Table des matières

Chapitre 1

Arithmétique

Notre but est ici de reprendre les bases de l'arithmétique et de voir leurs applications en cryptohraphies (transactions sécurisées sur internet, cartes bancaires, ...). Nous allons pour cela supposer le moins de prérequis possible et construire toute la théorie à partir de quelques principes "évidents" qui ne peuvent qu'être admis.
Nous désignerons pas $\mathbb{N}$ l'ensemble des nombres entiers positifs (0, 1, 2, ...) et par $\mathbb{Z}$ l'ensemble des entiers relatifs.

1. Propriétés fondamentales de $\mathbb{N}$

Le premier principe fondamental est celui du principe de récurrence qui provient de la construction de l'ensemble $\mathbb{N}$ et qui s'énonce de la manière suivante :

Théorème 1.1 (Principe de récurrence)

Soit A une partie de $\mathbb{N}$. Supposons qu'il existe un $n_0 \in A$ et que si $n \in A$ alors $n+1 \in A$. Alors, pour tout $n \geqslant n_0$ on a $n \in A$.

Le principe est ici qu'un entier $n \geqslant n_0$ peut être écrit sous la forme

$$n = (((n_0 + 1) + 1) \ldots + 1).$$

En utilisant la deuxième propriété de A, on obtient donc le résultat.

Exemple 1.2 : Utilisant le principe ci-dessus, nous allons montrer que pour tout $n \in \mathbb{N}$ on a $n^2 \geqslant n$. Pour cela, on considère la partie de A définie par

$$A = \{n \in \mathbb{N} \text{ tels que } n^2 \geqslant n\}.$$

On a évidement $0 \in A$ car $0^2 = 0 \geqslant 0$.
Soit $n \in A$ un nombre quelconque. Par hypothèse on a $n^2 \geqslant n$ et on veut montrer que $(n+1)^2 \geqslant n+1$. Pour cela, on calcule $(n+1)^2 = n^2 + 2n + 1$. Mais on sait, par hypothèse, que $n^2 \geqslant n$ et $2n \geqslant 0$ donc $(n+1)^2 \geqslant n + 0 + 1 = n + 1$. Le principe de récurrence permet donc de montrer que tout $n \geqslant 0$ vérifie $n^2 \geqslant n$.

Exercice 1.3
Quand il y en a pour un, il y en a pour deux. Montrer, en utilisant le principe de récurrence, que s'il y en a assez pour un, alors il y en a assez pour tout le monde.

Proposition 1.4
Soit A une partie de $\mathbb{N}$ non vide, alors A possède un plus petit élément.

Preuve : Si $0 \in A$ alors on a fini car il ne peut pas y avoir de plus petit élément. On suppose donc que $0 \notin A$. Nous allons regarder la partie complémentaire de A dans $\mathbb{N}$ (i.e. tout les entiers qui ne sont pas dans A), nous la notons $\mathbb{N} \setminus A$. Nous allons raisonner par l'absurde, c'est-à-dire que nous allons faire une hypothèse et aboutir à une contradiction, ce qui signifiera que notre hypothèse est fausse : on ne peut pas arriver à une conclusion fausse par un raisonnement correct si les hypothèses sont vraies !

L'hypothèse est la suivante : pour tout entier $n \in \mathbb{N}$, si tout les nombres $\leqslant n$ sont dans $\mathbb{N} \setminus A$ alors $n+1 \in \mathbb{N} \setminus A$.
Par le principe de récurrence et comme on a supposé que $0 \in \mathbb{N} \setminus A$, on en déduit que tout les entiers sont dans $\mathbb{N} \setminus A$. Mais on sait que A possède au moins un élément, donc ce n'est pas possible, et notre hypothèse est fausse.
Par suite, il existe un entier $n_0 \in \mathbb{N} \setminus A$ tel que tout les entiers $\leqslant n_0$ sont dans $\mathbb{N} \setminus A$ mais $n_0 + 1$ est dans A. On voit alors que $n_0 + 1$ est le plus petit élément de A : soit $n \in A$, alors $n \notin [\![0, n_0]\!]$ car cette partie est dans $\mathbb{N} \setminus A$, donc $n > n_0$ et donc $n \geqslant n_0 + 1$. □

Cette démonstration n'est pas compliquée mais illustre beaucoup de techniques de démonstration. Elle est donc à comprendre.

Remarque 1.5

L'ensemble $\mathbb{N}$ *est le seul ensemble à posséder la propriété précédente. Si on regarde d'autres ensembles, comme* $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, *le théorème n'est pas valable.*

Remarque 1.6

Ce théorème se démontrant par l'absurde, il n'est pas constructif et dit seulement qu'il existe un élément, sans moyen a priori *de le construire, et il est d'ailleurs parfois très difficile de trouver cet élément ! Ce fait sera à la base de la plupart des techniques de cryptographie.*

2. La division euclidienne

Le but est ici de montrer le théorème suivant, qui va avoir de profondes conséquences sur l'arithmétique de $\mathbb{Z}$. Ce théorème est très exactement une formalisation de la division apprise en classe de primaire.

Théorème 2.1 (Division euclidienne)

Soient $a, b \in \mathbb{Z}$ avec $b \neq 0$. Alors il **existe** des entiers $q, r \in \mathbb{Z}$ **uniques** vérifiant $a = bq + r$ et $0 \leqslant r < |b|$.
L'entier r s'appelle le reste de la division de a par b et q s'appelle le quotient.

Preuve : Il faut montrer l'existence et l'unicité. Pour cela, nous allons considérer la partie $A = \{\text{entiers de la forme } a - bk \in \mathbb{N} \text{ avec } k \in \mathbb{Z}\}$. Tout d'abord, cette partie est non vide. En effet, si $a \geqslant 0$ alors on peut prendre $k = 0$ et si $a < 0$ alors on peut prendre $k = a.\text{sign}(b)$ de sorte que $a - bk = a(1 - |b|) \geqslant 0$.
Comme A est une partie de $\mathbb{N}$, elle possède un plus petit élément : notons le r de sorte que, par définition, il existe $q \in \mathbb{Z}$ tel que $a = bq + r$.
Il s'agit de montrer que $0 \leqslant r < |b|$. Pour cela, nous allons raisonner par l'absurde en supposant que $r \geqslant |b|$, il nous faut maintenant aboutir à une contradiction.
On écrit $0 \leqslant r - |b| \leqslant a - bq - |b| = a - b(q + \text{sign}(b))$, mais cela contredit le fait que r est le plus petit élément de A, puisque $r - |b| \in A$ est plus petit que r. C'est absurde et donc $r < |b|$.
Il nous faut maintenant montrer que cette décomposition est unique. Supposons qu'on a deux décompositions $a = bq_1 + r_1 = bq_2 + r_2$ avec $0 \leqslant r_1 < |b|$ et $0 \leqslant r_2 < |b|$. On a alors $b(q_1 - q_2) = r_2 - r_1$ Supposons que $r_2 > r_1$, ce qui impose $q_2 \neq q_1$ et donc $|q_1 - q_2| \geqslant 1$, c'est-à-dire $r_2 - r_1 = |b|(q_1 - q_2) \geqslant |b|$. Ainsi $r_2 \geqslant r_1 + |b| \geqslant |b|$ car $r_1 \geqslant 0$. Mais ceci contredit la définition de r_2.
De la même manière, on montre que $r_2 < r_1$ est absurde et donc $r_2 = r_1$, puis $q_1 = q_2$ car $b \neq 0$. □

Encore une fois, ce théorème n'est pas constructif et dit seulement qu'il existe des éléments p et q quelque part. Pour les trouver effectivement, on recourt à l'algorithme vu en primaire !

Exercice 2.2
Calculer la division euclidienne de 17 *par* 5, *de* -17 *par* 5, *de* 17 *par* -5, *de* 5 *par* 17.

Définition 2.3

Soient a et b deux entiers relatifs. Si $b \neq 0$ nous dirons que b divise a si le reste de la division de a par b est nul, et on note $b|a$.
Si $b = 0$ alors nous dirons que $b|a$ si $a = 0$.
Dans tous les cas, cela équivaut à l'existence de $q \in \mathbb{Z}$ tel que $a = bq$.

Proposition 2.4

Soient a, b et c des entiers. Alors

- si $c|b$ et $b|a$ alors $c|a$,
- si $a|b$ et $b|a$ alors $a = b$ ou $a = -b$,
- si $a|b$ alors $ac|bc$,
- si $ac|bc$ et que $c \neq 0$ alors $a|b$,
- si $a|b$ et $a|c$ alors $a|(b + c)$.

Preuve : Exercice. □

Proposition 2.5

Soient a, b et c des entiers. Si c divise a et b, alors il divise tout les entiers de la forme $au + bv$.

Preuve : Écrivons $a = pc$ et $b = qc$. On a alors $au + bv = upc + vqc$ et donc $au + bv = (up + vq)c$. C'est-à-dire que $c|au + bv$. □

Définition 2.6

Soient a et b deux entiers non tous les deux nuls. Considérons l'ensemble définit par

$$\{\text{entiers} > 0 \text{ de la forme } au + bv \text{ avec } u,\ v \in \mathbb{Z}\}.$$

Comme cet ensemble est non vide, il possède un plus petit élément d'après la proposition 1. Nous l'appellerons le *plus grand commun diviseur* de a et b et le noterons $\text{pgcd}(a, b)$ (la raison pour une telle dénomination sera donnée un peu plus tard).
Si a et b sont tous les deux nuls, nous poserons $\text{pgcd}(a, b) = 0$.

