CODES EFFICACES

Si Alice et Bob communiquent avec un code, alors Alice envoie un mot y du code à Bob, qui ne reçoit pas exactement y, mais plutôt z, qui est proche à y. Que fait Bob? Il a une liste de tous les mots du code, et de toutes les boules et toutes les mots possibles (incluant son z). Il regarde donc dans sa liste pour savoir dans quelle boule se trouve z. Cette boule correspond à y, et donc il sait que Alice lui a envoyé y et non z.

Le travail de Alice est simple: elle envoie son mot. Bob a une tâche plus difficile: il doit chercher pour z dans une liste complète, chaque fois qu'il reçoit un mot d'Alice. Il y a une méthode beaucoup plus efficace, mais pour le comprendre il faut comprendre l'algèbre linéaire sur un corps fini.

CORPS

Un corps et un ensemble de "nombres" avec lesquels on peut faire de l'arithmétique. Quelques exemples que vous connaissez déjà sont $\mathbb{R}$ (les réels), $\mathbb{C}$ (les complexes), $\mathbb{Q}$ (les rationnels). Il y a (beaucoup!) d'autres.

Formellement un ensemble $\mathbb{K}$ avec une addition et une multiplication est un CORPS si les propriétés suivants sont valides pour tout $a, b, c \in \mathbb{K}$.

1) $a + b \in \mathbb{K}$
2) $ab \in \mathbb{K}$
3) $a + b = b + a$
4) $ab = ba$
5) $a + (b + c) = (a + b) + c$
6) $a(bc) = (ab)c$
7) $a(b + c) = ab + ac$
8) $0 \in \mathbb{K}$ et $0 + a = a$
9) $1 \in \mathbb{K}$ et $1a = a$
10) pour a on a $-a \in \mathbb{K}$ avec $a + (-a) = 0$ ($-a$ est l'INVERSE ADDITIVE de a)
11) pour $a \neq 0$ on a $a^{-1} \in \mathbb{K}$ avec $a\left(a^{-1}\right) = 1$ ($-a$ est l'INVERSE MULTIPLICATIVE de a)

Par exemple, ai a et b sont des fractions, alors $a + b$ est une fraction aussi: c'est propriété 1 pour $\mathbb{Q}$. Si on considère deux nombres complexes a et b, alors $ab = ba$: c'est propriété 4 pour $\mathbb{C}$. Une inverse additive est aussi connue comme la négative d'un chiffre; l'inverse multiplicative est la réciproque.

Exercice 14.1. Montrer que l'ensemble des entiers $\mathbb{Z}$ n'est *pas* un corps. Quelles propriétés sont valides? Quelles ne sont pas? □

ARITHMÉTIQUE MODULO n

Soit n un entier positif fixe. Si s est n'importe quel entier, on peut trouver t et r tel que $s = tn + r$ avec $0 \leq r < n$. C'est exactement la division: t est le quotient et r et le reste, obtenu en divisant s par n. On dit que s est équivalent à r modulo n; on l'écrit parfois comme $s \equiv r \mod n$. On peut comprendre ceci d'une autre manière: en commençant avec s, on soustrait (ou additionne) des multiples de n afin de la réduire à un chiffre positif inférieur à n. On parle donc parfois de *réduction* modulo n.

Exemple 14.2. Voici quelques calculs modulo 7 à titre d'exemple. On fait les calculs avec des entiers ordinaires, pour ensuite "réduire" modulo 7.

$$\begin{aligned} 3 + 6 = 9 = 1(7) + 2 \equiv 2 \mod 7 \\ 3 \times 5 = 15 \equiv 2(7) + 1 \equiv 1 \mod 7 \\ 5 \times (2 + 4) = 5 \times 6 = 30 = 4(7) + 2 \equiv 2 \mod 7 \\ 2 \times (1 - 6) = 2 \times (-5) = -10 = -2(7) + 4 \equiv 4 \mod 7 \end{aligned}$$

Typiquement on réserve "=" pour une égalité entre entiers (réels) et $\equiv$ pour une égalité entre entiers modulo n. Parfois on écrit pas le " mod 7" si le contexte le rend clair. □

On dénote par $\mathbb{Z}_n$ l'ensemble de chiffres positifs inférieurs à n, avec l'arithmétique modulo n. Donc $\mathbb{Z}_n = \{0, 1, 2, \cdots, n-1\}$, avec les calculs modulo n.

Exercice 14.3. Est-ce que $\mathbb{Z}_n$ est un corps, avec l'addition et la multiplication modulo n? Est-ce que les propriétés sont satisfaits? (On verra la réponse très bientôt) □

Exemple 14.4. On peut construire les tables d'addition et de multiplication pour $\mathbb{Z}_n$. Ce serait des tables *au complet*, car $\mathbb{Z}_n$ ne contient que n éléments ($\mathbb{R}$ contient une infinité d'éléments, donc une table au complet et impossible!). Voici pour $\mathbb{Z}_5$.

