MAT 504: Algèbre appliquée

Chapitre I: Arithmétique modulaire et le code ISBN

Le but de ce chapitre est d'appliquer l'arithmétique modulaire 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 Division et nombres premiers

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 $[\alpha] \leq \alpha < [\alpha] + 1$.

Exemple. $[8,75] = 8$ et $[-2,4] = -3$.

1.1.2. Algorithme 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.

Solution. D'abord, en divisant 22 par 6, on obtient $22 = 3 \times 6 + 4$. Donc

$$-22 = (-3) \times 6 - 4 = (-3) \times 6 - 6 + 6 - 4 = (-4) \times 6 + 2.$$

D'où, $q_6(-22) = -4$ et $r_6(-22) = 2$.

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 $\text{pgcd}(a, b) \geq 1$.

1.1.3. Théorème de Bachet-Bézout. Soient a, b deux entiers avec $b > 0$. En posant $r_0 = a$ et $r_1 = b$, on effectue des divisions suivante:

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

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. Posons $d = \text{pgcd}(a, b)$.

(1) 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 (1). En particulier, r_t est un commun diviseur de a et b. D'où, $r_t \leq d$.

(2) On prétend que $r_i = ax_i + by_i$, où $x_i, y_i \in \mathbb{Z}$, pour $i = 0, 1, \ldots, t$. En effet, comme $r_0 = a \cdot 1 + b \cdot 0$ et $r_1 = a \cdot 0 + b \cdot 1$, l'énoncé (2) est valide pour $i = 0, 1$. Supposons que $1 \leq i < t$ et l'énoncé (2) est vrai pour $j = 0, 1, \ldots, i-1, i$. Maintenant,

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

Ceci montre l'énoncé (2). 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 1.1.3 s'appelle *algorithme d'Euclide.*

Exemple. Trouver x, y tels que $196x + 60y = \text{pgcd}(196, 60)$.
Solution. On effectue successivement les divisions suivantes:

$$\begin{array}{rcl} 196 &=& 60 \times 3 \;+\; 16, \qquad (1)\\ 60 &=& 16 \times 3 \;+\; 12, \qquad (2)\\ 16 &=& 12 \times 1 \;+\; 4, \qquad (3)\\ 12 &=& 4 \times 3 \qquad\qquad (4). \end{array}$$

D'où, $\text{pgcd}(196, 60) = 4$. En outre,

$$\begin{array}{rcl} 4 &\overset{(3)}{=}& 16 \times 1 \;+\; 12 \times (-1)\\ &\overset{(2)}{=}& 60 \times (-1) \;+\; 16 \times 4\\ &\overset{(1)}{=}& 196 \times 4 \;+\; 60 \times (-13). \end{array}$$

MAPLE. Pour trouver $d = \text{pgcd}(a, b)$ et résoudre l'équation

$$ax + by = d,$$

en tapant la commande

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

on obtient le résultat

$$\begin{array}{r} d\\ x\\ y \end{array}$$

Exemple. En tapant la commande

$$\text{igcdex}(1004, 15678, x, y); x; y;$$

on obtient

$$\begin{array}{r} 2\\ -203\\ 13 \end{array}$$

C'est-à-dire, $\text{pgcd}(1004, 15678) = 2$ et

$$1004 \times (-203) + 15678 \times 13 = 2.$$

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

1.1.4. 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 $ab \mid c$.

Un entier p est dit *premier* si $p > 1$ et p n'a que deux diviseurs positifs 1 et p. Par exemple, les entiers $2, 3, 5, 7, 11, 13$, et 17 sont premiers, mais $1, 4, 6$, et 9 ne le sont pas.

Voici des propriétés de nombres premiers.

1.1.5. 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.

1.1.6. 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.

Exercice. Vérifier que 97 est premier.

Démonstration. D'abord, $\sqrt{97} < \sqrt{100} = 10$. Or, les nombres premiers ≤ 10 sont $2, 3, 5, 7$, qui ne sont pas diviseurs de 97. Donc, 97 est premier.

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

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

Exemple. En tapant la commande

isprime(100000000019);

on obtient la réponse "true".

En appliquant le lemme 1.1.6, on obtient une méthode pour chercher les nombres premiers plus petits ou égaux à un entier donné. Pour un entier a, on note $a\mathbb{N} = \{an \mid n \in \mathbb{N}\}$.

1.1.7. Crible d'Ératosthène. 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.
Solution.

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60

D'abord, on a $\sqrt{60} < 8$. En enlève les multiples propres de $2, 3, 5, 7$ dans le tableau ci-dessus, on trouve que les nombres premiers ≤ 60 sont les nombres suivants:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59.$$

1.1.8. 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 décimaux.

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

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

Exemple. On tape la commande

$$\text{nextprime}(10\hat{}12);$$

on obtient 1000000000039, le plus petit nombre premier $\geq 10^{12}$.

Le résultat suivant est bien connu.

1.1.9. Théorème. Tout entier $n(>1)$ admet une factorisation unique

$$n = p_1^{e_1} \cdots p_r^{e_r},$$

appelée *factorisation canonique* de n, où $p_1 < \cdots < p_r$ sont premiers et $e_1, \ldots, e_r > 0$.

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

(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 $p^0 \mid n$.

Exemple. $20 = 2^2 \times 5$.

On étudiera comment trouver la factorisation canonique de $n!$. Étant donné un ensemble X, on désigne par $|X|$ la cardinalité de X.

1.1.10. Lemme. Si $m, n \in \mathbb{Z}$ avec $m \geq 0$ et $n \geq 1$, alors

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

Démonstration. Posons $X = \{x \in \mathbb{Z} \mid 1 \leq x \leq m; n \mid x\}$ et $q = [\frac{m}{n}]$.

Si $0 \leq m < n$, alors $[\frac{m}{n}] = 0$, et $X = \emptyset$. L'énoncé est valide dans ce cas.

Supposons maintenant que $m \geq n$. Alors $q \geq 1$. Comme $q \leq \frac{m}{n} < q + 1$, on a $qn \leq m < (q+1)n$. Or, pour tout $x \in \{1, \ldots, m\}$, on voit que $n \mid x$ si et seulement si $x = ny$ avec $1 \leq y \leq q$. Par conséquent, $X = \{n, \ldots, (q-1)n, qn\}$. D'où, on a l'énoncé. Ceci achève la démonstration du lemme.

Exemple. Le nombre de multiples de 9 entre 1 et 100 est

$$\left[\frac{100}{9}\right] = 11.$$

On voit aisément que les diviseurs premiers de $n!$ sont les nombres premiers $\leq n$. Le résultat suivant nous permet de trouver la factorisation canonique de $n!$.

1.1.11. 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

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

Démonstration. L résultat est évident pour $n = 1$. Supposons que $n > 1$ et le résultat est valide pour $n-1$. Par définition, $n! = (n-1)!\, n$. Supposons que r, s sont les plus grands exposants tels que $p^r \mid (n-1)!$ et $p^s \mid n$. On prétend que $e = r + s$. En effet, par définition, $p^{r+s} \mid n!$. Si $p^{r+s+1} \mid (n-1)!n$, alors

$$p \mid \frac{(n-1)!}{p^r} \cdot \frac{n}{p}.$$

D'après le lemme 1.1.5(2), $p \mid \frac{(n-1)!}{p^r}$ ou $p \mid \frac{n}{p}$. C'est-à-dire, $P^{r+1} \mid (n-1)!$ ou $p^{s+1} \mid n$, une contradiction. Maintenant, par l'hypothèse de récurrence, on a

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

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

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

D'après le lemme 1.1.10, $[\frac{n-1}{p^i}] = |\mathcal{E}_{n-1}|$ et $[\frac{n}{p^i}] = |\mathcal{E}_n|$. On a toujour $\mathcal{E}_{n-1} \subseteq \mathcal{E}_n$. De plus, $\mathcal{E}_{n-1} \neq \mathcal{E}_n$ si et seulement si $n \in \mathcal{E}_n$ si et seulement si $p^i \mid n$; et dans ce cas, $\mathcal{E}_n = \mathcal{E}_{n-1} \cup \{n\}$. 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

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

D'où, 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.

Solution. Les nombres premiers ≤ 10 sont $2, 3, 5, 7$. Ainsi $10! = 2^{e_1}3^{e_2}5^{e_3}7^{e_4}$, où

$$e_1 = \left[\frac{10}{2}\right] + \left[\frac{10}{4}\right] + \left[\frac{10}{8}\right] = 5 + 2 + 1 = 8, \quad e_2 = \left[\frac{10}{3}\right] + \left[\frac{10}{9}\right] = 3 + 1 = 4.$$

et

$$e_3 = \left[\frac{10}{5}\right] = 2, \qquad e_4 = \left[\frac{10}{7}\right] = 1.$$

C'est-à-dire,

$$10! = 2^8 \times 3^4 \times 5^2 \times 7.$$

1.2 Anneaux

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

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

avec un *zéro* 0_A; et d'une multiplication

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

avec un *identité* 1_A, telles que, pour tous $a, b, c \in A$, on a

(1) $a + b = b + a$;
(2) $a + (b + c) = (a + b) + c$;
(3) $a + 0_A = a$;
(4) il existe un *opposé* $-a$ tel que $a + (-a) = 0_A$;
(5) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$;
(6) $1_A \cdot a = a \cdot 1_A = a$;
(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. (1) On définit la *soustraction* par

$$a - b = a + (-b), \text{ pour tous } a, b \in A.$$

(2) On note $A^* = \{a \in A \mid a \neq 0_A\}$.

Exemple. (1) L'ensemble $\mathbb{Z}$ est un anneau commutatif pour l'addition et la multiplication habituelle.

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

(3) L'ensemble $\mathbb{Z}[x]$ des polynômes à coefficients entiers est un anneau commutatif 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.

Le résultat suivant est évident.

1.2.2. Proposition. Soit A un anneau avec $a, b, c \in A$.
(1) A a un seul zero 0_A.
(2) A a un seul identité 1_A.
(3) a admet un seul opposé $-a$.
(4) $0_A \cdot a = a \cdot 0_A = 0_A$.
(5) $(-1_A) \cdot a = -a$.
(6) $-(-a) = a$.
(7) $a(b - c) = ab - ac$.
(8) $(a - b)c = ac - bc$.

1.2.3. Définition. Soit A un anneau. Un sous-ensemble B de A est dit *sous-anneau* si
(1) $1_A \in B$; et
(2) $a \pm b, ab \in B$ lorsque $a, b \in B$.

Remarque. Un sous-anneau B de A est un anneau avec $0_B = 0_A$ et $1_B = 1_A$, pour les opérations induites de celles de A.

Exemple. (1) Il est évident que $\mathbb{Z}$ est un sous-anneau de $\mathbb{Z}[x]$.
(2) On voit aisément que l'ensemble

$$D_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \mid a, b \in \mathbb{Z} \right\}$$

est un sous-anneau de $M_2(\mathbb{Z})$.

1.2.4. Définition. Soit A un anneau. Un élément $a \in A$ est dit *inversible* s'il existe $b \in A$, appelé *inverse* de a, tel que

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

et dans ce cas, on note $b = a^{-1}$.

En outre, A s'appelle *corps* si A est commutatif, non nul, et tous les éléments non nuls sont inversibles.

Exemple. (1) Les anneaux $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont des corps.
(2) $\mathbb{Z}$ est un sous-anneau de $\mathbb{Q}$, mais $\mathbb{Z}$ n'est pas un corps.

On rappelle la notion de groupe du cours MAT141.

1.2.5. Définition. Un *groupe* est un ensemble G muni d'une multiplication

$$\cdot : G \times G \to G : (g, h) \mapsto g \cdot h$$

avec un *identité* e, telle que, pour tous $f, g, h, \in G$, on a
(1) $e \cdot g = g \cdot e = g$;
(2) $f \cdot (g \cdot h) = (f \cdot g) \cdot h$;
(3) g admet un *inverse* g^{-1} tel que $g \cdot g^{-1} = g^{-1} \cdot g = e$.

Exemple. Les ensembles $\mathbb{Q}^*, \mathbb{R}^*$ et $\mathbb{C}^*$ sont des groupes pour la muliplication de nombres usuels.

1.2.6. Proposition. Si A est un anneau non nul, alors l'ensemble $U(A)$ des éléments inversibles de A est un groupe pour la multiplication de A, appelé *groupe multiplicatif* de 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, par définition, $U(F) = F^*$.
(2) $U(\mathbb{Z}) = \{1, -1\}$. En effet, un entier $n \in \mathbb{Z}$ est inversible si et seulement si $n = \pm 1$.

Exercice. Soit $\mathbb{Q}[x]$ l'anneau des polynômes rationnels. Vérifier que $U(\mathbb{Q}[x]) = \mathbb{Q}^*$.

Démonstration. Il est évident que $\mathbb{Q}^* \subseteq U(\mathbb{Q}[x])$. Soit $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Q}[x]$, où $n \geq 1$ et $a_n \neq 0$. Soit $g(x) \in \mathbb{Q}[x]$. Si $g(x) = 0$, alors $f(x)g(x) = 0 \neq 1$; sinon, $g(x) = \sum_{j=0}^{m} b_j x^j$ avec $b_m \neq 0$. Or

$$f(x)g(x) = a_n b_m x^{n+m} + h(x),$$

avec $h(x)$ de degré $< n + m$. En particulier, $f(x)g(x) \neq 1$. Ainsi $f(x) \notin U(\mathbb{Q}[x])$. Ceci achève la démonstration.

Le résultat suivant dit que comment former un nouveau anneau à partir de deux anneaux donnés.

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

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

est un anneau non nul 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.

Exemple. On a vu que $U(\mathbb{Z}) = \{1, -1\}$. D'après la proposition 1.2.7,

$$\mathbb{Z} \times \mathbb{Z} = \{(m, n) \mid m, n \in \mathbb{Z}\}$$

est un anneau commutatif avec

$$U(\mathbb{Z} \times \mathbb{Z}) = U(\mathbb{Z}) \times U(\mathbb{Z}) = \{(1, 1), (-1, 1), (1, -1), (-1, -1)\}.$$

1.2.8. Définition. Soient A, B deux anneaux. Une application bijective $\phi : A \to B$ s'appelle *isomorphisme* 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 $a, b \in A$.

Dans ce cas, on dit que A, B sont *isomorphes*, noté $A \cong B$.

Exemple. L'application-identité $\mathbb{1}_A : A \to A$ est un isomorphisme.

Exercice. Vérifier que $\mathbb{Z} \times \mathbb{Z} \cong D_2(\mathbb{Z})$.

Démonstration. On vérifie facilement que

$$\phi : \mathbb{Z} \times \mathbb{Z} \to D_2(\mathbb{Z}) : (a, b) \mapsto \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$$

est un isomorphisme d'anneaux.

1.2.9. Lemme. Si A, B sont deux anneaux isomorphes, alors $U(A) \cong U(B)$.

Démonstration. Soit $\phi : A \to B$ un isomorphisme. Si $a \in U(A)$, on a alors $aa^{-1} = a^{-1}a = 1_A$. D'où, $\phi(a)\phi(a^{-1}) = \phi(1_A) = 1_B$. De même, $\phi(a^{-1})\phi(a) = 1_B$. C'est-à-dire, $\phi(a^{-1}) = \phi(a)^{-1}$, et donc, $\phi(a) \in U(B)$. Ceci montre que ϕ induit une application

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

Comme ϕ est injective, ψ l'est aussi. Soit $c \in U(B)$. Comme ϕ est surjective, $c = \phi(a)$ et $c^{-1} = \phi(b)$, avec $a, b \in A$. Donc, $\phi(ab) = \phi(a)\phi(b) = cc^{-1} = 1_B = \phi(1_A)$. Comme ϕ est injective, $ab = 1_A$. De même, $ba = 1_A$. C'est-à-dire, $a \in U(A)$ tel que $\psi(a) = c$. Ainsi, ψ est bijective. Enfin, pour tous $a, b \in U(A)$, on a $\psi(ab) = \phi(ab) = \phi(a)\phi(b) = \psi(a)\psi(b)$. Ceci montre que ψ est un isomorphisme de groupes. La preuve du lemme s'achève.

1.3 Congruence sur les entiers

Cette section a pour but d'étudier la congruence sur les entiers. On commence par la notion d'une relation d'équivalence sur un ensemble.

1.3.1. 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, et on note $x\mathcal{R}y$.

(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 $\mathbb{Z}$. On voit aisément que $m\mathcal{R}n$ si, et seulement si, m, n ont la même parité.

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

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

(2) L'ensemble des classes d'équivalence

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

s'appelle *ensemble quotient* de E par la relation $\sim$.

Remarque. Comme $\sim$ est réflexive, on voit que $x \in \bar{x}$, pour tout $x \in E$.

1.3.3. Lemme. Soit $\sim$ une relation d'équivalence sur un ensemble E. Si $x, y \in E$, alors $\bar{x} = \bar{y}$ si, et seulement si, $x \sim y$.

Démonstration. Si $\bar{x} = \bar{y}$, alors $x \in \bar{x} = \bar{y}$, et donc, $x \sim y$.

Supposons que $x \sim y$. Si $z \in \bar{x}$, alors $z \sim x$, et donc, $z \sim y$. D'où, $z \in \bar{y}$. C'est-à-dire, $\bar{x} \subseteq \bar{y}$. En outre, comme $y \sim x$, on a $\bar{y} \subseteq \bar{x}$. D'où, $\bar{x} = \bar{y}$. La preuve du lemme s'achève.

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

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

En effet, $\bar{0} = \{2a \mid a \in \mathbb{Z}\}$ et $\bar{1} = \{2a + 1 \mid a \in \mathbb{Z}\}$. Ainsi $\bar{0} \neq \bar{1}$. Soit $x \in \mathbb{Z}$. Si x est pair, alors $\bar{x} = \bar{0}$; et si x est impair, alors $\bar{x} = \bar{1}$.

1.3.4. 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 de représentants de classes d'équivalence par* $\sim$ si tout $x \in E$ est en relation avec un unique $c \in C$.

Remarque. Si C est un ensemble complet de représentants de classes d'équivalence par $\sim$, alors les classes d'équivalence $\bar{c}$, avec $c \in C$, sont deux à deux distinctes telles que

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

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 est prêt d'introduire la relation de la congruence sur les entiers.

1.3.5. Définition. Soit un entier $m \geq 2$. Deux entiers a, b sont dit *congrus* (ou bien, a est *congru* à b) *modulo* m si $m \mid a - b$, noté $a \equiv b \pmod{m}$.

Remarque. Par définition, $a \equiv 0 \pmod{m}$ si et seulement si $m \mid a$.

Exemple. $11 \equiv 6 (\mathrm{mod}\, 5)$ et $39 \equiv 0 (\mathrm{mod}\, 3)$.

1.3.6. Lemme. Soit un entier $m \geq 2$, la congruence modulo m est une relation d'équivalence sur $\mathbb{Z}$.

Démonstration. Soient $a, b, c \in \mathbb{Z}$. Comme $a - a = 0$, on voit que $a \equiv a (\bmod m)$.
Si $a \equiv b (\bmod m)$, alors $m \mid a - b$, et donc, $m \mid b - a$. C'est-à-dire, $b \equiv a (\bmod m)$.
Si $a \equiv b (\bmod m)$ et $b \equiv c (\bmod m)$, alors $a - b = ms$ et $b - c = mt$. D'où,

$$a - c = (a - b) + (b - c) = m(s + t).$$

C'est-à-dire, $a \equiv c (\bmod m)$. Ceci achève la démonstration.

Le résultat suivant explique le reste divisé par m en vue de la congruence module m.

1.3.7. Lemme. Soit un entier $m \geq 2$. Si $a, r \in \mathbb{Z}$, alors $r = r_m(a)$ si et seulement si $a \equiv r (\bmod m)$ et $0 \leq r < m$.

Démonstration. 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, $a \equiv r (\bmod m)$ et $0 \leq r < m$. La preuve du lemme s'achève.

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

$$a \bmod m;$$

Exemple. En tapant la commande

$$234653423314678965 \bmod 1243256789;$$

on trouve que le reste de 234653423314678965 divisé par 1243256789 est 622113819.

1.3.8. Lemme. Soit un entier $m \geq 2$. Si $a \equiv b (\bmod m)$ et $c \equiv d (\bmod m)$, alors

$$a + c \equiv b + d (\bmod m) \text{ et } ac \equiv bd (\bmod m);$$

et par conséquent, $a^i \equiv b^i (\bmod m)$, pour tout entier $i \geq 0$.

Démonstration. Supposons que $a \equiv b (\bmod m)$ et $c \equiv d (\bmod m)$, alors $a - b = ms$ et $c - d = mt$ avec $s, t \in \mathbb{Z}$. Comme $(a + c) - (b + d) = (a - b) + (c - d) = m(s + t)$, on a $a + c \equiv b + d (\bmod m)$. En outre,

$$ac - bd = ac - bc + bc - bd = (a - b)c + b(c - d) = m(sc + bt).$$

D'où, $ac \equiv bd (\bmod m)$. Enfin, comme $a \equiv b (\bmod m)$ et $a \equiv b (\bmod m)$, on a $a^2 \equiv b^2 (\bmod m)$. En générale, $a^i \equiv b^i (\bmod m)$, pour tout entier $i \geq 0$. La preuve du lemme s'achève.

Exercice. Trouver $r_{100}(2357^2)$.

Solution. On voit aisément que $2357 \equiv 57 (\bmod 100)$. D'après le lemme 1.3.8, on a $2357^2 \equiv 57^2 (\bmod 100)$. Comme $57^2 = 3249 \equiv 49 (\bmod 100)$, on a $2357^2 \equiv 49 (\bmod 100)$. Comme $0 < 49 < 100$, d'après le lemme 1.3.7, on a $r_{100}(2357^2) = 49$.

1.3.9. 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 $a(x_0b_0) + m(y_0b_0) = db_0 = b$. D'où, $a(x_0b_0) \equiv b \,(\mathrm{mod} m)$.

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, puisque 34 n'est pas divisible par 5, un commun diviseur de 25 et 85.

(2) Considéons la congruence $4x \equiv 10 \,(\mathrm{mod}\, 18)$. Comme $\mathrm{pgcd}(4, 18) = 2$, qui divise 10, cette congruence admet des solutions. En effet, par l'algorithme d'Euclide, on trouve que $4 \times 5 + 18 \times (-1) = 2$. Ceci donne

$$4 \times 25 + 18 \times (-5) = 10.$$

Par conséquent, 25 est une solution de la congruence. En effet, tout $a \in 25 + 18\mathbb{Z}$ est également une solution.

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

$$\begin{aligned} x &\equiv a_1 \,(\mathrm{mod}\, m_1) \\ x &\equiv a_2 \,(\mathrm{mod}\, m_2) \\ &\vdots \\ x &\equiv a_r \,(\mathrm{mod}\, m_r). \end{aligned}$$

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

Démonstration. Supposons que $m_1, m_2, \ldots, m_r$ sont deux à deux co-premiers. Posons

$$\hat{m}_i = \frac{m_1 \cdots m_r}{m_i},\ i = 1, \ldots, r.$$

Si $i \neq j$, alors $m_i \mid \hat{m}_j$, et d'après la proposition 1.1.5(3), $\mathrm{pgcd}(m_i, \hat{m}_i) = 1$, Ainsi, il existe $x_i, y_i \in \mathbb{Z}$ tels que $\hat{m}_i x_i + m_i y_i = 1$, et donc,

$$\hat{m}_i x_i a_i + m_i y_i a_i = a_i,\ i = 1, \ldots, r.$$

Alors $\hat{m}_i x_i a_i \equiv a_i \,(\mathrm{mod}\, m_i)$ et $\hat{m}_j x_j a_j \equiv 0 \,(\mathrm{mod}\, m_i)$ pour $j \neq i$. Posant

$$a = \sum_{j=1}^{r} \hat{m}_j x_j a_j,$$

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

Pour tout $b \in \mathbb{Z}$, on a $b \equiv a_i \,(\mathrm{mod}\, m_i)$, $i = 1, \ldots, r$, si et seulement si, $b \equiv a \,(\mathrm{mod}\, m_i)$, $i = 1, \ldots, r$, 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, $b \equiv a \,(\mathrm{mod}\, m_1 \cdots m_r)$. 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?

Solution. Supposons que l'on a x objets. Alors

$$\begin{aligned} x &\equiv 2 \,(\mathrm{mod}\, 3) \\ x &\equiv 3 \,(\mathrm{mod}\, 5) \\ x &\equiv 2 \,(\mathrm{mod}\, 7). \end{aligned}$$

On calcule $\hat{m}_1 = 35,\ \hat{m}_2 = 21,\ \hat{m}_3 = 15$. Remarquons que

$$\begin{aligned} 35 \times 2 &+ 3 \times (-23) &&= 1; \\ 21 \times 1 &+ 5 \times (-4) &&= 1; \\ 15 \times 1 &+ 7 \times (-2) &&= 1. \end{aligned}$$

On a ainsi

$$\begin{aligned} 35 \times 2 \times 2 &+ 3 \times (-23) \times 2 &&= 2; \\ 21 \times 1 \times 3 &+ 5 \times (-4) \times 3 &&= 3; \\ 15 \times 1 \times 2 &+ 7 \times (-2) \times 2 &&= 2. \end{aligned}$$

En vue de la preuve du théorème 1.3.10, on obtient une solution

$$a = 35 \times 2 \times 2 + 21 \times 1 \times 3 + 15 \times 1 \times 2 = 233.$$

Comme $3 \times 5 \times 7 = 105$, les solutions sont les entiers x tels que

$$x \equiv 233 \,(\mathrm{mod}\, 105).$$

Comme $23 \equiv 233 (\mathrm{mod}\, 105)$, il y a 23 objects.

Maintenant, on utilisera la relation de congruence pour construire des anneaux quotients des entiers.

1.3.11. Définition. Soit un entier $m \geq 2$. Pour tout $a \in \mathbb{Z}$, la classe d'équivalence

$$\bar{a} = \{b \in \mathbb{Z} \mid b \equiv a \,(\mathrm{mod} m)\}$$

s'appelle *classe de congruence* de a *modulo* m.

1.3.12. Lemme. Soit un entier $m \geq 2$. Si $a, b \in \mathbb{Z}$, alors
(1) $\bar{a} = \{a + mx \mid x \in \mathbb{Z}\} =: a + m\mathbb{Z}$;
(2) $\bar{a} = \bar{b}$ si, et seulement si, $r_m(a) = r_m(b)$.

Démonstration. (1) Pour tout $b \in \mathbb{Z}$, on a $b \in \bar{a}$ si et seulement si $m \mid b - a$ si et seulement si $b = mx + a$, pour un certain $x \in \mathbb{Z}$.

(2) Posons $r_m(a) = s$ et $r_m(b) = t$. Alors $0 \leq r, s < m$. D'après le lemme 1.3.6, $\bar{a} = \bar{s}$ et $\bar{b} = \bar{t}$. Ainsi, $\bar{a} = \bar{b}$ si, et seulement si, $\bar{s} = \bar{t}$ si, et seulement si, $s \equiv t \,(\mathrm{mod} m)$ si, et seulement si, $m \mid s - t$ si, et seulement si, $s = t$. La preuve du lemme s'achève.

Exemple. Considérons la congruence modulo 2. D'après le lemme 1.3.12(1), on a $\bar{0} = \{2a \mid a \in \mathbb{Z}\}$, l'ensemble des entiers pairs; et $\bar{1} = \{2a + 1 \mid a \in \mathbb{Z}\}$, l'ensemble des entiers impairs.

1.3.13. Corollaire. Soit un entier $m \geq 2$. Alors $\{0, 1, \ldots, m - 1\}$ est un ensemble complet de resprésentants des classes de congruence modulo m.

Démonstration. Soit $a \in \mathbb{Z}$. D'après le lemme 1.3.7, $r_m(a) \in \{0, 1, \ldots, m - 1\}$ est tel que $a \equiv r_m(a) \,(\mathrm{mod} m)$. Si $s \in \{0, 1, \ldots, m - 1\}$ avec $s \neq r_m(a)$, d'après le lemme 1.3.7, $a \not\equiv s (\mathrm{mod}\, m)$. La preuve du corollaire s'achève.

Le résultat dit que la relation de la congruence nous permet de constriure des anneaux finis à partir de l'anneau infini $\mathbb{Z}$.

1.3.14. Proposition. Soit un entier $m \geq 2$. L'ensemble quotient

$$\mathbb{Z}_m = \{\bar{a} \mid a \in \mathbb{Z}\}$$

est un anneau dont le zéro est $\bar{0}$ et l'identité est $\bar{1}$, pour les opérations suivantes:

$$\bar{a} + \bar{b} = \overline{a + b} \;\text{ et }\; \bar{a} \cdot \bar{b} = \overline{ab}.$$

Démonstration. D'abord, on prétend que l'addition et la multiplication sont correctement définies. En effet, si $\bar{a} = \bar{c}$ et $\bar{b} = \bar{d}$, alors $a \equiv c \,(\mathrm{mod} m)$ et $b \equiv d \,(\mathrm{mod} m)$. D'après le lemme 1.3.8, $a + b \equiv c + d \,(\mathrm{mod} m)$ et $ab \equiv cd \,(\mathrm{mod} m)$. C'est-à-dire, $\overline{a + b} = \overline{c + d}$ et $\overline{ab} = \overline{cd}$.

Pour tout $\bar{a} \in \mathbb{Z}_m$, on a $\bar{a} + \bar{0} = \overline{a + 0} = \bar{a}$ et $\bar{1} \cdot \bar{a} = \overline{1 \cdot a} = \bar{a}$. D'où, $\bar{0}$ est le zéro et $\bar{1}$ est l'identié de $\mathbb{Z}_m$. On peut vérifier les autres axiomes énoncés dans la définition 1.2.1. La preuve de la proposition s'achève.

Remarque. D'après le corollaire 1.3.13, on voit que

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

est un anneau commutatif de m éléments, appelé *anneau quotient* de $\mathbb{Z}$ *modulo* m.

Les résultat suivant décrit en particulier les éléments inversibles de $\mathbb{Z}_m$.

1.3.15. Proposition. Soit $\bar{a} \in \mathbb{Z}_m$ avec $m \geq 2$.
(1) $\bar{a} = \bar{0}$ si et seulement si $m \mid a$.
(2) $\bar{a} \in U(\mathbb{Z}_m)$ si et seulement si a, m sont co-premiers.
(3) Si $ax + my = 1$, alors $\bar{a}^{-1} = \bar{x}$.

Démonstration. Soit $a \in \mathbb{Z}$. D'abord, $\bar{a} = \bar{0}$ si, et seulement si, $a \equiv 0 \,(\mathrm{mod} m)$ si, et seulement si, $m \mid a$.