Proposition 2.7

Soient a et b deux entiers. Alors $\text{pgcd}(a, b)$ divise a et divise b. De plus, pour tout diviseur d de a et b, on a $d|\text{pgcd}(a, b)$.

Preuve : Montrons que $c = \text{pgcd}(a, b)$ divise a et b. Pour cela, on raisonne par l'absurde et on suppose que c ne divise pas a. On peut alors écrire (par division euclidienne) $a = qc + r$ avec $0 < r < c$ (strict car on suppose que c ne divise pas a). Par définition, on peut écrire c sous la forme $au + bv$. On a alors $a = qc + r = q(au + bv) + r$ et donc $a(1 - qu) - bv = r > 0$. Mais cela contredit la définition de $\text{pgcd}(a, b)$ qui est le plus petit élément positif de cette forme, on a donc en fait

$r = 0$. Donc $\text{pgcd}(a, b)$ est un diviseur de a et de b (même raisonnement en faisant la division euclidienne de b par c).
Passons à la démonstration du second point. Soit d un diviseur commun de a et b, alors d'après la proposition précédente, d divise tout les élément de la forme $au+bv$ et donc en particulier $\text{pgcd}(a, b)$. □

Ainsi, on a montré que $\text{pgcd}(a, b)$ est un diviseur de a et de b, et que c'est le plus grand, d'où la dénomination de Plus Grand Diviseur Commun.

Remarquons que pour tout $r \geqslant 0$ on a $\text{pgcd}(r, 0) = r$.

Exercice 2.8
Calculer le pgcd *de* 5 *et* 6, *de* 6 *et* 6, *de* 3 *et* 2, *de* 9 *et* 3, *de* 3 *et* 6, *de* 6 *et* 9.

Théorème 2.9 (Bézout)

Soient a, b et c des entiers avec $c > 0$. Si c est de la forme $au + bv$ et divise a et b alors $c = \text{pgcd}(a, b)$.

Preuve : Exercice. □

Une relation de la forme $\text{pgcd}(a, b) = au + bv$ est appelée une relation de Bézout. Elle n'est pas unique.

Exercice 2.10
Trouver des relations de Bézout pour les pgcd *calculés précédemment.*

Proposition 2.11

Soient a et b deux entiers, et c un diviseur commun de a et de b. Notons $a = ca'$ et $b = cb'$. Alors $\text{pgcd}(a, b) = |c|\text{pgcd}(a', b')$.

Preuve : On raisonne avec les diviseurs. Soit d un diviseur de a' et de b', alors $cd|a$ et $cd|b$ et donc $cd|\text{pgcd}(a, b)$. En particulier, on trouve que $c \cdot \text{pgcd}(a', b')|\text{pgcd}(a, b)$. Réciproquement, $c|a$ et $c|b$ donc $c|\text{pgcd}(a, b)$. Écrivons $\text{pgcd}(a, b) = dc$. On a alors $dc|ca'$ et $dc|cb'$. Si $c = 0$ alors le résultat est évident (car alors $a = b = c = 0$), on peut donc le supposer non nul et on a alors $d|a'$ et $d|b'$. Ce qui impose que $d|\text{pgcd}(a', b')$. D'où le résultat. □

En particulier, on voit que si on prend $c = \text{pgcd}(a, b)$ et que celui-ci est non nul alors $\text{pgcd}(a', b') = 1$.

Définition 2.12

Nous dirons que deux entiers a et b sont premiers entre eux si leur pgcd est 1.

En particulier, 1 est premier avec tous les autres entiers. Les entiers 2 et 3 sont premiers entre eux. Les entiers 6 et 3 ne sont pas premiers entre eux.

Proposition 2.13

Soient a et b deux entiers. Écrivons $a = bq + r$. Alors $\text{pgcd}(a, b) = \text{pgcd}(b, r)$.

Preuve : Si c divise a et b, alors il divise r. Réciproquement, si c divise b et r, alors il divise a. □

Cette proposition est à la base de l'algorithme d'Euclide pour le calcul du pgcd : on calcule des divisions euclidiennes jusqu'à ce que le reste devienne 0.

L'algorithme se présente alors sous la forme suivante :

Entrée : (a, b)
tant que $b \neq 0$ **faire :**
$$a = bq + r$$
$$a \leftarrow b,\ b \leftarrow r$$
fin tant que
Sortie : a

TP 2.14
Implémenter l'algorithme d'Euclide.

On peut étendre cet algorithme afin de calculer non seulement le pgcd mais aussi une décomposition de Bézout. En effet, si on pose $r_0 = a$ et $r_1 = b$ alors on calcule récursivement

$$\begin{aligned} r_0 &= r_1 q_1 + r_2 \\ r_1 &= r_2 q_2 + r_3 \\ &\vdots \\ r_{k-2} &= r_{k-1} q_{k-1} + r_k \\ r_{k-1} &= r_k q_k + r_{k+1} \end{aligned}$$

On définit deux suites supplémentaires u_i et v_i par

$$u_0 = 1, u_1 = 0, v_0 = 0, v_1 = 1$$

et pour tout $n \geqslant 1$ on pose

$$u_n = u_{n-2} - q_{n-2} u_{n-1} \quad , \quad v_n = v_{n-2} - q_{n-2} v_{n-1}$$

Nous allons montrer qu'à chaque étape on a

$$r_n = u_n a + v_n b.$$

En effet, c'est vrai pour $n = 0$ (car $a = 1 \cdot a + 0 \cdot b$) et $n = 1$ (car $b = 0 \cdot a + 1 \cdot b$). Supposant alors le résultat vrai au rang n, on a donc $r_{n-1} = u_{n-1} a + v_{n-1} b$ et $r_n = u_n a + v_n b$.
Ainsi, on trouve que

$$\begin{aligned} u_{n+1} a + v_{n+1} b &= (u_{n-1} - q_{n-1} u_n) a + (v_{n-1} - q_{n-1} v_n) b \\ &= (u_{n-1} a + v_{n-1} b) - q_{n-1} (u_n a + v_n b) \\ &= r_{n-1} - q_{n-1} r_n = r_n. \end{aligned}$$

On arrive alors à l'algorithme suivant.
Entrée : (a, b)
$u_0 \leftarrow 1,\ u_1 \leftarrow 0,\ v_0 \leftarrow 0,\ v_1 \leftarrow 1$
tant que $b \neq 0$ **faire :**
$$a = bq + r$$
$$a \leftarrow b,\ b \leftarrow r$$
$$s \leftarrow u_1,\ u_1 \leftarrow u_0 - u_1 q,\ u_0 \leftarrow s$$
$$s \leftarrow v_1,\ v_1 \leftarrow v_0 - v_1 q,\ v_0 \leftarrow s$$
fin tant que
Sortie : $a,\ u_0,\ v_0$

Exercice 2.15
Tester cet algorithme sur des exemples.

TP 2.16
Implémenter l'algorithme d'Euclide étendu.

Avec les décompositions de Bézout, on peut obtenir de nouvelles propriétés de la divisibilité :

Proposition 2.17: Lemme de Gauss

Soient a, b, c trois entiers. Si a est premier à b et $a|bc$ alors $a|c$.

Preuve : Écrivons tout d'abord $bc = da$. Comme a est premier à b, il existe $u, v \in \mathbb{Z}$ tels que $au + bv = 1$. Multipliant tout par c on obtient $auc + bvc = c$ et comme $bvc = dav$ on a $auc + adv = c$ et donc $a(uc + dv) = c$, c'est-à-dire $a|c$. □

Si a et b ne sont plus premiers entre eux, alors ce résultat est faux en général. En effet, on a $6|2.3$ mais $6 \nmid 2$!

3. Les nombres premiers

Définition 3.1

Nous dirons qu'un nombre $p \in \mathbb{N}$, $p \geqslant 2$, est premier si les seuls entiers qui le divisent sont 1 et p.

Exemple 3.2 : Les premiers nombres premiers sont 2, 3, 5, 7, 11, 13, 17, ...

Il est très difficile (au sens de la théorie de la complexité) d'exhiber des grands nombres premiers ainsi que de prédire leur répartition. Une méthode assez simple pour trouver des nombres premiers (très coûteuse en temps de calcul) est la méthode du crible d'Eratoshtène qui permet de trouver tout les entiers inférieurs à un entier donné :
On commence par écrire la liste des $n-1$ nombres (de 2 à n). Tout d'abord, comme 2 est premier, on peut barrer tout les multiples de 2. Ensuite, 3 est premier (car non barré), on peut donc barrer tout les multiples de 3. Le nombre 4 est barré car multiple de 2. Le suivant est 5, non barré, on barre tout les multiples de 5, ... On s'arrête à $\sqrt{n}$ car on ne barrera plus d'autre nombre après (un nombre compris entre $\sqrt{n}$ et n qui n'est pas premier possède au moins un facteur $\leqslant \sqrt{n}$).

Voici ci-dessous le crible d'Ératosthène donnant les nombres premiers jusqu'à 100 (on barre les multiples des nombres $\leqslant 10$, c'est-à-dire les multiples des premiers $\leqslant 7$)

	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~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	~~83~~	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

Les nombres permiers $\leqslant 100$ sont donc ceux qui ne sont pas barrés !

