Université Paris Diderot 23 octobre 2017

Quelques notes sur l'algèbre et l'analyse de base

Juan Pablo Vigneaux

1. Résolution de systèmes linéaires

1.1 Une motivation

Dans les années 1930-1940, l'armée étasunienne voulait déterminer le régime alimentaire le moins cher, parmi tous ceux qui satisfont quelques besoins nutritionnels. L'économiste George Stigler a construit une modèle mathématique qui tenait en compte de 77 types de nourriture et 9 besoins nutritionnels. [1] Comment formuler ce problème mathématiquement ? Pour le moment, supposons qu'il n'y a que 3 types de nourriture (riz blanc, citron, brocoli) et 2 besoins nutritionnels (énergie, vitamine C). Les apports nutritionnels de ces produits alimentaires sont :

	Riz blanc (100 g)	Citron (100 g)	Brocoli (100 g)
Énergie (kcal)	135	39	34
Vitamine C (mg)	0	51	89

L'apport journalier recommandé de vitamine C est de 60 mg, et (pour un soldat !) le besoin énergétique est de 3400 kcal.

Soit x_R la quantité (annuelle) du riz dans le régime (comme multiple de 100 g), x_C la quantité du citron et x_B celle du brocoli. Ce sont nos *variables*, valeurs à déterminer. Notre modèle doit imposer deux *contraintes* :

$$135x_R + 39x_C + 34x_B = 3400 \cdot 365 \tag{1}$$

$$51x_C + 89x_B = 60 \cdot 365 \tag{2}$$

Y a-t-il une solution pour ces équations ? (C'est-à-dire : peut-on trouver de valeurs pour x_R, x_C et x_B tels que (1) et (2) soient satisfaites/vraies ?) On veut développer une méthode qui permettrait de résoudre ces équations et qui serait encore faisable dans le cas "réaliste" (77 variables, 9 contraintes). Ce méthode s'appelle "élimination

1. La solution publié en 1945 était la suivante : annuellement, on doit manger 370 livres de farine de blé, 57 boîtes de lait évaporé, 111 livres de chou, 25 livres d'épinards et 285 livres de haricots secs, pour un coût annuel 96 dollars (de l'époque).

de Gauss", mais en partie il est déjà décrit (pas dans sa forme actuelle, bien sûr) dans une texte chinois très ancien, " Les Neuf Chapitres sur l'art mathématique " (IIème siècle av. J.-C.). Avant de continuer : Avons-nous considérés toutes les contraintes dans la modélisation de ce problème ?

1.2 Systèmes avec deux variables

Supposons pour le moment qu'on a seulement deux variables, qu'on notera x, y.

(i) Si on n'a qu'une équation,

$$ax + by = c \tag{3}$$

avec a et b non-nuls, cette équation permet d'écrire une de ces variables (n'importe laquelle) en fonction de l'autre. On dira alors qu'il y a une variable libre et une variable liée. Par example, on peut voir x comme une variable libre (qui prend n'importe quel valeur) mais alors $y = (c - ax)/b$. Si on pense (x, y) comme un point du plan, l'équation représente alors une droite de pente $-a/b$ qui passe par le point $(0, c/b)$.
Si $a = 0$, l'équation (3) détermine la valeur de y $(= c/b)$. Dans ce cas, x est libre (elle n'apparait dans aucune équation). (C'est une droite horizontale qui passe par $(0, c/b)$. Le cas $b = 0$ est similaire (mais ça donne une droite verticale).

(ii) Supposons maintenant qu'on a deux équations pour x et y.

$$a_1x + b_1y = c_1 \tag{4}$$
$$a_2x + b_2y = c_2 \tag{5}$$

....

2. Sur les nombres

Notre lecteur ou lectrice devrait connaître déjà :

(i) L'ensemble $\mathbb{N}$ des entiers naturels $0, 1, 2, 3, 4, ...$ On peut sommer ou multiplier ces nombres sans problème, mais les équations $x + n = 0$ et $xn = 1$ en général n'ont pas de solution.

(ii) L'ensemble $\mathbb{Z}$ d'entiers relatifs $... - 3, -2, -1, 0, 1, 2, 3, ...$ Naturellement, on peut voir les entiers naturels comme un sous-ensemble de $\mathbb{Z}$. Pour chaque $p \in \mathbb{Z}$, l'équation $x + p = 0$ a une unique solution, noté $-p$: on parle de l'opposé de p.

(iii) L'ensemble $\mathbb{Q}$ de nombres rationnels, c'est-à-dire, des nombres qui s'écrivent comme un quotient (*ratio* en Latin) de deux nombres entiers relatifs. Symboliquement,

$$\mathbb{Q} := \left\{ \frac{p}{q} \,\middle|\, p, q \in \mathbb{Z} \right\}. \tag{6}$$

On parle aussi de "fractions" $\frac{p}{q}$; il faut faire attention, deux fractions sont équivalents quand elles déterminent le même quotient (i.e. le résultat de la division est le même). On écrit donc que $\frac{1}{2} = \frac{2}{4} = \frac{3}{6}$, *et cetera*. On peut voir les nombres entiers comme inclus dans $\mathbb{Q}$, car $p = p/1$.
On définit la somme et multiplications des fractions de la façon suivante :

$$\frac{p}{q} + \frac{s}{t} := \frac{pt + qs}{qt}$$
$$\frac{p}{q} \cdot \frac{s}{t} := \frac{ps}{qt}$$

D'habitude on omet le signe $\cdot$.[2]
L'équation $xq = 1$ a toujours une solution (unique) ; cette solution correspond a $\frac{1}{q}$, l'inverse de q. Tout élément de $\mathbb{Q}$ possède aussi un opposé.