Ensuite, $\bar{a} \in U(\mathbb{Z}_m)$ si et seulement si $\bar{a}\bar{b} = \bar{1}$ pour un certain $b \in \mathbb{Z}$ si, et seulement si, $\overline{ab} = \bar{1}$ pour un certain $b \in \mathbb{Z}$ si, et seulement si, $ab \equiv 1 \,(\mathrm{mod} m)$ pour un certain $b \in \mathbb{Z}$. D'après la proposition 1.3.9, cette dernière condition est équivalente à $\mathrm{pgcd}(a, m) \mid 1$, c'est-à-dire, a, m sont co-premiers. Enfin, supposons que $ax + my = 1$. D'après la définition,

$$\bar{1} = \overline{ax + my} = \overline{ax} + \overline{my} = \bar{a}\bar{x} + \bar{0} = \bar{a}\bar{x}.$$

D'où, $\bar{a}^{-1} = \bar{x}$. La preuve de la proposition s'achève.

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

Solution. En effet, 5 est premier, qui ne divise pas 171. Ainsi, $\mathrm{pgcd}(5, 171) = 1$. D'après le proposition 1.3.15(2), $\bar{5} \in U(\mathbb{Z}_{171})$. Pour trouver $\bar{5}^{-1}$, on doit résoudre premièrement l'équation $5x + 171y = 1$. En utilisant l'algorithme d'Euclide, on trouve

$$5 \times (-34) + 171 \times 1 = 1.$$

Ainsi, $\overline{-34} = \overline{137}$ est l'inverse de $\bar{5}$ dans $\mathbb{Z}_{171}$.

Le résultat suivant sera très utile pour réduire le taille d'un anneau quotient de $\mathbb{Z}$.

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

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

Démonstration. Pour tout $x \in \mathbb{Z}$, on écrit $\bar{x} = x + (mn)\mathbb{Z} \in \mathbb{Z}_{mn}$, $\hat{x} = x + m\mathbb{Z} \in \mathbb{Z}_m$ et $\tilde{x} = x + n\mathbb{Z} \in \mathbb{Z}_n$. Considérons l'application

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

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 correctement définie.

Fixons $(\hat{a}, \tilde{b}) \in \mathbb{Z}_m \times \mathbb{Z}_n$. Comme $\text{pgcd}(m, n) = 1$, en vertu du théorème 1.3.10(1), 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 $\bar{y} \in \mathbb{Z}_{mn}$ est aussi tel que $\phi(\bar{y}) = (\hat{a}, \tilde{b})$, 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 1.3.10(2), $y \equiv x \,(\text{mod } mn)$, c'est-à-dire, $\bar{y} = \bar{x}$. Ceci montre que ϕ est bijective. Enfin, il est évident que ϕ satisfait aux axiomes énoncés dans la définition 1.2.8. Ainsi, ϕ est un isomorphisme d'anneaux. La preuve de la proposition s'achève.

Exemple. Trouver $|U(\mathbb{Z}_{100})|$.

Solution. Comme $100 = 4 \times 25$ avec $\text{pgcd}(4, 25) = 1$, d'après la proposition 1.3.16, on a $\mathbb{Z}_{100} \cong \mathbb{Z}_4 \times \mathbb{Z}_{25}$. D'après le lemme 1.2.9 et la proposition 1.2.7, $U(\mathbb{Z}_{100}) \cong U(\mathbb{Z}_4) \times U(\mathbb{Z}_{25})$. Ainsi, $|U(\mathbb{Z}_{100})| = |U(\mathbb{Z}_4)| \times |U(\mathbb{Z}_{25})|$.

Comme $\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$, d'après la proposition 1.3.15(2), $U(\mathbb{Z}_4) = \{\bar{1}, \bar{3}\}$.

En outre, $\mathbb{Z}_{25} = \{\hat{0}, \hat{1}, \ldots, \widehat{24}\}$. Si $a \in \{0, 1, \ldots, 24\}$, alors $\hat{a} \notin U(\mathbb{Z}_{25})$ si et seulement si $\text{pgcd}(a, 25) \neq 1$ si et seulement si $5 \mid a$ si et seulement si $a \in \{0, 5, 10, 15, 20\}$. Ainsi $|\mathbb{Z}_{25}| = 25 - 5 = 20$. D'où, $|U(\mathbb{Z}_{100})| = 40$.

On conclut cette section par un critère pour que $\mathbb{Z}_m$ soit un corps.

1.3.17. Théorème. Soit un entier $m \geq 2$. 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 $1 < a, b < m$. D'après la proposition 1.3.15(1), $\bar{a}, \bar{b} \in \mathbb{Z}_m$ sont tous non nuls. Mais, $\bar{a} \cdot \bar{b} = \overline{ab} = \overline{m} = \bar{0}$. Par conséquent, $\mathbb{Z}_m$ n'est pas un corps.

Supposons 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 la proposition 1.3.15(2), $\bar{a}$ est inversible. Ceci montre que $\mathbb{Z}_m$ est un corps. La preuve du théorème s'achève.

Soit p un entier premier. Par abus de notation, on identifiera $r \in \{0, 1, \ldots, p-1\}$ avec $\bar{r} \in \mathbb{Z}_p$. De cette façon, $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$ muni des oppérations suivantes:

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

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 $a_{10}=\sum_{n=1}^{9} n\cdot a_n \in \mathbb{Z}_{11}$, appelé *clé de contrôle*.

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

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 $-1=10$ dans $\mathbb{Z}_{11}$, on obtient $\sum_{n=1}^{10} n\cdot a_n=0$.

(2) D'après l'énoncé (1), $(-i)\cdot a_i=\sum_{1\le n\le 10;\, n\neq i} n\cdot a_n$. Comme $-i=(11-i)\neq 0$, on obtient $a_i=(11-i)^{-1}\cdot\sum_{1\le n\le 10;\, n\neq i} n\cdot a_n$. 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 caractères.

Exemple. Est-ce que $023456712X$ est un code ISBN?
Solution. Dans le corps $\mathbb{Z}_{11}$, on a

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

Il ne s'agit pas d'un code ISBN.

1.5 Exercices

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

2. Montrer, pour tous $\alpha, \beta \in \mathbb{R}$, que

$$[\alpha] + [\beta] \leq [\alpha + \beta] \leq [\alpha] + [\beta] + 1.$$

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

4. 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 $p^{r+s} \mid ab$.

5. Vérifier que 103 est un nombre premier.

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

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

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

8. 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

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

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

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

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

11. Factoriser 30! en produit de puissances de nombres premiers.

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

13. 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:

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

14. Soit

$$A = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in \mathbb{Z} \right\}.$$

(1) Montrer que A est un sous-anneau de $M_2(\mathbb{Z})$.

(2) Trouver le groupe multiplicatif de A.

15. Donner le groupe multiplicatif de l'anneau $\mathbb{Z} \times \mathbb{Q}$.

16. 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.

17. 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) Pour tous $m, n \in \mathbb{Z}$, on définit $m\mathcal{R}n$ si et seulement si $nm \geq 0$.

(2) Pour tous $x, y \in \mathbb{R}$, on définit $x\mathcal{R}y$ si et seulement si $x \geq y$.

(3) Pour tous $x, y \in \mathbb{R}$, on définit $x\mathcal{R}y$ si et seulement si $|x - y| \leq 3$.

18. Considérer la relation binaire sur le plan $\mathbb{R}^2$ suivante:

$$\mathcal{R} = \{(x, y) \in \mathbb{R}^2 \mid y = ax + b\}.$$

Trouver les valeurs réelles de a, b pour que $\mathcal{R}$ soit une relation d'équivalence.

19. Considérer la relation binaire sur $\mathbb{Z}$ suivante:

$$\mathcal{R} = \{(m, n) \in \mathbb{Z} \times \mathbb{Z} \mid r_3(m) = r_3(n)\}.$$

(a) Vérifier que $\mathcal{R}$ est une relation d'équivalence.

(b) Donner un ensemble complet de représtantants des classes d'équivalence par $\mathcal{R}$.

(c) Donner les éléments sans redondance de l'ensemble quotient de $\mathbb{Z}$ par $\mathcal{R}$.

20. 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 $\frac{m}{n}$ la classe d'équivalence de (m,n) par $\sim$, 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.

21. 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.

22. Soient un entier $m \geq 2$ et un polynôme entier $f(x) = \sum_{i=0}^{n} a_i x^i$. Si $a, b \in \mathbb{Z}$ sont tels que $a \equiv b \pmod{m}$, montrer que $f(a) \equiv f(b) \pmod{m}$.

23. 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.

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

25. Dans chacun des cas suivants, déterminer si la congruence a des solutions ou non; si oui, donner une solution.

(1) $145x \equiv 15 \pmod{85}$; (2) $123x \equiv 217 \pmod{195}$;

(3) $209x \equiv 22 \pmod{77}$; (4) $142x \equiv 67 \pmod{792}$.

26. 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?

27. 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) $a = 131$.

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

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

30. (**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 $\bar{a}^{-1} = \bar{b}$.

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

32. 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.

33. 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. 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 $\varphi(m) \geq 1$.

Exemple. (1) Par définition, $\varphi(1) = 1$.
(2) Les entiers $a \in \{1, \ldots, 10\}$ avec $\text{pgcd}(a, 10) = 1$ sont $1, 3, 7, 9$. D'où, $\varphi(10) = 4$.

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. Comme $\bar{m} = \bar{0}$, on a $\mathbb{Z}_m = \{\bar{1}, \bar{2}, \ldots, \bar{m}\}$. 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.

Exemple. Comme $|U(\mathbb{Z}_{100})| = 40$, on a $\varphi(100) = 40$.

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

Démonstration. D'après le théorème 1.3.17, $\mathbb{Z}_p = \{\bar{0}, \bar{1}, \ldots, \overline{p-1}\}$ 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, $\varphi(p) = p - 1$. La preuve du corollaire s'achève.

Exemple. Comme 97 est premier, on a $\varphi(97) = 96$.

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

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

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

Démonstration. Supposons que $\text{pgcd}(m,n)=1$. D'après la proposition 1.3.16, on a $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$, et d'après le lemme 1.2.9 et la propositions 1.2.7,

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

Par conséquent,

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

La preuve du lemme s'achève.

Exemple. Comme $\varphi(10)=4$ et $\varphi(3)=2$, on a $\varphi(30)=8$.

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. Posons $X = \{x \mid 1 \leq x \leq p^e; \text{pgcd}(x,p^e) \neq 1\}$. Comme p est premier, $X = \{x \mid 1 \leq x \leq p^e; p \mid x\}$. D'après le lemme 1.1.10, $|X| = \left[\frac{p^e}{p}\right] = p^{e-1}$. Donc,

$$\varphi(p^e) = |\{x \mid 1 \leq x \leq p^e; \text{pgcd}(x,p^e)=1\}| = p^{\,e} - p^{\,e-1}.$$

Supposons que $r>1$ et le résultat est valide pour $r-1$. Comme les p_i sont 2 à 2 distincts, les $p_i^{e_i}$ sont 2 à 2 co-premiers. D'après la proposition 1.1.4(3), $p_1^{e_1}\cdots p_{r-1}^{e_{r-1}}$ et $p_r^{e_r}$ sont co-premiers. En vertu du lemme 2.1.4 et l'hypothèse de récurrence, on a

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

La preuve du théorème s'achève.

Exemple. Comme $1000 = 2^3 5^3$, on a

$$\varphi(1000) = 1000\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right) = 400.$$

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, $a^{\varphi(m)} \equiv 1 \,(\mathrm{mod} m)$. Ceci achève la preuve du théorème.

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

Solution. Il s'agit de trouver le reste de 2013^4 divisé par 10. On a vu que $\varphi(10) = 4$. Comme 2013 n'est pas divisible par ni 2 ni 5, $\mathrm{pgcd}(2013, 10) = 1$. Par conséquent, $2013^4 \equiv 1 (\mathrm{mod}\, 10)$. C'est-à-dire, le dernier chiffre décimal de 2013^4 est 1.

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 $a^{p-1} \equiv 1 (\mathrm{mod} p)$.

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

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

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

Démonstration. Si $p \mid a$, comme $a^p - a = a(a^{p-1} - 1)$, on a $p \mid a^p - a$, c'est-à-dire, $a^p \equiv a \,(\mathrm{mod} p)$. Sinon, $a^{p-1} \equiv 1$, et donc $a^p \equiv a \,(\mathrm{mod} p)$. 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 positif avec $n \equiv 1 (\mathrm{mod}\, \varphi(m))$. Alors, pour tout entier a, on a

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

Démonstration. Par l'hypothèse, $n = \varphi(m)\, s + 1$, pour un certain $s \geq 0$.

(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, $a^{\varphi(m)s} \equiv 1^s \equiv 1 \,(\mathrm{mod} m)$. Par conséquent, $a^n = a^{\varphi(m)s} a \equiv a \,(\mathrm{mod} m)$.

(3) Supposons que $p \mid a$ et $q \nmid a$. Alors $a = p^t b$, avec $t > 0$ et $p \nmid b$. Comme $q \nmid a$, on a $q \nmid b$. D'après le cas (2), $b^n \equiv b \,(\mathrm{mod} m)$.

Maintenant, 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,

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

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 $p \not| a$, alors $a^n \equiv a \,(\mathrm{mod} m)$. Ceci achève la preuve du théorème.

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 $\mathrm{pgcd}(e, \varphi(m)) = 1$, appelé *exposant de chiffrement*;

(3) d est tel que $0 < d < \varphi(m)$ et $ed \equiv 1 (\mathrm{mod}\, \varphi(m))$, 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.

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

Solution. On tape les commandes du MAPLE suivantes:

$p := 100000000019;$

$$100000000019$$

$q := 1000000000039;$

$$1000000000039$$

$m := p * q;$

$$1000000000229000000000741$$

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

$$1000000000218000000000684$$

Ainsi on obtient le module de chiffrement $m = 1000000000229000000000741$. En outre, on a $\varphi(m) = a = 1000000000218000000000684$. On choisit l'exposant de chiffrement $e = 1234567$. On continue avec les commandes suivants:

$e := 1234567;$

$$1234567$$

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

$$1$$
$$-36586511716129406504717$$
$$451685$$

$d := -36586511716129406504717 \bmod a;$

$$6341348830567059349596 7$$

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

$$(m, e) = (1000000000229000000000741, 1234567)$$

et la clé privée est

$$(m, d) = (1000000000229000000000741, 6341348830567059349596 7).$$

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.

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

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

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:

040513010914435010390918010950275017213002050340

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

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

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

$x :=$ power(n, e) mod $m;$

72572266814479924902350

Enfin, Bob envoie à Alice ce nombre $x = 72572266814479924902350$. 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

$d := 6341348830567059349596 7;$

6341348830567059349596 7

$x := 72572266814479924902350;$

72572266814479924902350

$y :=$ power(x, d) mod $m;$

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 22 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 $m, n \geq 1$. 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. Soient p, a, b des entiers avec p premier. Si $a^p \equiv b^p (\mathrm{mod}\, p)$, montrer que

   (1) $a \equiv b \,(\mathrm{mod}\, p^2)$; *Indice*: appliquer le corollaire 2.1.8;

   (2) $a^p \equiv b^p (\mathrm{mod}\, p^2)$. *Indice*: Factoriser $a^p - b^p$.

8. 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 $n = 5$.

9. Donner un entier positif n tel que, pour tout entier a, on a

$$a^{19n} \equiv a(\mathrm{mod}35).$$

   Indice: Appliquer le théorème 2.1.9.

10. 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.

11. (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.

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

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

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

$$(m, d) = (100000000193900000000741, 1122247721303526353851).$$

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 le 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

On étude la théorie des codes dans le but de concevoir des méthodes de transmission de données efficaces et fiables. Cela implique généralement la suppression de la redondance et la correction ou la détection d'erreurs dans les données transmises. 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 F de E s'appelle *sous-espace* si, pour tous $u, v \in F$ et $\alpha \in K$, on a $u + v \in F$ et $\alpha u \in F$.

(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 F est un sous-espace de E, alors $0_E \in F$.

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 de K^n engendré par les lignes de M et l'*espace-colonne* $\mathscr{C}(M)$ de M est le sous-espace de $K^{(m)}$ engendré par les colonnes de M. En outre,

$$\mathscr{N}(M) = \{u \in K^{(n)} \mid Mu = 0\}$$

est un sous-espace vectoriel de $K^{(n)}$, appelé le *noyau* de M. Rappelons que $\mathscr{N}(M)$ se compose des solutions du système homogène $MX = 0$.

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) $\mathrm{rg}(M) = n$ si et seulement si les colonnes de M sont linéairement indépendantes.

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.

3.1.3. Théorème. Soient M, N des matrices sur K.
(1) Si M s'échelonne à N, alors $\mathscr{L}(M) = \mathscr{L}(N)$ et $\mathscr{N}(M) = \mathscr{N}(N)$.
(2) Si N est obtenue à partir de M par enlevant des lignes nulles, alors $\mathscr{N}(M) = \mathscr{N}(N)$.
(3) Si M est échelonnée, alors les lignes non nulles de M forment une base de $\mathscr{L}(M)$.

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

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

Solution. Par définition, $F = \mathscr{L}(M)$, où

$$M = \begin{pmatrix} 0 & 2 & 3 & 2 & 5 \\ 0 & 1 & 2 & 2 & 7 \\ 0 & 1 & 2 & 1 & 5 \end{pmatrix}.$$

Maintenant,

$$\begin{pmatrix} 0 & 2 & 3 & 2 & 5 \\ 0 & 1 & 2 & 2 & 7 \\ 0 & 1 & 2 & 1 & 5 \end{pmatrix} \xrightarrow{\frac{1}{2}L_1} \begin{pmatrix} 0 & 1 & 2 & 1 & 5 \\ 0 & 1 & 2 & 2 & 7 \\ 0 & 1 & 2 & 1 & 5 \end{pmatrix} \xrightarrow[L_3-L_1]{L_2-L_1} \begin{pmatrix} 0 & 1 & 2 & 1 & 5 \\ 0 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

On voit que $\{(0,1,2,1,5),(0,0,0,1,2)\}$ est une base de F.

Le résultat suivant est vu dans le cours MAT153.

3.1.4. Lemme. Soit M une matrice sur K de lignes $L_1, \ldots, L_m$ et de colonnes $C_1, \ldots, C_n$. Si $a_1, \ldots, a_m; b_1, \ldots, b_n \in K$, alors

(1) $(a_1 \cdots a_m)M = a_1L_1 + \cdots + a_mL_m \in \mathscr{L}(M)$;

(2) $$M \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = b_1C_1 + \cdots + b_nC_n \in \mathscr{C}(M).$$

Plus généralement, on a le résultat suivant qui est vu dans le cours MAT153.

3.1.5. Lemme. Soient M, N des matrices sur K telles que MN est défini.
(1) Si $N_1, \ldots, N_s$ sont les colonnes de N, alors $MN = (MN_1, \ldots, MN_s)$.
(2) Si $M_1, \ldots, M_t$ sont les lignes de M, alors

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

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

3.1.6. Définition. Une application $T : E \to F$ est dite *linéaire* si, pour tous $u, v \in E$ et $\alpha \in K$, on a
(1) $T(\alpha u) = \alpha T(u)$;
(2) $T(u + v) = T(u) + T(v)$.
En outre, une application linéaire bijective s'appelle un *isomorphisme*.

Les deux résultats suivants sont vus dans le cours MAT253.

3.1.7. Proposition. Soit $T : E \to F$ une application linéaire. Si G est un sous-espace de E engendré par $u_1, \ldots, u_r$, alors son image

$$T(G) = \{T(u) \mid u \in G\}$$

est un sous-espace de F engendré par $T(u_1), \ldots, T(u_r)$. En particulier, $\mathrm{Im}(T) = T(E)$ est un sous-espace de F, appelé *image* de T.

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

3.1.9. Proposition. Soient des entiers $m, n > 0$. Une application $T : K^m \to K^n$ est linéaire si, et seulement si, il existe $M \in M_{m\times n}(K)$ telle que T est de la forme

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

Dans ce cas, $\mathrm{Im}(T) = \mathscr{L}(M)$.
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, $T(e_i) = e_iM$, ce qui est la i-ième ligne de M d'après le lemme 3.1.4(1), pour $i = 1, \ldots, m$. D'après la proposition 3.1.7, on a

$$\mathrm{Im}(T) =< e_1M, \ldots, e_mM >= \mathscr{L}(M).$$

Supposons maintenant que $T : K^m \to K^n$ est linéaire. Posant $u_i = T(e_i) \in K^n$, $i = 1, \ldots, m$, on obtient

$$M = \begin{pmatrix} u_1 \\ \vdots \\ u_m \end{pmatrix} \in M_{m\times n}(K).$$

Pour tout $u = (a_1, \cdots, a_m) \in K^m$, en vertu de la proposition 3.1.4(2), on a

$$T(u) = T(a_1e_1 + \cdots + a_me_m) = a_1T(e_1) + \cdots + a_mT(e_m) = a_1u_1 + \cdots + a_mu_m = uM.$$

Ceci achève la démonstration de la proposition.

Exemple. Soit l'application suivante:

$$T : \mathbb{R}^3 \to \mathbb{R}^5 : (x, y, z) \mapsto (x + z, x + y + 2z, y + z, x + z, 2x + y + 3z).$$

Vérifier que T est linéaire et donner son image.

Démonstration. Pour $u = (x, y, z) \in \mathbb{R}^3$, on voit que $T(u) = uM$, où

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

D'après la proposition 3.1.9, on a

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

3.2 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

3.2.1. Définition. Un *mot binaire*, ou simplement *mot*, de longueur n est une suite

$$b_1 \cdots b_n,$$

où $b_1, \ldots, b_n \in \mathbb{Z}_2$.

On désignera par $\mathbb{Z}_2^*$ l'ensemble des mots binaires. Les mots binaires peuvent être composés de la façon suivante.

3.2.2. Définition. La *concaténation* des 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

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

On a vu dans la section précédente, le chiffrement RSA convertit un message claire en un nombre naturel. En informatique, les nombres naturels sont écrit sous la notation binaire suivante.

3.2.3. Proposition. Tout entier positif 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 note $n = n_s \cdots n_1 n_0$, appelée *notation binaire* de n.

Démonstration. Le résultat 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 $2^s \leq n$. Posant $m = n - 2^s$, on a $0 \leq m < 2^s$. 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.

Remarque. La notation binaire de n est un mot binaire.

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

Exercice. Donner la notation binaire de 1234.
Solution. À l'aide de MAPLE, on voit $2^{10} < 1234 < 2^{11}$. Posons $a_1 = a_0 - 2^{10} = 210$.
Comme $2^7 < a_1 < 2^8$, posons $a_2 = a_1 - 2^7 = 82$.
Comme $2^6 < a_2 < 2^7$, posons $a_3 = a_2 - 2^6 = 18$.

Comme $2^4 < a_3 < 2^5$, posons $a_4 = a_3 - 2^4 = 2$.

Ceci nous donne

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

D'où, la notation binaire de 1234 est 10011010010.

3.2.4. 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 binaire de longueur 6.
(2) $\mathcal{C}_2 = \{00000, 01101, 10110, 11011\}$ est un code binaire 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.

3.2.5. Définition. Soient k, n des entiers avec $n > k > 0$. Un (n, k)-*codeur binaire*, ou simplement *codeur*, est une application de la forme:

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

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

Remarque. Un codeur est une application injective.

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.

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

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

Exemple. $d(00101, 01100) = 2$.

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

(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. Posons $\mathbf{x} = x_1 \cdots x_n$, $\mathbf{y} = y_1 \cdots y_n$ et $\mathbf{z} = z_1 \cdots z_n$. Les deux premiers énoncés sont évidents. Pour montrer l'énoncé (3), 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 $\Sigma_2 = \{i \mid 1 \leq i \leq n;\ z_i \neq y_i\}$. Si $i \notin \Sigma_1$ et $i \notin \Sigma_2$, alors $x_i = z_i = y_i$, c'est-à-dire, $i \notin \Sigma$. Ceci montre 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.

3.2.8. 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.

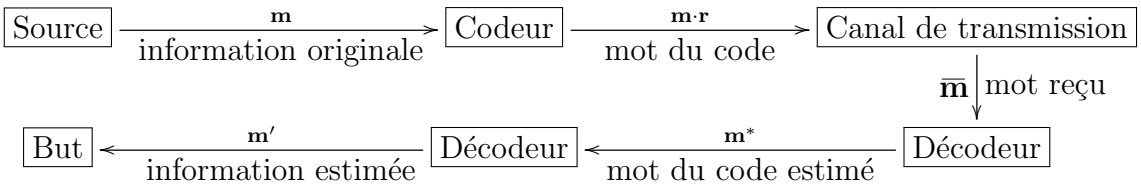
(1) Le mot expédié dans le canal de transmission est $\varphi(\mathbf{m}) = \mathbf{m} \cdot \mathbf{r}$.

(2) Si le décodeur reçoit un mot $\overline{\mathbf{m}}$, il cherche $\mathbf{m}^* \in \mathrm{Im}(\varphi)$ tel que $d(\overline{\mathbf{m}}, \mathbf{m}^*) \leq d(\overline{\mathbf{m}}, \mathbf{x})$, pour tout $\mathbf{x} \in \mathrm{Im}(\varphi)$.

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

Remarque. Si $\overline{\mathbf{m}} \in \mathrm{Im}(\varphi)$, on a alors $\mathbf{m}^* = \overline{\mathbf{m}}$.

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 000000 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 correct.

(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 correct.

(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.

3.2.9. 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. Pour tous $\mathbf{x}, \mathbf{y} \in \mathbb{Z}_2^n$, on a $\mathbf{y} \in \mathbf{B}(\mathbf{x}, \varepsilon)$ si et seulement si $\mathbf{x} \in \mathbf{B}(\mathbf{y}, \varepsilon)$.

Exemple. (1) Pour tout mot binaire $\mathbf{x}$, on voit que $B(\mathbf{x}, 0) = \{\mathbf{x}\}$.
(2) Considérons le mot binaire 0101. Alors

$$B(0101, \sqrt{2}) = \{0101, 1101, 0001, 0111, 0100\}.$$

En particulier, $0000 \notin B(0101, \sqrt{2})$.

3.2.10. 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 $\mathbf{x} \in \mathbb{Z}_2^n$.

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 $0 \leq s \leq t$.

Le résultat suivant explique la signification d'être capable de corriger t erreurs.

3.2.11. Proposition. Soit $\mathcal{C}$ un code capable de corriger t erreurs. Soient $\mathbf{x}_0 \in \mathcal{C}$ un mot expédié dans le canal de transmission et $\mathbf{x}$ le mot reçu par le décodeur. Si $d(\mathbf{x}_0, \mathbf{x}) \leq t$, alors l'estimé de $\mathbf{x}$ par le décodeur sera $\mathbf{x}_0$.

Démonstration. Supposons que $d(\mathbf{x}_0, \mathbf{x}) \leq t$. Alors $\mathbf{x}_0 \in \mathcal{C} \cap B(\mathbf{x}, t)$. Supposons que $\mathbf{y}$ est l'estimé de $\mathbf{x}$ par le décodeur. Alors $\mathbf{y} \in \mathcal{C}$, et comme $\mathbf{x}_0 \in \mathcal{C}$, on a $d(\mathbf{y}, \mathbf{x}) \leq d(\mathbf{x}_0, \mathbf{x}) \leq t$. C'est-à-dire, $\mathbf{y} \in \mathcal{C} \cap B(\mathbf{x}, t)$. Comme $|\mathcal{C} \cap B(\mathbf{x}, t)| \leq 1$ par l'hypothèse, $\mathbf{y} = \mathbf{x}_0$. La preuve de la proposition s'achève.

Exemple. Considérons le code $\mathcal{C}_1 = \{000000, 010101, 101010, 111111\}$. On voit que $\mathcal{C}_1$ est incapable de corriger 2 erreurs. En effet, $000000, 010101 \in \mathcal{C}_1$ avec $d(000000, 000101) \leq 2$ et $d(010101, 000101) \leq 2$. C'est-à-dire, $000000, 010101 \in \mathcal{C}_1 \cap B(000101, 2)$.

3.2.12. 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 $\mathbf{x}_1, \mathbf{x}_2 \in \mathcal{C} \cap B(\mathbf{y}, t)$, 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 $\mathbf{x}_1, \mathbf{x}_2 \in \mathcal{C} \cap B(\mathbf{y}, t)$. Ainsi $\mathcal{C}$ est incapable de corriger t erreurs. Ceci achève la démonstration de la proposition.

3.2.13. 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.

Exemple. Considérons $\mathcal{C}_1 = \{000000, 010101, 101010, 111111\}$. Comme $\mathcal{C}_1$ est incapable de corriger 2 erreurs, $\delta(\mathcal{C}_1) < 2$.

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

3.2.14. Définition. Soit $\mathcal{C}$ un code non trivial. On définit la *distance minimum* de $\mathcal{C}$ comme étant

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

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 éloignés les uns des autres.

Exemple. (1) On voit que $d(\mathcal{C}_1) = d(\mathcal{C}_2) = 3$, où

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

(2) Si $\mathcal{C} = \mathbb{Z}_2^n$, alors $d(\mathcal{C}) = 1$. En effet, $d(\mathcal{C}) \geq 1$. De l'autre côté, on voit que $\mathbf{0} = 00\cdots0$ et $\mathbf{x} = 10\cdots0 \in \mathcal{C}$ sont tels que $d(\mathbf{0}, \mathbf{x}) = 1$. D'où, $d(\mathcal{C}) \leq d(\mathbf{0}, \mathbf{x}) = 1$. Par conséquent, $d(\mathcal{C}) = 1$.

3.2.15. 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 $s = [\frac{d(\mathcal{C})-1}{2}] \geq 1$. Par définition, $2s \leq d(\mathcal{C}) - 1 < 2(s+1)$. On veut montrer que $\mathcal{C}$ est capable de corriger s erreurs, mais incapable de corriger $s+1$ erreurs.

Supposons que $\mathcal{C}$ est incapable de corriger s erreurs. D'après la proposition 3.2.12, 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.

Ensuite, on a

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

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 $z_i = x_i = y_i$ 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 $\mathbf{z} \in B(\mathbf{y}, s + 1)$. Donc, $B(\mathbf{x}, s + 1) \cap B(\mathbf{y}, s + 1)$ est non vide. D'après la proposition 3.2.12, $\mathcal{C}$ est incapable de corriger $s + 1$ 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.

Exemple. (1) Si $\mathcal{C} = \mathbb{Z}_2^n$, alors $d(\mathcal{C}) = 1$, et donc $\delta(\mathcal{C}) = 0$.

(2) Considérons les codes suivants:

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

On a vu que $d(\mathcal{C}_1) = d(\mathcal{C}_2) = 3$, d'après le théorème 3.2.15, $\delta(\mathcal{C}_1) = \delta(\mathcal{C}_2) = 1$. Autrement dit, $\mathcal{C}_1$ et $\mathcal{C}_2$ sont tous capables de corriger une erreur, mais incapables de corriger deux erreurs.

La cardinalité d'un code $\mathcal{C}$ s'appelle *capacité expressive* de $\mathcal{C}$. Plus la capacité expressive est grande, plus le code est capable d'exprimer. En vertu du théorème 3.2.15, pour qu'un code soit fiable, il faut que ses mots soient éloignés 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 éloignés les uns des autres, plus la capacité expressive est petite.

