta_j^2 \in \mathbb{Q}(\beta_1, \ldots, \beta_{j-1})$, pour $j = 2, \ldots, s$. Posant $\alpha_{i+j} = \beta_j$, pour$j = 1, \ldots, s$, on obtient

$$y \pm z, yz, yz^{-1} \in \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_{r+s}),$$

où $\alpha_1^2 \in Q$, et $\alpha_i^2 \in \mathbb{Q}(\alpha_1, \ldots, \alpha_{i-1})$, pour $i = 1, \ldots, r+s$. Donc, $y \pm z, yz, yz^{-1} \in E$. Ceci montre que E est un sous-corps de $\mathbb{C}$. D'après les énoncés (2) et (3), E est stable pour l'extraction de racines carrées et pour la conjugaison. D'après le théorème 4.4.9, $F \subseteq E$. En outre, d'après lénoncé (1), $E \subseteq F$. Donc, $E = F$. Ceci achève la démonstration du théorème.

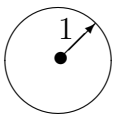
4.4.11. Corollaire. Si $z \in \mathbb{C}$ est constructible, alors $[\mathbb{Q}(z) : \mathbb{Q}] = 2^n$ avec $n \geq 0$.

Démonstration. Supposons que z est constructible. D'après le théorème 4.4.10, z appartient à un sous-corps $\mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_r)$ de $\mathbb{C}$, où $\alpha_1^2 \in \mathbb{Q}$, et $\alpha_i^2 \in \mathbb{Q}(\alpha_1, \ldots, \alpha_{i-1})$, pour $i = 2, \ldots, r$. On voit aisément que $[\mathbb{Q}(\alpha_1, \ldots, \alpha_{i-1}, \alpha_i) : \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_{i-1})] = 1$ ou 2. Donc $[\mathbb{Q}(\alpha_1, \ldots, \alpha_r) : \mathbb{Q}] = 2^s$ avec $0 \leq s \leq r$. Par conséquent, $[\mathbb{Q}(z) : \mathbb{Q}] = 2^n$ avec $0 \leq n \leq s$. Ceci achève la démonstration du corollaire.

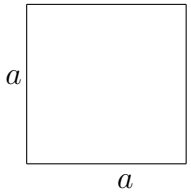
On est maintenant prêt de donner une réponse négative pour chacune des questions posées dans l'introduction de ce chapitre.

4.4.12. Théorème. La quadrature du cercle à la règle et au compas est impossible.

Démonstration. Considérons le cercle de l'unité



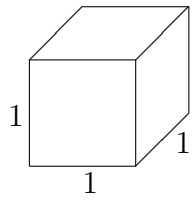
dont l'aire est π. Supposons que l'on peut construire un carré



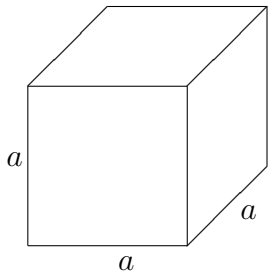
d'aire π, c'est-à-dire, $a^2 = \pi$. Alors $\sqrt{\pi} = a$ est un nombre constructible. D'après le corollaire 4.4.11, $[\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}] = 2^n$ avec $n \geq 0$. Comme $\pi = (\sqrt{\pi})^2 \in \mathbb{Q}(\sqrt{\pi})$, on voit que $\mathbb{Q}(\pi)$ est fini sur $\mathbb{Q}$, ce qui est impossible car π est transcendant sur $\mathbb{Q}$. La preuve du théorème s'achève.

4.4.13. Théorème. La duplication du cube à la règle et au compas est impossible.

Démonstration. Considérons le cube



dont le volume est 1. Supposons que l'on peut construire à la règle et au compas un cube



de volume 2, c'est-à-dire, $a^3 = 2$. Alors $\sqrt[3]{2}$ est un nombre constructible. Remarquons que $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, ce qui contredit le corollaire 4.4.11. La preuve du théorème s'achève.

4.4.14. Lemme. Un angle θ est constructible si et seulement si $\cos\theta$ est un nombre constructible.

Démonstration. On sait que l'axe D_x, le cercle C de l'unité et l'origine $(0, 0)$ sont constructibles. Désigons par D_θ la droite passant par $(0, 0)$ et $p = (\cos\theta, \sin\theta)$.

Supposons que $\cos\theta$ est constructible. D'après le théorème 4.4.9, $\sin\theta = \sqrt{1 + \cos^2\theta}$ est constructible. Ainsi le point p est constructible, et donc la droite D_θ est constructible. Par conséquent, l'angle θ est constructible.