TP 3.3

Implémenter le crible d'Eratosthène permettant de trouver toutsles nombres permiers $\leqslant n$ et tracer la fonction de répartition

$$\ell \mapsto \pi(\ell) = \text{card}\,\{p \leqslant \ell, p \text{ premiers}\}.$$

Proposition 3.4

Soit $n \geqslant 2$ un entier. Alors il existe un nombre premier p tel que $p|n$.

Preuve : On considère l'ensemble $D_n = \{m \in \mathbb{N}, m \geqslant 2 \text{ tel que } m|n\}$. Cet ensemble est non vide (il contient au moins n) donc il possède un plus petit élément p. Nous allons montrer que p est premier.
Soit m un diviseur de p avec $m \geqslant 2$. Alors $m|p$ et comme $p|n$ on a $m|n$. Par suite, $m \in D_n$ et $m \leqslant p$. Mais p est le plus petit élément de D_n donc $m = p$, ce qui prouve que p est premier. □

Encore une fois, cette preuve est non constructive, et dans les faits il est très difficile (algorithmiquement) de trouver un facteur premier.

Proposition 3.5

L'ensemble des nombres premiers est infini.

Preuve : Par l'absurde, supposons qu'il n'en existe qu'un nombre fini et notons les $p_1, \ldots, p_n$. Alors aucun des p_i ne divise le nombre $p_1 \ldots p_n + 1$. Comme ce dernier possède un facteur premier d'après la proposition précédente, on aboutit à une contradiction. □

Proposition 3.6

Soient a et b deux entiers. Si a est premier et ne divise par b, alors $\text{pgcd}(a, b) = 1$.
En particulier, si $a \neq b$ et que ces deux nombres sont premiers alors $\text{pgcd}(a, b) = 1$.

Preuve : Exercice. □

Les nombres premiers permettent une nouvelle représentation des nombres. Cette représentation est très pratique mais se prête malheureusement très mal à l'addition des nombres (mais permet une multiplication très rapide).

Théorème 3.7 (Théorème fondamental de l'arithmétique)

Soit $m \in \mathbb{N}$. Alors il existe des entiers $n_1, \ldots, n_r$ strictement positifs et des nombres premiers $p_1 < \ldots < p_r$ distincts tels que $m = p_1^{n_1} \ldots p_r^{n_r}$. De plus, si on a deux décompositions de cette forme, alors elles sont égales.

Preuve : Nous allons d'abord montrer l'existence, et ceci se fait par récurrence (généralisée) sur la taille de m. Pour $m = 1$, pas de problème. Pour m plus grand, on sait qu'il a au moins un facteurs premier p. On peut donc écrire $m = pm'$ et $m' < m$. Par hypothèse de récurrence, m' possède une décomposition en facteur premier $m' = p_1^{n_1} \ldots p_r^{n_r}$. Si $p = p_i$ pour un i alors on augmente n_i de 1, sinon on rajoute ce nouveau nombre premier.
Il reste à voir que la décomposition est unique. Pour cela, on en prend deux $p_1^{n_1} \ldots p_r^{n_r} = p_1'^{n_1'} \ldots p_{r'}'^{n_{r'}'}$. Comme p_1 divise le produit et que p_1 est premier, il divise au moins un des termes (ceci s'obtient par récurrence avec le lemme de Gauss) on peut donc supposer que $p_1 = p_1'$. D'autre part, quitte à échanger les termes, on peut supposer que $n_1 \leqslant n_1'$ et quitte à diviser par $p_1^{n_1}$ on se ramène au cas $n_1 = 0$. Supposons que $n_1 \neq n_1'$. Alors p_1 divise l'un des termes de gauches et donc apparaît dans la décomposition (i.e. on a $p_1 = p_i$ pour un $i > 1$) mais cela contredit l'hypothèse que les p_i sont distincts. On a donc $n_1 = n_1'$. En faisant la même chose avec les autres facteurs, on obtient le résultat. □

Exercice 3.8

Calculer les décompositions en facteur premiers des nombres 1, 2, 3, 5, 9, 17, 21, 48, 91, 100, 1183.

TP 3.9
Écrire un algorithme de factorisation des entiers et l'implémenter.

4. Calcul dans $\mathbb{Z}/n\mathbb{Z}$

On fixe un entier $n > 0$ et on souhaite définir des opérations sur l'ensemble $\mathbb{Z}/n\mathbb{Z}$ composé des éléments $0, 1, 2, 3, \ldots, n-1$. On rappelle que pour tout entier $\ell \in \mathbb{Z}$ le reste de la division de ℓ par n est un élément de $\{0, 1, 2, 3, \ldots, n-1\}$.
Il nous arrivera de considérer des éléments de $\mathbb{Z}$ comme des éléments de $\mathbb{Z}/n\mathbb{Z}$. Pour faire cela, nous considérerons en fait le reste de la division par n et, pour différencier l'égalité dans $\mathbb{Z}/n\mathbb{Z}$ de l'égalité dans $\mathbb{Z}$, nous dirons que deux nombres $a, b \in \mathbb{Z}$ sont égaux dans $\mathbb{Z}/n\mathbb{Z}$ (noté $a \equiv b$) si les restes des divisions de a et b par n sont égaux.
Par exemple, dans $\mathbb{Z}/12\mathbb{Z}$, on a $25 \equiv 2 \cdot 12 + 1 \equiv 1$.
On définit alors une addition $a +_n b =$ reste de la division par n de $a + b$.

Proposition 4.1
Pour tout $a, b, c \in \mathbb{Z}/n\mathbb{Z}$ on a

$$(a +_n b) +_n c \equiv a +_n (b +_n c).$$

Preuve : Par division euclidienne, on a $a + b = q_1 n + r_1$ et $r_1 + c = q_2 n + r_2$. Ainsi on a $(a +_n b) +_n c = r_2$. Or $(a + b + c) = (q_1 + q_2)n + r_2$ donc r_2 est le reste de la division de $(a + b + c)$ par n.
On montre alors de même que $a +_n (b +_n c)$ est le reste de la division de $(a + b + c)$ par n, c'est-à-dire r_2. □

Exemple 4.2 : La table d'addition dans $\mathbb{Z}/2\mathbb{Z}$ s'écrit

$+_n$	0	1
0	0	1
1	1	0

Exercice 4.3
Écrire la table d'addition pour $n = 3, 4$.

De même, on définit la soustraction (notée $-_n$) et la multiplication (notée $._n$) en prenant le reste de la division par n.

Proposition 4.4
Pour tout $a, b, c \in \mathbb{N}$ on a

$$(a -_n b) -_n c \equiv a -_n (b +_n c)$$
$$(a._n b)._n c \equiv a._n (b._n c)$$
$$a._n (b +_n c) \equiv (a._n b) +_n (a._n c)$$

Preuve : Exercice. □

Exercice 4.5
Écrire les tables de multiplications pour $n = 2, 3, 4, 5$.

En particulier, on voit que la multiplication n'est pas intègre : il peut exister deux éléments non nuls dont le produit est nul.
En général, il n'est pas possible de définir la division par un nombre même s'il est non nul car l'inverse d'un nombre x est un nombre y tel que $xy \equiv 1$. Or on a constaté que, dans $\mathbb{Z}/4\mathbb{Z}$, le nombre 2 n'a pas d'inverse.

Proposition 4.6

Soient $n \in \mathbb{N}$ et $\ell \in \mathbb{Z}/n\mathbb{Z}$. Alors ℓ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si ℓ est premier à n.
En particulier, si n est premier alors tout élément non nul de $\mathbb{Z}/n\mathbb{Z}$ est inversible.

Preuve : Supposons que ℓ est premier à n. Prenant une décomposition de Bézout, on trouve qu'il existe $u, v \in \mathbb{Z}$ tels que $un + v\ell = 1$. C'est-à-dire que $v\ell = (-u)n + 1$, i.e. $v._n \ell \equiv 1$, et donc ℓ est inversible.
Réciproquement, si ℓ est inversible, alors il existe $v \in \mathbb{Z}$ tel que $v._n \ell \equiv 1$. Faisant la division euclidienne de $v\ell$ par n, on trouve que $v\ell = qn + 1$, c'est-à-dire que $(-q)n + v\ell = 1$ et donc $\text{pgcd}(n, \ell) = 1$. □

On remarque que la preuve de cette proposition fournit de plus un moyen de calculer l'inverse d'un élément !

Définition 4.7

Nous noterons $(\mathbb{Z}/n\mathbb{Z})^*$ l'ensemble des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ et $\varphi(n)$ le nombre d'éléments de $(\mathbb{Z}/n\mathbb{Z})^*$.

En particulier, on voit que si n est premier alors $\varphi(n) = n - 1$.

4.1. Théorème chinois et conséquences. Notre but est d'étudier l'ensemble $\mathbb{Z}/pq\mathbb{Z}$ et d'en déduire certaines propriétés lorsque p et q sont premiers entre eux. Pour cela nous allons étudier tout d'abord le nouvel ensemble $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ composé des couples (a, b) avec $a \in \mathbb{Z}/p\mathbb{Z}$ et $b \in \mathbb{Z}/q\mathbb{Z}$.
En particulier, cet ensemble hérite d'une addition $+_{(p,q)}$ et d'une multiplication $\cdot_{(p,q)}$ en utilisant $+_p, +_q, \cdot_p$ et $\cdot_q$ en les faisant opérer sur les coordonnées.