3.2.16. 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 3.2.15, on a $2\,\delta \leq d(\mathcal{C}) - 1 < n$. Posant $m = n - (d(\mathcal{C}) - 1)$, on obtient $0 < m \leq n - 2\,\delta$. 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. En effet, si l'on considère un mot de longueur n comme un vecteur du $\mathbb{Z}_2$-espace vectoriel $\mathbb{Z}_2^n$, un code de longueur n est considéré comme un sous-ensemble non vide du $\mathbb{Z}_2$-espace vectoriel $\mathbb{Z}_2^n$.

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. En effet,

$$11001 + 11100 = 00101,\ 11001 + 00101 = 11100,\ 11100 + 00101 = 11001.$$

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*.

3.3.3. Proposition. Si $\mathcal{C}$ est un (n,k)-code linéaire avec $0 < k \leq n$, alors $\mathcal{C} = \mathscr{L}(G)$, où G est une matrice binaire de type $k \times n$, appelée une *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 $\{u_1, \ldots, u_k\}$. Posons G la matrice dont les lignes sont $u_1, \ldots, u_k \in \mathbb{Z}_2^n$. Alors G est de type $k \times n$ telle que $\mathscr{L}(G) =< u_1, \ldots, u_k >= \mathcal{C}$. La preuve de la proposition s'achève.

Le résultat suivant donne une autre interprétation d'une matrice génératrice d'un code linéaire.

3.3.4. Proposition. Soit $\mathcal{C}$ un (n,k)-code linéaire avec $0 < k \leq n$. Si G est une matrice binaire de n colonnes, alors les conditions suivantes sont équivalentes.

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

(2) Les lignes de G sont linéairement indépendantes telles que $\mathcal{C} = \mathscr{L}(G)$.

(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 les lignes G sont $G_1, \ldots, G_s$. En particulier, G est de type $s \times n$.

Supposons que $\mathcal{C} = \mathscr{L}(G)$ et $s = k = \dim \mathcal{C}$. Ainsi $s = \dim \mathscr{L}(G) = \mathrm{rg}(G)$. D'après le théorème 3.1.2(3), $G_1, \ldots, G_s$ sont linéairement indépendantes. Ainsi, (1) implique (2).

Supposons que $G_1, \ldots, G_s$ sont linéairement indépendantes et $\mathcal{C} =< G_1, \ldots, G_s >$. C'est-à-dire, $\{G_1, \ldots, G_s\}$ est une base de $\mathcal{C}$. Donc, (2) implique (3).

Supposons que $\{G_1, \ldots, G_s\}$ est une base de $\mathcal{C}$. Alors $\mathcal{C} =< G_1, \ldots, G_s >= \mathscr{L}(G)$ et $s = \dim \mathcal{C} = k$. Ainsi, G est une matrice génératrice de $\mathcal{C}$. En particulier, (3) implique (4).

Supposons que G s'échelonne à une matrice génératrice G' de $\mathcal{C}$. En particulier, G est de type $k \times n$. D'après le théorème 3.1.3(1), $\mathscr{L}(G) = \mathscr{L}(G') = \mathcal{C}$. C'est-à-dire, G est une matrice génératrice de $\mathcal{C}$. Donc, (4) implique (1). La preuve de la proposition s'achève.

En tant que conséquence immédiate du théorème 3.1.3(3) et de la proposition 3.3.4(3), on a une méthode pour trouver une matrice génératrice d'un code linéaire.

3.3.5. Corollaire. Soit $\mathcal{C}$ un code linéaire non trivial tel que $\mathcal{C} = \mathscr{L}(M)$, où M est une matrice binaire. Si N est une forme échelonnée de M, alors les lignes non nulles de N forment une matrice génératrice de $\mathcal{C}$.

Exemple. Trouver une matrice de génératrice du code linéaire

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

Solution. Il est évident que $\mathcal{C} = \mathscr{L}(M)$, où

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

Maintenant M s'échelonne à la matrice échelonnée

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

D'après le corollaire 3.3.5, $\mathcal{C}$ a pour matrice génératrice

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

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

3.3.6. Théorème. Soit $\mathcal{C}$ un (n, k)-code linéaire non trivial, dont G est une matrice génératrice. Si M est une matrice formée par tous les éléments de $\mathbb{Z}_2^k$, alors les lignes de MG sont 2 à 2 distinctes et sont les mots de $\mathcal{C}$. En particulier, $|\mathcal{C}| = 2^k$.

Démonstration. D'après le lemme 3.3.4(3), on a

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

où $G_1, \ldots, G_k$ forment une base de $\mathcal{C}$. Or, les éléments de $\mathbb{Z}_2^k$ s'écrivent $u_i = (a_{i1}, \ldots, a_{ik})$ avec $a_{ij} \in \mathbb{Z}_2$, pour $i = 1, \ldots, 2^k$. Posons

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

D'après le lemme 3.1.5(2), on a

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

et d'après le lemme 3.1.4(1), on a

$$u_iG = (a_{i1}, \ldots, a_{ik})G = a_{i1}G_1 + \cdots + a_{ik}G_k \in \mathcal{C};\ i = 1, 2, \ldots, 2^k.$$

Comme $\{G_1, \ldots, G_k\}$ est libre, les u_iG 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

$$u = a_1G_1 + \cdots + a_kG_k = (a_1, \ldots, a_k)G,$$

où $(a_1, \ldots, a_k) \in \mathbb{Z}_2^k$. Or $(a_1, \ldots, a_k) = u_j$, pour un certain 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

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

Solution. Par l'hypothèse, $\mathcal{C}$ est un $(6, 2)$-code linéaire. Les éléments de $\mathbb{Z}_2^2$ forment une matrice

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

Calculons

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

D'après le théorème 3.3.6, on a

$$\mathcal{C} = \{000000, 100110, 010101, 110011\}.$$

Soit $M \in M_{m\times n}(\mathbb{Z}_2)$. En transposant les vecteurs de $\mathscr{N}(M)$, on obtient

$$\mathscr{N}^T(M) = \{\mathbf{x} \in \mathbb{Z}_2^n \mid M\mathbf{x}^T = \mathbf{0}\},$$

un sous-espace vectoriel de $\mathbb{Z}_2^n$. Ceci nous donne une autre méthode pour trouver des codes linéaires.

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

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

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

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

3.3.8. Définition. Soit $\mathcal{C}$ un (n, k)-code linéaire avec $0 \leq k < n$. Une *matrice de contrôle* de $\mathcal{C}$ est, par définition, une matrice binaire H de type $(n - k) \times n$ telle que $\mathcal{C} = \mathscr{N}^T(M)$.

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

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

Le résultat suivant donne, en particulier, une autre intéprétation de matrice de contrôle d'un code linéiare.

3.3.9. 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) Les lignes de H sont linéairement indépendantes telles que $\mathcal{C} = \mathscr{N}^T(H)$.

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

Démonstration. Supposons que $\mathcal{C} = \mathscr{N}^T(H)$ avec H de type $(n - k) \times n$. On a alors $k = \dim \mathcal{C} = \dim \mathscr{N}^T(H) = n - \text{rg}(H)$. D'où, $\text{rg}(H) = n - k$. D'après le théorème 3.1.2(3), les lignes de H sont linéairement indépendantes. Ainsi, (1) implique (2).

Supposons que $\mathcal{C} = \mathscr{N}^T(H)$ avec H de s lignes linéairement indépendantes. D'après le théorème 3.1.2(3), $\text{rg}(H) = s$. D'après le lemme 3.3.7, $n - s = \dim(\mathcal{C}) = k$. D'où, $s = n - k$. C'est-à-dire, H est une matrice de contôle de $\mathcal{C}$. En particulier, (2) implique (3).

Supposons 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 $(n - k) \times n$. Ainsi, H est de type $(n - k) \times n$. En outre, d'après le théorème 3.1.3(1), $\mathscr{N}(H') = \mathscr{N}(H)$. Par conséquent, $\mathcal{C} = \mathscr{N}^T(H') = \mathscr{N}^T(H)$. C'est-à-dire, H est aussi une matrice de contrôle de $\mathcal{C}$. Ainsi, (4) implique (1). La preuve du lemme s'achève.

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

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

Solution. Pour tout $\mathbf{x} = x_1x_2x_3 \in \mathbb{Z}^3$, on voit que $\mathbf{x} \in \mathcal{C}$ si et seulement si $\mathbf{x} \in \mathrm{Im}(\phi)$ si et seulement si $x_3 = x_1 + x_2$ si et seulement si $x_1 + x_2 + x_3 = 0$ si et seulement si $x_1x_2x_3 \in \mathscr{N}^T(H)$, où $H = (1\,1\,1)$. C'est-à-dire, $\mathcal{C} = \mathscr{N}^T(H)$. Comme la seule ligne de H est non nulle, d'après le lemme 3.3.9(2), H est une matrice de contrôle de $\mathcal{C}$.

Le résultat suivant nous dit comment trouver une matrice de contrôle d'un code linéaire.

3.3.10. Corollaire. 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. En vue du théorème 3.1.3, on voit que les lignes de H sont linéairement indépendantes telles que $\mathscr{N}(H) = \mathscr{N}(M)$. D'où, $\mathscr{N}^T(H) = \mathscr{N}^T(M) = \mathcal{C}$. D'après le lemme 3.3.9(2), H est une matrice de contrôle de $\mathcal{C}$. La preuve du corollaire s'achève.

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

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

Solution. Comme M s'échelonne à la matrice échelonnée

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

D'après le corollaire 3.3.10, la matrice

$$H = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \end{pmatrix}$$

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

On étudiera un genre spécial de codes linéaires.

3.3.11. Définition. Un (n, k)-code linéaire $\mathcal{C}$ avec $0 < k < n$ est dit *standard* s'il admet une matrice génératrice de la forme $(I_k \mid A)$, appelée *matrice génératrice canonique* de $\mathcal{C}$.

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

Démonstration. D'abord, on a

$$101 + 011 = 110,\ 101 + 110 = 011,\ 011 + 110 = 101 \in \mathcal{C}$$

D'après le lemme 3.3.2, $\mathcal{C}$ est un code linéaire. Ainsi $\mathcal{C} = \mathscr{L}(M)$, où

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

Maintenant, M s'échelonne à une matrice échelonnée

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

D'après le corollaire 3.3.5, $\mathcal{C}$ a pour matrice génératrice

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

Ainsi, $\mathcal{C}$ est un $(3, 2)$-code standard dont G est la matrice génératrice canonique.

Pour étudier les codes standards, on a besoin du résulat suivant.

3.3.12. Lemme. Soient M, N des matrices binaires de n colonnes.
(1) Si M est de la forme $(A \mid I_k)$, alors $\mathrm{rg}(M) = k$.
(2) $\mathscr{L}(N) \subseteq \mathscr{N}^T(M)$ si et seulement si $MN^T = 0$.

Démonstration. (1) Supposons que $M = (A \mid I_k)$. Alors $\mathrm{rg}(M) \leq k$. Comme les dernières k colonnes de M sont linéairement indépendantes, $k \geq \dim\mathscr{C}(M) = \mathrm{rg}(M)$. D'où, $\mathrm{rg}(M) = k$.

(2) Soient $N_1, \ldots, N_p$ les lignes de N. Alors $N^T = (N_1^T \cdots N_p^T)$ partagée en colonnes. D'après le lemme 3.1.5(1), on a

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

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.

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

3.3.13. Théorème. Soit $\mathcal{C}$ un (n,k)-code standard. Si $G = (I_k \mid A)$ est la matrice génératrice canonique de $\mathcal{C}$, alors $H = (A^T \mid I_{n-k})$ est une matrice de contrôle de $\mathcal{C}$.

Démonstration. Par hypothèse, H est de type $(n-k)\times n$. D'après le lemme 3.3.12(1), $\mathrm{rg}(H) = n-k$. D'après le lemme 3.3.7, $\dim \mathscr{N}^T(H) = n-(n-k) = k = \dim \mathcal{C}$. En outre, appliquant la multiplication par blocs, on trouve

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

D'après le lemme 3.3.12(2), $\mathcal{C} = \mathscr{L}(G) \subseteq \mathscr{N}^T(H)$. Donc, $\mathcal{C} = \mathscr{N}^T(H)$. Ainsi, H est une matrice de contrôle de $\mathcal{C}$. Ceci achève la démonstration du théorème.

Remarque. Une matrice de contrôle d'un (n,k)-code standard de la forme $(B \mid I_{n-k})$ s'appelle *matrice de contrôle canonique*.

Exemple. Considérer le code $\mathcal{C} = \{00000, 10101, 11100, 01001\}$.

(1) Vérifier que $\mathcal{C}$ est standard.

(2) Donner la matrice de contrôle canonique de $\mathcal{C}$.

Solution. Comme

$$10101 + 11100 = 01001, 10101 + 01001 = 11100, 11100 + 01001 = 10101,$$

on voit que $\mathcal{C}$ est linéaire. Donc, $\mathcal{C} = \mathscr{L}(M)$, où

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

Comme M séchelonne à

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

D'après le corollaire 3.3.5, $\mathcal{C}$ a pour matrice génératrice

$$G = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix} = (I_2 \mid A).$$

C'est-à-dire, $\mathcal{C}$ est un $(5,2)$-code standard. D'après le théorème 3.3.13, la matrice

$$H = (A^T \mid I_{5-2}) = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

est la matrice de contrôle canonique de $\mathcal{C}$. C'est-à-dire, pour tout $\mathbf{x} = x_1x_2x_3x_4x_5 \in \mathbb{Z}_2^5$, on a que $\mathbf{x} \in \mathcal{C}$ si et seulement si

$$\begin{array}{rcrcrcrcl} x_1 & & & + & x_3 & & & = & 0 \\ & & & & & & x_4 & = & 0 \\ x_1 & + & x_2 & & & + & x_5 & = & 0. \end{array}$$

Réciproquement, on peut trouver la matrice génératrice canonique d'un code standard à partir de sa matrice de contrôle canonique.

3.3.14. Théorème. Soit $\mathcal{C} = \mathscr{N}^T(H)$. Si $H = (A \mid I_{n-k})$, alors $\mathcal{C}$ est un (n,k)-code standard dont H est la matrice de contrôle canonique et $G = (I_k \mid A^T)$ est la matrice génératrice canonique.

Démonstration. D'après le lemme 3.3.12, $\mathrm{rg}(H) = n - k$. Ainsi les lignes de H sont linéairement indépendantes. D'après le lemme 3.3.9(2), H est une matrice de contrôle de $\mathcal{C}$.

Posons $\mathcal{D} = \mathscr{L}(G)$, où $G = (I_k \mid A^T)$. Comme G est échelonnée de rang k, ses lignes sont linéairement indépendantes. D'après la proposition 3.3.4(2), G est une matrice génératrice de $\mathcal{D}$. Par définition, $\mathcal{D}$ est un (n,k)-code standard dont G est la matrice génératrice canonique. D'après le théorème 3.3.13, $\mathcal{D}$ a pour matrice de contrôle $((A^T)^T \mid I_{n-k}) = H$. Ainsi, $\mathcal{D} = \mathscr{N}^T(H) = \mathcal{C}$. La preuve du théorème s'achève.

Exemple. Soit $\mathcal{C} = \mathscr{N}^T(M)$, où

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

Vérifier que $\mathcal{C}$ est standard et donner sa matrice de contrôle canonique et sa matrice génératrice canonique.

Solution. On échelonne M à la matrice suivante

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

En vertu du théorème 3.1.3(1) et (2), $\mathcal{C} = \mathscr{N}^T(H)$, où

$$H = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} = (A \mid I_3).$$

D'après le théorème 3.3.14, $\mathcal{C}$ est un code standard ayant dont la matrice de contrôle canonique est H et la matrice génératrice canonique est la matrice suivante:

$$G = (I_2 \mid A^T) = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \end{pmatrix}.$$

On donnera une autre interprétation de codes standards.

3.3.15. Définition. Soient des entiers $n > k > 0$. Un (n, k)-codeur

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

est dit *linéaire* si φ est une application linéaire.

Le résultat suivant nous dit que les codes standards sont exactement les codes définis par les codeurs binaires linéaires.

3.3.16. Théorème. Un code $\mathcal{C}$ est un (n, k)-code standard dont G est la matrice génératrice canonique si, et seulement si, $\mathcal{C}$ est défini par un (n, k)-codeur linéaire suivant:

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

Démonstration. Supposons que $\mathcal{C}$ est un (n, k)-code standard, dont $G = (I_k \mid A)$ est la matrice génératrice canonique, où $A \in M_{k\times(n-k)}(\mathbb{Z}_2)$. Considérons l'application linéaire

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

où $\mathbf{r}_\mathbf{x} = \mathbf{x}A$. Par définition, φ est un (n, k)-codeur linéaire. D'après la proposition 3.1.9, $\mathrm{Im}(\varphi) = \mathscr{L}(G) = \mathcal{C}$. C'est-à-dire, $\mathcal{C}$ est le code défini par φ.

Supposons réciproquement 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. Comme φ est injective, en vertu de la proposition 3.1.8(2), dim$\mathcal{C}$ est un sous-espace de $\mathbb{Z}_2^n$ de dimension k. C'est-à-dire, $\mathcal{C}$ est un (n, k)-code linéaire.

D'après la proposition 3.1.9, il existe une matrice $G = (B \mid A)$, où $B \in M_{k\times k}(\mathbb{Z}_2)$ et $A \in M_{k\times(n-k)}(\mathbb{Z}_2)$, telle que φ est de la forme

$$\varphi : \mathbb{Z}_2^k \to \mathbb{Z}_2^n : \mathbf{x} \mapsto \mathbf{x}G = (\mathbf{x}B \mid \mathbf{x}A).$$

D'après la proposition 3.1.9, $\mathcal{C} = \mathscr{L}(G)$. Ainsi, G est une matrice génératrice de $\mathcal{C}$.

En outre, pour tout $\mathbf{x} \in \mathbb{Z}_2^k$, comme $\mathbf{x} \cdot \mathbf{r}_\mathbf{x} = (\mathbf{x}B \mid \mathbf{x}A)$, on a $\mathbf{x} = \mathbf{x}B$. Soit $\{e_1, \ldots, e_k\}$ la base canonique de $\mathbb{Z}_2^k$. On a $e_i = e_iB$, ce qui est la i-ième ligne de B, pour $i = 1, \ldots, k$.

Ainsi, $B = I_k$. Donc, $\mathcal{C}$ est standard ayant G pour matrice génératrice canonique. La preuve du théorème s'achève.

Exemple. Trouver le codeur linéaire qui définit le code standard

$$\mathcal{C} = \{000, 101, 011, 110\}.$$

Solution. On a vu que la matrice génératrice canonique de $\mathcal{C}$ est

$$G = \left(\begin{array}{cc|c} 1 & 0 & 1 \\ 0 & 1 & 1 \end{array}\right).$$

D'après le théorème 3.3.16, $\mathcal{C}$ est le code défini par le codeur lináire suivant:

$$\varphi : \mathbb{Z}_2^2 \to \mathbb{Z}_2^3 : \mathbf{x} \mapsto \mathbf{x}G.$$

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 $\mathcal{C}$.

Solution. Remarquons que φ est de la forme

$$\varphi_2 : \mathbb{Z}_2^2 \to \mathbb{Z}_2^5 : (a_1, a_2) \mapsto (a_1, a_2, a_1 + a_2, a_1, a_2) = (a_1, a_2)G,$$

où

$$G = \left(\begin{array}{cc|ccc} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{array}\right).$$

Ainsi φ_2 est un codeur linéaire. Par conséquent, le code

$$\mathcal{C} = \{00000, 01101, 10110, 11011\}$$

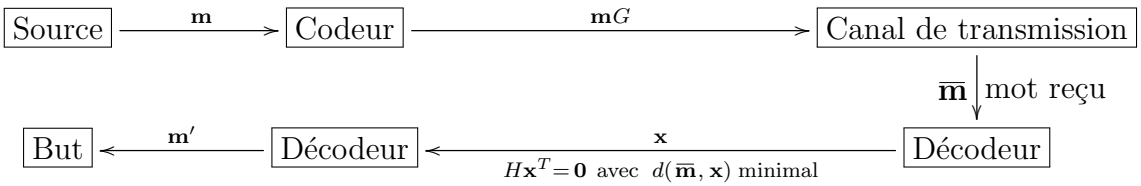
est standard de dimension 2, dont G est la matrice génératrice canonique. D'après le théorème 3.3.13, $\mathcal{C}$ a pour matrice de contrôle

$$H = \left(\begin{array}{cc|ccc} 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{array}\right).$$

C'est-à-dire, $a_1a_2a_3a_4a_5 \in \mathcal{C}$ si et seulement si $(a_1, a_2, a_3, a_4, a_4)$ est la solution du système homogène d'équations linéaires suivant:

$$\begin{array}{rcrcrcrcl} x_1 & + & x_2 & + & x_3 & & & = & 0 \\ x_1 & & & & & + & x_4 & = & 0 \\ & & x_2 & & & & + \ x_5 & = & 0. \end{array}$$

Voici 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 $\mathbf{x}$.

On conclut cette section par une étude de la capacité correctrice de codes linéaires.

3.3.17. Définition. Le *poids* d'un mot $\mathbf{x}$, noté $w(\mathbf{x})$, est le nombre de ses bits non nuls.

Remarque. Pour tout mot $\mathbf{x}$, on a $w(\mathbf{x}) = 0$ si, et seulement si, $\mathbf{x} = \mathbf{0}$.

Exemple. $w(111) = 3$ et $w(100010) = 2$.

3.3.18. Définition. Soit $\mathcal{C}$ un code linéaire non trivial. On définit *poids minimum* de $\mathcal{C}$ comme étant

$$w(\mathcal{C}) = \min\{w(\mathbf{x}) \mid \mathbf{0} \neq \mathbf{x} \in \mathcal{C}\}.$$

3.3.19. Théorème. 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,

$$d(\mathcal{C}) = d(\mathbf{x}, \mathbf{y}) = |\{1 \leq i \leq n \mid x_i \neq y_i\}| = |\{1 \leq i \leq n \mid z_i \neq 0\}| = w(\mathbf{x} - \mathbf{y}) \geq w(\mathcal{C}).$$

D'où, $d(\mathcal{C}) = w(\mathcal{C})$. La preuve du lemme s'achève.

Exemple. Considérons le code linéaire

$$\mathcal{C} = \{00000, 01101, 10110, 11011\}.$$

On voit que $w(\mathcal{C}) = 3$. D'où, $\delta(\mathcal{C}) = [\frac{3-1}{2}] = 1$.

Voici une autre interprétation du poids minimum de $\mathcal{C}$.

3.3.20. Lemme. Soit $\mathcal{C}$ un code linéaire non trivial, dont H est une matrice de contrôle.
(1) Les colonnes de H sont linéairement dépendantes.
(2) $w(\mathcal{C})$ est le plus petit entier s tel que H admet s colonnes linéairement dépendantes.
Démonstration. Écrivons $H = (H_1 H_2 \cdots H_n)$ en colonnes.
(1) Par l'hypothèse, $\mathcal{C}$ contient un mot non nul $\mathbf{x} = x_1 \cdots x_n$. Ceci donne

$$x_1 H_1 + \cdots + x_n H_n = H\mathbf{x}^T = \mathbf{0}.$$

Comme $x_1, \ldots, x_n$ ne sont pas tous nuls, $H_1, \ldots, H_n$ sont linéairement dépendantes.

(2) 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

$$\mathbf{0} = H\,\mathbf{y}^T = \sum\nolimits_{j=1}^{n} b_j H_j = b_{i_1} H_{i_1} + \cdots + b_{i_d} H_{i_d}.$$

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.

3.3.21. Théorème. Soit $\mathcal{C}$ un code linéaire non trivial, dont H est une matrice de contrôle. Il exists un entier maximal m avec $0 \leq m < n$ tel que toute famille de m colonnes de H est libre; et dans ce cas,

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

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 trivial, $\{H_1, \ldots, H_n\}$ est liée. Ainsi il existe un entier maximal m avec $0 \leq m \leq n$ tel que toute famille de m colonnes de H est libre.

Posons $w(\mathcal{C}) = s$, le plus petit entier tel qu'il existe une famille liée $\{H_{i_1}, \cdots, H_{i_s}\}$ avec $1 \leq i_1 < \cdots < i_s \leq n$. Par la maximalité de m, il existe une famille liée de $m+1$ colonnes de H. Ainsi, $s \leq m+1$. Si $s \leq m$, alors $\{H_{i_1}, \cdots, H_{i_s}\}$ est contenue dans une famille $\{H_{j_1}, \ldots, H_{j_m}\}$ avec $1 \leq j_1 < \cdots < j_m \leq n$. D'après la définition de m, $\{H_{j_1}, \ldots, H_{j_m}\}$ est libre, et donc, $\{H_{i_1}, \cdots, H_{i_s}\}$ est libre, une contradiction. Ainsi $s \geq m+1$, et donc $s = m+1$. 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.

Exemple. Calculer la capacité correctrice d'un code linaire $\mathcal{C}$, dont une matrice de contrôle est

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

Solution. Soit m le plus grand entier tel que toute famille de m colonnes de H est libre. Comme les colonnes de H sont toutes non nulles et deux à deux distinctes, toute famille de 2 colonnes de H est libre, et donc $m \geq 2$. De l'autre côté, on voit que les trois premières colonnes de H sont linéairement dépendantes. Ainsi $m < 3$, et donc $m = 2$. D'après le théorème 3.3.21, $\delta(\mathcal{C}) = [\frac{m}{2}] = 1$.

3.4 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 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.

3. 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 $\mathscr{N}(M)$.

4. (1) Vérifier que $u_1 = (-1, 1, 1)$, $u_2 = (1, 2, 1)$, $u_3 = (0, 1, 2)$ forment une base de $\mathbb{R}^3$.
   (2) Exprimer $u = (x, y, z) \in \mathbb{R}^3$ comme une combinaison linéaire de u_1, u_2, u_3.
   (3) Trouver une application linéaire $T : \mathbb{R}^3 \to \mathbb{R}^4$ satisfait à la condition suivante:
   $$T(u_1) = T(u_2) = (1, 0, 2, 1),\ T(u_3) = (0, 1, -1, 2).$$
   Indice: Utiliser la partie (2).
   (4) Donner une base de l'image de l'application linéaire T trouvée ci-dessus. *Indice*: Utiliser la proposition 3.1.7 et le théorème 3.1.3.

5. 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.

6. Trouver la notation binaire de 1762.

7. 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?

8. 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 $\mathbf{x} \neq \mathbf{0}, \mathbf{1}$.

9. 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.

10. 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 $B(\mathbf{y}, 3)$.

11. 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.

12. 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 $\delta(\mathcal{C})$.

13. 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.

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

(2) Donner à l'aide du théorème 3.3.6, tous les mots de $\mathcal{C}$.

15. Considérer le code suivant:

$$\mathcal{C} = \{000000, 011110, 101101, 110011, 001011, 010101, 100110, 111000\}.$$

(1) Vérifier, à l'aide du lemme 3.3.2, que $\mathcal{C}$ est linéaire.

(2) Vérifier que $\mathcal{C}$ est un code standard en donnant sa matrice génératrice canonique.

(3) Trouver la matrice de contrôle canonique de $\mathcal{C}$.

16. 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.

17. Considérer le code linéaire $\mathcal{C} = \mathscr{L}(M)$, où

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

(1) Vérifier que $\mathcal{C}$ est standard en donnant sa matrice génératrice canonique.

(2) Trouver la matrice de contrôle canonique de $\mathcal{C}$.

(3) Donner, à l'aide du théorème 3.3.6, la capacité expressive de $\mathcal{C}$.

18. 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.

19. Soit $\mathcal{C}$ un code linéaire dont H est une matrice de contrôle. Montrer que $\mathcal{C}$ ne contient que le mot nul $\mathbf{0}$ (c'est-à-dire, le mot dont tous les bits sont 0) si et seulement si les colonnes de H sont linéairement indépendantes.

20. Si n, k sont des entiers avec $0 < k < n$, trouver le nombre de (n, k)-codes standards.

21. 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 $\mathbf{m}$?

22. Donner un $(6, 3)$-code standard $\mathcal{C}$ contenant le mot 111111, en spécifiant ses mots et une matrice de contrôle.

23. 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 $HG^T = 0$.

24. 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.

25. 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.

26. Considérer le code linéaire $\mathcal{C} = \mathscr{L}(M)$, où

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

(1) Vérifier que $\mathcal{C}$ est standard en donnant sa matrice génératrice canonique.
(2) Trouver la matrice de contrôle canonique de $\mathcal{C}$.
(3) Donner, à l'aide du théorème 3.3.6, tous les mots de $\mathcal{C}$.
(4) Donner le poids minimum de $\mathcal{C}$.
(5) Donner, à l'aide du théorème 3.3.19, la capacité correctrice de $\mathcal{C}$.

27. 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) Vérifier que $\mathcal{C}$ est standrad en donnant sa matrice de contrôle canonique.

(2) Trouver la matrice génératrice canonique de $\mathcal{C}$.

(3) À l'aide du théorème 3.3.21, donner la capcité correctrice de $\mathcal{C}$.

28. 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.

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 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 ?

La construction des polygones réguliers. Pour quel entier $n > 2$, on peut construire à la régle et au compas un polygone de n côtés égaux ?

La solubilité par radicaux d'équations polynomiales. Étant donnée une équation polynomiale complexe, est-ce que ses racines s'obtiennent toujours à partir de ses coefficients par un nombre fini d'opérations d'addition, soustraction, multiplication, division et extraction de la racine ?

4.1 Polynômes

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 $\partial(f(x))$, est défini par

$$\partial(f(x)) = \begin{cases} n, & \text{si } f(x) \neq 0; \\ -\infty, & \text{si } f(x) = 0. \end{cases}$$

En outre, si $f(x)$ est non nul, alors a_n s'appelle le *coefficient directeur* de $f(x)$. 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 $g(x)$.

Solution. En faisant une division, on trouve $f(x) = g(x)(-3-x^3)+(7+9x+2x^3)$ avec $\partial(7+9x+2x^3) < \partial(g(x)$. D'où, le quotient est $-3-x^3$ et le reste est $7+9x+2x^3$.

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. Définition. Soit $f(x) \in F[x]$. 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.

4.1.6. 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 $r \in F$. Cela donne $f(a) = (a-a)q(a)+r = r$. 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.

4.1.7. 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 $\partial(g(x)), \partial(h(x)) < \partial(f(x))$.

4.1.8. 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 $\mathbb{R}$. En effet, il est de degré deux et a deux racine réelles $\pm\sqrt{2}$.

On étudiera l'irréductibité de polynômes rationnels. On commence par la notion suivante.

4.1.9. Définition. Un polynôme non nul entier

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n, \quad \text{où } a_i \in \mathbb{Z}$$

est dit *primitif* si le plus grand commun facteur des coefficients $a_0, a_1, \ldots, a_n$ est 1.

Exemple. Déterminer lequel des polynômes suivants est primitif.

(1) $f(x) = x^3 + 2x + 3$;

(2) $g(x) = 2x^2 + 4x + 10$.

Solution. (1) Les coefficients de $f(x)$ sont $1, 2, 3$. Comme $\text{pgcd}(1, 2, 3) = 1$, d'après la définition 4.1.9, $f(x)$ est primitif.