Supposons maintenant que θ est constructible. Alors la droite D_θ est constructible. Étant un point d'intersection de D_θ et le cercle C, le point p est constructible. C'est-à-dire, $\cos\theta + i\sin\theta$ est constructible. En particulier, $\cos\theta$ est constructible. La preuve du lemme s'achève.

4.4.15. Théorème. La trisection de l'angle à la règle et au compas est impossible.

Démonstration. Supposons au contraire que l'on peut triséquer $\frac{\pi}{3}$ 'a la règle et au compas. Alors l'angle $\frac{\pi}{9}$ est constructible. D'après le lemme 4.4.14, $b = \cos\frac{\pi}{9}$ est constructible.

Comme

$$\cos 3\theta = 4\cos^3\theta - 3\cos\theta,$$

on a $4b^3 - 3b = \frac{1}{2}$. Ainsi b est une racine de $x^3 - \frac{3}{4}x - \frac{1}{8}$. On a vu que ce dernier est irréductible sur $\mathbb{Q}$. Ainsi $[\mathbb{Q}(b) : \mathbb{Q}] = 3$, une contradiction au corollaire 4.4.11. Ceci achève la démonstration du théorème.

Exemple. On peut construire à la règle et au compas un triangle équilatéral.

Démonstration. Comme $\cos\frac{2\pi}{3} = -\frac{\sqrt{3}}{2}$ est constructible, l'angle $\frac{2\pi}{3}$ est constructible. En partagent le cercle de l'unité en trois secteurs égaux d'angle $\frac{2\pi}{3}$, on obtient un triangle équilatéral.

Exemple. Il est impossible de construire à la règle et au compas un heptagone régulier.

Démonstration. Si l'on peut construire à la règle et au compas un heptagone régulier, alors l'angle $\frac{2\pi}{7}$ est constructible, et donc le point $(\cos\frac{2\pi}{7}, \sin\frac{2\pi}{7})$ est constructible. C'est-à-dire, le complexe

$$\zeta_7 = \cos\frac{2\pi}{7} + i\sin\frac{2\pi}{7}$$

est constructible. Comme $\zeta_7^7 = 1$ et $\zeta_7 \neq 1$, on voit que ζ_7 est une racine de

$$\Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1,$$

qui est irréductible sur $\mathbb{Q}$. Donc, $m_{\mathbb{Q}}^{\zeta}(x) = \Phi_7(x)$. Par conséquent, $[\mathbb{Q}(\zeta_7) : \mathbb{Q}] = 6$. Ceci contredit le corollaire 4.4.11.

4.5 Exercices

1. Considérer les polynômes rationnels suivants:

$$f(x) = 3x^5 - x^3 + 2x^2 + 1, \quad g(x) = x^3 + x^2 + x - 2.$$

Trouver le quotient et les reste de $f(x)$ par $g(x)$.

2. Considérer les polynômes rationnels suivants:

$$p(x) = x^3 - 7x^2 + 3x + 6;\ f(x) = x^2 - 2x + 1.$$

(1) Vérifier que $\overline{\mathbb{Q}} = \mathbb{Q}[x]/<p(x)>$ est un corps.

(2) Vérifier que $\overline{f(x)}$ est inversible et trouver son inverse dans $\overline{\mathbb{Q}}$.

3. Déterminer les polynômes rationnels suivants sont réductibles ou irréductibles sur $\mathbb{Q}$:

(1) $x^4 + 1$; (2) $x^3 - 7x^2 + 3x + 3$.

4. (1) Si $m = p_1 \cdots p_r$ avec $p_1, \ldots, p_r$ des nombres premiers deux à deux distincts, montrer que $\sqrt{m}$ est irrationnel. *Indice*: Appliquer le critère d'Eisenstein à $x^2 - m$.

   (2) Si $a > 1$ est un entier, montrer que $\sqrt{a}$ est un entier ou un nombre irrationnel. *Indice*: Vérifier que $a = n^2 m$, où n un nombre naturel, et $m = 1$ ou un produit de nombres premiers distincts.

5. Soient m, n des entiers non nuls avec $m \neq 2$. Montrer que $x^3 - mn^2x + n^3$ est irréductible sur $\mathbb{Q}$. *Indice*: Si $a^3 + n^3 = mn^2a$ avec a un entier, à l'aide des décompositions canoniques de a et de n, trouver une contradiction.

6. Si p est un nombre premier, montrer que

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1,$$

   appelé *polynôme cyclotomique*, est irréductible sur $\mathbb{Q}$.

7. Soit $E : F$ une extension de corps. Soient $m(x) \in F[x]$ monique et $\alpha \in E$ tels que $\partial(m(x)) = [F(\alpha) : F]$. Si α est racine de $m(x)$, montrer que $m(x)$ est le polynôme minimal de α sur F.