Exercice 4.8

Écrire les tables d'addition et de multiplication dans $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ *et* $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

On peut alors regarder les inversibles de $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$, l'élément 1 devant être remplacé par le couple $(1, 1)$. On voit que les inversibles de $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ sont exactement les couples (a, b) avec $a \in (\mathbb{Z}/p\mathbb{Z})^*$ et $b \in (\mathbb{Z}/q\mathbb{Z})^*$. Il y en a donc $\varphi(p)\varphi(q)$.
Pour relier $\mathbb{Z}/pq\mathbb{Z}$ à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$, on définit une application

$$\psi : \mathbb{Z}/pq\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$$

en prenant les restes des divisions par p et q.

Exemple 4.9 : Pour $p = 3$ et $q = 2$ on a

a	0	1	2	3	4	5
$\psi(a)$	$(0,0)$	$(1,1)$	$(2,0)$	$(0,1)$	$(1,0)$	$(2,1)$

Proposition 4.10

L'application ψ respecte l'addition et la multiplication, i.e. pour tout $a, b \in \mathbb{Z}/pq\mathbb{Z}$ on a

$$\psi(a +_{pq} b) \equiv \psi(a) +_{(p,q)} \psi(b) \quad \text{et} \quad \psi(a._{pq} b) \equiv \psi(a).{}_{(p,q)}\psi(b)$$

Preuve : Exercice. □

Proposition 4.11

Si p et q sont premiers entre eux, alors ψ est bijectif, i.e. ψ conserve tout l'information, et il y en a autant à l'arrivée qu'au départ.

Preuve : Soient a, b tels que $\psi(a) \equiv \psi(b)$. En particulier, les restes des divisions de a et b par p sont égaux, et de même pour les restes des divisions par q.
C'est-à-dire que $p|a-b$ et $q|a-b$. Comme p et q sont premiers entre eux, le lemme de Gauss assure que $pq|a-b$ et comme $a, b \in \{0, \dots, pq-1\}$ on a forcément $a = b$.
Ainsi, l'application ψ conserve l'information, on dit qu'elle est injective.
Il reste à montrer qu'il y a autant d'information au début qu'à la fin (on dit que ψ est surjective). Pour cela, étant donné un élément $(c, d) \in \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$, il s'agit de montrer qu'il existe $a \in \mathbb{Z}/pq\mathbb{Z}$ tel que $\psi(a) = (c, d)$.
Comme p et q sont premiers entre eux, il existe une décomposition de Bézout $up + vq = 1$. Considérons le nombre $a = dup + cvq$.
On a $a = dup + cvq = d(1 - vq) + cvq = (cv - dv)q + d$ donc le reste de la division de a par q est d. De même on montre que le reste de la division de a par p est c.
On a donc bien $\psi(a) \equiv (c, d)$. □

La preuve de la surjectivité (qui est constructive car utilisant une décomposition de Bézout), est en fait un résultat très ancien découvert par les chinois (d'où le nom !)

Théorème 4.12 (Théorème Chinois)

Soient p et q des entiers premiers entre eux et $c \in \mathbb{Z}/p\mathbb{Z}$, $d \in \mathbb{Z}/q\mathbb{Z}$. Alors il existe un unique élément $a \in \mathbb{Z}$, $0 \leqslant a < pq$ tel que le reste de la division de a par p (resp. q) est c (resp. d).

Remarque 4.13

Il est fondamental que p et q soient premiers entre eux ! Si on regarde le cas $p = q = 2$, on voit que l'application

$$\psi \colon \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

est bien définie, mais n'est ni injective ($\psi(2) \equiv (0,0) \equiv \psi(0)$) ni surjective ($(1,0)$ n'est pas dans l'image !).

Exemple 4.14 : Trouver $x \in \mathbb{N}$, $x < 63$ tel que $x = 4$ dans $\mathbb{Z}/7\mathbb{Z}$ et $x = 7$ dans $\mathbb{Z}/9\mathbb{Z}$.
Même question avec $x \in \mathbb{N}$, $x < 434$ tel que $x = 9$ dans $\mathbb{Z}/14\mathbb{Z}$ et $x = 13$ dans $\mathbb{Z}/31\mathbb{Z}$.

En corollaire de la proposition, on montre qu'un élément inversible provient d'un élément inversible.

Corollaire 4.15

Si p et q sont premiers entre eux, alors $\varphi(pq) = \varphi(p)\varphi(q)$.

Preuve : D'après la proposition précédente, on a autant d'inversible à la source et au but de l'application ψ donc

$$|(\mathbb{Z}/pq\mathbb{Z})^*| = |(\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^*|.$$

□

On peut même être plus précis si p et q sont premiers.

Proposition 4.16

Soient p et q deux nombres premiers distincts. Alors $\varphi(pq) = (p-1)(q-1)$

4.2. Ordre des éléments de $(\mathbb{Z}/n\mathbb{Z})^*$. Pour $x \in (\mathbb{Z}/n\mathbb{Z})^*$, on peut s'autoriser n'importe quelles puissances, positives où négatives (alors qu'on ne peut prendre que les puissances positives d'un élément quelconque de $\mathbb{Z}/n\mathbb{Z}$!).
Si l'on y prend garde, le calcul des puissances peut demander beaucoup de temps sur un ordinateur. Voici un algorithme efficace pour calculer des puissances en utilisant la décomposition en base 2 de l'exposant.

Proposition 4.17

Soient $a \in (\mathbb{Z}/n\mathbb{Z})^*$ et $\ell \in \mathbb{N}$ non nul. Écrivons $\ell = \sum_{i=0}^{m} u_i 2^i$ avec $u_i \in \{0,1\}$ pour tout i.
Considérons les suite a_i et b_i définies par

$$b_1 = a \qquad a_1 = \begin{cases} b_1 \text{ si } u_0 = 1 \\ 1 \text{ sinon} \end{cases}$$

puis

$$b_{i+1} = (b_i)^2 \qquad a_{i+1} = \begin{cases} a_i b_{i+1} \text{ si } u_i = 1 \\ a_i \text{ sinon.} \end{cases}$$

Alors on a $a_\ell = a^\ell$.

TP 4.18
Essayer cet algorithme sur un exemple, puis l'implémenter.

Définition 4.19

Soit $a \in (\mathbb{Z}/n\mathbb{Z})^*$. On appelle ordre de a, et on note $\mathrm{ord}(a)$, le plus petit entier $\ell \geqslant 1$ tel que $a^\ell \equiv 1$.

On voit tout de suite que $o(1) = 1$.

Exemple 4.20 : Calculer les ordres de tous les éléments de $(\mathbb{Z}/n\mathbb{Z})^*$ pour $n \leqslant 6$.

Proposition 4.21

Tout élément de $(\mathbb{Z}/n\mathbb{Z})^*$ à un ordre.

Preuve : Le résultat repose sur le principe des tiroirs : si je possède une étagère à n tiroirs et que j'ai $n+1$ chaussettes, il y aura au moins un tiroir qui contiendra deux chaussettes !
Appliqué à notre problème, prenons un élément $a \in (\mathbb{Z}/n\mathbb{Z})^*$ et considérons toutes les puissances $a^1, a^2, \ldots, a^n \in (\mathbb{Z}/n\mathbb{Z})^*$. Comme $(\mathbb{Z}/n\mathbb{Z})^*$ contient $\varphi(n) < n$ élément, il y en à au moins deux qui sont égaux : il existe $\ell_1 < \ell_2$ tels que $a^{\ell_1} \equiv a^{\ell_2}$.
On a donc $a^{\ell_2 - \ell_1} \equiv 1$.
Ainsi, l'ensemble $\{\ell \in \mathbb{N}, \ell > 0 \text{ et } a^\ell \equiv 1\}$ est non vide, donc il contient un plus petit élément. □

Proposition 4.22

Soit $a \in (\mathbb{Z}/n\mathbb{Z})^*$, si $a^m \equiv 1$ alors $\mathrm{ord}(a) | m$.

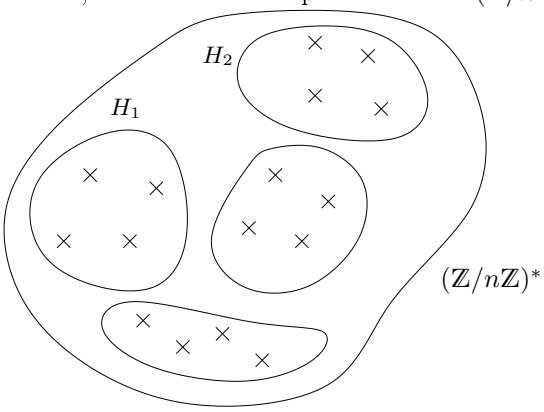
Preuve : Soit d le pgcd de m et $\mathrm{ord}(a)$. En particulier, $1 \leqslant d \leqslant \mathrm{ord}(a)$. Alors il existe u et v entiers tels que $um + v\mathrm{ord}(a) = d$. On a donc

$$a^d \equiv a^{um + v\mathrm{ord}(a)} \equiv (a^m)^u (a^{\mathrm{ord}(a)})^v \equiv 1.$$

Donc, par définition de l'ordre (plus petit entier ℓ tel que $a^\ell \equiv 1$) on trouve que $\mathrm{ord}(a) \leqslant d$, d'où le résultat car $\mathrm{ord}(a) = d | m$. □

Proposition 4.23
Soit $a \in (\mathbb{Z}/n\mathbb{Z})^*$, alors $\mathrm{ord}(a)|\varphi(n)$.