(2) Les coefficients de $g(x)$ sont $2, 4, 10$ dont 2 est un facteur commun. D'après la définition 4.1.9, $g(x)$ n'est pas primitif.

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 $f(x) = \alpha g(x)$.

Exemple. Considérons le polynôme

$$f(x) = \frac{2}{3}x^3 + \frac{6}{5}x + 4.$$

Écrivons $f(x) = \alpha g(x)$, où $\alpha \in \mathbb{Q}$ et $g(x) \in \mathbb{Z}[x]$ est primitif.

Solution. Les coefficients de $f(x)$ sont $\frac{2}{3}, \frac{6}{5}, 4$, dont les deux fractions ont pour dénominateurs communs 15. Ainsi

$$\begin{aligned} f(x) &= \frac{10}{15}x^3 + \frac{18}{15}x + \frac{60}{15} \\ &= \frac{1}{15}\left(10x^3 + 18x + 60\right) \\ &= \frac{2}{15}\left(5x^3 + 9x + 30\right) \end{aligned}$$

où $5x^3 + 9x + 30$ est un polynôme primitif puisque $\text{pgcd}(5, 9, 30) = 1$.

4.1.10. 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, $p \nmid a_r b_s$. 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.

4.1.11. Théorème de Gauss. Si $f(x) \in \mathbb{Z}[x]$ est non constant, alors f 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 4.1.10. Posons

$$g_1(x)h_1(x) = a_0 + a_1x + \cdots + a_nx^n;\ a_i \in \mathbb{Z}.$$

Alors

$$f(x) = \sum_{i=0}^{n} (\gamma a_i)x^i \in \mathbb{Z}[x].$$

D'où, $\gamma a_i \in \mathbb{Z}$, 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.

Exemple. Les polynômes $x^3 + 2x - 3$ et $5x + 2$ sont primitifs. Leur produit est

$$(x^3 + 2x - 3)(5x + 2) = (5x^4 + 10x^2 - 15x) + (2x^3 + 4x - 6) = 5x^4 + 2x^3 + 10x^2 - 11x - 6,$$

ce qui est aussi primitif, car le plus grand facteur commun de $5, 2, 10, -11, -6$ est 1.

Le résultat suivant est un critère très pratique pour qu'un polynôme rationnel soit irréductible sur $\mathbb{Q}$.

4.1.12. Critère d'Eisenstein. Soit un polynôme non constant entier

$$f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + a_nx^n \in \mathbb{Z}[x].$$

S'il existe un nombre premier p tel que

(1) $p \mid a_i$, $i = 0, 1, \ldots, n-1$;

(2) $p \nmid a_n$;

(3) $p^2 \nmid a_0$;

alors $f(x)$ est irréductible sur $\mathbb{Q}$.

Démonstration. Supposons que les conditions sont vérifiées. Supposons au contraire que $f(x)$ est réductible sur $\mathbb{Q}$. D'après le théorème de Gauss, $f(x)$ est réductible sur $\mathbb{Z}$. C'est-à-dire,

$$f(x) = (b_0 + b_1x + \cdots + b_rx^r)(c_0 + c_1x + \cdots + c_sx^s);\ \text{ où } r, s > 0;\ b_i, c_j \in \mathbb{Z}$$

avec $b_r \neq 0, c_s \neq 0$.

Comme $r + s = n$, on a $0 < r, s < n$.

Comme $a_0 = b_0 c_0$, par l'hypothèse, $p \mid b_0 c_0$. Comme p est premier, $p \mid b_0$ ou $p \mid c_0$. On peut supposer $p \mid b_0$. Comme $a_n = b_r c_s$, par l'hypothèse, $p \nmid b_r c_s$. En particulier, $p \nmid b_r$.

Par conséquent, il existe un indice t avec $0 < t \leq r$ tel que $p \mid b_i$, pour $i = 0, \ldots, t-1$, et $p \nmid b_t$. Maintenant, par la définition du produit de polynômes, on a

$$a_t = \sum\nolimits_{i+j=t} b_i c_j = b_t c_0 + \sum\nolimits_{i+j=t,\, i<t} b_i c_j.$$

Comme $t \leq r < n$, on a $p \mid a_t$ par l'hypothèse; et $p \mid b_i c_j$ pour tout $0 \leq i < t$. Ceci implique $p \mid b_t c_0$. Comme $p \nmid b_t$, on a $p \mid c_0$. Ainsi $p^2 \mid b_0 c_0 = a_0$, une contradiction. Donc $f(x)$ est irréductible sur $\mathbb{Q}$. Ceci achève la démonstration du théorème.

Exercice. Soit p un nombre premier. Vérifier, pour tout $n > 1$, que $\sqrt[n]{p}$ est irrationnel.

Preuve. Considérons $f(x) = x^n - p \in \mathbb{Z}[x]$. Or p est premier tel que

(i) $p \mid (-p)$;

(ii) $p \nmid 1$;

(iii) $p^2 \nmid (-p)$.

D'après le critère d'Eisenstein, $f(x)$ est irréductible sur $\mathbb{Q}$. Comme $f(\sqrt[n]{p}) = p - p = 0$, on voit que $\sqrt[n]{p}$ est une racine réelle de $h(x)$. Comme $n \geq 2$, d'après le lemme 4.1.8(2), $f(x)$ n'a aucune racine rationnelle. D'où, $\sqrt[n]{p}$ est irrationnel.

Exercice. Vérifier que

$$f(x) = \frac{2}{9}x^5 + \frac{5}{3}x^4 + x^3 + \frac{1}{3}$$

est irréductible sur $\mathbb{Q}$.

Preuve. Comme $f(x) \notin \mathbb{Z}[x]$, on ne peut pas appliquer directement le critère d'Eisenstein. Mais, on peut considérer

$$g(x) = 9f(x) = 2x^5 + 15x^4 + 9x^3 + 3 \in \mathbb{Z}[x].$$

Or 3 est premier tel que

(i) $3 \mid 3, 9, 15$;

(ii) $3 \nmid 2$;

(iii) $3^2 \nmid 3$.

D'après le critère d'Eisenstein, $g(x)$ est irréductible sur $\mathbb{Q}$. Donc $f(x)$ l'est également.

Pour la plupart de polynômes entiers, on ne peut pas trouver un premier p qui vérifie les conditions du critère d'Esenstein. Le résultat suivant nous permet de changer les coefficients d'un tel polynôme.

4.1.13. 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. D'abord, comme $a \neq 0$, on voit que $\partial(f(ax+b)) = \partial(f(x))$. Supposons premièrement que $f(x) = f_1(x)f_2(x)$, où $f_1(x), f_2(x) \in \mathbb{Q}[x]$ avec $\partial(f_1),\ \partial(f_2) > 0$. Alors

$$g(x) = f(ax + b) = f_2(ax + b)f_2(ax + b) = g_1(x)g_2(x),$$

où $g_i(x) = f_i(ax + b)$. Comme $\partial(g_i(x)) = \partial(f_i(x))$, on voit que $g(x)$ est réductible sur $\mathbb{Q}$.

Supposons réciproquement que $g(x)$ est réductible sur $\mathbb{Q}$. Alors

$$g\left(\frac{1}{a}x - \frac{b}{a}\right) = f\left(a \cdot \frac{x - b}{a} + b\right) = f(x),$$

ce qui est réductible sur $\mathbb{Q}$. Ceci achève la démonstration de la proposition.

Exercice. Vérifier que

$$f(x) = x^3 - \frac{3}{4}x - \frac{1}{8}$$

est irréductible sur $\mathbb{Q}$.

Démonstration. Remarquons que le critère d'Eisenstein ne s'applique qu'aux polynômes sur $\mathbb{Z}$. Ainsi, on écrit

$$f(x) = \frac{1}{8}\left(8x^3 - 6x - 1\right)$$

et considère $g(x) = 8x^3 - 6x - 1$. Dans ce cas, on ne peut pas trouver un premier p qui satisfait aux conditions énoncées dans le critère d'Eisenstein. Ainsi, on doit appliquera la propoisition 4.1.13 pour changer les coefficients. En remplaçant x par $x - 1$, on trouve

$$g(x - 1) = 8x^3 - 24x^2 + 18x - 3 := h(x).$$

Maintenant, 3 est premier tel que

(i) $3 \mid -3, 18, -24$;

(ii) $3 \nmid 8$;

(iii) $3^2 \nmid -3$.

D'après le critère d'Eisenstein, $h(x)$ est irréductible sur $\mathbb{Q}$. D'après la proposition 4.1.13, $g(x)$ est irréductible sur $\mathbb{Q}$. Par conséquent, $f(x)$ est irréductible sur $\mathbb{Q}$.

4.2 Extensions de corps

Rappelons qu'un corps est un anneau commutatif dont tous les élements non nuls sont inversibles et qu'un *sous-anneau* d'un anneau est un sous-ensemble qui contient l'identité et est stable pour l'addition, la soustraction et la multiplication.

Partout dans cette section, E désigne un corps. En particulier, E est un anneau.

4.2.1. Définition. 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) $a+b, a-b, a\cdot b, a\cdot b^{-1}$(lorsque $b \neq 0_E$) $\in F$ pour tous $a, b \in F$.

Remarque. Un sous-corps de E est un sous-anneau qui est stable pour l'inversion.

Exemple. Considérons le corps $\mathbb{C}$ des nombres complexes.

(1) $\mathbb{Z}$ est un sous-anneau de $\mathbb{C}$, qui n'est pas un sous-corps.

(2) On voit que $\mathbb{Q}, \mathbb{R}$ sont deux sous-corps de $\mathbb{C}$.

(3) Si F est un sous-corps de $\mathbb{C}$, on a vu dans MAT153 que $\mathbb{Q} \subseteq F$.

(4) Dans MAT153, on a vu que

$$\mathbb{Q}[i] = \{a + bi \mid a, b \in \mathbb{Q}\}$$

est un sous-corps de $\mathbb{C}$.

4.2.2. Lemme. Si F est un sous-corps de E, alors F est un corps pour l'addition et la multiplication induites de celles de E comme suit:

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

et

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

Démonstration. D'après la définition, F est stable pour l'addition et la multiplication de E. Ainsi, les opérations ci-haut définies sont bien des opérations sur F. En outre,

(1) Comme $1_E \in F$, on a $0_E = 1_E - 1_E \in F$.

(2) Si $a \in F$, alors $-a = 0_E - a \in F$.

(3) Si $b \in F$ avec $b \neq 0_E$, alors $b^{-1} = 1_E \cdot b^{-1} \in F$.

Ainsi, F est un corps avec $0_F = 0_E$ et $1_F = 1_E$. Ceci achève la démonstration.

4.2.3. Définition. Si F est un sous-corps de E, on dit que $E : F$ une *extension de corps*, ou bien, E est une *extension* de F.

Exemple. (1) Comme E est un sous-corps de E, on a une extension de corps $E : E$.

(2) En considérant le corps $\mathbb{C}$, on obtient trois extensions de corps suivantes:

$$\mathbb{R} : \mathbb{Q}; \quad \mathbb{C} : \mathbb{R}; \quad \mathbb{Q}[i] : \mathbb{Q}.$$

Soit $E : F$ une extension de corps. D'après le lemme, F est un corps. Maintenant, on voit que E est un espace vectoriel sur F, noté ${}_FE$, pour l'addition

$$+ : E \times E \to E : (\alpha, \beta) \mapsto \alpha + \beta$$

et la multiplication externe

$$\cdot : F \times E \to E : (a, \alpha) \mapsto a\alpha.$$

Remarque. Dans cet espace vectoriel ${}_FE$, les vecteurs sont les éléments de E et les scalaire sont les éléments de F.

Exemple. Considérons l'extension de corps $\mathbb{C} : \mathbb{R}$. En MAT153, on a vu que $\mathbb{C}$ est un espace vectoriel sur $\mathbb{R}$ pour l'addition

$$(a + bi) + (c + di) = (a + c) + (b + d)i$$

et la multiplication externe

$$c(a + bi) = (ca) + (cb)i.$$

4.2.4. Définition. Soit $E : F$ une extension de corps. On définit son *degré* comme étant la dimension de l'espace vectoriel ${}_FE$, noté $[E : F]$.

Exercice. Trouver $[\mathbb{C} : \mathbb{R}]$, le degré de l'extension de corps $\mathbb{C} : \mathbb{R}$.

Solution. Par définition, $[\mathbb{C} : \mathbb{R}] = \dim({}_{\mathbb{R}}\mathbb{C})$. Dans MAT153, on a vu que $\{1, i\}$ est une base de l'espace vectoriel ${}_{\mathbb{R}}\mathbb{C}$. Ainsi, $[\mathbb{C} : \mathbb{R}] = \dim({}_{\mathbb{R}}\mathbb{C}) = |\{1, i\}| = 2$.

Étant donnée une extension de corps $E : F$. Comme ${}_FE$ est un espace vectoriel non nul, on a vu dans MAT153 que $\dim({}_FE) > 0$. C'est-à-dire, $[E : F] \geq 1$.

4.2.5. Lemme. Soit $E : F$ une extension de corps. Alors $[E : F] = 1$ si, et seulement si, $E = F$.

Démonstration. Supposons premièrement que $E = F$. Alors $\{1_E\}$ est une base de l'espace vectoriel ${}_EE$. Donc, $[E : F] = \dim({}_EE) = 1$.

Supposons réciproquement $[E : F] = 1$. C'est-à-dire, $\dim({}_FE) = 1$. Ainsi, toute base de ${}_FE$ ne contient qu'un élément, disons, $\{\alpha\}$ est une base de ${}_FE$.

En particulier, 1_E s'écrit comme une combinaison linéiare de α à un coefficient de F, c'est-à-dire, $1_E = a\alpha$ pour un certain scalaire $a \in F$. En particulier, a est non nul. Par conséquent, $\alpha = a^{-1}$. Comme F est un sous-corps de E, on voit que $a^{-1} \in F$. Ainsi, $\alpha = a^{-1} \in F$.

Considérons un élément quelconque $\beta \in E$. Comme $\{\alpha\}$ est une base de ${}_FE$, on a $\beta = b\alpha$ pour un certain scalaire $b \in F$. Comme F est stable pour la multiplication, $\beta = b\alpha \in F$. Ceci donne $E \subseteq F$, et donc $E = F$. La preuve du lemme s'achève.

Exemple. (1) Considérons l'extension de corps $\mathbb{R} : \mathbb{R}$. D'après le lemme 4.2.5, on voit que $[\mathbb{R} : \mathbb{R}] = 1$.

(2) Considérons l'extension de corps $\mathbb{R} : \mathbb{Q}$. Comme $\mathbb{Q} \neq \mathbb{R}$, d'après le lemme 4.2.5, on voit que $[\mathbb{R} : \mathbb{Q}] > 1$.

4.2.6. 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. (1) Considérons l'extension de corps $\mathbb{C} : \mathbb{R}$. On a vu que $[\mathbb{C} : \mathbb{R}] = 2$. Ainsi, $\mathbb{C}$ est fini sur $\mathbb{R}$.

(2) Considérons l'extension de corps $E : E$. D'après le lemme 4.2.5, $[E : E] = 1$. Ainsi, E est toujours fini sur E.

On verra que le résult suivant est très utile dans le calcul de degré d'extension de corps.

4.2.7. Théorème de la base téléscopique. Soient F, L deux sous-corps de E avec $F \subseteq L$. Alors, l'extension $E : F$ est finie si, et seulement si, les extensions $E : L$ et $L : F$ sont toutes finies; et dans ce cas,

$$[E : F] = [E : L][L : F].$$

Démonstration. Supposons premièrement que $E : F$ est finie, disons $[E : F] = n$. C'est-à-dire, $\dim({}_FE) = n$. Comme $F \subseteq L$, on voit que L est un sous-espace vectoriel de ${}_FE$. D'après un résulat du MAT153, on a

$$[L : F] = \dim({}_FL) \leq \dim({}_FE) = n.$$

En outre, prenons une base $\{\alpha_1, \ldots, \alpha_n\}$ de ${}_FE$. Pour tout $\alpha \in E$, on a

$$\alpha = a_1\alpha_1 + \cdots + a_n\alpha_n, \text{ où } a_1, \ldots, a_n \in F.$$

Comme $F \subseteq L$, on a aussi on a

$$\alpha = a_1\alpha_1 + \cdots + a_n\alpha_n, \text{ où } a_1, \ldots, a_n \in L.$$

Donc l'espace vectoriel ${}_LE$ est engendré par $\alpha_1, \ldots, \alpha_n$. D'après un résultat du MAT153, on a $\dim({}_LE) \leq n$. C'est-à-dire, $[E : L] \leq n$.

Supposons réciproquement que $[E : L] = r$ et $[L : F] = s$. C'est-à-dire, $\dim({}_LE) = r$ et $\dim({}_FL) = s$. Prenons une base $\{\beta_1, \ldots, \beta_r\}$ de ${}_LE$ et une base $\{\gamma_1, \ldots, \gamma_s\}$ de ${}_FL$. On prétend que

$$\mathcal{B} = \{\beta_i\gamma_j \,|\, 1 \leq i \leq r, 1 \leq j \leq s\}$$

est une base de ${}_FE$.

En effet, tout $\alpha \in E$ s'écrit $\alpha = \sum_{i=1}^{r} b_i\beta_i$, où $b_i \in L$. En outre, $b_i = \sum_{j=1}^{s} c_{ij}\gamma_j$, où $c_{ij} \in F$, pour $i = 1, \ldots, r$. Ceci nous donne

$$\alpha = \sum_{i=1}^{r} b_i\beta_i = \sum_{i=1}^{r}\left(\sum_{j=1}^{s} c_{ij}\gamma_j\right)\beta_i = \sum_{i=1}^{r}\sum_{j=1}^{s} c_{ij}(\beta_i\gamma_j), \quad \text{où } c_{ij} \in F.$$

Ainsi l'espace vectoriel ${}_FE$ est engendré par $\mathcal{B}$.

Il reste à montrer que $\mathcal{B}$ est une famille libre. Supposons que

$$\sum_{i=1}^{r}\sum_{j=1}^{s} a_{ij}(\beta_i\gamma_j) = 0, \quad \text{où } a_{ij} \in F.$$

Alors

$$\sum_{i=1}^{r}\left(\sum_{j=1}^{s} a_{ij}\gamma_j\right)\beta_i = 0, \quad \text{où } \sum_{j=1}^{s} a_{ij}\gamma_j \in L.$$

Comme $\beta_1, \ldots, \beta_r$ sont linéairement indépendants sur L, on a

$$\sum_{j=1}^{s} a_{ij}\gamma_j = 0, \quad \text{où } a_{ij} \in F,$$

pour $i = 1, \ldots, r$. Comme $\gamma_1, \ldots, \gamma_s$ sont linéairement indépendants sur F, on a $a_{ij} = 0$, pour tous $1 \leq j \leq s; 1 \leq i \leq r$. Ceci montre que $\mathcal{B}$ est libre sur F. Donc, $\mathcal{B}$ est une base de ${}_FE$. Par conséquent,

$$[E : F] = rs = [E : L][L : F].$$

Ceci achève la démonstration du théorème.

4.2.8. Définition. Soit $E : F$ une extension de corps.

(1) Un élément $\alpha \in E$ est dit *algébrique sur* F s'il est une racine d'un polynôme non nul sur F; et *transcendant sur* F sinon.

(2) 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. Tout $a \in F$ est algébrique sur F. En effet, $x - a$ est un polnôme non nul sur F, dont a est une racine.

Exercice. Considérer l'extension de crops $\mathbb{R} : \mathbb{Q}$. Vérifier que

$$\sqrt[3]{2+3\sqrt{5}} \in \mathbb{R}$$

est algébrique sur $\mathbb{Q}$.

Preuve. Posons $\alpha = \sqrt[3]{2+3\sqrt{5}}$. Alors $\alpha^3 = 2+3\sqrt{5}$. Donc, $(\alpha^3-2)^2 = 45$. D'où,

$$\alpha^6 - 4\alpha^3 - 41 = 0.$$

C'est-à-dire, α est une racine de $x^6 - 4x^3 - 41 \in \mathbb{Q}[x]$. Par définition, α est algébrique sur $\mathbb{Q}$.

Exercice. Considérer l'extension de crops $\mathbb{C} : \mathbb{R}$. Vérifier que $\mathbb{C}$ est algébrique sur $\mathbb{R}$.

Preuve. Soit $\alpha = a + b\sqrt{-1}$, où $a, b \in \mathbb{R}$. Alors $(\alpha - a)^2 = -b^2$, et donc,

$$\alpha^2 - 2a\alpha + a^2 + b^2 = 0.$$

C'est-à-dire, α est une racine de $x^2 - 2ax + a^2 + b^2 \in \mathbb{R}[x]$. Ainsi, α est algébrique sur $\mathbb{R}$. Ceci montre que $\mathbb{C} : \mathbb{R}$ est une extension algébrique.

On accepte le résultat célèbre suivant sans preuve.

4.2.9. Théorème de Lindemann. Le nombre réel π est transcendant sur $\mathbb{Q}$.

Exemple. L'extension $\mathbb{R} : \mathbb{Q}$ n'est pas algébrique.

4.2.10. 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 $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in F[x]$ non nul tel que $f(\alpha) = 0$, si et seulement si, il existent $a_0, a_1, \ldots, a_n \in F$ non tous nuls, tels que

$$a_0 \cdot 1 + a_1 \cdot \alpha + \cdots + a_n \cdot \alpha_n = 0,$$

c'est-à-dire, $\{1, \alpha, \ldots, \alpha^n\}$ est liée sur F. Ceci achève la démonstration du lemme.

Exercice. Vérifier $\mathbb{R} : \mathbb{Q}$ est une extension infinie de corps.

Preuve. D'apr''es le théorème de Lindemann, π est transcendant sur $\mathbb{Q}$. D'après le lemme 4.2.8, on voit que $\{1, \pi, \pi^2, \ldots, \pi^n, \ldots,\}$ est une famille libre infinie de ${}_{\mathbb{Q}}\mathbb{R}$. On a vu dans MAT153 que $\dim({}_{\mathbb{Q}}\mathbb{R}) = \infty$. C'est-à-dire, $\mathbb{R}$ est infini sur $\mathbb{Q}$.

4.2.11. Proposition. Toute extension finie de corps est algébrique.

Démonstration. Soit $E : F$ une extension de corps avec $[E : F] = n < \infty$, c'est-à-dire, le F-espace vectoriel E est de dimension n. Pour tout $\alpha \in E$, d'après un résultat du

MAT153, $\{1, \alpha, \ldots, \alpha^n\}$ est liée sur F car elle contient $n+1$ vecteurs. D'après le lemme 4.2.10, α est algébrique sur F. Ceci montre que E est algébrique sur F. La preuve s'achève.

Exercice. Considérer l'extension de corps $\mathbb{Q}[i] : \mathbb{Q}$, où $\mathbb{Q}[i] = \{a+bi \mid a, b \in \mathbb{Q}\}$. Vérifier que $\mathbb{Q}[i]$ est algèbre sur $\mathbb{Q}$.

Preuve. D'après la définition, le $\mathbb{Q}$-espace vectoriel $\mathbb{Q}[i]$ est engendré par $1, i$. Si $a, b \in \mathbb{Q}$ sont tels que $a \cdot 1 + b \cdot i = 0$, alors $a + bi = 0$. Comme $a, b \in \mathbb{R}$, par definition de nombres complexes, on a $a = 0$ et $b = 0$. C'est-à-dire, $\{1, i\}$ est libre sur $\mathbb{Q}$. Ceci montre que $\{1, i\}$ est une base de ${}_{\mathbb{Q}}\mathbb{Q}[i]$. Par conséquent, $[\mathbb{Q}[i] : \mathbb{Q}] = \dim({}_{\mathbb{Q}}\mathbb{Q}[i]) = 2$. D'après la proposition 4.2.9, $\mathbb{Q}[i] : \mathbb{Q}$ est une extension algébrique.

4.3 Extensions simples

Partout dans cette section, on se fixe une extension de corps $E : F$. C'est-à-dire, E est un corps dont F est un sous-corps.

4.3.1. Définition. Sout S un sous-ensemble de E. 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. En d'autres termes, $F(S)$ est le sous-corps de E satisfaisant les deux conditions suivantes:

(1) $F(S)$ est un sous-corps de E contenant F et S;

(2) Si L est un autre sous-corps de E contenant F et S, alors $F(S) \subseteq L$.

Exemple. Si $S \subseteq F$, alors $F(S) = F$.

Preuve. Dans ce cas, F est un sous-corps de E contenant F et S. Si L est un autre sous-corps de E contenant F et S, alors $F \subseteq L$. Ainsi, F est le plus petit sous-corps de E contenant F et S. C'est-à-dire, $F(S) = F$.

Exercice. Considérer l'extension de corps $\mathbb{C} : \mathbb{R}$. Montrer que $\mathbb{R}(\sqrt{-1}) = \mathbb{C}$.

Preuve. Il est evident que $\mathbb{C}$ est un sous-corps de $\mathbb{C}$ contenant $\mathbb{R}$ et $\sqrt{-1}$. Supposons que L est un sous-corps de $\mathbb{C}$ contenant $\mathbb{R}$ et $\sqrt{-1}$. Soit $\alpha \in \mathbb{C}$. Alors $\alpha = a + b\sqrt{-1}$, où $a, b \in \mathbb{R} \subseteq L$. Comme L est un sous-corps de $\mathbb{C}$, par définition, $\alpha = a + b \cdot \sqrt{-1} \in L$. Ceci montre que $\mathbb{C}$ est le plus petit sous-corps de $\mathbb{C}$ contenant $\mathbb{R}$ et $\sqrt{-1}$. C'es-à-dire, $\mathbb{R}(\sqrt{-1}) = \mathbb{C}$.

Étant deux sous-ensembles S_1, S_2 de E, par définition, $F(S_1)(S_2)$ est le sous-corps de E engendré par S_2 sur $F(S_1)$, c'est-à-dire, $F(S_1)(S_2)$ est le plus petit sous-corps de E contenant $F(S_1)$ et S_2. Le résultat suivant sera pratique dans notre calcul.

4.3.2. Lemme. Si S_1, S_2 sont des sous-ensembles de E, alors

$$F(S_1)(S_2) = F(S_1 \cup S_2) = F(S_2)(S_1).$$

Démonstration. Par définition, $F(S_1 \cup S_2)$ est un sous-corps de E contenant F, S_1 et S_2. Comme $F(S_1)$ est le plus petit sous-corps de E contenant F et S_1, on a $F(S_1) \subseteq F(S_1 \cup S_2)$. Ainsi, $F(S_1 \cup S_2)$ est un sous-corps de E contenant $F(S_1)$ et S_2. Comme $F(S_1)(S_2)$ est le plus petit sous-corps de E contenant $F(S_1)$ et S_2, on a $F(S_1)(S_2) \subseteq F(S_1 \cup S_2)$.

De l'autre côté, $F(S_1)(S_2)$ est un sous-corps de E contenant $F(S_1)$ et S_2. Comme $F(S_1)$ contient F et S_1, on voit que $F(S_1)(S_2)$ est un sous-corps de E contenant F et $S_1 \cup S_2$. Comme $F(S_1 \cup S_2)$ est le plus petit sous-corps de E contenant F et $S_1 \cup S_2$ par définition, on a $F(S_1 \cup S_2) \subseteq F(S_1)(S_2)$. Par conséquent, $F(S_1)(S_2) = F(S_1 \cup S_2)$.

Enfin, comme $S_2 \cup S_1 = S_1 \cup S_2$, on a

$$F(S_2)(S_1) = F(S_2 \cup S_1) = F(S_1 \cup S_2) = F(S_1)(S_2).$$

La preuve du lemme s'achève.

Remarque. Si $\alpha_1, \alpha_2, \ldots, \alpha_n \in E$, alors

$$F(\alpha_1, \alpha_2, \ldots, \alpha_n) = F(\alpha_1)(\alpha_2)\cdots(\alpha_n),$$

où $F(\alpha_1)\cdots(\alpha_{i-1})(\alpha_i)$ est le sous-corps de E engendré par α_i sur $F(\alpha_1)\cdots(\alpha_{i-1})$, pour tout $i = 2, \ldots, n$.

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 élément $\alpha \in E$.

Exemple. Considérons l'extension de corps $\mathbb{C} : \mathbb{R}$. On a vu que $\mathbb{C} = \mathbb{R}(\sqrt{-1})$. Ainsi, $\mathbb{C} : \mathbb{R}$ est une extension simple.

Exercice. Considérer le sous-corps $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ de $\mathbb{R}$ engendré par $\sqrt{2}$ et $\sqrt{3}$ sur $\mathbb{Q}$. Montrer que l'extension $\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}$ est simple.

Démonstration. Par hypothèse, $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ est le sous-corps de $\mathbb{R}$ engendré par deux nombres $\sqrt{2}$ et $\sqrt{3}$ sur $\mathbb{Q}$. On prouvera qu'il peut être engendré par un nombre α sur $\mathbb{Q}$.

Par définition, $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ est un sous-corps de $\mathbb{R}$ contenant $\mathbb{Q}$, $\sqrt{2}$ et $\sqrt{3}$. En particulier, $\alpha = \sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$. C'est-à-dire, $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ est un sous-corps de $\mathbb{R}$ contenant $\mathbb{Q}$ et α. Comme $\mathbb{Q}(\alpha)$ est le plus petit sous-corps de $\mathbb{R}$ contenant $\mathbb{Q}$ et α, on voit que $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

D'autre part, $\alpha - \sqrt{2} = \sqrt{3}$ et $\alpha - \sqrt{3} = \sqrt{2}$, et donc, $(\alpha - \sqrt{2})^2 = 3$ et $(\alpha - \sqrt{3})^2 = 2$. C'est-à-dire,

$$\alpha^2 - 2\alpha\sqrt{2} + 2 = 0 \text{ et } \alpha^2 - 2\alpha\sqrt{3} + 3 = 0.$$

D'où $\alpha \neq 0$ et

$$\sqrt{2} = \frac{\alpha^2 - 1}{2\alpha},\ \sqrt{3} = \frac{\alpha^2 + 1}{2\alpha}.$$

Comme $Q(\alpha)$ est un sous-corps de $\mathbb{R}$ contenant $1, 2$ et α, on voit que $\alpha^2-1, \alpha^2+1, 2\alpha \in \mathbb{Q}(\alpha)$, et par conséquent,

$$\frac{\alpha^2 - 1}{2\alpha},\ \frac{\alpha^2 + 1}{2\alpha} \in \mathbb{Q}(\alpha).$$

C'est-à-dire, $\mathbb{Q}(\alpha)$ est un sous-corps de $\mathbb{R}$ contenant $\mathbb{Q}$ et $\sqrt{2}, \sqrt{3}$. Comme $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ est le plus petit sous-corps de $\mathbb{R}$ contenant $\mathbb{Q}$ et $\sqrt{2}, \sqrt{3}$, on a $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{Q}(\alpha)$. Par conséquent, $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\alpha)$. C'est-à-dire, $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ est simple sur $\mathbb{Q}$.