8. Soient F, L des sous-corps d'un corps E avec $F \subseteq L$. Si $\alpha \in E$ est algébrique sur F, montrer que α est algébrique sur L avec $\partial_L(\alpha) \leq \partial_F(\alpha)$.

9. Trouver le degré de chacune des extensions suivantes:

   (1) $\mathbb{Q}(3, \sqrt{5}, \sqrt{11}) : \mathbb{Q}$; (2) $\mathbb{Q}(\alpha) : \mathbb{Q}$ avec $\alpha \in \mathbb{C}$ tel que $\alpha^7 = 3$.

10. Montrer qu'une extension de corps de degré premier est simple.

11. Considérer le corps $\mathbb{Q}(\alpha)$, où $\alpha = \sqrt{2 + \sqrt{2}}$.

    (1) Trouver le polynôme minimal de α sur $\mathbb{Q}$. *Indice*: Calculer $(\alpha^2 - 2)^2$ et appliquer le critère d'Eisenstein.

    (2) Donner l'inverse de $\alpha^2 + \alpha + 1$. *Indice*: Appliquer l'algorithme d'Euclide au couple $(x^2 + x + 1,\ m_{\mathbb{Q}}^{\alpha}(x))$.

    (3) Déterminer si $\sqrt[3]{2}$ appartient à $\mathbb{Q}(\alpha)$ ou non. *Indice*: Calculer $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]$.

12. Considérer le nombre réel $\alpha = \sqrt{2 + \sqrt[3]{2}}$.

    (1) Trouver le polynôme minimal de α sur $\mathbb{Q}$.

    (2) Donner l'inverse de $\alpha^4 - \alpha^2 + 2\alpha - 1$ dans $\mathbb{Q}(\alpha)$.

(3) Trouver le polynôme minimal de α sur $\mathbb{Q}(\sqrt{2})$. *Indice*:

$$[\mathbb{Q}(\sqrt{2},\alpha):\mathbb{Q}(\sqrt{2})] = [\mathbb{Q}(\sqrt{2},\alpha):\mathbb{Q}(\sqrt{2},\sqrt[3]{2})][\mathbb{Q}(\sqrt{2},\sqrt[3]{2}):\mathbb{Q}(\sqrt{2})].$$

13. Considérer le corps $\mathbb{Q}(\sqrt{5},\sqrt{7})$.
    (1) Trouver le polynôme minimal de $\sqrt{5}$ sur $\mathbb{Q}(\sqrt{7})$. *Indice*: Vérifier que $\sqrt{5} \notin \mathbb{Q}(\sqrt{7})$.
    (2) Donner le degré de l'extension $\mathbb{Q}(\sqrt{5},\sqrt{7}):\mathbb{Q}]$.
    (3) Vérifier que $\mathbb{Q}(\sqrt{5},\sqrt{7}):\mathbb{Q}]$ est une extension simple.

14. Considérer les nombres réels $\alpha = \sqrt{2}$ et $\beta = \sqrt[3]{3}$.
    (1) Vérifier que $\beta \notin \mathbb{Q}(\alpha)$ et $\alpha \notin \mathbb{Q}(\beta)$.
    (2) Trouver le degré $[\mathbb{Q}(\alpha,\beta):\mathbb{Q}]$.
    (3) Vérifier que $\{1,\beta,\beta^2,\alpha,\alpha\beta,\alpha\beta^2\}$ est une $\mathbb{Q}$-base de $\mathbb{Q}(\alpha,\beta)$.
    (4) Montrer que l'extension $\mathbb{Q}(\alpha,\beta):\mathbb{Q}$ est simple.

15. Montrer que $\sqrt{\pi}$ et $\pi^3 + \sqrt{\pi} + 1$ sont transcendants sur $\mathbb{Q}$.

16. Soient $L : F$ et $E : L$ deux extensions algébriques de corps. Montrer que $E : F$ est une extension algébrique.

17. Soit F un sous-corps de $\mathbb{C}$. Si $\alpha \in \mathbb{C}$ avec $[F(\alpha) : F] = 2$, montrer que $F(\alpha) = F(\beta)$ avec $\beta^2 \in F$.

18. Si $\alpha \in \mathbb{C}$ est de degré 2 sur $\mathbb{Q}$, montrer que α est constructible. *Indice*: Considérer le polynôme minimal de α sur $\mathbb{Q}$.

19. Montrer qu'on peut construire un pentagone régulier à la règle et au compas.

20. Déterminer lequel des polygones suivants est constructible à la règle et au compas.
    (1) Décagone régulier (10 côtés).
    (2) Hendécagone régulier (11 côtés).

    Indice: La question est de déterminer si la racine n-ième primitive de l'unité

    $$\zeta_n = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$$

    est constructible ou non. Pour (1), remarquer ζ_{10} est une racine carrée de ζ_5.