Preuve : Pour montrer cela, nous allons découper l'ensemble $(\mathbb{Z}/n\mathbb{Z})^*$:



On définit des parties de la manière suivante : pour tout $\alpha \in (\mathbb{Z}/n\mathbb{Z})^*$ notons $H_\alpha = \{\alpha a^\ell, \ell \in \mathbb{Z}\}$.
En particulier, on voit que H_α possède très exactement $\mathrm{ord}(a)$ éléments. En effet, si on prend $\ell \in \mathbb{Z}$ alors on peut l'écrire sous la forme $\ell = p\mathrm{ord}(a) + q$ avec $0 \leqslant q < \mathrm{ord}(a)$. On a donc $a^\ell \equiv (a^{\mathrm{ord}(a)})^p a^q$. Donc dans la définition, on peut supposer que $0 \leqslant \ell < \mathrm{ord}(a)$. De plus, si $\alpha a^m \equiv \alpha a^\ell$ avec $0 \leqslant \ell, m < \mathrm{ord}(a)$ alors $a^{m-\ell} \equiv 1$ et donc $\mathrm{ord}(a)|m-\ell$. Mais comme $-\mathrm{ord}(a) < m-\ell < \mathrm{ord}(a)$ on trouve que $\ell - m = 0$. On obtient donc le nombre d'éléments prédits.

Tout élément de $(\mathbb{Z}/n\mathbb{Z})^*$ est dans au moins l'un des H_α car $\alpha \in H_\alpha$ (on a $a^0 \equiv 1$). Maintenant, nous allons montrer que pour $\alpha, \beta \in (\mathbb{Z}/n\mathbb{Z})^*$ on a $H_\alpha = H_\beta$ ou bien $H_\alpha \cap H_\beta = \emptyset$.
Tout d'abord, si $\alpha \in H_\beta$ alors tout les éléments de H_α sont dans H_β. Comme ils ont le même nombre d'éléments, les deux ensembles sont égaux.
Supposons maintenant qu'ils ont un élément en commun γ. Alors $\gamma \equiv \alpha a^\ell \equiv \beta a^m$. En particulier, on a $\alpha \equiv \beta a^{m-\ell}$ donc $\alpha \in H_\beta$ et on applique le résultat précédent.
On se retrouve donc avec une décomposition de $(\mathbb{Z}/n\mathbb{Z})^*$ en paquets distincts de $\mathrm{ord}(a)$ éléments. Si m est le nombre de ces paquets alors par définition, on a $\varphi(n) = m\mathrm{ord}(a)$. (il suffit de compter le nombre d'éléments). □

Exemple 4.24 : On regarde dans $\mathbb{Z}/11\mathbb{Z}$. Comme 11 est premier, $\varphi(11) = 10 = 2 \cdot 5$. Par suite, les éléments de $(\mathbb{Z}/11\mathbb{Z})^*$ sont d'ordre 1, 2, 5 où 10. Regardons par exemple le cas de 2. On a $2^2 \equiv 4 \not\equiv 1$. On a $2^5 \equiv 2^2 2^2 2 \equiv 32 \equiv 10$. On voit donc que l'ordre n'est ni 1, ni 2, ni 5. C'est donc forcément 10.

Exercice 4.25
Calculer l'ordre de 3 *dans* $\mathbb{Z}/11\mathbb{Z}$ *et l'ordre de* 2 *dans* $\mathbb{Z}/19\mathbb{Z}$.

Comme conséquence directe de la proposition on voit que pour tout $a \in (\mathbb{Z}/n\mathbb{Z})^*$ on a $a^{\varphi(n)} \equiv 1$.

Proposition 4.26
Soient p et q deux nombres premiers distincts et soit $n = pq$. Soit t un entier dont le reste de la division par $\varphi(n)$ est 1. Alors pour tout $a \in \mathbb{Z}/n\mathbb{Z}$ on a $a^t \equiv a$.

Preuve : Écrivons $t = 1 + k\varphi(n)$. Supposons tout d'abord a inversible. Alors on a $a^{\varphi(n)} \equiv 1$ et donc $a^t \equiv a$.

Supposons maintenant que a n'est pas inversible et regardons son image par

$$\psi : \mathbb{Z}/pq\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}.$$

On sait par définition que cette image n'est pas inversible : notons la (b, c). On connait les inversibles de $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$: il faut que les deux coordonnées soient inversibles. Par suite, l'une des deux ne l'est pas. Mais comme p et q sont premiers, dire qu'une coordonnée n'est pas inversible, c'est dire qu'elle est nulle.
Supposons que $b \equiv 0$. Si $c \equiv 0$ on a fini car cela veut dire que $a \equiv 0$ et donc $a^t \equiv 0 \equiv a$.
Si $c \not\equiv 0$ alors $c^{\varphi(q)} \equiv 1$. Comme $\varphi(pq) = \varphi(p)\varphi(q)$ on trouve que

$$c^t \equiv c^{1+k\varphi(p)\varphi(q)c} \equiv c(c^{\varphi(q)})^{k\varphi(p)}.$$

Par suite, $\psi(a^t) \equiv \psi(a)^t \equiv (0, c)^t \equiv (b, c)^t \equiv (b^t, c^t) \equiv (0, c) \equiv \psi(a)$ et, comme ψ est injective, on trouve que $a^t \equiv a$.
Si $b \not\equiv 0$ mais que $c \equiv 0$, une démonstration identique permet d'arriver au résultat. □

4.3. Logarithme discret dans les corps finis. Nous aurons besoin dans la suite d'un résultat que nous ne démontrerons pas, mais qui est comprehensible avec les outils à notre disposition.

Proposition 4.27

Soit p un nombre premier. Alors il existe un élément $g \in (\mathbb{Z}/p\mathbb{Z})^*$ d'ordre exactement $\varphi(p) = p - 1$.

Preuve : Non démontré ! □

En particulier, l'ensemble des $\{g^\ell, 0 \leqslant \ell < p - 1\}$ contient $p - 1$ éléments, c'est-à-dire tout les éléments de $(\mathbb{Z}/p\mathbb{Z})^*$. Il s'ensuit que pour tout élément $a \in (\mathbb{Z}/p\mathbb{Z})^*$ il existe un unique $\ell \in \mathbb{N}$ avec $0 \leqslant \ell < p - 1$ tel que $a \equiv g^\ell$.
Ce nombre ℓ est appelé le *logarithme discret* de a en base g car, comme le logarithme en base x pour les réels, il permet de retrouver la puissance.
Dans les faits, il est algorithmiquement compliqué de calculer ce logarithme (i.e. cela prend beaucoup de temps !).

5. La cryptographie

La cryptographie (du grec κρυπτός, caché, et γράφειν, écrire) a pour but l'échange de messages qui ne peuvent être compris que par les personnnes possédant la clef pour les comprendre.
Depuis les techniques très simples utilisée par Jules César (qui consistait à sustituer à chaque lettre celle qui la suit en troisième position dans l'alphabet, i.e. $a \to d$, $b \to e$, ...) jusqu'à l'utilisation de langues exotiques pendant la guerre du pacifique (la langue des Navajos), la cryptographie utilise désormais des systèmes basés sur les chiffres et l'arithmétique. Si nous pourrons en étudier certains à l'aide de la théorie étudiée précédemment (El Gamal, RSA), d'autres vont bien au-delà du cadre de ce cours (par exemple les courbes elliptiques).
Quelques usages quotidiens de la cryptographie sont les transactions sur internet, la carte bancaire, ... et il est donc impossible de présupposer que l'émetteur et le récepteur du message possèdent tous deux une même clef secrète car il faudrait pour cela transmettre celle-ci de manière sécurisée (par exemple en la faisant voyager dans un fourgon sécurisé et dans les mains de personnes de confiance) ce qui ralentirait considérablement l'échange de l'information. Pour remédier à ce problème, nous allons étudier deux systèmes de cryptographie assymétrique à clef publique.

Problème 5.1
Considérons deux individus, traditionnellement appelés Alice et Bob. Alice souhaite transmettre un message à Bob et ne veut pas qu'il puisse être compris par une tierce personne. Pour cela, Bob aura au préalable construit deux clefs, une privée qu'il gardera pour lui, et une qu'il rendra publique. La clef publique permettra à tout le monde (par exemple Alice) de coder des messages et de lui envoyer, et seule la clef privée permettra de décoder le message.
Comment trouver un système assurant la sécurité des données ? Comme être sûr que personne d'autre que Bob ne pourra décoder, mais que Bob le pourra effectivement ?

Problème 5.2: Variante
Comment s'assurer qu'Alice est bien Alice ?

5.1. RSA pour l'envoit de message. Une réponse est fournie par l'algorythme RSA (pour Rivest, Shamir et Adleman) qui a été publié en 1978. Il est très utilisé pour le commerce éléctronique !
Le principe de génération des clefs est le suivant :

- Bob choisit deux nombres premiers p et q et calcule $n = pq$.
- Il calcule également $\varphi(n) = (p-1)(q-1)$.
- Il choisit alors un entier e premier à $\varphi(n)$ tel que $0 < e < \varphi(n)$ et calcule son inverse d dans $\mathbb{Z}/\varphi(n)\mathbb{Z}$.
- Bob publie la clef publique (n, e) et conserve la clef secrète d (après cette étape, les autres nombres ne sont plus utiles !).