Rappelons qu'un élément $\alpha \in E$ est dit *algébrique* sur F s'il est une racince d'un polynôme non nul sur F. Dans la définition suivante, on considérera un tel polynôme de degré minimal.

4.3.4. Définition. Soit $\alpha \in E$ un élément algébrique sur F. Un polynôme $m(x) \in F[x]$ s'appelle un *polynôme minimal* de α sur F si les conditions suivantes sont vérifiées:

(1) $m(\alpha) = 0$.

(2) $m(x)$ est monique (c'est-à-dire, son coefficient directeur est 1_F).

(3) Si $f(x) \in F[x]$ est non-constant avec $f(\alpha) = 0$, alors $\partial(m(x)) \leq \partial(f(x))$.

Remarque. (1) La condition (3) explique la minimalité de $m(x)$.

(2) On verra plus tard que la condition (2) garantira l'unicité de polynôme minimal.

Exemple. Considérer un extension de corps $E : F$. Si $a \in F$, alors $x-a$ est un polynôme minimal de a sur F.

Preuve. Il est evident que $x-a \in F[x]$ est monique dont a est une racince. Si $f(x) \in F[x]$ est non-constant tel que $f(\alpha) = 0$, alors $\partial(f) \geq 1 = \partial(x - a)$. Par définition, $x - a$ est un polynôme minimal de a sur F.

Exercice. Considérer l'extension $\mathbb{R} : \mathbb{Q}$. Vérifier que $\sqrt{2} \in \mathbb{R}$ est algébrique sur $\mathbb{Q}$, et donner un polynôme minimal de $\sqrt{2}$ sur $\mathbb{Q}$.

Solution. D'abord, $x^2 - 2 \in \mathbb{Q}[x]$ est monique dont $\sqrt{2}$ est une racine. Soit $f(x) \in \mathbb{Q}[x]$ non constant avec $f(\sqrt{2}) = 0$. Supposons au contraire que $\partial(f) < \partial(x^2 - 2) = 2$. Alors $\partial(f) = 1$. C'est-à-dire, $f(x) = ax + b$, où $a, b \in \mathbb{Q}$ avec $a \neq 0$. Maintenant,

$$0 = f(\sqrt{2}) = a\sqrt{2} + b.$$

D'où,

$$\sqrt{2} = -\frac{b}{a} \in \mathbb{Q},$$

une contradiction. Ainsi $\partial(x^2-2) \leq \partial(f)$. Cela implique que x^2-2 est un polynôme minimal de $\sqrt{2}$ sur $\mathbb{Q}$.

Le résultat suivant ramasse des propriétés d'un polynôme minimal d'un élément algébrique. Rappelons que le produit de deux éléments non nuls d'un corps est non nul.

4.3.5. Lemme. Soit $\alpha \in E$ un élément algébrique sur F. Soit $m(x)$ un polynôme minimal de α sur F.

(1) $m(x)$ est irréductible sur F.

(2) Si $f(x) \in F[x]$, alors $f(\alpha) = 0$ si, et seulement si, $m(x) \mid f(x)$.

Démonstration. (1) Supposons au contraire que $m(x)$ est réductible sur F. Alors $m(x) = m_1(x)m_2(x)$, où $m_1(x), m_2(x) \in F[x]$ avec $0 < \partial(m_1), \partial(m_2) < \partial(m)$. D'après la définition 4.3.4(1), on a

$$0 = m(\alpha) = m_1(\alpha)m_2(\alpha), \text{ où } m_1(\alpha), m_2(\alpha) \in E.$$

Comme E est un corps, on a $m_1(\alpha) = 0$ ou $m_2(\alpha) = 0$. Ceci contredit la condition énoncée dans la définition 4.3.4(3). Donc, $m(x)$ est irréductible sur F.

(2) Considérons $f(x) \in F[x]$. En divisant $f(x)$ par $m(x)$; voir le théorème 4.1.4, on obtient $q(x), r(x) \in F[x]$ avec $\partial(r(x)) < \partial(m(x))$ tels que

$$(*) \qquad f(x) = m(x)q(x) + r(x).$$

Si $m(x) \mid f(x)$, alors $r(x) = 0$, et donc, $f(x) = m(x)q(x)$. Par conséquent, on obtient $f(\alpha) = m(\alpha)q(\alpha) = 0$.

Supposons réciproquement que $f(\alpha) = 0$. D'après la définition 4.3.4(1), $m(\alpha) = 0$. En vue de l'équation $(*)$, on a

$$r(\alpha) = f(\alpha) - m(\alpha)q(\alpha) = 0.$$

Si $r(x) \neq 0$, d'après la définition 4.3.4(3), on a $\partial(m(x)) \leq \partial(r(x))$, une contradiction. Ainsi, $r(x) = 0$, et donc $m(x) \mid f(x)$. Ceci achève la démonstration.

Le résultat suivant donne une méthode pour trouver le polynême minimal d'un élément algébrique.

4.3.6. Corollaire. Soit $\alpha \in E$ algébrique sur F.

(1) L'élémment α admet un seul polynôme minimal sur F, noté $m_F^\alpha(x)$.

(2) Si $p(x) \in F[x]$ est irréductible et monique tel que $p(\alpha) = 0$, alors $m_F^\alpha(x) = p(x)$.

Démonstration. (1) Soient $m_1(x), m_2(x)$ deux polynômes minimaux de α sur F. D'après le lemme 4.3.5(2), on a $m_1(x) \mid m_2(x)$ et $m_2(x) \mid m_1(x)$. D'où, $m_1(x) = am_2(x)$ avec

$a \in F$. Comme le coefficient directeur de $m_2(x)$ est 1_F, le coefficient directeur de $am_2(x)$ est a. Comme le coefficient directeur de $m_1(x)$ est 1_F, on a $a = 1_F$. C'est-à-dire, $m_1(x) = m_2(x)$.

(2) Supposons que $p(x) \in F[x]$ est irréductible et monique tel que $p(\alpha) = 0$. D'après le lemme 4.3.5(2), $m_F^\alpha(x) \mid p(x)$. Comme $p(x)$ est irréductible sur F, on a $p(x) = b\, m_F^\alpha(x)$, où $b \in F$. Comme $p(x)$ et $m_F^\alpha(x)$ sont moniques, on a vu que $b = 1_F$. Ainsi $m_F^\alpha(x) = p(x)$. Ceci achève la démonstration du corollaire.

Exercice. Considérer l'extension $\mathbb{C} : \mathbb{Q}$. Soit $\alpha = \sqrt{1 - \sqrt{2}} \in \mathbb{C}$.

(1) Vérifier α est algébrique sur $\mathbb{Q}$.

(2) Trouver le polynôme minimal de α sur $\mathbb{Q}$.

Solution. (1) Par hypothèse, $\alpha^2 = 1 - \sqrt{2}$, et donc, $(\alpha^2 - 1)^2 = (-\sqrt{2})^2 = 2$. D'où,

$$\alpha^4 - 2\alpha^2 - 1 = 0.$$

C'est-à-dire, α est racine de $x^4 - 2x^2 - 1 \in \mathbb{Q}[x]$. En particulier, α est algébrique sur $\mathbb{Q}$.

(2) On montrera que $m(x) = x^4 - 2x^2 - 1$ est le polynôme minimal de α sur $\mathbb{Q}$. D'après le corollaire 4.3.6(2), il suffit de vérifier que $m(x)$ est irréductible sur $\mathbb{Q}$. Comme on ne peut pas trouver un premier p qui satisfait à les trois conditions énoncées dans le critère d'Eisenstein, on doit appliquer la proposition 4.1.13 pour changer les coefficients de $m(x)$. Pour ce faire, on considère

$$g(x) := m(x + 1) = x^4 + 4x^3 + 4x^2 - 2.$$

En appliquant le critère d'Eisenstein avec $p = 2$, on voit que $g(x)$ est irréductible sur $\mathbb{Q}$. D'après la proposition 4.1.13, $m(x)$ est aussi irréductible sur $\mathbb{Q}$. D'après le corollaire 4.3.6(2), on trouve $m_{\mathbb{Q}}^\alpha(x) = x^4 - 2x^2 - 1$.

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. Considérons $\alpha = \sqrt{1 - \sqrt{2}} \in \mathbb{C}$. On a vu que

$$m_{\mathbb{Q}}^\alpha(x) = x^4 - 2x^2 - 1.$$

Par définition, $\partial_{\mathbb{Q}}(\alpha) = 4$.

Exercice. Considérer l'extension de corps $\mathbb{R} : \mathbb{Q}$. Étant donnés un premier p et un entier $n > 0$, trouver le degré de $\sqrt[n]{p} \in \mathbb{R}$ sur $\mathbb{Q}$.

Solution. D'abord, $\sqrt[n]{p}$ est une racine de $x^n - p \in \mathbb{Q}[x]$. Ainsi, $\sqrt[n]{p}$ est algébrique sur $\mathbb{Q}$. En appliquant le critère d'Eisenstein, on voit que $x^n - p$ est irréductible sur $\mathbb{Q}$. D'après le corollaire 4.3.6(2), $x^n - p$ est le polynôme minimal de $\sqrt[n]{p}$ sur $\mathbb{Q}$. Par définition, $\partial_{\mathbb{Q}}(\sqrt[n]{p}) = n$.

Étant donné un élément $\alpha \in E$, on a défini $F(\alpha)$ comme étant le plus petit sous-corps de E contenant F et α. Cette définition ne décrit pas les éléments de $F(\alpha)$. Lorsque α est algébrique sur F, on sera capable de décrire explicitement les éléments de $F(\alpha)$.

4.3.8. Théorème. Soit $E = F(\alpha)$ une extension simple de F. Si α est algébrique de degré n sur F, alors $\{1_F, \alpha, \ldots, \alpha^{n-1}\}$ est une base de ${}_FE$. En particulier,

(1) $[F(\alpha) : F] = \partial_F(\alpha)$;

(2) $E = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \mid a_0, a_1 \ldots, a_{n-1} \in F\}$.

Démonstration. Supposons que $\partial(m_F^\alpha(x)) = n$. On voit aisément que l'ensemble

$$F[\alpha] := \{f(\alpha) \mid f(x) \in F[x]\}$$

est un sous-anneau (voir 1.2.3) de E contenant F et α. On prédend que $E = F[\alpha]$.

On se fixe un élément quelconque $\beta \in F[\alpha]$. Par hypothèse, $\beta = f(\alpha)$, où $f(x) \in F[x]$. Supposons que $\beta \neq 0$. On montrera que β est inverseible et trouvera β^{-1}. En effet, d'après le lemme 4.3.5(2), $m_F^\alpha(x) \not| f(x)$. Comme $m_F^\alpha(x)$ est irréductible sur F par le lemme 4.3.5(1), on voit que $m_F^\alpha(x)$ et $f(x)$ sont co-premiers. Ainsi il existe $u(x), v(x) \in F[x]$ tels que

$$f(x)u(x) + m_F^\alpha(x)v(x) = 1.$$

Comme $m_F^\alpha(\alpha) = 0$ par la définition 4.3.4(1), on a

$$1 = f(\alpha)u(\alpha) + m_F^\alpha(\alpha)v(\alpha) = f(\alpha)u(\alpha) = \beta \cdot u(\alpha).$$

D'où, $\beta^{-1} = u(\alpha) \in F[\alpha]$. Ceci montre que $F[\alpha]$ est un sous-corps de E contenant F et α. Comme $E = F(\alpha)$, le plus sous-corps de E contenant F et α, on a $E \subseteq F[\alpha]$. Ainsi, $E = F[\alpha]$. Il nous reste à montrer que $\{1_F, \alpha, \ldots, \alpha^{n-1}\}$ est une base de ${}_FE$.

En divisant $f(x)$ par $m_F^\alpha(x)$, on obtient $q(x), r(x) \in F[x]$ avec $\partial(r(x)) < n$ tels que

$$(*) \qquad f(x) = m_F^\alpha(x)q(x) + r(x).$$

Écrivons $r(x) = b_0 + b_1x + \cdots + b_{n-1}x^{n-1}$, où $b_i \in F$. Comme $m_F^\alpha(\alpha) = 0$; voir 4.3.4(1), on obtient

$$\beta = f(\alpha) = m_F^\alpha(\alpha)q(\alpha) + r(\alpha) = r(\alpha) = b_0 \cdot 1 + b_1 \cdot \alpha + \cdots + b_{n-1} \cdot \alpha^{n-1}.$$

Cela dit que le F-espace vectoriel E est engendré par $1_F, \alpha, \ldots, \alpha^{n-1}$. Supposons au contraire que $1_F, \alpha, \ldots, \alpha^{n-1}$ sont linéairement dépendants sur F. Alors, il existe $a_0, a_1, \ldots, a_{n-1} \in F$, non tous nuls, tels que

$$a_0 \cdot 1 + a_1 \cdot \alpha + \cdots + a_{n-1} \cdot \alpha^{n-1}0.$$

C'est-à-dire, $g(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$ est un polynôme non nul sur F, dont α est une racine. Comme $\partial(g(x)) < \partial(m_F^\alpha(x))$, on obtient une contradiction à la définition 4.3.4(3). Donc, $\{1_F, \alpha, \ldots, \alpha^{n-1}\}$ est libre sur F, et donc, elle est une base de ${}_FE$. La preuve du théorème s'achève.

Exercice. Considérer $\mathbb{Q}(\alpha)$, le sous-corps de $\mathbb{C}$ engendré par α sur $\mathbb{Q}$, où

$$\alpha = -\frac{1}{2} + \frac{\sqrt{-3}}{2}.$$

(1) Vérifier que $\mathbb{Q}(\alpha) = \{a + b\alpha \mid a, b \in \mathbb{Q}\}$.

(2) Calculer $(\alpha + 4)^{-1}$ dans $\mathbb{Q}(\alpha)$.

Solution. (1) IL nous faudra montrer que $\partial_{\mathbb{Q}}(\alpha) = 2$, c'est-à-dire, $\partial(m_{\mathbb{Q}}^\alpha(x)) = 2$. En effet, comme $\alpha + \frac{1}{2} = \frac{\sqrt{-3}}{2}$, on a $(\alpha + \frac{1}{2})^2 = -\frac{3}{4}$. D'où,

$$\alpha^2 + \alpha + 1 = 0.$$

C'est-à-dire, α est une racine de $m(x) = x^2 + x + 1 \in \mathbb{Q}[x]$. On montrera que $m(x)$ est irréductible sur $\mathbb{Q}$. Pour ce faire, on considère

$$m(x + 1) = x^2 + 3x + 3 := g(x).$$

En appliquant le critère d'Eisenstein avec $p = 3$, on voit que $g(x)$ est irréductible sur $\mathbb{Q}$. D'après la proposition 4.1.13, $m(x)$ l'est aussi. D'après le corollaire 4.3.6(2), on voit que $m_{\mathbb{Q}}^\alpha(x) = x^2 + x + 1$. Par la définition 4.3.7, $\partial_{\mathbb{Q}}(\alpha) = 2$. D'après le théorème 4.3.8(2), on trouve que $\mathbb{Q}(\alpha) = \{a + b\alpha \mid a, b \in \mathbb{Q}\}$.

(2) Pour calculer $(\alpha + 4)^{-1}$, on considère $\beta = f(\alpha)$, où $f(x) = x + 4 \in \mathbb{Q}[x]$. Il faut trouver $u(x), v(x) \in \mathbb{Q}[x]$ tels que

$$(x + 4)u(x) + m_{\mathbb{Q}}^\alpha(x)v(x) = 1.$$

Pour ce faire, on appliquera l'algorithme d'Euclid. Comme $\partial(x + 4) < \partial(m_{\mathbb{Q}}^\alpha(x))$, on divise $m_{\mathbb{Q}}^\alpha(x)$ par $x + 4$. Cela nous donne

$$x^2 + x + 1 = (x + 4)(x - 3) + 13.$$

D'où,

$$(x + 4) \cdot \frac{3 - x}{13} + (x^2 + x + 1) \cdot \frac{1}{13} = 1.$$

Remplaçant x par α, on obtient

$$(\alpha + 4) \cdot \frac{3 - \alpha}{13} + (\alpha^2 + \alpha + 1) \cdot \frac{1}{13} = 1.$$

Comme $\alpha^2 + \alpha + 1 = 0$, on obtient

$$(\alpha + 4) \cdot \frac{3 - \alpha}{13} = 1.$$

D'où

$$(\alpha + 4)^{-1} = \frac{3}{13} - \frac{\alpha}{13}.$$

Exercice. Considérer l'extension $\mathbb{C} : \mathbb{Q}$ et $\alpha = \sqrt{1 - \sqrt{2}} \in \mathbb{C}$.

(1) Vérifier que $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\alpha)$.

(2) Trouver $m^{\alpha}_{\mathbb{Q}(\sqrt{2})}(x)$, le polynôme minimal de α sur $\mathbb{Q}(\sqrt{2})$.

Solution. (1) Par hypothèse, $\alpha^2 = 1 - \sqrt{2}$. D'où, $\sqrt{2} = 1 - \alpha^2 \in \mathbb{Q}(\alpha)$. Ainsi, $\mathbb{Q}(\alpha)$ est un sous-corps de $\mathbb{C}$ contenant $\mathbb{Q}$ et $\sqrt{2}$. Comme $\mathbb{Q}(\sqrt{2})$ est le plus petit sous-corps de $\mathbb{C}$ contenant $\mathbb{Q}$ et $\sqrt{2}$, on a $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\alpha)$.

(2) Comme $\alpha^2 + \sqrt{2} - 1 = 0$, on voit que α est une racine de $x^2 + \sqrt{2} - 1 \in \mathbb{Q}(\sqrt{2})[x]$. D'après le lemme 4.3.5(2), $m^{\alpha}_{\mathbb{Q}(\sqrt{2})}(x)$ est un facteur de $x^2 + \sqrt{2} - 1$. D'après le théorème 4.3.8,

$$\partial(m^{\alpha}_{\mathbb{Q}(\sqrt{2})}(x)) = [\mathbb{Q}(\sqrt{2})(\alpha) : \mathbb{Q}(\sqrt{2})].$$

D'après le lemme 4.3.2, $\mathbb{Q}(\sqrt{2})(\alpha) = \mathbb{Q}(\alpha)(\sqrt{2}) = \mathbb{Q}(\alpha)$, où la dernière équation est valide puisque $\sqrt{2} \in \mathbb{Q}(\alpha)$. Par conséquent,

$$\partial(m^{\alpha}_{\mathbb{Q}(\sqrt{2})}(x)) = [\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{2})].$$

En considérant les corps $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\alpha)$, d'après le théorème 4.2.5, on a

$$(*) \qquad [\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}[\sqrt{2}] : \mathbb{Q}].$$

Dans l'exercice suivant le corollaire 4.3.6, on a vu que $m^{\alpha}_{\mathbb{Q}}(x) = x^4 - 2x^2 - 1$. En outre, on a vu que $m^{\sqrt{2}}_{\mathbb{Q}}(x) = x^2 - 2$. D'après le théorème 4.3.8, on a

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = \partial(m^{\alpha}_{\mathbb{Q}}(x)) = 4 \text{ et } [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = \partial(m^{\sqrt{2}}_{\mathbb{Q}}(x)) = 2.$$

En vertu de l'équation $(*)$, $4 = 2[\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{2})]$. Ainsi,

$$\partial(m^{\alpha}_{\mathbb{Q}(\sqrt{2})}(x)) = [\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{2})] = 2.$$

Ainsi, $m^{\alpha}_{\mathbb{Q}(\sqrt{2})}(x)$ est un facteur de $x^2 + \sqrt{2} - 1$ de degré 2. Ainsi, $m^{\alpha}_{\mathbb{Q}(\sqrt{2})}(x) = a(x^2 + \sqrt{2} - 1)$, où $a \in \mathbb{Q}(\sqrt{2})$. Comme $m^{\alpha}_{\mathbb{Q}(\sqrt{2})}(x)$ est monique, on a $a = 1$. C'est-à-dire,

$$m^{\alpha}_{\mathbb{Q}(\sqrt{2})}(x) = x^2 + \sqrt{2} - 1.$$

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) $F(\alpha) : F$ est une extension algébrique.

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.

Exemple. Soit $\alpha = 2 - 3\sqrt[4]{3} + 5\sqrt[4]{9} - 7\sqrt[4]{27}$. Vérifier que α est algébrique sur $\mathbb{Q}$.

Solution. On voit que

$$\alpha = 2 - 3\sqrt[4]{3} + 5\left(\sqrt[4]{3}\right)^2 - 7\left(\sqrt[4]{3}\right)^3 \in \mathbb{Q}(\sqrt[4]{3}).$$

Étant une racine de $x^4 - 3 \in \mathbb{Q}[x]$, le nombre réel $\sqrt[4]{3}$ est algébrique sur $\mathbb{Q}$. D'après le corollaire 4.3.9, $\mathbb{Q}(\sqrt[4]{3})$ est une extension algébrique de $\mathbb{Q}$; voir la définition 4.2.6(2). En particulier, α est algébrique sur $\mathbb{Q}$.

Étant donné un polynôme de plusieurs variables $f(x_1, \ldots, x_s) \in F[x_1, \ldots, x_s]$, on désignera par $\partial_{x_i}(f)$ le degré de x_i dans $f(x_1, \ldots, x_s)$.

En tant que généralisation du théorème 4.3.8, le résultat suivant décrit les éléments d'une extension de F engendrée par un nombre fini déléments algébriques.

4.3.10. Théorème. Soit $E = F(\alpha_1, \ldots, \alpha_s)$. Si $\alpha_1, \ldots, \alpha_s$ sont algébriques sur F, alors E est fini sur F avec

$$E = \{f(\alpha_1, \cdots, \alpha_s) \mid f(x_1, \cdots, x_s) \in F[x_1, \cdots, x_s], \partial_{x_i}(f) < \partial_F(\alpha_i)\}.$$

Démonstration. Si $s = 1$, d'après le théorème 4.3.8, le résultat est valide. Supposons que $s > 1$ et le résultat est valide pour $s - 1$. En particulier, $[F(\alpha_1, \ldots, \alpha_{s-1}) : F]$ est fini. Comme α_s est algébrique sur F, il 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 $F(\alpha_1, \ldots, \alpha_{s-1})$. D'après le 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.

Exercice. Considérer l'extension $\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}$. Donner une $\mathbb{Q}$-base de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Solution. On a vu que $m_{\mathbb{Q}}^{\sqrt{2}}(x) = x^2 - 2$ et $m_{\mathbb{Q}}^{\sqrt{3}}(x) = x^2 - 3$. D'après la définition 4.3.7, $\partial_{\mathbb{Q}}(\sqrt{2}) = \partial_{\mathbb{Q}}(\sqrt{3}) = 2$. Remarquant que $\sqrt{2} \cdot \sqrt{3} = \sqrt{6}$, d'après le théorème 4.3.10, on obtient

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q}\}.$$

Donc, le $\mathbb{Q}$-espace vectoriel $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ est engendré par $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$. On montrera que $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ est une base de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ sur $\mathbb{Q}$.

En effet, comme $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{3}, \sqrt{2}) = \mathbb{Q}(\sqrt{3})(\sqrt{2})$, d'après le théorème 4.2.5,

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2[\mathbb{Q}(\sqrt{3})(\sqrt{2}) : \mathbb{Q}(\sqrt{3})].$$

Comme $\sqrt{2}$ est racine du polynôme $x^2 - 2$ sur $\mathbb{Q}(\sqrt{3})$, le polynôme minimal de $\sqrt{2}$ sur $\mathbb{Q}(\sqrt{3})$ est de degré ≤ 2. D'après le théorème 4.3.8(1), $[\mathbb{Q}(\sqrt{3})(\sqrt{2}) : \mathbb{Q}(\sqrt{3})] \leq 2$.

Supposons que $[\mathbb{Q}(\sqrt{3})(\sqrt{2}) : \mathbb{Q}(\sqrt{3})] = 1$. D'après le lemme 4.2.3, $\mathbb{Q}(\sqrt{3})(\sqrt{2}) = \mathbb{Q}(\sqrt{3})$. En particulier, $\sqrt{2} \in \mathbb{Q}(\sqrt{3})$. Comme $\partial_{\mathbb{Q}}(\sqrt{3}) = 2$, d'après le théorème 4.3.8(2), on voit que $\sqrt{2} = a + b\sqrt{3}$ avec $a, b \in \mathbb{Q}$. Si $b = 0$, alors $\sqrt{2} \in \mathbb{Q}$, une contradiction. Donc $b \neq 0$. Comme $(\sqrt{2} - b\sqrt{3})^2 = a^2$, on a

$$\sqrt{6} = \frac{2 + 3b^2 - a^2}{2b} \in \mathbb{Q},$$

une contradiction.

Par conséquent, $[\mathbb{Q}(\sqrt{3})(\sqrt{2}) : \mathbb{Q}(\sqrt{3})] = 2$, et donc $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$. C'est-à-dire, le $\mathbb{Q}$-espace vectoriel $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ est de dimension 4. D'après un résultat du MAT153, on sait que $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ est une base du $\mathbb{Q}$-espace vectoriel $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

On conclut cette section par la solubilité par radicaux d'équations polynômiales complexes. Étant donnée un extension de corps $E : F$, on s'intérèsse aux éléments E qui sont des racinces n-ièmes des éléments de F. Par exemple, le nombre complexe i est une racine carrée du nombre réelle -1.

4.3.11. Définition. On dit que $E : F$ est *radicale* s'il existe une suite

$$F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_r = E$$

de sous-corps de E telle que $F_i = F_{i-1}(\alpha_i)$ avec $\alpha_i^{n_i} \in F_{i-1}$ pour un certain $n_i > 0$, pour $i = 1, \ldots, r$.

Exemple. L'extension $\mathbb{C} : \mathbb{R}$ est radicale. En effet, $\mathbb{R} \subset \mathbb{C} = \mathbb{R}(i)$ avec $i^2 \in \mathbb{R}$.

Exercice. Vérifier que $\mathbb{Q}(\alpha) : \mathbb{Q}$ est une extension radicale, où

$$\alpha = \sqrt[5]{5 + \sqrt[3]{3 + \sqrt{2}}}.$$

Démonstration. Par hypothèse, $\alpha^5 = 5 + \sqrt[3]{3 + \sqrt{2}} \notin \mathbb{Q}$. Plustôt, $\alpha^5 \in \mathbb{Q}(\beta)$ où $\beta = \sqrt[3]{3 + \sqrt{2}}$. Maintenant, $\beta^3 = 3 + \sqrt{2} \notin \mathbb{Q}$, mais $\beta^3 \in \mathbb{Q}(\gamma)$, où $\gamma = \sqrt{2}$. Remarquant que $\gamma^2 = 2 \in \mathbb{Q}$, on obtient une suite de sous-corps de $\mathbb{C}$ comme suit:

$$\mathbb{Q} \subset \mathbb{Q}(\gamma) \subset \mathbb{Q}(\gamma, \beta) \subset \mathbb{Q}(\gamma, \beta, \alpha)$$

avec $\gamma^2 \in \mathbb{Q}$, $\beta^3 = 2 + \gamma \in \mathbb{Q}(\gamma)$ et $\alpha^5 = 5 + \beta \in \mathbb{Q}(\gamma, \beta)$.

Enfin, $\beta = \alpha^5 - 5 \in \mathbb{Q}(\alpha)$. Donc, $\gamma = \beta^3 - 3 \in \mathbb{Q}(\alpha)$. En vertu du lemme 4.3.2, on a

$$\mathbb{Q}(\gamma, \beta, \alpha) = \mathbb{Q}(\alpha)(\gamma, \beta) = \mathbb{Q}(\alpha),$$

où la deuxième équation décole de l'exemple suivant la définition 4.3.1. Par définition, l'extension $\mathbb{Q}(\alpha) : \mathbb{Q}$ est radicale.

On dit qu'un élément de E est une *expression radicale* des éléments de F s'il est obtenu à partir des éléments de F par un nombre fini d'opérations d'addition, soustraction, multiplication, division et extraction de la racine.

Exemple. (1) Considérons l'extension $\mathbb{C} : \mathbb{R}$. On voit que $1 + 2\sqrt{\pi}$ est une expression radicale des nombres réels, mais il n'est pas une expression radicale des nombres rationnels.

(2) Considérons l'extension $\mathbb{C} : \mathbb{Q}$. Le nombre complexe

$$\frac{\sqrt[5]{5 + 7\sqrt[3]{3 - 11\sqrt{2}}}}{3 - \sqrt[6]{2 - \sqrt{7}}}$$

est une expression de nombres rationnels.

4.3.12. Proposition. Si $E : F$ est une extension radicale, alors tout élément de E est une expression radicale des éléments de F.

Démonstration. Considérons une suite de sous-corps de E comme suit:

$$F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_r = E,$$

o'u $F_i = F_{i-1}(\alpha_i)$ avec $\alpha_i^{n_i} \in F_{i-1}$ pour un certain $n_i > 0$, pour $i = 1, \ldots, r$.

IL est évident que tout élément de F_0 est une expression radicale des éléments de F. Supposns que $i > 0$ et tout élément de F_{i-1} est une expression radicale des éléments de F. Par l'hypothèse, $a_{i-1} = \alpha_i^{n_i} \in F_{i-1}$. On note $\alpha_i = \sqrt[n_i]{a_{i-1}}$. Comme α_i est une racine

de $x^{n_i} - a_{i-1} \in F_i$, il est algébrique sur F_{i-1} de degré $\leq n_i$. Pour tout $\beta \in F_i$, d'après le théorème 4.3.8, on a

$$\beta = b_0 + b_1 \sqrt[n_i]{a_{i-1}} + \cdots + b_{n_i-1}(\sqrt[n_i]{a_{i-1}})^{n_i-1}, \text{ où } a_{i-1}, b_0, b_1, \ldots, b_{n_i-1} \in F_{i-1}.$$

Par l'hypothèse de récurrence, $a_{i-1}, b_0, b_1, \ldots, b_{n_i-1}$ sont des expressions radicales des éléments de F, et donc, β l'est aussi. La preuve de la proposition s'achève.

Exemple. Considerons l'extension radicale $\mathbb{C} : \mathbb{R}$. Tout nombre complexe

$$a + b\sqrt{-1},$$

où $a, b \in \mathbb{R}$ est évidemment une expression radicale des nombres réels.

4.3.13. Définition. Un polynôme complexe non constant

$$f(x) = \alpha_0 + \alpha_1 x + \cdots + \alpha_n x^n$$

est dit *soluble par radicaux* si ses racines sont contenues dans une extension radicale de $\mathbb{Q}(\alpha_0, \alpha_1, \ldots, \alpha_n)$, le sous-corps de $\mathbb{C}$ engendré par les coefficients de $f(x)$ sur $\mathbb{Q}$.

Remarque. En d'autres termes, un polynôme est soluble par radicaux si ses racines s'obtiennent à partir de nombres rationnels et ses coefficients par un nombre fini d'opérations d'addition, soustraction, multiplication, division et extraction de la racine.

Exercice. Soit une constante $\beta \in \mathbb{C}$. Montrer, pour tout entier $n > 0$, que

$$f(x) = x^n - \beta$$

est soluble par radicaux.