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Par exemple, les valeurs en boîte s'expliquent avec les calculs suivants.

$$\begin{aligned} 1 + 4 = 5 = 1(5) + 0 \equiv 0 \mod 5 \\ 2 \times 3 = 6 = 1(5) + 1 \equiv 1 \mod 5 \end{aligned}$$

On découvre que $1 + 4 \equiv 0 \mod 5$. Donc 4 est la négative de 1, car $-1 \equiv 4 \mod 5$. On a aussi que $2 \times 3 \equiv 1 \mod 5$. Donc 3 est la réciproque de 2, car $2^{-1} \equiv 3 \mod 5$. □

Exercice 14.5. Vérifier les tables d'addition et de multiplication données pour $\mathbb{Z}_5$. Trouver l'inverse additive de 2 dans la table d'addition (dans la rangée de 2, chercher la valeur 0: la colonne correspondante donne l'inverse additive de 2). Trouver l'inverse additive de chaque élément de $\mathbb{Z}_5$, si possible. Trouver l'inverse multiplicative de chaque élément non-nul de $\mathbb{Z}_5$, si possible. □

Exercice 14.6. Est-ce que $\mathbb{Z}_5$ est un corps? L'exercice précédant se montre utile, car il faudrait que tout élément de $\mathbb{Z}_5$ possède une inverse additive (propriété 10), et que tout élément non-nul de $\mathbb{Z}_5$ possède une inverse multiplicative (propriété 11). □

L'ensemble $\mathbb{Z}_2$ est un cas intéressant. On a $\mathbb{Z}_2 = \{0, 1\}$ avec l'addition et la multiplication modulo 2. Note qu'il n'y a pas beaucoup d'arithmétique modulo 2.

Exemple 14.7. Si a est un entier pair, alors $a \equiv 0 \mod 2$, et si b est un entier impair, alors $b \equiv 1 \mod 2$. Donc on peut comprendre l'arithmétique en $\mathbb{Z}_2$ comme l'arithmétique de la parité: si le résultat est pair alors c'est zéro, et si le résultat est impair alors c'est 1. En particulier on a $1 + 1 \equiv 0 \mod 2$!

Exercice 14.8. Construire les tables d'addition et de multiplication pour $\mathbb{Z}_2$. Trouver les inverses additives de chaque élément de $\mathbb{Z}_2$. Trouver les inverses multiplicatives de chaque élément non-nul de $\mathbb{Z}_2$. Montrer que "additionner" et "soustraire" sont des synonymes pour des éléments de $\mathbb{Z}_2$. Montrer que "multiplier" et "diviser" sont des synonymes pour les éléments non-nuls de $\mathbb{Z}_2$. □

L'ensemble $\mathbb{Z}_2$ représente l'arithmétique des ordinateurs: c'est une chose très pratique. De plus, c'est un corps.

Exercice 14.9. Montrer directement que $\mathbb{Z}_2$ est un corps. C'est-à-dire, pour chaque propriété, montrer directement selon vos tables que la propriété est satisfaite pour tout $a, b, c \in \mathbb{Z}_2$. (Note que "tout $a, b, c \in \mathbb{Z}_2$ n'est pas beaucoup. . .). □

Par contre l'arithmétique modulo n ne donne pas toujours un corps.

Exercice 14.10. Montrer que $\mathbb{Z}_4$ n'est pas un corps. C'est-à-dire, trouver une propriété n'est pas toujours valide (indice: propriété 11). Est-ce que votre contre-exemple est unique? □

Un nombre n est PREMIER si il possède exactement deux diviseurs positifs: 1 et n. Donc $2, 3, 17$ sont premiers, tandis que $1, 4, 437$ ne sont pas.

Théorème 14.11. *L'ensemble Z_p avec l'arithmétique modulo p est un corps lorsque p est un nombre premier. Si n n'est pas un nombre premier, alors $\mathbb{Z}_n$ n'est pas un corps, car propriété 11 n'est pas satisfaite (un diviseur non-trivial de n ne possède pas d'inverse multiplicative).* □

En général, il existe un corps fini avec q éléments si et seulement si $q = p^k$ pour un nombre premier k. Donc il existe un corps ayant 4 éléments, mais ce n'est pas $\mathbb{Z}_4$! On ne démontrera pas se résultat fondamental: on se contente de travailler avec les corps $\mathbb{Z}_p$.

ALGÈBRE LINÉAIRE EN $\mathbb{Z}_p$

On peut faire l'algèbre linéaire avec n'importe quel corps. Il s'agit de l'algèbre "ordinaire", mais avec l'arithmétique du corps.

Exemple 14.12. Résoudre $2x = 3$ sur le corps $\mathbb{R}$, sur le corps $\mathbb{Z}_2$ et sur le corps $\mathbb{Z}_5$.