Munie des données publiques (n, e), Alice peut désormais envoyer des messages à Bob :

- Elle choisit un nombre $m < n$ qui sera le message.
- Elle calcule $M = m^e$ dans $\mathbb{Z}/n\mathbb{Z}$, c'est le message crypté !
- Elle fait parvenir à Bob le chiffre M.

De son côté, lorsque Bob reçoit M, il peut caluler M^d dans $\mathbb{Z}/n\mathbb{Z}$ (c'est le seul qui possède d). Mais par définition le reste de la division de $t = ed$ par $\varphi(n)$ est 1 et d'après la proposition 4.2 on a

$$M^d \equiv (m^e)^d \equiv m^{ed} \equiv m^t \equiv m \text{ dans } \mathbb{Z}/n\mathbb{Z}$$

on a donc bien décodé le message !
Pourquoi se système est-il sûr ?

1 *A priori*, étant donné M et e on ne peut pas calculer la racine e-ième de M (qui serait alors m) pour plusieurs raisons : il peut y avoir plusieurs solutions à ce problème et le calcul de racines est très long.

2 Il est *a priori* possible de calculer les facteurs p et q de n, mais on sait que la factorisation est très longue ! Si on les avait toutefois, on pourrait alors calculer $\varphi(n)$ puis e, qui permet à son tour de décoder !

Comme on le voit, le facteur limitant est donc seulement le temps et non une impossibilité théorique de décoder le message : étant donné un peu de temps ou bien des ordinateurs suffisamment puissant, il n'y a aucun problème pour casser le système !
Toutefois, la plupart des transactions en commerce éléctronique ne prennent pas plus de quelques secondes (on parle ici du temps effectif de transmission), et si l'on peut s'assurer qu'il faut quelques minutes pour décoder le message, alors la

transaction est sécurisée : une fois qu'elle est effectuée et que la banque vous a identifié ainsi que le montant à débiter, les informations deviennent inutiles.
Afin d'être sûr que le décriptage du système soit suffisamment long, il convient toutefois de prendre des précautions dont voici quelques unes (liste évidemment non exhaustive ! et il se pourrait aussi qu'on trouve demain de nouvelles attaques nous obligeant à allonger cette liste...)

- il faut que les nombres premiers choisis p et q soient grand (ce qui est en pratique difficile à construire !)
- il faut que e ne soit pas trop petit ($e = 1$ serait stupide car il n'y aurait alors pas d'encodage, mais si $e = 2$ ou 3, cela peut déjà poser des problèmes !)
- il est bon d'utiliser au préablable un algorithme de remplissage visant à transformer le message m qu'on veut transmettre en un message qui prend plus de place (si vous souhaitez, par exemple, transmettre le message $m = 0$ ou $m = 1$, il n'y aura aucun codage et le message M est égal au message original !)

5.2. RSA pour la signature. Alice souhaite cette fois-ci pouvoir assurer Bob que c'est bien elle qui envoit le message. Pour cela, elle crée ses propres clefs privée d et publique (n, e).
Elle choisit alors un message m qui lui servira de signature, ce qu'elle peut faire de manière publique et qu'elle peut fixer pour toujours, par exemple $m = 1234567890$ (pour signer un autre jour, il suffira de changer les clefs) et calcule $M \equiv m^d$. C'est la seule qui puisse calculer M car elle seule possède l'information d.
Elle peut alors envoyer à Bob le message M, qui sera en mesure de calculer M^e dans $\mathbb{Z}/n\mathbb{Z}$ car e est publique. S'il trouve que $M^e \equiv 1234567890$ alors c'est bien Alice qui l'a envoyé (même justification que dans le chapitre précédent) !
Ce système de signature est par exemple utilisé, en combinaison avec d'autres (!), dans PGP.
Les restrictions de sécurité décrites pour l'encryptage par RSA sont bien sûr encore valable ici !

5.3. El Gamal. Le système ElGamal a été inventé par Taher ElGamal en 1984 et repose sur l'arithmétique des corps finis (au moins dans la version présentée ici). Il est rarement utilisé dans la pratique, mais des variantes sont par contre largement répandue, parmi lesquelles PGP.
Le principe est le suivant

- Bob choisit un grand nombre premier p et un générateur g de $(\mathbb{Z}/p\mathbb{Z})^*$.
- Il choisit aussi un nombre aléatoire $x \in \mathbb{N}$ tel que $0 < x < p - 1$ et calcule $h \equiv g^x$ dans $\mathbb{Z}/p\mathbb{Z}$.
- La clef publique est alors (p, g, h) et la clef privée est x (comme le calcul du logarithme discret est difficile, personne ne pourra connaître x en temps raisonnable).

Alice peut alors envoyer un message de la manière suivante :

- Elle choisit un nombre aléatoire $y \in \{0, \dots, p-2\}$ et calcule $c_1 = g^y$ (y est généré pour chaque message, on l'appelle parfois la clef éphémère).
- Elle calcule ensuite $s = h^y$.
- Alice code son message en un élément m de $(\mathbb{Z}/p\mathbb{Z})^*$ et calcule $c_2 = ms$.
- Puis elle envoit l'ensemble (c_1, c_2) à Bob.

Bob, recevant le message d'Alice, pourra le décoder en calculant $c_2 c_1^{-x}$ car on a

$$c_2 c_1^{-x} \equiv ms(g^y)^{-x} \equiv mh^y g^{-yx} \equiv m(g^x)^y g^{-xy} \equiv .$$

La sécurité de ce système repose sur le fait que, connaissant seulement (c_1, c_2), retrouver m équivaut à connaître x, ce qui est compliqué.

Tout comme pour RSA, il est nécessaire d'utiliser un algorithme de remplissage car il est sinon aisé de décrypter les messages.

Remarque 5.3

Il est possible de remplacer $(\mathbb{Z}/p\mathbb{Z})^*$ *par d'autres groupes, mais il faut alors s'assurer que le problème du logarithme discret dans ce groupe est difficile. C'est le cas pour les courbes elliptiques, ça ne l'est pas pour* $\mathbb{Z}/n\mathbb{Z}$ *!*

Chapitre 2

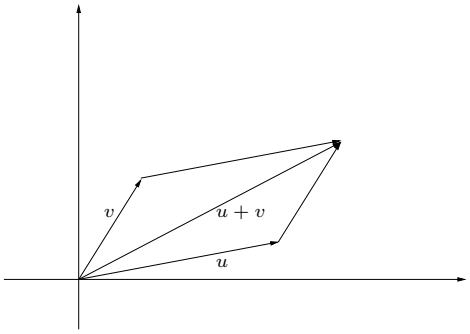
Algèbre linéaire

1. Exemple et définition

Considérons l'ensemble $\mathbb{R}^2$. C'est l'ensemble composé des éléments $\begin{pmatrix} x \\ y \end{pmatrix}$ avec $x, y \in \mathbb{R}$.

Considérons $u, v \in \mathbb{R}^2$, $u = \begin{pmatrix} x \\ y \end{pmatrix}, v = \begin{pmatrix} x' \\ y' \end{pmatrix}$. On peut alors définir une addition par

$$u + v = \begin{pmatrix} x + x' \\ y + y' \end{pmatrix}.$$



En particulier, on voit que l'addition est commutative, c'est-à-dire

$$u + v = v + u.$$

D'autre part, l'addition est associative. Cela siginifie que $\forall u, v, w \in \mathbb{R}^2$ on a

$$(u + v) + w = u + (v + w).$$

(attention à l'ordre des parenthèses ! ! !).

Il existe un élément particulier dans $\mathbb{R}^2$, à savoir $0_{\mathbb{R}^2} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$. Il est particulier dans le sens où c'est *le* neutre pour l'addition : pour tout $u \in \mathbb{R}^2$ on a

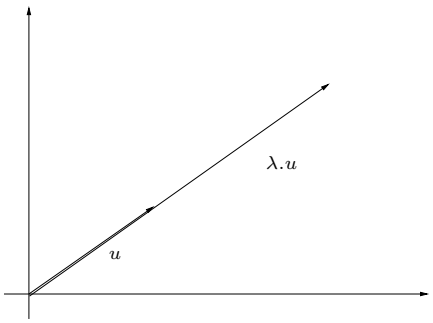
$$u + 0_{\mathbb{R}^2} = u$$

(découle directement des définitions *via* le calcul). Remarquons que ce neutre est unique (exercice).

Finalement, tout élément a un opposé (on parle parfois d'inverse pour l'addition). En effet, si $u = \begin{pmatrix} x \\ y \end{pmatrix}$, définissons $-u = \begin{pmatrix} -x \\ -y \end{pmatrix}$. On a alors $u + (-u) = 0_{\mathbb{R}^2}$.

Il existe une autre opération sur $\mathbb{R}^2$: la multiplication par un scalaire. Pour tout $u \in \mathbb{R}^2$, $u = \begin{pmatrix} x \\ y \end{pmatrix}$ et tout $\lambda \in \mathbb{R}$, on définit

$$\lambda.u = \begin{pmatrix} \lambda x \\ \lambda y \end{pmatrix}.$$



La multiplication par un scalaire vérifie certaines conditions. Par exemple la multiplication est distributive par rapport à l'addition : pour tout $\lambda, \mu \in \mathbb{R}$ et tout $u, v \in \mathbb{R}^2$ on a $(\lambda + \mu).u = \lambda.u + \mu.u$ et $\lambda.(u + v) = \lambda.u + \lambda.v$.
Elle est associative, i.e. $(\lambda\mu).u = \lambda.(\mu.u)$.
La multiplication est unitaire, c'est-à-dire que pour tout $u \in \mathbb{R}^2$ on a $1.u = u$.