Démonstration. D'abord, les coefficient sont $1, \beta$. On considère ainsi le corps

$$\mathbb{Q}(1, \beta) = \mathbb{Q}(1)(\beta) = \mathbb{Q}(\beta).$$

Un complex α est une racine de $f(x)$ si et seulement si $f(\alpha) = 0$, si et seulement si, $\alpha^n = \beta$, c'est-à-dire, une racine n-ième de α. Par conséquent, les racinces de $f(x)$ sont les racines n-ièmes de β, notées $\alpha_1, \ldots, \alpha_n$. Considérons la suite de sous-corps de $\mathbb{C}$ suivante:

$$\mathbb{Q}(\beta) = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_{n-1} \subseteq F_n,$$

où $F_i = \mathbb{Q}(\beta, \alpha_1, \ldots, \alpha_i)$, pour $i = 1, \ldots, n$. D'après le lemme 4.3.2,

$$F_i = \mathbb{Q}(\beta, \alpha_1, \ldots, \alpha_i) = \mathbb{Q}(\beta, \alpha_1, \ldots, \alpha_{i-1})(\alpha_i) = F_{i-1}(\alpha_i)$$

avec $\alpha_i^n = \beta \in F_{i-1}$, pour $i = 1, 2, \ldots, n$. Par la définition 4.3.11, F_n est une extension radicale de $\mathbb{Q}(\beta)$, qui contient toutes les racines de $f(x)$. Par la définition 4.3.13, $x^n - \beta$ est soluble par radicaux.

Exercice. Soit a un nombre réel positif. Montrer que les racines de $x^n - a$ sont

$$\sqrt[n]{a}, \quad \omega\sqrt[n]{a}, \quad \cdots, \quad \omega^{n-1}\sqrt[n]{a},$$

où $\sqrt[n]{a}$ désigne la seule racine n-ième réelle positive de a et

$$\omega = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}.$$

Démonstration. Les racines de $x^n - a$ sont les racines n-ièmes complexes de a. Dans MAT153, on a vu que les racines n-ièmes de 1 sont $1, \omega, \ldots, \omega^{n-1}$. Or

$$(\omega^j\sqrt[n]{a})^n = (\omega^j)^n\sqrt[n]{a}^n = (\omega^n)^j\sqrt[n]{a}^n = 1^j \cdot a = a,$$

pour $j = 0, 1, \ldots, n-1$. Étant 2 à 2 distincts, les n nombres complexes

$$\sqrt[n]{a}, \quad \omega\sqrt[n]{a}, \quad \cdots, \quad \omega^{n-1}\sqrt[n]{a}$$

sont les racines n-ièmes de a.

Exercice. Vérifier que le polynôme suivant est soluble par radicaux

$$g(x) = x^6 - 4x^3 + 1.$$

Démonstration. D'abord, les non-zero coefficients de $g(x)$ sont $1, -4, 1$. Considérons ainsi le corps $\mathbb{Q}(1, -4, 1) = \mathbb{Q}$. En suite,

$$\begin{aligned} g(x) &= (x^3)^2 - 2\cdot 2\cdot x^3 + 2^2 - 2^2 + 1 \\ &= (x^3 - 2)^2 - \sqrt{3}^2 \\ &= \left(x^3 - (2+\sqrt{2})\right)\left(x^3 - (2-\sqrt{2})\right), \end{aligned}$$

where $2+\sqrt{2}$ and $2-\sqrt{2}$ sont réels et positifs. On a vu dans MAT153 que les racines cubiques de 1 sont

$$1, \omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i, \omega^2 = -\frac{1}{2} - \frac{\sqrt{3}}{2}i.$$

Posant $\alpha = \sqrt[3]{2+\sqrt{3}}$ et $\beta = \sqrt[3]{2-\sqrt{2}}$, on a vu que les racines de $x^3 - (2+\sqrt{2})$ sont

$$1\cdot\alpha, \omega\cdot\alpha, \omega^2\cdot\alpha;$$

et les racines de $x^3 - (2-\sqrt{2})$ sont

$$1\cdot\beta, \omega\cdot\beta, \omega^2\cdot\beta.$$

Par conséquent, les racines de $f(x)$ sont

$$\alpha, \omega\alpha, \omega^2\alpha, \beta, \omega\beta, \omega^2\beta \in \mathbb{Q}(\sqrt{3}, \alpha, \beta, \omega) := E.$$

Considérons la suite de sous-corps de E suivante:

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{3}) \subset \mathbb{Q}(\sqrt{3})(\alpha) \subset \mathbb{Q}(\sqrt{3})(\alpha)(\beta) \subset \mathbb{Q}(\sqrt{3})(\alpha)(\beta)(\omega) = E.$$

Comme

$$\sqrt{3}^2 = 2 \in \mathbb{Q};\ \alpha^3 = 2 + \sqrt{3} \in \mathbb{Q}(\sqrt{3});\ \beta^3 = 2 + \sqrt{3} \in \mathbb{Q}(\sqrt{3})(\alpha);\ \omega^3 = 1 \in \mathbb{Q}(\sqrt{3})(\alpha)(\beta),$$

par la définition 4.3.11, E est une extension radicale de $\mathbb{Q}$. D'après la définition 4.3.13, $g(x)$ est résoluble par radicaux.

On accepte sans preuve le résultat célèbre suivant, dont la deuxième partie s'appelle *théorème d'Abel*, qui règle une question de très long temps si toute équation polynomiale est soluble par radicaux.

4.3.14. Théorème. (1) Tout polynôme complexe non constant de degré < 5 est soluble par radicaux.

(2) Pour tout entier $n \geq 5$, il y a des polynômes complexes de degré n qui sont non solubles par radicaux.

4.4 Construction géométrique

Cette section a pour but d'appliquer la théorie des corps pour répondre à des problèmes depuis très longtemps sur la construction géométrique à la règle et au compas. On ne s'intéresse que les figures géométriques formées de points et de droites. Ainsi le point clé est d'identifier les points du plan $\mathbb{R}^2$ qui sont constructibles à la règle et au compas. Ceci nous conduit à la construction suivante.

(1) Posons $\mathcal{P}_0 = \{(0,0), (1,0)\}$, un ensemble de deux points de $\mathbb{R}^2$.

(2) Supposons que l'ensemble $\mathcal{P}_n$ de points de $\mathbb{R}^2$ est défini pour un entier $n \geq 0$. Désigons 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 $\mathcal{P}_n$.

(3) Posons $\mathcal{P}_{n+1}$ l'union de $\mathcal{P}_n$ et l'ensemble de tout point, qui est un point d'intersection

(i) de deux droites distinctes de $\mathcal{D}_n$,

(ii) de deux cercles distincts de $\mathcal{C}_n$, ou

(iii) 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:

$$\mathcal{P}_0 \subseteq \mathcal{P}_1 \subseteq \cdots \subseteq \mathcal{P}_n \subseteq \cdots$$

Exercice. Trouver les ponts de $\mathcal{P}_1$.

Solution. Comme $\mathcal{P}_0 = \{(0,0),(1,0)\}$, on voit que $\mathcal{D}_0$ se compose d'une seule droite D_x, l'axe des x. En outre, $\mathcal{C}_0$ se compose de deux cercles C_1, C_2 de rayon 1 et de centers $(0,0)$ et $(1,0)$ respectivement.

On voit aisément que $D_x \cap C_1 = \{(-1,0),(1,0)\}$ et $D_x \cap C_2 = \{(0,0),(2,0)\}$.

Maintenant, supposons que $(x,y) \in C_1 \cap C_2$. On a alors

$$x^2 + y^2 = 1 \text{ et } (x-1)^2 + y^2 = 1.$$

Ceci nous donne

$$x^2 - (x-1)^2 = 0.$$

D'où,

$$x = \frac{1}{2}.$$

Donc,

$$y = \pm\sqrt{1-x^2} = \pm\frac{\sqrt{3}}{2}.$$

Ainsi,

$$C_1 \cap C_2 = \left\{ \left(\tfrac{1}{2}, \tfrac{\sqrt{3}}{2}\right), \left(\tfrac{1}{2}, -\tfrac{\sqrt{3}}{2}\right) \right\}.$$

Par définition, on a

$$\begin{aligned} \mathcal{P}_1 &= \mathcal{P}_0 \cup (D_x \cap C_1) \cup (D_x \cap C_2) \cup (C_1 \cap C_2) \\ &= \{(0,0),(1,0),(-1,0),(2,0),(\tfrac{1}{2},\tfrac{\sqrt{3}}{2}),(\tfrac{1}{2},-\tfrac{\sqrt{3}}{2})\}. \end{aligned}$$

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, d'une droite constructible et d'un cercle constructible) est constructible.

Exemple. (1) Étant les éléments de $\mathcal{P}_1$, les points

$$(0,0),(1,0),(-1,0),(2,0),(\tfrac{1}{2},\tfrac{\sqrt{3}}{2}),(\tfrac{1}{2},-\tfrac{\sqrt{3}}{2})$$

sont tous constructibles.

(2) Passant par deux points constructibles $(0,0)$ et $(1,0)$, l'axe des x est constructible.

(3) On verra que le point $(0, \sqrt[3]{2})$ n'est pas constructible.

4.4.2. Lemme. Si $p_1, \ldots, p_s$ sont des points constructibles, il existe un entier $n \geq 0$ tel que $p_1, \ldots, p_s \in \mathcal{P}_n$.

Démonstration. On procède par récurrence sur s. Si $s = 1$, alors l'énoncé est évident. Supposons que $s > 1$ et l'énoncé est valide pour $s - 1$. Alors, il existe un entier $m \geq 0$ tel que $p_1, \ldots, p_{s-1} \in \mathcal{P}_m$. En outre, par définition, $p_s \in \mathcal{P}_n$ pour un certain $n \geq 0$.

Si $m \leq n$, alors $\mathcal{P}_m \subseteq \mathcal{P}_n$, et donc, $p_1, \ldots, p_{s-1}, p_s \in \mathcal{P}_n$.

Si $n \leq m$, alors $\mathcal{P}_n \subseteq \mathcal{P}_m$, et donc, $p_1, \ldots, p_{s-1}, p_s \in \mathcal{P}_m$.

Ainsi, l'énoncé est valide pour s. La preuve du lemme s'achève.

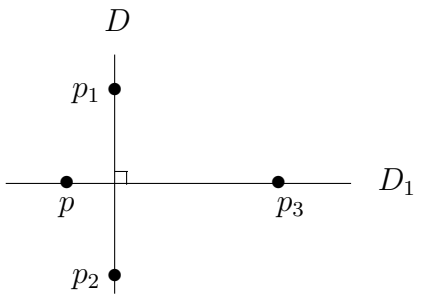
Étant donnés deux points p, q, on désigne par $\overline{pq}$ la distance entre p et q.

4.4.3. Lemme. Soient D une droite constructible et p un point constructible. Alors la perpendiculaire, ainsi que la parallèle, à D passant par p est constructible.

Démonstration. Par définition, D contient au moins deux points constructibles dont au moins un est différent de p, noté p_1. D'après le lemme 4.4.2, $p, p_1 \in \mathcal{P}_n$, pour un certain entier $n \geq 0$.

La droite D coupe le cercle constructible de centre p et de rayon $\overline{pp_1}$ en p_1 et un autre point, noté p_2. En particulier, p_2 est constructible.

Les deux cercles constructibles de centre p_1 et de centre p_2 respectivement et de même rayon $\overline{p_1p_2}$ se coupent en deux points, dont au moins un est différent de p, noté p_3. En particulier, p_3 est constructible. Par conséquent, la droite D_1 passant par p, p_3 est constructible. Ceci est illustré par le diagramme suivant:



Comme $\overline{p_1p_3} = \overline{p_2p_3}$, on voit que D_1 est perpendiculaire à D.

Comme on a vu, la droite D_2 qui est perpendiculaire à D_1 et passe par p est constructible D_2. Il est évident que D_2 est parallèlle à D. La preuve du lemme s'achève.

Exemple. L'axe des y est perpendiculaire à l'axe des x et passe par $(0,0)$. D'après le lemme 4.4.3, il est constructible.

Dans MAT153, on a vu que les nombres complexes peuvent être représentés par les points du plan de sorte qu'un complexe $a+bi$ correspond au point (a,b), où $a,b \in \mathbb{R}$. C'est la raison pourquoi certains problèmes en géométrie peuvent être résolus en algèbre.

4.4.4. Définition. Un nombre complexe $z = a + bi$, où $a,b \in \mathbb{R}$, est dit *constructible* si le point (a,b) du plan est constructible.

Exemple. On a vu que

$$\mathcal{P}_1 = \{(0,0),(1,0),(-1,0),(2,0),(\tfrac{1}{2},\tfrac{\sqrt{3}}{2}),(\tfrac{1}{2},-\tfrac{\sqrt{3}}{2})\}.$$

Ainsi, les nombres complexes

$$0, 1, -1, 2, \tfrac{1}{2}+\tfrac{\sqrt{3}}{2}i, \tfrac{1}{2}-\tfrac{\sqrt{3}}{2}i.$$

sont tous constructibles.

4.4.5. Lemme. Étant donné un nombre réel a, les énoncés suivants sont équivalents:
(1) Le nombre a est constructible.
(2) Le point $(a,0)$ est constructible.
(3) Le point $(0,a)$ est constructible.
(4) Le nombre ai est constructible.

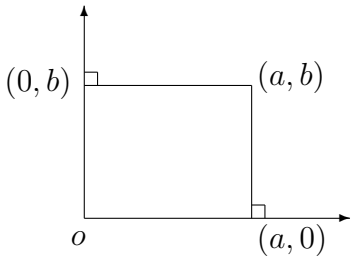
Démonstration. Par définition, on voit que les énoncés (1) et (2) sont équivalents. De même, les énoncés (3) et (4) sont équivalents.

Supposons que le point $(a,0)$ est contructible. Alors le cercle C de center $(0,0)$ et de rayon a est constructible. Étant un point d'intersection de C et l'axe des y, le point $(0,a)$ est constructible.

Supposons que $(0,a)$ est un point constructible. De la même façon, on peut montrer que $(a,0)$ est aussi constructible. La preuve du lemme s'achève.

4.4.6. Lemme. Un nombre complexe $a + bi$ est constructible si, et seulement si, a et b sont tous constructibles.

Démonstration. Considérons le diagramme



où l'axe des x et l'axe des y sont tous constructibles.

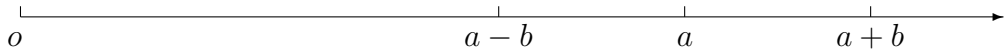
Supposons que $a + bi$ est constructible. C'est-à-dire, le point (a, b) est constructible. D'après le lemme 4.4.3, la droite passant par $(0, b)$ et (a, b) et la droite passant par $(a, 0)$ et (a, b) sont toutes constructibles. Par conséquent, $(0, b)$ et $(a, 0)$ sont des points constructibles. D'après le lemme 4.4.5, les nombres a et b sont constructibles.

Supposons que a, b sont constructibles. D'après le lemme 4.4.5, les points $(0, b)$ et $(a, 0)$ sont constructibles. D'après le lemme 4.4.3, la droite passant par $(0, b)$ et (a, b) et la droite passant par $(a, 0)$ et (a, b) sont toutes constructibles. Ainsi, le point (a, b) est constructible. C'est-à-dire, le complexe $a + bi$ est constructible. La preuve du lemme s'achève.

Exemple. Comme $0, 1$ sont constructibles, le complexe $i = \sqrt{-1}$ est constructible.

4.4.7. 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.

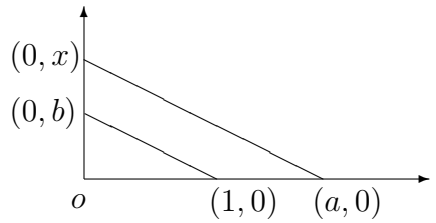
Exemple. On sait que $1, 2$ sont constructibles. Comme $3 = 1 + 2$, d'après le lemme 4.4.7, il est constructible.

Exercice. Si $a + bi \in \mathbb{C}$ est constructible, vérifier que $a - bi$ l'est aussi.

Preuve. Supposons que $a+bi \in \mathbb{C}$ est constructible. D'après le lemme 4.4.6, les nombres réels a, b sont constructibles. D'après le lemme 4.4.7, $-b = 0 - b$ est constructibel. D'après le lemme 4.4.6, le complexe $a - bi$ est constructible.

4.4.8. Lemme. Si $a, b \in \mathbb{R}$ sont constructibles, alors ab est constructible.

Démonstration. D'après la remarque précédente, on peut supposer que a, b sont tous positifs. Considérons le diagramme suivant:



où la droite passant par $(a, 0)$ et $(0, x)$, notée D_1, est parallèle à la droite constructible passant par $(1, 0)$ et $(0, b)$, notée D_2. D'après le lemme 4.4.3, D_1 est constructible, et donc, le point $(0, x)$ est constructible. Ainsi, le nombre x est constructible.

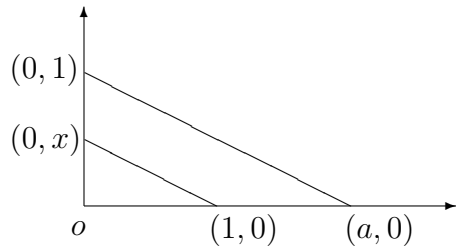
Maintenant, le triangle de sommets o, $(1,0)$ et $(0,b)$ est semblable au triangle de sommets $o,(a,0)$ et $(0,x)$. Par conséquent,

$$\frac{x}{b}=\frac{a}{1},$$

c'est-à-dire, $x=ab$. La preuve du lemme s'achève.

4.4.9. Lemme. Si $0\neq a\in\mathbb{R}$ est constructible, alors a^{-1} est constructible.

Démonstration. On peut supposer que a est positif. Considérons le diagramme suivant:



où où la droite passant par $(1,0)$ et $(0,x)$, notée D_1, est parallèle à la droite constructible passant par $(1,0)$ et $(a,0)$, notée D_2. D'après le lemme 4.4.3, D_1 est constructible, et donc, le point $(0,x)$ est constructible. Ainsi, le nombre x est constructible.

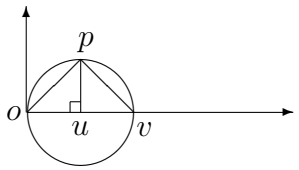
Maintenant, le triangle de sommets $o,(1,0)$ et $(0,x)$ est semblable au triangle de sommets $o,(a,0)$ et $(0,1)$. Par conséquent,

$$\frac{1}{a}=\frac{x}{1}=x.$$

La preuve du lemme s'achève.

4.4.10. Lemme. Si $a\in\mathbb{R}^+$ est constructible, alors $\sqrt{a}$ est constructible.

Démonstration. Comme a est constructible, d'après le lemme 4.4.7, $1+a$ est constructibe. D'après les lemmes 4.4.8 et 4.4.9, $\frac{1+a}{2}$ est constructible. Ainsi, le cercle de centre $(0,\frac{1+a}{2})$ et de rayon $1+a$ est constructible. Considérons le diagramme suivant:



où $v=(1+a,0)$, $u=(1,0)$ et $p=(1,x)$. Comme u est constructible, d'après le lemme 4.4.3, la droite passant par u et p est constructible. Ainsi, le nombre x est constructible.

Enfin, remarquant que le triangle de sommets o,u,p est semblable au triangle de sommets p,u,v, on a

$$\frac{x}{a}=\frac{1}{x}.$$

Par conséquent, $x=\sqrt{a}$. Ceci achève la démonstration du lemme.

4.4.11. Proposition. (1) Les nombre réels constructibles forment un sous-corps de $\mathbb{R}$.

(2) La distance entre deux points constructibles est un nombre constructible.

Démonstration. L'énoncé (1) découle des lemmes 4.4.7, 4.4.8 et 4.4.9.

(2) Supposons que $p = (a, b)$ et $q = (c, d)$ sont deux points constructibles. D'après le lemme 4.4.5, les nombres a, b, c, d sont constructibles. D'après lemmes 4.4.7 et 4.4.8, le nombre $(a - c)^2 + (b - d)^2$ est constructible. Maintenant, la distance entre p, q est

$$\sqrt{(a - c)^2 + (b - d)^2}.$$

D'après le lemme 4.4.10, ce dernier est constructible. La preuve de la proposition s'achève.

4.4.12. Définition. Un angle θ est dit *constructible* s'il est formé par deux droites constructibles.

Exemple. Comme les axes des x et des y sont tous constructibles, les angles

$$0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}$$

sont tous constructibles.

4.4.13. Lemme. Étant donné un angle θ, les conditions suivantes sont équivalentes.

(1) L'angle θ est constructible.

(2) Le nombre $\cos\theta + i\sin\theta$ est constructible.

(3) Le nombre $\cos\theta$ est constructible

Dans ce cas, l'angle $\frac{\theta}{2}$ est constructible.

Démonstration. Remarquons que le point $(\cos\theta, \sin\theta)$ est un point d'intersection du cercle unitaire C et la droite D_θ passant par les points $(0, 0)$ et $(\cos\theta, \sin\theta)$.

Comme l'axe des x est constructibles, par définition, on voit que θ est constructible si, et seulement si, D_θ est constructible. Comme C est constructible, D_θ est constructible si et seulement si le point $(\cos\theta, \sin\theta)$ est constructible si, et seulement si, $\cos\theta + i\sin\theta$ est constructible. Ceci montre l'équivalence des énoncés (1) et (2).

Si $\cos\theta$ est constructible, d'après les lemmes 4.4.7 et 4.4.8, $1 - \cos^2\theta$ est constructible, et d'après le lemme 4.4.10, $\sin\theta = \sqrt{1 - \cos^2\theta}$ est constructible. Donc, $\cos\theta$ est constructible si et seulement si $\cos\theta$ et $\sin\theta$ sont tous constructibles. D'après le lemme 4.4.6, cette dernière condition est valide si et seulement si $\cos\theta + i\sin\theta$ est constructible. Ceci montre l'équivalence des énoncés (2) et (3).

Supposons enfin que $\cos\theta$ est constructible. Rappelons que

$$\cos\frac{\theta}{2} = \sqrt{\frac{1 + \cos\theta}{2}}.$$

D'après les lemmes 4.4.7, 4.4.8, 4.4.9 et 4.4.10, ce dernier est constructible. Ainsi, l'angle $\frac{\theta}{2}$ est constructible. La preuve du lemme s'achève.

Exemple. Comme $(-\frac{1}{2}, \frac{\sqrt{3}}{2})$ est un point construcble, d'après le lemme 4.4.6, le complexe

$$\cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$$

est constructible. D'après le lemme 4.4.12, l'angle $\frac{2\pi}{3}$ est constructible.

4.4.14. Corollaire. Si z est un complexe constructible, alors ses racinces carrées d' sont constructibles.

Démonstration. On peut supposer que $z = a + bi \neq 0$. Écrivons

$$z = r(\cos\theta + i\sin\theta)$$

sous la forme polaire. Étant la distance entre $(0,0)$ et le point constructible (a,b), d'après la proposition 4.4.11, r est constructible. En outre, d'après le lemme 4.4.13, θ est un angle constructible. Dans MAT153, on a vu que z admet deux racines carrées

$$z_1 = \sqrt{r}\left(\cos\frac{\theta}{2} + i\sin\frac{\theta}{2}\right), \quad z_2 = -\sqrt{r}\left(\cos\frac{\theta}{2} + i\sin\frac{\theta}{2}\right),$$

où $\sqrt{r}$ est constructibe d'après le lemme 4.4.10. D'après le lemme 4.4.13, l'angle $\frac{\theta}{2}$ est constructible, et donc, $\cos\frac{\theta}{2}$ et $\sin\frac{\theta}{2}$ sont tous constructibles. En vertu du lemme 4.4.8, on voit que

$$z_1 = \sqrt{r}\cos\frac{\theta}{2} + i\sqrt{r}\sin\frac{\theta}{2}$$

est constructible, et donc, $z_2 = -z_1$ l'est aussi. La preuve du corollaire s'achève.

4.4.15. 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. Posons F l'ensemble des nombres complexes constructibles. En vertu des lemmes 4.4.7, 4.4.8 et 4.4.9, F est un sous-corps de $\mathbb{C}$ qui est stable pour la conjugaison. D'après le corollaire 4.4.14, F est stable pour l'extraction de racines carrées. Supposons maintenant que E est un sous-corps de $\mathbb{C}$ qui est stable pour l'extraction de racines carrées et pour la conjugaison. On veut montrer que $F \subseteq E$. Pour ce faire, on montrera les énoncés suivants.

(1) $i = \sqrt{-1} \in E$.

En effet, comme E est un sous-corps de $\mathbb{C}$, on a vu que $\mathbb{Q} \subseteq E$. Comme E est stable pour l'extraction de racines carrées, $i \in E$.

(2) *Pour tout $a + bi \in \mathbb{C}$, on a $a + bi \in E$ si et seulement si $a, b \in E$.*

En effet, si $a+bi \in E$, alors $a-bi \in E$ par l'hypothèse,. Ainsi, $a \in E$, et donc, $b \in E$. Si $a, b \in E$, comme $i \in E$ par l'énoncé (1), on voit que $a+bi \in E$.

(3) *Si* $\alpha x^2+\beta x+\gamma \in E[x]$ *avec* $\alpha \neq 0$ *, alors ses racines sont dans* E*.*

En effet, on a vu dans MAT152 que les deux racines sont

$$z_1 = \frac{-\beta+\sqrt{\beta^2+4\alpha\gamma}}{2\alpha}; z_2 = \frac{-\beta-\sqrt{\beta^2+4\alpha\gamma}}{2\alpha}.$$

Comme E est stable pour l'extraction de racines carrées, $z_1, z_2 \in E$.

(4) *Si* $a+bi, c+di \in E$*, alors la distance entre les points* (a,b) *et* (c,d) *appartient à* E*.*

En effet, d'après l'énoncé (2), $a, b, c, d \in E$. Comme E est stable pour l'extraction de racines carrées, on a

$$\sqrt{(a-c)^2+(b-d)^2} \in E.$$

(5) *Si* $(a,b) \in \mathcal{P}_n$ *avec* $n \geq 0$*, alors* $a+bi \in E$*.*

En effet, si $n=0$, comme $\mathcal{P}_0 = \{(0,0),(1,0)\}$, on a $z=0$ ou 1. L'énoncé (4) est valide.

Supposons que $n>0$ et l'énoncé (5) est valide pour $n-1$. Considérons les cas suivants.

(i) 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_j passe par deux points distincts (a_j,b_j) et (c_j,d_j) de $\mathcal{P}_{n-1}$, et donc,

$$(*) \qquad (a-a_j)(d_j-b_j) = (c_j-a_j)(b-b_j),\ j=1,2.$$

D'après l'énoncé (2), $a_1, a_2, b_1, b_2, c_1, c_2, d_1, d_2 \in E$. En résolvant le système $(*)$, on voit que $a, b \in E$. Ainsi, $a+bi \in E$.

(ii) Le point (a,b) est un 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 $\mathcal{P}_{n-1}$. Alors

$$\begin{aligned} (a-a_1)(b_2-b_1) &= (a_2-a_1)(b-b_1) \\ (a-c_0)^2+(b-d_0)^2 &= r_0^2. \end{aligned}$$

D'après les énoncés (2) et (4), $a_1, a_2, b_1, b_2, c_0, d_0, r_0 \in E$. Comme $a_2-a_1 \neq 0$ ou $b_2-b_1 \neq 0$, en résolvant le système ci-dessus, on voit que $a, b \in E$. Donc, $z=a+bi \in E$.

(iii) Le point (a,b) est un point d'intersection de deux cercles distincts C_1, C_2 de $\mathcal{C}_{n-1}$. Par définition, C_j est de centre $(a_j,b_j) \in \mathcal{P}_{n-1}$ et de rayons r_j, la distance entre des points de $\mathcal{P}_{n-1}$, $j=1,2$. Comme deux cercles se coupent, $(a_1,b_1) \neq (a_2,b_2)$. Par définition, on a

$$(a-a_j)^2+(b-b_j)^2 = r_j^2,\ j=1,2.$$

Ceci donne

$$(a_2-a_1)(2a-(a_1+a_2))+(b_2-b_1)(2b-(b_1+b_2)) = r_1^2-r_2^2.$$

D'après les énoncés (2) et (4), $a_1, a_2, b_1, b_2, r_1, r_2 \in E$. Comme $a_2 - a_1 \neq 0$ ou $b_2 - b_1 \neq 0$, en résolvant les équations ci-dessu, on voit que $a, b \in E$. Par conséquent, $z = a + bi \in E$.

Enfin, si $a + bi \in F$, alors (a, b) est constructible. D'après la définition 4.4.4, $(a, b) \in \mathcal{P}_n$ pour un certain $n \geq 0$. D'après l'énoncé (5), $a + bi \in E$. Ceci achève la démonstration du théorème.

Remarque. Comme $\mathbb{Q}$ est le plus petit sous-corps de $\mathbb{C}$, d'après le théorème 4.4.15, tous les nombres rationnels sont constructibles.

Le résultat suivant donne un critère en termes de corps pour un point soit constructible à la règele et au compas. Pour ce prouver, étant donné un sous-corps L de $\mathbb{C}$, on note

$$\overline{L} = \{\bar{\alpha} \mid \alpha \in L\},$$

ce qui est aussi un sous-corps de $\mathbb{C}$.

4.4.16. Théorème. Un nombre complexe z est constructible si, et seulement si, $z \in \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_r)$, où $\alpha_1, \alpha_2, \ldots, \alpha_r \in \mathbb{C}$ sont tels que

(1) $\alpha_1^2 \in \mathbb{Q}$;

(2) $\alpha_i^2 \in \mathbb{Q}(\alpha_1, \ldots, \alpha_{i-1})$, pour $i = 2, \ldots, r$.

Démonstration. D'après le théorème 4.4.15, l'ensemble F des nombres complexes constructibles est un sous-corps de $\mathbb{C}$ qui est stable pour les racines carrées et pour la conjugaison. En particulier, $\mathbb{Q} \subseteq F$.

Posons E l'ensemble des complexes satisfaisant à la condition énoncée dans le théorème. Fixons $z \in E$ non nul. Supposons que $z \in \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_r)$, où $\alpha_1^2 \in \mathbb{Q}$ et $\alpha_i^2 \in \mathbb{Q}(\alpha_1, \ldots, \alpha_{i-1})$, pour $i = 2, \ldots, r$. On montrera les énoncés suivants.

(1) $z \in F$.

Il suffit de prouver que $\mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_r) \subseteq F$. Par hypothèse, $\alpha_1^2 = a_0 \in \mathbb{Q}$, d'où, α_1 est une racine carrée de $a_0 \in F$. Comme F est stable pour les racines carrées, $\alpha_1 \in F$, et d'après la définition 4.3.1, $\mathbb{Q}(\alpha_1) \subseteq F$.