(iv) Les nombres réels, notés $\mathbb{R}$. On trouve ici quelques nombres dits "irrationnels" i.e. qui ne peuvent pas s'écrire comme quotient d'entiers ; ce le cas de $\sqrt{2}$ (Exercice !). Quelques nombres très importants comme π et e sont aussi irrationnels. On reviendra après sur la définition précise de l'ensemble de nombres réels ; mais voici une image à avoir en tête : les nombres rationnels forment un ensemble ordonnée, on peut alors les représenter sur une droite
Mais cette droite a quelques trous : on sait que éventuellement on peut placer aussi $\sqrt{2}$, π, e.... sur cette droite (par exemple, étant donné $q \in \mathbb{Q}$ on peut toujours dire si $\sqrt{2} > q$ ou $\sqrt{2} < q$). Si on remplit tous les trous de cette droite rationnel, on obtient $\mathbb{R}$.[3]

(v) Les nombres complexes, $\mathbb{C}$. Ils sont obtenus à partir du nombre réels, en ajoutant un nombre i ("l'unité imaginaire") qui est solution de l'équation $x^2+1 = 0$. Concrètement, les nombres complexes correspondent à combinaisons de la forme $a + bi$, où $a, b \in \mathbb{R}$. La somme et les produit sont définies par :

$$(a + bi) + (c + di) := (a + c) + (b + d)i \tag{7}$$
$$(a + bi) \cdot (c + di) := (ac - bd) + (ad + bc)i \tag{8}$$

Les ensembles $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ partagent quelques caractéristiques :

2. Le lecteur/la lectrice devrait vérifier avec quelques exemples que ces opérations correspondent bien à l'interprétation usuelle d'une fraction comme un morceau de quelque chose ; par exemple, un tiers de la moitié d'un gâteau correspond à $\frac{1}{6}$ de gâteau ($= \frac{1}{2} \cdot \frac{1}{3}$).

3. On peut formaliser tout ça, le terme clé est "coupure de Dedekind".

(i) On peut définir la somme de deux éléments.
(ii) On peut définir le produit de deux éléments. De plus, l'ordre des facteurs n'est pas important (on dit que le produit est commutatif).
(iii) La somme et le produit satisfont quelques "règles de calcul" ; par exemple, $(x+y)+z = x+(y+z)$, $x(y+z) = xy+xz$, etc.
(iv) Chaque élément a une opposé. Ça veut dire qu'il y a une notion de soustraction : $x - y := x + (-y)$.
(v) Chaque élément différent de zéro a une inverse. Alors, les quotients sont bien définies $\frac{x}{y} = x \cdot \left(\frac{1}{y}\right)$.

En jargon mathématique, un ensemble avec ces propriétés s'appelle un *corps*.

En pratique, tout ça veut dire que si on commence avec quelques éléments de $\mathbb{Q}$ et on applique des opération "élémentaires" $+, -, \cdot, /$, ces opérations sont toujours bien définies et les résultats sont dans $\mathbb{Q}$ aussi. Pareil pour $\mathbb{R}$ ou $\mathbb{C}$. En particulier, la méthode de pivot de Gauss utilise seulement ces opérations ; alors, **si les coefficients d'un système linéaire sont dans un corps $\mathbb{K}$, les solutions (s'ils existent) appartient aussi à $\mathbb{K}$.**

Jusqu'au moment on a parlé des corps infinies. Mais il y a aussi des ensembles finis qui ont une structure de corps, ils s'appellent "corps de Galois". [4] L'exemple plus simple est le corps $\mathbb{F}_2$ à deux éléments $\{\mathbf{1}, \mathbf{0}\}$. La somme est le produit avec ces nombres est décrit par les tableaux :

$+$	$\mathbf{0}$	$\mathbf{1}$
$\mathbf{0}$	$\mathbf{0}$	$\mathbf{1}$
$\mathbf{1}$	$\mathbf{1}$	$\mathbf{0}$

$\cdot$	$\mathbf{0}$	$\mathbf{1}$
$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$
$\mathbf{1}$	$\mathbf{0}$	$\mathbf{1}$

Donc, la somme correspond à l'opérateur logique XOR ("ou exclusif") et la multiplication est pareil à celle de $\mathbb{N}$. Notez que $-\mathbf{1} = \mathbf{1}$.

Normalement on ne parle pas de ce corps fini dans les cours introductifs d'algèbre. Mais comme vous savez, dans un ordinateur tout est codifié comme une suite de 1 et 0 (physiquement, les deux états possibles d'un transistor) et l'arithmétique sur $\mathbb{F}_2$ a naturellement beaucoup d'applications en informatique.

4. Ce qu'on connaît de la vie d'Évariste Galois (1811-1832) fait penser à un roman de l'époque. Même s'il y avait déjà fait de découvertes mathématiques quand il était au lycée, on l'a refusé l'entrée à l'École Polytechnique et en général ses contributions ont été ignorés quand il vivait encore. À la même époque, il participait à une société politique secrète, la Société des amis du peuple ; il a passé quelques mois en prison à cause de son républicanisme. Finalement, il est mort dans un duel au pistolet. L'influence des travaux Galois dans le mathématiques contemporaines est énorme.