Nous allons maintenant définir ce qu'est un espace vectoriel. Moralement, c'est un espace muni de deux lois (addition et multiplication par un scalaire) qui vérifient toutes les propriétés que nous venons d'énoncer pour $\mathbb{R}^2$.
Pour toute la suite de ce cours, nous noterons $\mathbb{K}$ un corps, c'est-à-dire, pour nous, $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$ ou $\mathbb{Z}/p\mathbb{Z}$ (pour un nombre premier p).

Définition 1.1

Soient $\mathbb{K}$ un corps, E un ensemble, $+ : E \times E \to E$ et $. : \mathbb{K} \times E \to E$ deux applications. Le triplet $(E, +, .)$ sera dit $\mathbb{K}$-espace vectoriel si les propriétés suivantes sont vérifiées :

i) ($+$ est associative) $\forall u, v, w \in E$ on a $(u + v) + w = u + (v + w)$

ii) (existence d'un neutre) $\exists 0_E \in E$ tel que $\forall u \in E$ on a $u + 0_E = u$

iii) (existence d'un opposé) $\forall u \in E, \exists v \in E$ tel que $u + v = 0_E$

iv) ($+$ est commutative) $\forall u, v \in E$ on a $u + v = v + u$
on résume ces 4 propriétés en disant que $(E, +)$ est un groupe commutatif.

v) (la loi . est distributive par rapport à $+$) $\forall u, v \in E$ et $\forall \lambda, \mu \in \mathbb{K}$ on a $(\lambda + \mu).u = \lambda.u + \mu.u$ et $\lambda.(u + v) = \lambda.u + \lambda.v$

vi) (la loi . est unitaire) $\forall u \in E$ on a $1.u = u$.

vii) (la loi . est associative) $\forall \lambda, \mu \in \mathbb{K}$ et $\forall u \in E$ on a $(\lambda\mu).u = \lambda.(\mu.u)$

Exemples d'espace vectoriels :

- $\mathbb{R}^n$ est un $\mathbb{R}$-espace vectoriel pour tout n,

- $\mathbb{C}^n$ est un $\mathbb{C}$-espace vectoriel pour tout n,

- $\mathbb{C}$ est un $\mathbb{R}$-espace vectoriel,

- l'ensemble des polynôme à coefficients dans $\mathbb{R}$ est un $\mathbb{R}$-espace vectoriel,

- l'ensemble des fonctions continues de $\mathbb{R}$ dans $\mathbb{R}$ est un $\mathbb{R}$-espace vectoriel.

Les règles énoncées dans la définition des espaces vectoriels sont les règles minimales qui nous permettent de travailler. À partir de ces règles, il est possible d'en déduire d'autre. Par exemple :

Proposition 1.2

Dans un $\mathbb{K}$-espace vectoriel E, les règles de calculs suivantes sont vraies :

i) Le neutre est unique, i.e. s'il existe $v \in E$ tel que $\forall u \in E\ u + v = u$ alors $v = 0_E$.

ii) L'opposé est unique, i.e : s'il existe $u, v, w \in E$ tels que $u + v = u + w = 0_E$ alors $v = w$.

iii) Pour tout $\lambda \in \mathbb{K}$ on a $\lambda.0_E = 0_E$.

iv) Pour tout $u \in E$ on a $0.u = 0_E$

v) $(-1).u = -u$ (souvenez vous que $-u$ était défini comme l'opposé de u et non comme $(-1).u$).

Preuve : Exercice (attention à n'utiliser que les propriétés des espaces vectoriels). □

Nous passons maintenant à la définition de sous-espace vectoriel, qui fournit une méthode pour construire des espaces vectoriels.

Définition 1.3

Soient E un $\mathbb{K}$-espace vectoriel et $F \subset E$ un sous-ensemble. L'ensemble F sera dit être un sous-espace vectoriel si

i) $E \neq \emptyset$

ii) si $u, v \in F$ alors $u + v \in F$

iii) si $u \in F$ et $\lambda \in \mathbb{K}$ alors $\lambda.u \in F$

Exemple 1.4 : $\left\{ \begin{pmatrix} x \\ y \end{pmatrix}, x + y = 0 \right\} \subset \mathbb{R}^2$, $\mathbb{R} \subset \mathbb{C}$.

Proposition 1.5

Soit E un $\mathbb{K}$-espace vectoreil et $F \subset E$ un sous-espace vectoriel. Alors F est un $\mathbb{K}$-espace vectoriel.

Preuve : Exercice (il faut vérifier tous les axiomes). □

2. Combinaisons linéaires

Définition 2.1

Soient E un $\mathbb{K}$-espace vectoriel, $u_1, \ldots, u_n \in E$. Un élément de la forme $\lambda_1 u_1 + \cdots + \lambda_n u_n$ est appelé une combinaison linéaire de $u_1, \ldots, u_n$.

Exemple 2.2 : Dans $\mathbb{R}^2$, on a $\begin{pmatrix} 3 \\ 2 \end{pmatrix} = 3.\begin{pmatrix} 1 \\ 0 \end{pmatrix} + 2\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ donc $\begin{pmatrix} 3 \\ 2 \end{pmatrix}$ est combinaison linéaire de $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ et $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$.

On montre qu'une combinaison linéaire de combinaisons linéaires des u_i est une combinaison linéaire des u_i.

Définition 2.3

Soient E un $\mathbb{K}$-espace vectoriel et $X \subset E$ une partie non vide de E. L'ensemble des combinaisons linéaires d'éléments de X est un espace vectoriel (exercice). Il sera noté $\langle X \rangle$ et appelé espace vectoriel engendré par X. Si $\langle X \rangle = E$, la partie X sera appelée système générateur.

Une partie est génératrice si tout élément peut être écrit (d'au moins une manière) comme combinaison linéaire d'éléments de cette partie.

Exemple 2.4 : Dans $E = \mathbb{R}^2$, $\left\langle \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right\rangle = \left\{ \begin{pmatrix} x \\ 0 \end{pmatrix},\ x \in \mathbb{R} \right\}$.
D'autre part $\left\langle \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\rangle = \mathbb{R}^2$ donc $\left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}$ est une famille génératrice

$$\begin{pmatrix} x \\ y \end{pmatrix} = x. \begin{pmatrix} 1 \\ 0 \end{pmatrix} + y. \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

Remarquez que $\left\langle \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\rangle = E$. On a donc une autre famille génératrice.

$$\begin{pmatrix} x \\ y \end{pmatrix} = x. \begin{pmatrix} 1 \\ 1 \end{pmatrix} + (y - x). \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

Il peut y avoir beaucoup de familles génératrices.
Finalement $\left\langle \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right\rangle = E$ cela découle des deux calculs précédents. Si on rajoute un élément à une famille génératrice, on obtient une famille génératrice.
Par contre, ici on n'a plus unicité de l'écriture

$$\begin{pmatrix} x \\ y \end{pmatrix} = x. \begin{pmatrix} 1 \\ 0 \end{pmatrix} + y. \begin{pmatrix} 0 \\ 1 \end{pmatrix} = x. \begin{pmatrix} 1 \\ 1 \end{pmatrix} + (y - x). \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

Nous allons maintenant définir une propriété qui assure l'unicité de l'écriture.

Définition 2.5

Soient E un $\mathbb{K}$-espace vectoriel et $u_1, \ldots, u_n \in E$. Nous dirons que la famille $\{u_1, \ldots, u_n\}$ est libre si la propriété suivante est vérifiée :

$$\forall \lambda_1, \ldots, \lambda_n \in \mathbb{K},\ \text{si } \lambda_1.u_1 + \cdots \lambda_n.u_n = 0_E \text{ alors } \forall i \text{ on a } \lambda_i = 0.$$

Dans ce cas, on dit aussi que les vecteurs $u_1, \ldots, u_n$ sont linéairement indépendants.
Des vecteurs qui ne sont pas linéairement indépendants sont dit liés, ou linéairement dépendants.

Exemple 2.6 : Dans $\mathbb{R}^2$, la famille $\left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}$ est libre. En effet, si

$$x \begin{pmatrix} 1 \\ 0 \end{pmatrix} + y \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

alors $\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$ et donc, en regardant les coordonnées $x = 0$ et $y = 0$.

Par contre, la famille $\left\{\begin{pmatrix}1\\0\end{pmatrix},\begin{pmatrix}0\\1\end{pmatrix},\begin{pmatrix}1\\1\end{pmatrix}\right\}$ n'est pas libre. En effet on a

$$\begin{pmatrix}1\\1\end{pmatrix}-\begin{pmatrix}1\\0\end{pmatrix}-\begin{pmatrix}0\\1\end{pmatrix}=0.$$

Proposition 2.7

Soient E un espace vectoriel et $u_1,\dots,u_n\in E$. Alors la famille $\{u_1,\dots,u_n\}$ est libre si et seulement si un élément peut s'écrire au plus d'une manière comme combinaison linéaire de $u_1,\dots,u_n$.