$\mathbb{R}$:	$2x = 3 \to (2^{-1})2x = (2^{-1})3 \to x = 3/2$	solution: $x = 3/2$
$\mathbb{Z}_2$:	$2x \equiv 3 \to 0x \equiv 1 \to 0 \equiv 1$	aucune solution
$\mathbb{Z}_5$:	$2x \equiv 3 \to (2^{-1})2x \equiv (2^{-1})3 \to (3)2x \equiv (3)3 \to 1x \equiv 4$	solution: $x \equiv 4$

On s'étonne peut-être qu'il n'y a aucune solution en $\mathbb{Z}_2$: une équation linéaire a "toujours" une solution, non? En fait, non: l'équation $0x = 1$ n'a pas de solution en $\mathbb{R}$. L'équation donnée n'est pas vraiment en $\mathbb{Z}_2$, car "2" et "3" ne sont pas dans $\mathbb{Z}_2$. Donc il a fallu réduire premièrement, et on découvre que cette équation est donc "$0x = 1$" (qui ne possède aucune solution peut importe le corps). □

Exercice 14.13. Solutionner $3x - 4 = x$ sur $\mathbb{Z}_5$, et aussi sur $\mathbb{Z}_2$.

Donner la liste de toutes les équations linéaires de la forme $ax + b = 0$ sur $\mathbb{Z}_2$. Solutionner chaque équation individuellement. □

On peut manipuler des matrices sur $\mathbb{Z}_p$ comme sur $\mathbb{R}$. Les opérations de rangées, les pivots, le rang, la dimension, les combinaisons linéaires, l'indépendance... tout est "pareil" sauf qu'on utilise l'arithmétique modulo p au lieu de l'arithmétique de $\mathbb{R}$.

Exemple 14.14. Soit la matrice $A = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$. Donner sa forme échelonnée réduite sur $\mathbb{R}$, sur $\mathbb{Z}_5$ et sur $\mathbb{Z}_2$.

$$\mathbb{R}: \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \xrightarrow[R_2 \to R_2 + (-1)R_1]{} \begin{bmatrix} 1 & 1 & 0 \\ 0 & -1 & 1 \\ 0 & 1 & 1 \end{bmatrix} \xrightarrow[R_3 \to R_3 + (1)R_2]{R_1 \to R_1 + (1)R_2} \begin{bmatrix} 1 & 0 & 1 \\ 0 & -1 & 1 \\ 0 & 0 & 2 \end{bmatrix}$$
$$\xrightarrow[R_3 \to (\frac{1}{2})R_3]{R_2 \to (-1)R_2} \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{bmatrix} \xrightarrow[R_1 \to R_1 + (-1)R_3]{R_2 \to R_2 + (1)R_3} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$\mathbb{Z}_5: \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \xrightarrow[R_2 \to R_2 + (-1)R_1]{} \begin{bmatrix} 1 & 1 & 0 \\ 0 & 4 & 1 \\ 0 & 1 & 1 \end{bmatrix} \xrightarrow[R_3 \to R_3 + (-4)R_2]{R_1 \to R_1 + (-4)R_2} \begin{bmatrix} 1 & 0 & 1 \\ 0 & 4 & 1 \\ 0 & 0 & 2 \end{bmatrix}$$
$$\xrightarrow[R_3 \to (2^{-1})R_3]{R_2 \to (4^{-1})R_2} \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 4 \\ 0 & 0 & 1 \end{bmatrix} \xrightarrow[R_1 \to R_1 + (-1)R_3]{R_2 \to R_2 + (1)R_3} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$\mathbb{Z}_2: \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \xrightarrow[R_2 \to R_2 + R_1]{} \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix} \xrightarrow[R_1 \to R_1 + R_2]{R_3 \to R_3 + R_2} \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix}$$

Note que pour les opérations sur $\mathbb{Z}_5$, "$R_1 \to R_1 + (-4)R_2$" est la même chose que "$R_1 \to R_1 + 1R_2$". Sur le corps $\mathbb{Z}_2$, il y a seulement deux sortes d'opérations: "$R_j \to R_j + R_i$" et "$R_j \to iR_j$".

On a que le rang de A sur $\mathbb{R}$ ou $\mathbb{Z}_2$ est 3, tandis que le rang de A sur $\mathbb{Z}_2$ est 2. □

Exercice 14.15. Expliquer pourquoi les seules opérations de rangée sur $\mathbb{Z}_2$ sont d'ajouter une rangée à une autre, ou d'échanger deux rangées: "$R_j \to R_j + R_i$" et "$R_i \rightleftharpoons R_j$". □

Exemple 14.16. Est-ce que $\mathbf{u} = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}$ est vecteur propre de $A = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$ sur $\mathbb{R}$? Sur $\mathbb{Z}_2$?

$$\mathbb{R}: A\mathbf{u} = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 2 \\ 1 \end{bmatrix} \neq \lambda \mathbf{u}$$

$$\mathbb{Z}_2: A\mathbf{u} = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} = 1\mathbf{u}$$

Le vecteur $\mathbf{u}$ n'est pas un vecteur propre de A sur $\mathbb{R}$; par contre, c'est un vecteur propre avec valeur propre $\lambda = 1$ sur $\mathbb{Z}_2$. □