Supposons que $\mathbb{Q}(\alpha_1, \ldots, \alpha_{i-1}) \subseteq F$, avec $1 < i \leq r$. Comme $\alpha_i^2 = a_{i-1} \in \mathbb{Q}(\alpha_1, \ldots, \alpha_{i-1})$ par l'hypothèse, α_i est une racine carrée de $a_{i-1} \in F$, et donc, $\alpha_i \in F$. D'après le lemme 4.3.2 et la définition 4.3.1, on a $\mathbb{Q}(\alpha_1, \ldots, \alpha_i) = \mathbb{Q}(\alpha_1, \ldots, \alpha_{i-1})(\alpha_i) \subseteq F$. Par récurrence, on a montré que $\mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_r) \subseteq F$.

(2) $\bar{z} \in E$.

Comme $\alpha_1, \ldots, \alpha_r$ sont algébriques sur $\mathbb{Q}$, d'après le théorème 4.3.10, $z = f(\alpha_1, \ldots, \alpha_r)$, où $f(x_1, \ldots, x_r) \in \mathbb{Q}[x_1, \ldots, x_r]$. D'après un résultat de MAT153, on a

$$\bar{z} = \overline{f(\alpha_1, \ldots, \alpha_r)} = f(\overline{\alpha}_1, \ldots, \overline{\alpha}_r) \in \mathbb{Q}(\overline{\alpha}_1, \ldots, \overline{\alpha}_r).$$

Comme $\alpha_1^2 \in \mathbb{Q}$, on voit que $\overline{\alpha}_1^2 = \overline{\alpha_1^2} = \alpha_1^2 \in \mathbb{Q}$, et

$$\overline{\alpha}_i^2 = \overline{\alpha_i^2} \in \overline{\mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_{i-1})} = \mathbb{Q}(\overline{\alpha}_1, \ldots, \overline{\alpha_{i-1}}), \text{ pour } i = 2, \ldots, r.$$

D'après la définition, $\bar{z} \in E$.

(3) Si β est une racine carrée de z, alors $\beta \in E$.

Posant $\alpha_{r+1} = \beta$, on a $\beta \in \mathbb{Q}(\alpha_1, \ldots, \alpha_r, \alpha_{r+1})$, où $\alpha_1^2 \in \mathbb{Q}$ et $\alpha_i^2 \in \mathbb{Q}(\alpha_1, \ldots, \alpha_{i-1})$, pour $i = 2, \ldots, r, r+1$. Par définition de E, on voit que $\beta \in E$.

(4) E est un sous-corps de $\mathbb{C}$.

Supposons que $y \in E$, disons $y \in \mathbb{Q}(\beta_1, \beta_2, \ldots, \beta_s)$, où $\beta_1^2 \in \mathbb{Q}$ 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

$$y \pm z, yz, yz^{-1} \in \mathbb{Q}(\alpha_1, \ldots, \alpha_r, \alpha_{r+1}, \ldots, \alpha_{r+s}),$$

où $\alpha_1^2 \in Q$, et $\alpha_i^2 \in \mathbb{Q}(\alpha_1, \ldots, \alpha_{i-1})$, pour $i = 1, \ldots, r+s$. D'après la définition de E, on a

$$y \pm z, yz, yz^{-1} \in E.$$

Ainsi, E est un sous-corps de $\mathbb{C}$.

D'après les énoncés (2), (3) et (4), E est un sous-corps de $\mathbb{C}$ qui est stable pour l'extraction de racines carrées et pour la conjugaison. D'après le théorème 4.4.15, $F \subseteq E$, et d'après lénoncé (1), $E \subseteq F$. Donc, $E = F$. Ceci achève la démonstration du théorème.

Exercice. Vérifier que le nombre complexe suivant est constructibe:

$$\alpha = \sqrt{11 - 2\sqrt{\sqrt{2} - 2\sqrt{7}} - 5\sqrt{1 - 2\sqrt{3}}}.$$

Preuve. Posons $\alpha_1 = \sqrt{2}$, $\alpha_2 = \sqrt{7}$, $\alpha_3 = \sqrt{3}$, $\alpha_4 = \sqrt{\sqrt{2} - 2\sqrt{7}}$ et $\alpha_5 = \sqrt{1 - 2\sqrt{3}}$ et $\alpha_6 = \alpha$. Alors $\alpha \in \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6)$, où

$$\alpha_1^2 = 2 \in \mathbb{Q}; \alpha_2^2 = 7 \in \mathbb{Q}(\alpha_1); \alpha_3^2 = 3 \in \mathbb{Q}(\alpha_1, \alpha_2); \alpha_4^2 = \alpha_1 - 2\alpha_2 \in \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$$

et

$$\alpha_5^2 = 1 - 2\alpha_3 \in \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4); \alpha_6^2 = 11 - 2\alpha_4 - 5\alpha_5 \in \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5).$$

D'après le théorème 4.4.16, α est constructible.

Le résultat suivant nous permet de donner une réponse négative pour plusieurs de constructions géométriques à la règle et au compas.

4.4.17. Corollaire. Si $z \in \mathbb{C}$ est constructible, alors

$$[\mathbb{Q}(z) : \mathbb{Q}] = 2^n, \text{ où } n \geq 0.$$

Démonstration. Supposons que z est constructible. D'après le théorème 4.4.16, on a $z \in \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_r)$, où $\alpha_1^2 = a_0 \in \mathbb{Q}$ et $\alpha_i^2 = a_{i-1} \in \mathbb{Q}(\alpha_1, \ldots, \alpha_{i-1})$, pour $i = 2, \ldots, r$.

Posons $F_0 = \mathbb{Q}$ et $F_i = F_{i-1}(\alpha_i) = \mathbb{Q}(\alpha_1, \ldots, \alpha_i)$, pour $i = 1, \ldots, r$. On prédent que

$$[F_i : \mathbb{Q}] = 2^{n_i}, \text{ où } n_i \geq 0, \text{ pour } i = 0, 1, \ldots, r.$$

En effet, d'après le lemme 4.2.3, $[F_0 : \mathbb{Q}] = [\mathbb{Q} : \mathbb{Q}] = 1 = 2^0$. Supposons que cet énoncé est valide pour $i - 1$ avec $0 < i \leq r$. Comme $\alpha_i^2 - a_{i-1} = 0$, on voit que α_i est une racine de $x^2 - a_{i-1} \in F_{i-1}[x]$. D'après les définitions 4.3.7 et 4.3.4(3),

$$\partial_{F_{i-1}}(\alpha_i) = \partial(m_{F_{i-1}}^{\alpha_i}(x)) \in \{1, 2\}.$$

D'après le théorème 4.3.8, $[F_{i+1} : F_i] = \partial_{F_{i-1}}(\alpha_i) = 2^{e_i}$ avec $e_i \in \{0, 1\}$. En vue du théorème 4.2.7, on voit que

$$[F_i : \mathbb{Q}] = [F_i : F_{i-1}][F_{i-1} : \mathbb{Q}] = 2^{n_{i-1}+e_i}.$$

Par récurrence, on a montré l'énoncé. En particulier, $[F_r : \mathbb{Q}] = 2^{n_r}$, où $n_r \geq 0$.

Maintenant, comme $z \in F_r$, on a $\mathbb{Q}(z) \subseteq F_r$. D'après le théorème 4.2.7,

$$2^{n_r} = [F_r : \mathbb{Q}] = [F_r : \mathbb{Q}(z)][\mathbb{Q}(z) : \mathbb{Q}].$$

D'où, $[\mathbb{Q}(z) : \mathbb{Q}] = 2^n$ avec $n \geq 0$. Ceci achève la démonstration du corollaire.

Exercice. Vérifier que le nombre réel $\sqrt[3]{2}$ est non constructible.

Preuve. Il est évident que $\sqrt[3]{2}$ est une racine de $x^3 - 2$. Comme 2 est premier, d'après le critère d'Eisenstein, $x^3 - 2$ est irréductibe sur $\mathbb{Q}$, et d'après le corollaire 4.3.6(2), on voit que $m_{\mathbb{Q}}^{\sqrt[3]{2}}(x) = x^3 - 2$. D'après le théorème 4.3.8 et la définition 4.3.7, on a

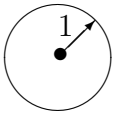
$$[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = \partial_{\mathbb{Q}}(\sqrt[3]{2}\,) = \partial(m_{\mathbb{Q}}^{\sqrt[3]{2}}(x)) = 3.$$

Comme $3 \neq 2^n$ pour tout $n \geq 0$, d'après le corollaire 4.4.17, $\sqrt[3]{2}$ est non constructible. La preuve s'achève.

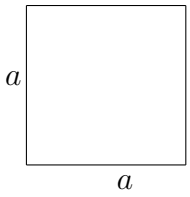
Rappelons que la quadrature du cercle signifie le suivant: étant donné un cercle quelconque, on construit à la règle et au compas un carré ayant le même aire que le cercle donné.

4.4.18. Théorème. La quadrature du cercle à la règle et au compas est impossible.

Démonstration. Considérons le cercle unitaire



dont l'aire est π. Supposons qu'on puisse construire à la règle et au compas un carré



d'aire π, c'est-à-dire, $a^2 = \pi$. Comme le carré est constructible, ses sommets sont constructibles. D'après la proposition 4.4.11(2), a est constructible. C'est-à-dire, $\sqrt{\pi}$ est constructible. D'après le corollaire 4.4.12, $[\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}] = 2^n$ pour un certain $n \geq 0$. Comme

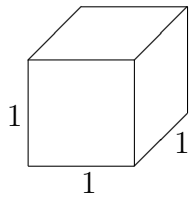
$$\pi = (\sqrt{\pi})^2 \in \mathbb{Q}(\sqrt{\pi}),$$

on voit que $\mathbb{Q}(\pi) \subseteq \mathbb{Q}(\sqrt{\pi})$. D'après le théorème 4.2.7, $[\mathbb{Q}(\pi) : \mathbb{Q}]$ est fini. D'après le théorème 4.3.8, π est algébrique sur $\mathbb{Q}$, ce qui contredit le théorème de Lindemann. La preuve du théorème s'achève.

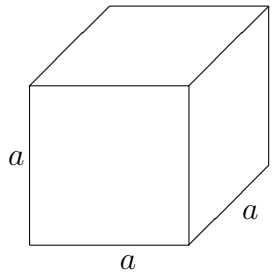
La duplication du cube signifie le suivant: étant donné un cube quelconque, on construit à la règle et au compas un cube qui double le volume du cube donné.

4.4.19. Théorème. La duplication du cube à la règle et au compas est impossible.

Démonstration. Considérons le cube unitaire



dont le volume est 1. Supposons qu'on puisse construire à la règle et au compas un cube



de volume 2. Alors $a^3 = 2$. C'est-à-dire, $a = \sqrt[3]{2}$. Comme le cube est constructible, ses sommets sont constructibles. D'après la proposition 4.4.11(2), a est constructible. Cependant, on a déjà vu que $\sqrt[3]{2}$ est non constructible, une contradiction. La preuve du théorème s'achève.

La trisection de l'angle signifie le suivant: étant donné un angle quelconque, on construit à la règle et au compas deux demi-droites qui partagent l'angle donné en trois angles égaux.

4.4.20. Théorème. La trisection de l'angle à la règle et au compas est impossible.

Démonstration. Supposons qu'on puisse triséquer l'angle $\frac{\pi}{3}$ à la règle et au compas. Alors l'angle $\frac{\pi}{9}$ est constructible. D'après le lemme 4.4.13, $b = \cos\frac{\pi}{9}$ est un nombre constructible. Remarquons, pour tout angle θ, que

$$\cos 3\theta = 4\cos^3\theta - 3\cos\theta.$$

Posant $\theta = \frac{\pi}{9}$, on trouve que

$$4b^3 - 3b = \cos\frac{\pi}{3} = \frac{1}{2}.$$

D'où,

$$b^3 - \frac{3}{4}b - \frac{1}{8} = 0.$$

C'est-à-dire, b est une racine de

$$x^3 - \frac{3}{4}x - \frac{1}{8}.$$

On a vu que ce dernier est irréductible sur $\mathbb{Q}$, et d'après le corollaire 4.3.6(2), il est le polynôme minimal de b sur $\mathbb{Q}$. D'après le théorème 4.3.8, on a

$$[\mathbb{Q}(b) : \mathbb{Q}] = 3,$$

cei qui contredit le corollaire 4.4.17. La démonstration du théorème s'achève.

Soit un entier $n \geq 3$. Un *n-polygone régulier* est un polygone de n sommets, qui partagent le cercle unitaire en n secteurs égaux.

4.4.21. Proposition. Soit un entier $n \geq 3$. Les conditions suivantes sont équivalentes.
(1) Un n-polygone régulier est constructible à la règle et au compas.
(2) L'angle $\frac{2\pi}{n}$ est constructible.
(3) La racine n-ième primitive de 1 suivante est constructible:

$$\zeta_n = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}.$$

Démonstration. D'après la définition, les énoncés (1) et (2) sont équivalents. D'après le lemme 4.4.13, les énoncés (2) et (3) sont équivalents. La preuve de la proposition s'achève.

Exemple. On peut construire à la règle et au compas un triangle équilatéral.

Démonstration. D'abord, un triangle équilatéral est un 3-polygone régulier. Comme

$$\cos\frac{2\pi}{3} = -\frac{\sqrt{3}}{2}$$

est un nombre constructible, d'après le lemme 4.4.13, l'angle $\frac{2\pi}{3}$ est constructible. Ainsi, un triangle équilatéral est constructible.

Exercice. Il est impossible de construire à la règle et au compas un heptagone régulier.

Démonstration. Supposons qu'un heptagone régulier soit constructible. D'après la proposition 4.4.21, le complexe

$$\zeta_7 = \cos\frac{2\pi}{7} + i\sin\frac{2\pi}{7}$$

est constructible. Comme $\zeta_7^7 = 1$, on voit que ζ_7 est une racine de

$$x^7 - 1 = (x-1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1).$$

Comme $\zeta_7 \neq 1$, on voit que ζ_7 est une racine de

$$\Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1.$$

Comme 7 est premier, d'après le numéro deux des Exercices dirigés VII, $\Phi_7(x)$ est irréductible sur $\mathbb{Q}$. D'après le corollaire 4.3.6, $m_{\mathbb{Q}}^{\zeta_7}(x) = \Phi_7(x)$. D'après le théorème 4.3.8, on a

$$[\mathbb{Q}(\zeta_7) : \mathbb{Q}] = \partial(m_{\mathbb{Q}}^{\zeta_7}(x)) = 6.$$

Ceci contredit le corollaire 4.4.17. Ainsi, un heptagone régulier est non constructible.

4.4.22. Définition. (1) Pour $n \geq 0$, le nombre $F_n = 2^{2^n} + 1$ s'appelle *n-ième nombre* de Fermat.

(2) Un nombre de Fermat s'appelle un *premier de Fermat* s'il est premier.

Exemple. (1) Posant $n = 0, 1, 2, 3, 4$, on obtient des premiers de Fermat

$$3, 5, 17, 257, 65537.$$

(2) Il est connu que F_5 n'est pas premier.

(3) Les premiers $7, 11, 13, 19$ ne sont pas des nombres de Fermat.

4.4.23. Lemme. Soit $p = 2^n + 1$ avec $n \geq 0$. Si p est premier, alors il est un premier de Fermat.

Démonstration. Supposons que $n = mq$, où $m \geq 1$ et $q > 1$ est impaire. Alors $a = 2^m \geq 2$. Donc

$$p = a^q + 1 = (a+1)((a^{q-1} - a^{q-2}) + \cdots + (a^2 - a) + 1),$$

ce qui n'est pas premier. La preuve du lemme s'achève.

On accepte le résultat suivant sans preuve.

4.4.24. Théorème de Gauss. Soit un entier $n \geq 3$. Le n-polygone régulier est constructible si, et seulement si,

$$n = 2^r p_1 \cdots p_s,$$

où $r, s \geq 0$ et $p_1, \ldots, p_s$ sont des premiers de Fermat deux à deux distincts.

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 le reste de $f(x)$ par $g(x)$.

2. Déterminer les polynômes rationnels suivants sont réductibles ou irréductibles sur $\mathbb{Q}$:

   (1) $x^4 + 1$; (2) $x^3 - 7x^2 + 3x + 3$.

3. (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.

4. 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.

5. 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 $\mathbb{Q}$.

6. En sachant que $\mathbb{Q}[\sqrt{7}] = \{a + b\sqrt{7} \mid a, b \in \mathbb{Q}\}$ est un sous-corps de $\mathbb{C}$ contenant $\mathbb{Q}$, trouver le degré de l'extension de corps $\mathbb{Q}[\sqrt{7}] : \mathbb{Q}$. *Indice*: Montrer, à l'aide du numéro 3(1), que la famille $\{1, \sqrt{7}\}$ est libre dans le $\mathbb{Q}$-espace vectoriel $\mathbb{Q}[\sqrt{7}]$.

7. Considérer l'extension de corps $\mathbb{R} : \mathbb{Q}$. Vérifier que $\alpha = \sqrt[3]{5 - \sqrt{2 - \sqrt{2}}} \in \mathbb{R}$ est algèbre sur $\mathbb{Q}$.

8. Soit $z = a + bi \in \mathbb{C}$, où $a, b \in \mathbb{R}$ avec $b \neq 0$. Donner un polynôme minimal de z sur $\mathbb{Q}$.

9. Soit $E : F$ une extension de corps de degré premier p. Montrer que $E : F$ est une extension simple. *Indice*: Appliquer le lemme 4.2.5 et le théorème 4.2.7.

10. 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.

11. 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 $\partial_L(\alpha) \leq \partial_F(\alpha)$.

12. Trouver le degré de l'extension de corps $\mathbb{Q}(\alpha) : \mathbb{Q}$, où $\alpha \in \mathbb{C}$ tel que $\alpha^7 = 3$.

13. Considérer $\mathbb{Q}(\alpha)$, le sous-corps de $\mathbb{R}$ engendré par α sur $\mathbb{Q}$, où $\alpha = \sqrt{2 + \sqrt{2}}$.
    (1) Trouver $m_{\mathbb{Q}}^{\alpha}(x)$, le polynôme minimal de α sur $\mathbb{Q}$. *Indice*: Calculer $(\alpha^2 - 2)^2$ et appliquer le critère d'Eisenstein.
    (2) Vérifier que $\mathbb{Q}(\alpha) = \{a_0 + a_1\alpha + a_2\alpha^2 + \alpha_3\alpha^3 \mid \alpha_0, \alpha_1, \alpha_2, \alpha_3 \in \mathbb{Q}\}$.
    (3) Mettre $(1 + \alpha - \alpha^2)(3 + \alpha^2)$ sous la forme de la partie (2).
    (4) Mettre $(\alpha^2 + \alpha + 1)^{-1}$ sous la forme de la partie (2). *Indice*: Appliquer l'algorithme d'Euclide au couple $(m_{\mathbb{Q}}^{\alpha}(x), x^2 + x + 1)$.
    (5) Déterminer si $\sqrt[3]{2}$ appartient à $\mathbb{Q}(\alpha)$ ou non. *Indice*: Calculer $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]$.

14. 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*:
    $$[\mathbb{Q}(\sqrt{2}, \alpha) : \mathbb{Q}(\sqrt{2})] = [\mathbb{Q}(\sqrt{2}, \alpha) : \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})][\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}(\sqrt{2})].$$

15. 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 une base du $\mathbb{Q}$-espace vectoriel $\mathbb{Q}(\sqrt{5}, \sqrt{7})$.
    (3) Vérifier que $\mathbb{Q}(\sqrt{5}, \sqrt{7}) : \mathbb{Q}]$ est une extension simple. *Indice*: Considérer le nombre $\sqrt{5}, \sqrt{7}$.

16. 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.

17. Montrer que $\sqrt{\pi}$ et $\pi^3 + \sqrt{\pi} + 1$ sont transcendants sur $\mathbb{Q}$.

18. Soient $L : F$ et $E : L$ deux extensions algébriques de corps. Montrer que $E : F$ est une extension algébrique.

19. Donner une extension radicale de $\mathbb{Q}$ qui contient le nombre suivant:

$$\sqrt[7]{7 - 6\sqrt[5]{3 - 13\sqrt[3]{11}}}.$$

20. Vérifier que $f(x) = x^6 - 10x^3 + 23$ est soluble par radicaux.

21. Soient $L : F$ et $E : L$ deux extensions radicales de corps. Montrer que $E : F$ est une extension radicale.

22. 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 $\beta^2 \in F$.

23. 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 $\mathbb{Q}$.

24. Vérifier que le nombre complexe suivant est constructibe:

$$\sqrt{\sqrt{3 - 5\sqrt{5}} - 2\sqrt{5 - 4\sqrt{-7}}}.$$

25. Montrer qu'on peut construire un pentagone régulier à la règle et au compas.

26. 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.

Chapitre V: Algorithme PageRank

Le but de ce chapitre est d'étudier l'algorithme PageRank, ce qui est inventé par Larry Page et utilisé par Google pour mésurer l'importance de chacune des pages web d'un réseau internet de sorte que la page la plus importante apparaît en premier. Il s'agit d'une application de valeurs propres et de vecteurs propres de matrices colonne-stochastiques.

5.1 Valeurs propres et vecteurs propres

Le but de cette section est de faire un petit rappel de valeurs propres et de vecteurs propres de matrices du cours MAT253.

5.1.1. Définition. Soit $A \in M_n(\mathbb{R})$. Un nombre réel λ_0 est une *valeur propre* de A s'il existe un vecteur non nul $u_0 \in \mathbb{R}^n$ (c'est-à-dire, une matrice de type $n \times 1$) tel que $Au_0 = \lambda_0 u_0$. Dans ce cas, u_0 est dit *vecteur propre* associé à λ_0.

Exemple. Considérons la matrice carrée réelle

$$A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}.$$

On voit que

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

Ainsi, la valeur 0 est une valeur propre de A et le vecteur

$$\begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

est un vecteur propre de A associés à cette valeur propre 0. En outre, on voit aussi que

$$\begin{pmatrix} 2 \\ -2 \end{pmatrix}, \begin{pmatrix} 3 \\ -3 \end{pmatrix}$$

sont des vecteurs propres de A associés à 0.

On étudiera comment les valeurs propres d'une matrice carrée. Pour ce faire, on introduit la notion suivante.

5.1.2. Définition. Soient $A \in M_n(\mathbb{R})$ et λ une variable. On appelle

$$\chi_A(\lambda) = \det(A - \lambda I_n) = (-1)^n \lambda^n + a_{n-1}\lambda^{n-1} + \cdots + a_1\lambda + a_0$$

le *polynôme caractéristique* de A.

Voici la méthode promise pour trouver les valeurs propres.

5.1.3. Théorème. Une valeur $\lambda_0 \in \mathbb{R}$ est une valeur propre de $A \in M_n(\mathbb{R})$ si et seulement si λ_0 est une racine de $\chi_A(\lambda)$.

Exercice. Trouver les valeurs propres de A, où

$$A = \begin{pmatrix} 1 & -1 \\ 2 & 4 \end{pmatrix}.$$

Solution. D'après le théorème 5.1.3, on calcule

$$\chi_A(\lambda) = \det(A - \lambda I_2) = \begin{vmatrix} 1-\lambda & -1 \\ 2 & 4-\lambda \end{vmatrix}.$$

Effectuant les opérations $L_1 + L_2$ et $C_2 - C_1$, on obtient

$$\chi_A(\lambda) = \begin{vmatrix} 1-\lambda & -1 \\ 2 & 4-\lambda \end{vmatrix} = \begin{vmatrix} 3-\lambda & 3-\lambda \\ 2 & 4-\lambda \end{vmatrix} = \begin{vmatrix} 3-\lambda & 0 \\ 2 & 2-\lambda \end{vmatrix} = (3-\lambda)(2-\lambda).$$

D'après le théorème 5.1.3, les valeurs propres de A sont 2 et 3.

5.1.4. Corollaire. Si $A \in M_n(\mathbb{R})$, alors A et A^T ont les mêmes valeurs propres.

Démonstration. Un résultat du MAT253 dit qu'une matrice et sa transposée ont le même déterminant. Ainsi,

$$\chi_A(\lambda) = \det(A - \lambda I_n) = \det(A - \lambda I_n)^T = \det(A^T - \lambda I_n) = \chi_{A^T}(\lambda).$$

D'après le théorème 5.1.3, A et A^T ont les même valeurs propres. La preuve du corollaire s'achève.

Remarque. En général, A et A^T n'ont pas les mêmes vecteurs propres.

Exemple. Considérons

$$A = \begin{pmatrix} 2 & 2 \\ 3 & 1 \end{pmatrix}, u = \begin{pmatrix} 1 \\ 1 \end{pmatrix}.$$

On voit aisément que $Au = 4u$, mais

$$A^T u = \begin{pmatrix} 5 \\ 3 \end{pmatrix} \neq au, \text{ pour tout } a \in \mathbb{R}.$$

D'où, u est un vecteur propre de A associé à la valeur propre 4, mais u n'est pas un vecteur propre de A^T.

Le résultat suivant dit comment trouver les vecteurs propres d'une matrice associés à une valeur propre donnée.

5.1.5. Théorème. Soit $A \in M_n(\mathbb{R})$. Si λ_0 est une valeur propre de A, alors $u_0 \in \mathbb{R}^n$ est un vecteur propre de A associé à λ_0 si, et seulement si, u_0 est une solution non nulle du sysème homogène $(A - \lambda_0 I_n)X = 0$.

Remarque. On a vu dans MAT153 que les solutions de $(A - \lambda_0 I_n)X = 0$ forment un sous-espace vectoriel de $\mathbb{R}^n$. Ainsi, toute combinaison linéaire non nulle de vecteurs propres de A associés à λ_0 est un vecteur propre associé à λ_0.

Soit $A \in M_n(\mathbb{R})$. Pour tout polynôme réel $f(\lambda) = \sum_{i=1}^{r} a_i \lambda^i$, on pose

$$f(A) = a_0 I_n + a_1 A + \cdots + a_r A^r \in M_n(\mathbb{R}).$$

5.1.6. Proposition. Soient $A \in M_n(\mathbb{R})$ et un polynôme réel $f(\lambda)$.

(1) Si λ_0 est une valeur propre de A, alors $f(\lambda_0)$ est une valeur propre de $f(A)$.

(2) Si u_0 est un vecteur propre de A associé à λ_0, alors u_0 est un vecteur propre de $f(A)$ associé à $f(\lambda_0)$.

Démonstration. Supposons que u_0 est un vecteur propre de A associé à une valeur propre λ_0. Comme $Au_0 = \lambda_0 u_0$, on a

$$A^2 u_0 = A(Au_0) = A(\lambda_0 u_0) = \lambda_0(Au_0) = \lambda_0(\lambda_0 u_0) = \lambda_0^2 u_0.$$

En général, on a $A^i u_0 = \lambda_0^i u_0$, pour tout $i \geq 0$. Posant $f(\lambda) = \sum_{i=1}^{r} a_i \lambda^i$, on obtient

$$f(A)u_0 = \sum_{i=0}^{r} a_i A^i u_0 = \sum_{i=0}^{r} a_i \lambda_0^i u_0 = \left(\sum_{i=0}^{r} a_i \lambda_0^i \right) u_0 = f(\lambda_0) u_0.$$

C'est-à-dire, $f(\lambda_0)$ est une valeur propre de $f(A)$, associé auquel u_0 est un vecteur propre de $f(A)$. La preuve de la proposition s'achève.

Exemple. Considérons $f(\lambda) = 3 - \lambda + \lambda^2$ et

$$A = \begin{pmatrix} 1 & -1 \\ 2 & 4 \end{pmatrix}; u = \begin{pmatrix} 1 \\ -1 \end{pmatrix}.$$

On voit que $Au = 2u$. C'est-à-dire, u est un vecteur propre de A associé à la valeur propre 2. D'après la proposition 5.1.6, u est un vecteur propre associé à la valeur propre $f(2) = 5$ de la matrice

$$f(A) = 3I_2 - A + A^2 = 3\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} - \begin{pmatrix} 1 & -1 \\ 2 & 4 \end{pmatrix} + \begin{pmatrix} -1 & -5 \\ 10 & 14 \end{pmatrix} = \begin{pmatrix} 1 & -4 \\ 8 & 13 \end{pmatrix}.$$

Effectivement, on a

$$\begin{pmatrix} 1 & -4 \\ 8 & 13 \end{pmatrix}\begin{pmatrix} 1 \\ -1 \end{pmatrix} = \begin{pmatrix} 5 \\ -5 \end{pmatrix} = 5 \cdot \begin{pmatrix} 1 \\ -1 \end{pmatrix}.$$

5.2 Matrices colonne-stochastiques

En théorie des probabilités, une matrice stochastique est la matrice de transition d'une chaîne de Markov. Dans cette section, on s'intéresse aux transposées de matrices stochastiques. D'abord, une matrice réelle $A = (a_{ij})_{m\times n}$ est dite

(1) *positive* si $a_{ij} > 0$, pour $i = 1, \ldots, m; j = 1, \ldots, n$;

(2) *non négative* si $a_{ij} \geq 0$ pour $i = 1, \ldots, m; j = 1, \ldots, n$;

(3) *non positive* si $a_{ij} \leq 0$ pour $i = 1, \ldots, m; j = 1, \ldots, n$.

Il est évident que le produit de deux matrices non négatives est non négatif.

5.2.1. Définition. Une matrice non négative $A \in M_{m\times n}(\mathbb{R})$ est dite *colonne-stochastique* si les termes de chaque colonne de A somment à 1; ou bien, si

$$A_1 + \cdots + A_m = (1, \ldots, 1),$$

où $A_1, \ldots, A_m$ sont les lignes de A.

Remarque. On voit que A est colonne-stochastique si et seulement si chaque colonne de A est colonne-stochastique.

Exemple. (1) Toute matrice-identitié I_n est colonne-stochastique.

(2) La matrice

$$\begin{pmatrix} 0,2 & 0,4 & 0,7 \\ 0,8 & 0,6 & 0,3 \end{pmatrix}$$

est colonne-stochastique, et ses colonnes

$$\begin{pmatrix} 0,2 \\ 0,8 \end{pmatrix}, \begin{pmatrix} 0,4 \\ 0,6 \end{pmatrix}, \begin{pmatrix} 0,7 \\ 0,3 \end{pmatrix}$$

sont toutes colonne-stochastiques.

On étudiera les propriétés de matrices colonne-stochastiques.

5.2.2. Lemme. Soient des matrices colonne-stochastiques $A_1, \ldots, A_r \in M_{m\times n}(\mathbb{R})$. Si $a_1, \ldots, a_r \in \mathbb{R}$ sont non négatifs tels que $\sum_{j=1}^{r} a_j = 1$, alors la matrice

$$a_1A_1 + \cdots + a_rA_r$$

est colonne-stochastique.

Démonstration. Posons $A = a_1A_1 + \cdots + a_rA_r$. Comme les a_i sont non négatifs, A est non négative. On partage les matrices A_j en lignes comme suit:

$$A_j = \begin{pmatrix} A_{1,j} \\ \vdots \\ A_{m,j} \end{pmatrix}, j = 1, \ldots, r.$$

Comme A_j est colonne-stochastique par l'hypothèse, on a

$$A_{1,j} + \cdots + A_{m,j} = (1, \cdots, 1).$$

On a maintenant que

$$A = a_1A_1 + \cdots + a_rA_r = \begin{pmatrix} a_1A_{1,1} + \cdots + a_rA_{1,r} \\ \vdots \\ a_1A_{m,1} + \cdots + a_rA_{m,r} \end{pmatrix},$$

dont les lignes somment à

$$\sum_{i=1}^{m}\left(\sum_{j=1}^{r} a_jA_{i,j}\right) = \sum_{j=1}^{r} a_j\left(\sum_{i=1}^{m} A_{i,j}\right) = \sum_{j=1}^{r} a_j\,(1, \ldots, 1) = \left(\sum_{j=1}^{r} a_j, \ldots, \sum_{j=1}^{r} a_j\right) = (1, \ldots, 1).$$

C'est-à-dire, A est colonne-stochastique. La preuve du lemme s'achève.

Exemple. Considérons deux matrices colonne-stochastiques suivantes:

$$\begin{pmatrix} 0,2 \\ 0,8 \end{pmatrix}, \begin{pmatrix} 0,4 \\ 0,6 \end{pmatrix}.$$

Considérant $\frac{1}{4}$ et $\frac{3}{4}$, on trouve

$$\frac{1}{4}\begin{pmatrix} 0,2 \\ 0,8 \end{pmatrix} + \frac{3}{4}\begin{pmatrix} 0,4 \\ 0,6 \end{pmatrix} = \begin{pmatrix} 0,35 \\ 0,65 \end{pmatrix},$$

ce qui est aussi colonne-stochastique.

5.2.3. Lemme. Si $A \in M_{m\times n}(\mathbb{R})$ et $B \in M_{n\times p}(\mathbb{R})$ sont colonne-stochastiques, alors AB est colonne-stochastique.

Démonstration. Écrivons $A = (A_1, \cdots, A_n)$ et $B = (B_1, \cdots, B_p)$ en colonnes. En outre, écrivons $B = (b_{ij})_{n\times p}$. D'après la multiplication par blocs; voir 3.1.5(1) et 3.1.4(2), on obtient

$$AB = (AB_1, \ldots, AB_p),$$

où

$$AB_j = b_{1j}A_1 + \cdots + b_{nj}A_n,\ j = 1, \ldots, p.$$

Comme A est colonne-stochastique, $A_1, \ldots, A_n$ sont colonne-stochastiques. Comme B est colonne-stochastique, $b_{1j} + \cdots + b_{nj} = 1$, pour $j = 1, \ldots, n$. D'après le lemme 5.2.2, AB_j est colonne-stochastique, pour $j = 1, \ldots, p$. C'est-à-dire, AB est colonne-stochastique. La preuve du lemme s'achève.

Remarque. Si $A \in M_n(\mathbb{R})$ est colonne-stochastique, d'après le lemme 5.2.3, A^r l'est aussi pour tout $r \geq 0$.

Le résultat suivant est essentiel pour l'algorithme PageRank.

5.2.4. Proposition. Si $A \in M_n(\mathbb{R})$ est colonne-stochastique, alors la valeur 1 est une valeur propre de A.

Démonstration. Soient $A_1, \ldots, A_n$ les lignes de A. D'après le lemme 3.1.4(2),

$$(1, \cdots, 1)A = A_1 + \cdots + A_n = (1, \cdots, 1).$$

En transposant les membres de ces équations, on trouve

$$A^T \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} = 1 \cdot \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}.$$

Ainsi, 1 est une valeur propre de A^T. D'après le corollaire 5.1.4, 1 est aussi une valeur propre de A. La preuve de la proposition s'achève.

Exemple. Considérons la matrice colonne-stochastique

$$A = \begin{pmatrix} 0,2 & 0,4 \\ 0,8 & 0,6 \end{pmatrix}.$$

On a

$$\chi_A(\lambda) = \begin{vmatrix} 0,2-\lambda & 0,4 \\ 0,8 & 0,6-\lambda \end{vmatrix} = (0,2-\lambda)(0,6-\lambda) - 0,32 = \lambda^2 - 0,8\lambda - 0,2.$$

Comme $\chi_A(1) = 1 - 0,8 - 0,2 = 0$, on voit que 1 est effectivement une valeur propre de A.

Lorsqu'une matrice colonne-stochastique est positive, ses vecteurs propres associés à 1 ont des propriétés très spéciales.

5.2.5. Lemme. Soit $A \in M_n(\mathbb{R})$ colonne-stochastique et positive. Alors tout vecteur propre de A associé à 1 est non négatif ou non positif.

Démonstration. Posons $A = (a_{ij})_{n\times n}$, où $a_{ij} > 0$ pour tous $1 \leq i, j \leq n$. Comme A est colonne-stochastique, $\sum_{i=1}^{n} a_{ij} = 1$, pour $j = 1, \ldots, n$.

Supposons que $u = (a_i)_{n\times 1}$ est un vecteur propre de A associé à 1. Comme $Au = u$, d'après la définition de la multiplication de matrices, on a

$$\sum_{j=1}^{n} a_{ij}a_j = a_i, \text{ pour } i = 1, \ldots, n.$$

Supposons au contraire que les valeurs $a_1, \ldots, a_n$ sont de signes mélangés. Comme $a_{ij} > 0$, les valeurs $a_{i1}a_1, \ldots, a_{in}a_n$ sont aussi de signes mélangés, pour tout $1 \leq i \leq n$. Comparant les valeurs absolues, on voit que

$$\left|\sum_{j=1}^{n} a_{ij}a_j\right| < \sum_{j=1}^{n} |a_{ij}a_j|, \text{ pour } i = 1, \ldots, n.$$

Cela nous donne

$$\sum_{i=1}^{n} |a_i| = \sum_{i=1}^{n} \left|\sum_{j=1}^{n} a_{ij}a_j\right| < \sum_{j=1}^{n} |a_{ij}a_j| = \sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}|a_j| = \sum_{j=1}^{n} \left(\sum_{i=1}^{n} a_{ij}\right) |a_j| = \sum_{j=1}^{n} |a_j|,$$

une contradiction. La preuve du lemme s'achève.

Remarque. Le lemme 5.2.5 n'est pas valide si A n'est pas positive. Considérons, par exemple, la matrice colonne-stochastique non positive

$$I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Elle a un vecteur propre associé à 1 suivant:

$$\begin{pmatrix} 1 \\ -1 \end{pmatrix},$$

dont les termes sont de signes mélangés.

5.2.6. Proposition. Soit $A \in M_n(\mathbb{R})$ colonne-stochastique et positive. Tous les deux vecteurs propres de A associés à 1 sont linéairement dépendants (c'est-à-dire, l'un est un multiple de l'autre).

Démonstration. Supposons au contraire que A admet deux vecteurs propres linéairement indépendants $u = (a_i)_{n\times 1}$ et $v = (b_i)_{n\times 1}$ associés à 1. Posons

$$a = a_1 + \cdots + a_n \text{ et } b = b_1 + \cdots + b_n.$$

D'après le lemme 5.2.5, $a_1, \ldots, a_n$ sont tous positifs ou tous négatifs. En particulier, $a \neq 0$. Comme $\{u, v\}$ est libre, on voit que

$$w := av - bu = (ab_i - ba_i)_{n\times 1} \neq 0.$$

Comme u, v sont deux vecteurs propres de A associés à 1, le vecteur w l'est aussi. Posant $w = (c_i)_{n\times 1}$, on a

$$c_1 + \cdots + c_n = a(b_1 + \cdots + b_n) - b(a_1 + \cdots + a_n) = ab - ba = 0.$$

D'où, $c_1, \ldots, c_n$ sont de signes mélangés. Ceci contredit le lemme 5.2.5. La preuve du lemme s'achève.

Remarque. La proposition 5.2.6 n'est pas valide si A n'est pas positive. Considérons, par exemple, la matrice colonne-stochastique non positive

$$I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Elle a deux vecteurs propres linéairement indépendants associé à 1 suivants:

$$\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \end{pmatrix}.$$

On va généraliser la proposition 5.2.6. Pour ce faire, on introduit la notion suivante.

5.2.7. Définition. Une matrice non négative $A \in M_n(\mathbb{R})$ est dite *éventuellement positive* si

$$I_n + A + \cdots + A^r$$

est positive pour un certain entier $r > 0$.

Remarque. Une matrice positive est éventuellement positive.

Exercice. Déterminer laquelle des matrices colonne-stochastiques suivantes est éventuellement positive

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix};\ B = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Solution. (1) Pour tout $r > 0$, on a

$$I_2 + A + \cdots + A^r = (r+1)I_2 = \begin{pmatrix} r+1 & 0 \\ 0 & r+1 \end{pmatrix},$$

ce qui est non positive. D'où, A est non éventuellement positive.

(2) On voit que

$$I_3 + B = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix};\ I_3 + B + B^2 = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} + \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}.$$

D'où, B est éventuellement positive.

Le résultat suivant garantit l'algorithme PageRank fonctionne.

5.2.8. Théorème. Soit $A \in M_n(\mathbb{R})$ colonne-stochastique et éventuellement positive. Alors A a un unique vecteur propre non négatif associé à 1, dont les termes somment à 1.

Démonstration. Par l'hypothèse, $I + A + \cdots + A^r$ est positive pour un certain $r > 0$. On a alors une matrice positive

$$B := \frac{1}{r+1}(I_n + A + A^2 + \cdots + A^r) = \frac{1}{r+1} \cdot I_n + \frac{1}{r+1} \cdot A + \cdots + \frac{1}{r+1} \cdot A^r.$$

Comme les A^i sont colonne-stochastiques; voir (5.2.3), on déduit du lemme 5.2.2 que B est colonne-stochastique. Remarquons que $B = f(A)$, où

$$f(\lambda) = \frac{1}{r+1} + \frac{1}{r+1}\lambda + \cdots + \frac{1}{r+1}\lambda^r.$$

D'après la proposition 5.2.4, A admet un vecteur propre $u_0 = (a_i)_{n\times 1}$ associé à 1. D'après la proposition 5.1.6, u_0 est un vecteur propre de $f(A) = B$ associé à $f(1) = 1$. D'après le lemme 5.2.5, $a_i \leq 0$ pour tout $1 \leq i \leq n$ ou $a_i \geq 0$ pour tout $1 \leq i \leq n$. Comme u_0 est non nul, $a_1 + \cdots + a_n < 0$, ou bien, $a_1 + \cdots + a_n > 0$, respectivelement. Alors

$$v_0 = \frac{1}{a_1 + \cdots + a_n} u_0$$

est un vecteur propre de A associé à 1. Posant $v_0 = (b_i)_{n\times 1}$, on voit que

$$b_i = \frac{a_i}{a_1 + \cdots + a_n} \geq 0,\ \text{pour } i = 1, \ldots, n,$$

tels que

$$\sum_{i=1}^{n} b_i = \sum_{i=1}^{n} \frac{a_i}{a_1 + \cdots + a_n} = \frac{a_1 + \cdots + a_n}{a_1 + \cdots + a_n} = 1.$$

C'est-à-dire, u_0 est non négatif dont les termes somment à 1.

Supposons que $w_0 = (c_i)_{n\times 1}$ est aussi un vecteur propre non négatif de A associé à 1 avec $c_1 + \cdots + c_n = 1$. D'après la proposition 5.1.6, w_0 est un vecteur propre de B associé à 1. D'après la propisition 5.2.6, $w_0 = av_0$ pour un certain $a \in \mathbb{R}$. On a alors $c_i = ab_i$ pour $i = 1, \ldots, n$, et

$$1 = \sum_{i=1}^{n} c_i = \sum_{i=1}^{n} ab_i = a(\sum_{i=1}^{n} b_i) = a.$$

C'est-à-dire, $w_0 = v_0$. Ceci achève la démonstration du théorème.

Exemple. Considérons la matrice colonne-stochastique positive suivante:

$$A = \begin{pmatrix} 0,2 & 0,4 \\ 0,8 & 0,6 \end{pmatrix}.$$

On a vu que

$$\begin{pmatrix} 1 \\ 2 \end{pmatrix}$$

est un vecteur propre de A associé à la valeur 1. Par conséquent,

$$\begin{pmatrix} \frac{1}{3} \\ \frac{2}{3} \end{pmatrix}$$

est le seul vecteur propre non négatif de A associé à 1 dont les termes somment à 1.

5.3. Algorithme PageRank

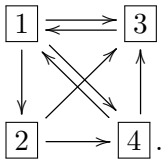
Un réseau de pages web se compose d'un nombre fini de pages et des liens entre eux. Un moteur de recherche affiche les pages de ce réseau selon leur importance de telle sorte que la page la plus importante apparaît en premier.

Le PageRank, inventé par Larry Page, est l'algorithme utilisé par Google pour déterminer l'importance de chacune des pages d'un réseau. Pour établir le modèle mathématique, on doit représenter un réseau de pages web par un graphe orienté comme suit.

5.3.1. Définition. Un réseau de n pages web est représenté par un graphe orienté tel que défini ci-dessous:

(1) Les pages sont représentées par les entiers $1, 2, \ldots, n$.
(2) Un lien de la page i vers la page j sera représenté par une flèche $i \to j$.

Exemple. Le graphe orienté suivant représente un réseau de 4 pages web et 8 liens



Pour appliquer l'algèbre linéaire, on a besoin de matrice.

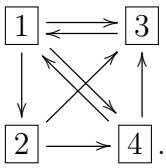
5.3.2. Définition. Soit W un réseau de n pages $1, 2, \ldots, n$. Soit l_j le nombre de liens sortant de la page j, pour $j = 1, 2, \ldots, n$. On définit la *matrice des liens* de W comme suit:

$$L = (l_{ij})_{n\times n},$$

où

$$l_{ij} = \begin{cases} \frac{1}{l_j}, & \text{s'il existe un lien de la page } j \text{ vers la page } i; \\ 0, & \text{sinon.} \end{cases}$$

Exemple. Soit W le réseau de pages web représenté par le graphe



On voit que $l_1 = 3$, $l_2 = 2$, $l_3 = 1$ et $l_4 = 2$. La matrice des liens de W est donnée par

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

La matrice des liens d'un réseau de pages web est toujours non négatif. On étudiera quand cette matrice est éventuellement positive. Pour ce faire, on donnera une déscription de ses puissances en termes du graphe orienté du réseau.

5.3.3. Lemme. Soit W un réseau de pages web, dont $L = (l_{ij})_{n\times n}$ est la matrice des liens. Pour tout entier $p \geq 1$, posons

$$L^p = \left(l_{ij}^{(p)}\right)_{n\times n}.$$

Alors $l_{ij}^{(p)} > 0$ si, et seulement si, le graphe orienté de W contient a un chemin

$$j \longrightarrow j_1 \longrightarrow \cdots \longrightarrow j_{p-1} \longrightarrow i$$

de longueur p de la page j vers la page i.

Démonstration. D'abord, $l_{ij}^{(p)} \geq 0$ pour $1 \leq i, j \leq n$. On procède par récurrence sur p.

D'après le définition, $l_{ij} > 0$ si, et seulement si, il existe une flèche $j \to i$. Ainsi, le résultat est valide pour $p = 1$.

Supposons que le résultat est valide pour un certain $p \geq 1$. Comme $L^{p+1} = LL^p$, on a

$$l_{ij}^{(p+1)} = \sum_{k=1}^{n} l_{ik} l_{kj}^{(p)}.$$

Comme $l_{ik} l_{kj}^{(p)} \geq 0$ pour tout $1 \leq k \leq n$, on voit que $l_{ij}^{(p+1)} \neq 0$ si, et seulement si, $l_{i,j_p} l_{j_p,j}^{(p)} \neq 0$ pour un entier $1 \leq j_p \leq n$ si, et seulement si, $l_{i,j_p} \neq 0$ et $l_{j_p,j}^{(p)} \neq 0$ pour un entier $1 \leq j_p \leq n$ si, et seulement si, il existe une flèche $j_p \to i$ et un chemin de longueur p suivant:

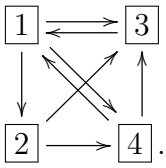
$$j \longrightarrow j_1 \longrightarrow \cdots \longrightarrow j_{p-1} \longrightarrow j_p,$$

pour un entier $1 \leq j_p \leq n$ si, et seulement si, il existe un chemin de longueur $p+1$ suivant:

$$j \longrightarrow j_1 \longrightarrow \cdots \longrightarrow j_{p-1} \longrightarrow j_p \longrightarrow i.$$

La preuve du lemme s'achève.

Exemple. Soit W le réseau des pages web représenté par le graphe orienté



On voit que la matrice des liens L de W et L^2 sont comme suit:

$$L = \begin{pmatrix} 0 & 0 & 1 & \frac{1}{2} \\ \frac{1}{3} & 0 & 0 & 0 \\ \frac{1}{3} & \frac{1}{2} & 0 & \frac{1}{2} \\ \frac{1}{3} & \frac{1}{2} & 0 & 0 \end{pmatrix}; \; L^2 = \begin{pmatrix} \frac{1}{2} & \frac{3}{4} & 0 & \frac{1}{2} \\ 0 & 0 & \frac{1}{3} & \frac{1}{6} \\ \frac{1}{3} & \frac{1}{4} & \frac{1}{3} & \frac{1}{6} \\ \frac{1}{6} & 0 & \frac{1}{3} & \frac{1}{6} \end{pmatrix}.$$

Le $(2,3)$-terme de L est nul, mais celui de L^2 est positif. D'après le lemme 5.3.3, il n'y a aucun chemin de longueur 1 (c'est-à-dire, une flèche) de la page 3 vers la page 2, mais il y a un chemin de longueur 2 de la page 3 vers la page 2.

Le résultat suivant dit quand la matrice des lignes d'un réseau est colonne-stochastique.

5.3.4. Lemme. Soit W un réseau des pages web dont L est la matrice des lignes. Si chaque page de W admet au moins un lien sortant, alors L est colonne-stochastique.

Démonstration. Posons $L = (l_{ij})_{n\times n}$, qui est non négative. Supposons qu'il existe $l_j\,(>0)$ liens de la page j vers les pages $i_1, \ldots, i_{l_j}$, pour tout $j = 1, \ldots, n$. Par définition,

$$l_{ij} = \begin{cases} \frac{1}{l_j}, & \text{si } i \in \{i_1, \ldots, i_{l_j}\}; \\ 0, & \text{sinon.} \end{cases}$$

D'où,

$$\sum_{i=1}^{n} l_{ij} = \sum_{p=1}^{l_j} l_{i_p,j} = \sum_{p=1}^{l_j} \frac{1}{l_j} = 1, \text{ pour } j = 1, \ldots, n.$$

C'est-à-dire, L est colonne-stochastique. La preuve du lemme s'achève.

Voici une condtion pour que la matrice des lignes d'un réseau de pages web soit éventuellement positive.

5.3.5. Définition. Un réseau de pages web est dit *fortement connexe* si toutes les deux pages distinctes i, j peuvent être rejointes par un chemin comme suit:

$$i \longrightarrow j_1 \longrightarrow \cdots \longrightarrow j_s \longrightarrow j.$$

Remarque. Un réseau de pages web est fortement connexe si, et seulement si, son graphe orienté admet un cycle orienté passant par toutes les pages.

5.3.6. Proposition. Soit W un réseau de pages web. Si W est fortement connexe, alors sa matrice des lignes est colonne-stochastique et éventuellement positive.

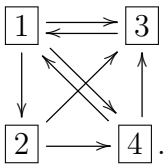
Démonstration. Soit $L = (l_{ij})_{n\times n}$, la matrice des liens de W. Supposons que le graphe orienté de W contient un cycle passant par toutes les pages de W. En particuleir, toute page admet au moins un lien sortant. D'après le lemme 5.3.4, L est colonne-stochastique.

En vertu du cycle, pour tous $1 \le i, j \le n$, il y a un chemin de la page i vers la page j de longueur $r_{ij} > 0$. D'après le lemme 5.3.3, le (i, j)-terme de $L^{r_{ij}}$ est positif. Posant r le maximum des r_{ij} avec $1 \le i, j \le n$, on voit que

$$I + L + \cdots + L^r$$

est positive. La preuve de la proposition s'achève.

Exemple. Soit W le réseau de pages web représenté par le graphe orienté



.

On a vu que la matrice des liens est

$$L = \begin{pmatrix} 0 & 0 & 1 & \frac{1}{2} \\ \frac{1}{3} & 0 & 0 & 0 \\ \frac{1}{3} & \frac{1}{2} & 0 & \frac{1}{2} \\ \frac{1}{3} & \frac{1}{2} & 0 & 0 \end{pmatrix},$$

ce qui n'est pas positive. Comme le graphe orienté contient un cycle

$$\boxed{1} \longrightarrow \boxed{2} \longrightarrow \boxed{4} \longrightarrow \boxed{3} \longrightarrow \boxed{1},$$

qui passe toutes les 4 pages, W est fortement connexe. D'après la propistion 5.3.6, L est éventuellement positive.

L'algorithme PageRank attribue à chaque page une valeur entre 0 et 1, appelée *score d'importance*, selon le principal suivant: le score d'importance d'une page est d'autant plus grand qu'elle a un grand nombre de pages importantes la référençant. On donnera la définition précise comme suit.

5.3.7. Définition. Soit W un réseau des pages $1, \ldots, n$. Soit l_j le nombre de liens sortant de la page j, pour $j = 1, \ldots, n$. À chaque page i, on donne une valeur x_i avec $0 \leq x_i < 1$, appelée *score d'importance* de la page i, de sorte que

$$\sum_{i=1}^{n} x_i = 1$$

et

$$x_i = \sum_{\exists\, j \to i} \frac{x_j}{l_j} = \sum_{j=1}^{n} l_{ij} x_j, \quad \text{pour } i = 1, \ldots, n.$$

Dans ce cas, le vecteur

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

s'appelle un *vecteur des scores d'importance*.

Le résultat suivant donne l'interprétation algébrique d'un vecteur des scores d'importance.

5.3.8. Proposition. Soit W un réseau de pages web dont la matrice des liens est L. Un vecteur des scores d'importance de W est un vecteur propre non négatif de L associé à 1, dont les termes somment à 1.

Démonstration. Soit $L = (l_{ij})_{n\times n}$. Si $x_1, \ldots, x_n$ sont les scores d'importance, alors

$$x_i = \sum_{j=1}^{n} l_{ij}x_j = (l_{i1}, \ldots, l_{in}) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, i = 1, \ldots, n.$$

D'où,

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} l_{11} & \cdots & l_{1n} \\ \vdots & \ddots & \vdots \\ l_{n1} & \cdots & l_{nn} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$$

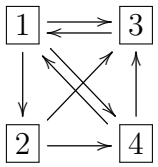
Ceci achève la démonstration de la proposition.

En général, un réseau de pages web n'admet aucun vecteur des scores d'importance. Le résultat suivant dit que c'est le cas pour les réseaux fortement connexes.

5.3.9. Théorème. Soit W un réseau de pages web. Si W est fortement connexe, alors W admet un et un seul vecteur des scores d'importance.

Démonstration. Soit L la matrice des liens de W. D'après la proposition 5.3.6, L est colonne-stochastique et éventuellement positive. D'après le théorème 5.2.8, L admet un unique vecteur propre non négatif v associé à 1, dont les termes somment à 1. D'après la proposition 5.3.8, v est le seul vecteur des scores d'importance de W. La preuve du théorème s'achève.

Exemple. Donner le vecteur des scores d'importance du réseau de pages web suivant:



Solution. La matrice des liens est donnée par

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

D'après la proposition 5.3.8, il s'agit de trouver un vecteur prore non négatif de L associé à 1, dont les termes somment à 1.

On commence par trouver un vecteur prore de L associé à 1. D'après le théorème 5.1.5, on doit résoudre le système homogène

$$(L - I_4)X = 0.$$

D'après un résultat du MAT153, on doit échelonner la matrice

$$L - I_4 = \begin{pmatrix} -1 & 0 & 1 & \frac{1}{2} \\ \frac{1}{3} & -1 & 0 & 0 \\ \frac{1}{3} & \frac{1}{2} & -1 & \frac{1}{2} \\ \frac{1}{3} & \frac{1}{2} & 0 & -1 \end{pmatrix}.$$

Pour faciliter le calcul, on élimine premièrement les fractions en effectuant les opérations $2L_1$, $3L_2$, $6L_3$ et $6L_4$. Ceci nous donne

$$\begin{pmatrix} -2 & 0 & 2 & 1 \\ 1 & -3 & 0 & 0 \\ 2 & 3 & -6 & 3 \\ 2 & 3 & 0 & -6 \end{pmatrix} \begin{matrix} \\ L_1 \leftrightarrow L_2 \\ \Longrightarrow \\ \\ \end{matrix} \begin{pmatrix} 1 & -3 & 0 & 0 \\ -2 & 0 & 2 & 1 \\ 2 & 3 & -6 & 3 \\ 2 & 3 & 0 & -6 \end{pmatrix} \begin{matrix} \\ L_2 + 2L_1 \\ L_3 - 2L_1 \\ L_4 - 2L_1 \\ \Longrightarrow \end{matrix} \begin{pmatrix} 1 & -3 & 0 & 0 \\ 0 & -6 & 2 & 1 \\ 0 & 9 & -6 & 3 \\ 0 & 9 & 0 & -6 \end{pmatrix}$$

$$\begin{matrix} \\ L_2 \leftrightarrow \frac{1}{3}L_4 \\ \Longrightarrow \\ \frac{1}{3}L_3 \end{matrix} \begin{pmatrix} 1 & -3 & 0 & 0 \\ 0 & 3 & 0 & -2 \\ 0 & 3 & -2 & 1 \\ 0 & -6 & 2 & 1 \end{pmatrix} \begin{matrix} \\ L_3 - L_2 \\ L_4 + 2L_2 \\ \Longrightarrow \\ \\ \end{matrix} \begin{pmatrix} 1 & -3 & 0 & 0 \\ 0 & 3 & 0 & -2 \\ 0 & 0 & -2 & 3 \\ 0 & 0 & 2 & -3 \end{pmatrix} \begin{matrix} \\ L_4 + L_3 \\ \Longrightarrow \\ -L_3 \\ \\ \end{matrix} \begin{pmatrix} 1 & -3 & 0 & 0 \\ 0 & 3 & 0 & -2 \\ 0 & 0 & 2 & -3 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$\begin{matrix} \\ L_1 + L_2 \\ \Longrightarrow \\ \\ \\ \end{matrix} \begin{pmatrix} 1 & 0 & 0 & -2 \\ 0 & 3 & 0 & -2 \\ 0 & 0 & 2 & -3 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Cette dernière matrice représente le système homogène échelonné suivant:

$$\begin{array}{rrrrrrr} y_1 & & & - & 2y_4 & = & 0 \\ & 3y_2 & & - & 2y_4 & = & 0 \\ & & 2y_3 & - & 3y_4 & = & 0, \end{array}$$

dont l'inconnue libre est y_4. Pour éviter les fractions, en posant $y_4 = 6$ on obtien une soultion

$$y_1 = 12; y_2 = 4; y_3 = 9; y_4 = 6.$$

C'est-à-dire, L a pour propre associé à 1 le vecteur suivant:

$$\begin{pmatrix} 12 \\ 4 \\ 9 \\ 6 \end{pmatrix},$$

dont les termes somment à 31. Ainsi,

$$\frac{1}{31}\begin{pmatrix} 12 \\ 4 \\ 9 \\ 6 \end{pmatrix}$$

est le vecteur propre non négatif de L associé à 1, dont les termes somment à 1. Par conséquent, les scores d'importance des pages sont donnés par

$$x_1 = \frac{12}{31},\ x_2 = \frac{4}{31},\ x_3 = \frac{9}{31},\ x_4 = \frac{6}{31}.$$

C'est-à-dire, le moteur de recherche affiche les pages de ce réseau de l'ordre suivant: page 1, page 3, page 4, page 2.

5.4. Exercices

1. Considérer la matrice réelle suivante:

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 1 & -7 \end{pmatrix}.$$

   Vérifier que la valeur 2 est une valeur propre de A; et calculer sa multiplicité géométrique.

2. Dans chacun des cas suivants, trouver la valeur réelle de a pour que la valeur 3 soit une valeur propre, et dans ce cas, calculer la multiplicité géométrique de 2.

   (1) $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 1 & a \end{pmatrix}$; (2) $\begin{pmatrix} 3 & 2 & 1 \\ a & 1 & 3 \\ 2 & 3 & 1 \end{pmatrix}$.

3. Montrer qu'une matrice carrée A est inversible si et seulement si la valeur 0 n'est pas valeur propre A.

4. Soit A une matrice inversible. Montrer que si λ_0 est une valeur propre de A, alors $\dfrac{1}{\lambda_0}$ est une valeur propre de A^{-1}.

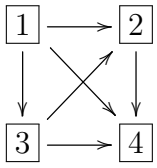
5. Montrer, d'après la définition, que la valeur 1 est une valeur propre avec $\mathrm{mg}(1) = 1$ de la matrice suivante:

$$A = \begin{pmatrix} \frac{1}{n} & \frac{1}{n} & \cdots & \frac{1}{n} \\ \frac{1}{n} & \frac{1}{n} & \cdots & \frac{1}{n} \\ \vdots & \vdots & \cdots & \vdots \\ \frac{1}{n} & \frac{1}{n} & \cdots & \frac{1}{n} \end{pmatrix}_{n\times n}.$$

6. Calculer, d'après la définition, la multiplicité géométrique de la valeur propre 1 des matrices colonne-stochastiques suivantes:

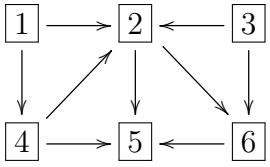
$$(1) \quad \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ \frac{1}{2} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & \frac{1}{2} \\ 0 & 0 & 1 & 0 & \frac{1}{2} \\ \frac{1}{2} & 0 & 0 & 0 & 0 \end{pmatrix}; \qquad (2) \quad \begin{pmatrix} 0,03 & 0,88 & 0,03 & 0,03 & 0,03 \\ 0,88 & 0,03 & 0,03 & 0,03 & 0,03 \\ 0,03 & 0,03 & 0,03 & 0,88 & 0,455 \\ 0,03 & 0,03 & 0,88 & 0,03 & 0,455 \\ 0,03 & 0,03 & 0,03 & 0,03 & 0,03 \end{pmatrix}.$$

7. Soit W un réseau des pages web représenté par le graphe orienté suivant:



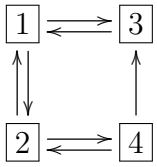
   (1) Donner la matrice des liens L de W.
   (2) Sans calculer les puissances de L, à l'aide du lemme 5.3.3, trouver un entier p tel que $L^p \neq 0$ et $L^{p+1} = 0$.

8. Soit W un un réseau des pages web représenté par le graphe orienté suivant:



   (1) Donner la matrice des liens L de W.
   (2) Sans calculer les puissances de L trouver, à l'aide du lemme 5.3.3, un entier p tel que $L^p \neq 0$ et $L^{p+1} = 0$.

9. Soit W un réseau de pages web représenté par le graphe suivant:



(1) Donner la matrice des liens L de W.

(2) Vérifier que W est fortement connexe.

(3) Donner le vecteur des scores d'importance de W.