Preuve : $\Rightarrow$ Supposons qu'un vecteur $u\in E$ possède deux écritures comme combinaison linéaire des u_i. C'est-à-dire $u=\sum\lambda_i u_i=\sum_i\lambda'_i u_i$. En regroupant tout du même côté on trouve que $\sum_i(\lambda_i-\lambda'_i)u_i=0$ mais comme la famille $\{u_i\}$ forme une famille libre, on a, pour tout i, $(\lambda_i-\lambda'_i)=0$.
$\Leftarrow$ en exercice. □

Remarque 2.8

Une famille qui contient le vecteur nul n'est jamais libre.
Une famille qui contient une partie génératrice est génératrice
Une famille contenue dans une famille libre est libre.
Une famille de vecteur est liée si et seulement si l'un de ses vecteurs s'écrit comme combinaison linéaire des autres.

3. Base et dimension

Définition 3.1

Soit E un espace vectoriel et $u_1,\dots,u_n$ une famille de vecteurs. On dit que la famille $\{u_1,\dots,u_n\}$ est une base si elle est libre et génératrice.

Exemple 3.2: Base canonique : Dans $\mathbb{R}^2$, la famille $\left\{\begin{pmatrix}1\\0\end{pmatrix},\begin{pmatrix}0\\1\end{pmatrix}\right\}$ est une base.
Plus généralement, pour tout n la famille

$$\left\{\begin{pmatrix}1\\0\\\vdots\\0\end{pmatrix},\begin{pmatrix}0\\1\\\vdots\\0\end{pmatrix}\dots,\begin{pmatrix}0\\0\\\vdots\\1\end{pmatrix}\right\}$$

est une base de $\mathbb{K}^n$. On l'appelle la base canonique de $\mathbb{K}^n$.

Proposition 3.3

Soit E un $\mathbb{K}$-espace vectoriel et $u_1,\dots,u_n$ des éléments de E. Les propriétés suivantes sont équivalentes :

(1) La famille $\{u_1,\dots,u_n\}$ est une base
(2) La famille $\{u_1,\dots,u_n\}$ est libre et maximale (i.e. si on rajoute un vecteur, elle n'est plus libre).
(3) La famille $\{u_1,\dots,u_n\}$ est génératrice et minimale (i.e. si on envlève un vecteur, elle n'est plus génératrice).

Preuve : Exercice. □

Théorème 3.4 (Non prouvé)

Tout espace vectoriel admet une base

Dans les faits, pour trouver une base, on utilise le processus décrit dans la proposition suivante qui assure que toute famille libre se laisse compléter en une base en prenant les vecteurs parmi une famille quelconque de générateur.

Proposition 3.5

Soit E un $\mathbb{K}$-espace vectoriel, $u_1, \dots, u_n$ une famille libre et $v_1, \dots, v_m$ une famille génératrice. Alors il existe des vecteurs $v_{i(n+1)}, \dots, v_{i(\ell)}$ tels que $u_1, \dots, u_n, v_{i(n+1)}, \dots, v_{i(\ell)}$ forment une base de E.

Preuve : Supposons que la famille $u_1, \dots, u_n$ ne soit pas génératrice. Alors il existe un vecteur $v_{i(n)}$ qui ne soit pas combinaison linéaire des u_i et la famille $u_1, \dots, u_n, v_{i(n)}$ est donc libre. On continue ce processus jusqu'à épuiser les v_i. □

On a une proposition duale qui dit que de tout système générateur on peut extraire une base.

Proposition 3.6

Soit E un espace vectoriel et $u_1, \dots, u_n$ une famille génératrice. Alors il existe $i(1), \dots, i(m) \in \mathbb{N}$ tels que $u_{i(1)}, \dots, u_{i(m)}$ forment une base.

Preuve : Supposons que la famille soit liée. Alors il existe un de ses vecteurs qui est combinaison linéaire des autres et on peut l'enlever (il ne rajoute rien lorsqu'on fait des combinaisons linéaires). On poursuit jusqu'à obtenir la famille soit génératrice minimale, qui sera donc une base. □

Théorème 3.7

Soit E un $\mathbb{K}$-espace vectoriel, $\{u_1, \dots, u_n\}$ une base de E et $\{v_1, \dots, v_m\}$ une famille génératrice E. Alors on a $n \leqslant m$. Si $\{v_1, \dots, v_m\}$ est de plus une base alors $m = n$.

Preuve : D'après la proposition précédente, la famille $u_2, \dots, u_n$ se laisse compléter en une base en prenant des vecteurs v_i, on a donc $\{v_{i(1)}, \dots, v_{i(r_1)}, u_2, \dots, u_n\}$ est une base. De plus, $r_1 \geqslant 1$ car la famille $u_1, \dots, u_n$ étant une base, elle est génératrice et minimale, ce qui assure que $\{u_2, \dots, u_n\}$ n'est pas génératrice et qu'il faut donc ajouter au moins un vecteur.

On recommence avec la famille $\{v_{i(1)}, \dots, v_{i(r_1)}, u_3, \dots, u_n\}$ qui se laisse compléter en une base $v_{i(1)}, \dots, v_{i(r_1)}, v_{i(r_1+1)}, \dots, v_{i(r_1+r_2)}, u_3, \dots, ..u_n$ avec $r_2 \geqslant 1$.

En itérant ce procédé, on trouve une famille

$$v_{i(1)}, \dots, v_{i(r_1)}, \dots, v_{i(r_1+\dots+r_{n-1}+1)}, \dots, v_{i(r_1+\dots+r_n)}$$

avec $r_i \geqslant 1$, et on obtient ainsi que

$$m \geqslant \sum_{i=1}^{n} r_i \geqslant \sum_{i=1}^{n} 1 = n.$$

□

Définition 3.8

Nous dirons qu'un $\mathbb{K}$-espace vectoriel est de dimension n sur $\mathbb{K}$ si l'une de ses bases (et donc toutes ses bases) possède exactement n éléments. On note $\dim_{\mathbb{K}} E = n$.

Exemple 3.9 : Pour tout n, $\dim_{\mathbb{K}} \mathbb{K}^n = n$ mais $\dim_{\mathbb{R}} \mathbb{C} = 2$ (attention aux indices !).
Si $\mathbb{R}[x]$ désigne l'ensemble des polynômes à coefficients réels alors $\dim_{\mathbb{R}} \mathbb{R}[x] = \infty$.

Proposition 3.10

Soit E un espace vectoriel de dimension n.

i) Une famille libre de vecteurs de E possédant n éléments est une base.

ii) Une famille génératrice de vecteurs de E possédant n éléments est une base.

Preuve : Exercice. □

4. Applications linéaires

Définition 4.1

Soient E et F deux $\mathbb{K}$-espaces vectoriels. Une application $f : E \to F$ sera dite linéaire si, pour tout $x, y \in E$ et tout $\lambda \in \mathbb{K}$ on a

$$f(x + \lambda y) = f(x) + \lambda f(y).$$

En particulier, on voit que $f(0_E) = f(0.0_E) = 0.f(0_E) = 0_F$.

Exemple 4.2 : L'application

$$\begin{array}{ccc} \mathbb{R}^2 & \to & \mathbb{R}^3 \\ \begin{pmatrix} x \\ y \end{pmatrix} & \mapsto & \begin{pmatrix} 3x + 4y \\ y \\ -x \end{pmatrix} \end{array}$$

est linéaire. De même que l'application

$$\begin{array}{ccc} \mathbb{R}[X] & \to & \mathbb{R}[X] \\ P & \mapsto & P'. \end{array}$$

Définition 4.3

Pour toute application linéaire $f : E \to F$, l'ensemble

$$\mathrm{Im}(f) = \{y \in F, \exists x \in E \text{ tel que } f(x) = y\}$$

sera appelé image de f et l'ensemble

$$\ker f = \{x \in E, f(x) = 0_F\}$$

noyau de f.

Proposition 4.4

Soit $f : E \to F$ une application linéaire. Alors $\ker f$ est un sous-especae vectoriel de E et $\mathrm{Im} f$ est un sous-espace vectoriel de F

Preuve : Exercice. □

Proposition 4.5

Soit $f : E \to F$ une appliction linéaire. Alors f est injective si et seulement si $\ker f = \{0_E\}$.

Preuve : Exercice. □

Théorème 4.6 (du rang)

Soit $f\colon E \to F$ une application linéaire et supposons que E soit de dimension finie. Alors

$$\dim E = \dim \ker f + \dim \mathrm{Im} f$$

Preuve : L'espace vectoriel $\mathrm{Im}(f)$ possède une famille génératrice finie car il suffit de prendre l'image d'une base. On peut donc en extraire une base $f_1, \ldots, f_n$ puis, par définition, trouver des vecteurs $g_1, \ldots, g_n \in E$ tels que $f(g_i) = f_i$ pour tout i.

Considérons d'autre part une base $e_1, \ldots, e_m$ de $\ker f$ qui est de dimension finie car sous-espace vectoriel de E.

Il s'agit alors de montrer que $\{e_1, \ldots, e_m, g_1, \ldots, g_n\}$ est une base de E. Montrons tout d'abord que c'est une famille génératrice : soit $x \in E$. Comme $f_1, \ldots, f_n$ est une base de $\mathrm{Im} f$, il existe $\lambda_1, \ldots, \lambda_n \in \mathbb{K}$ tels que $f(x) = \lambda_1 f_1 + \ldots + \lambda_n f_n$.
On voit alors que $f(x - \sum_i \lambda_i g_i) = 0_F$ et donc que $x - \sum_i \lambda_i g_i \in \ker f$. Ainsi, il existe $\mu_1, \ldots, \mu_m \in \mathbb{K}$ tel que $x - \sum_i \lambda_i g_i = \sum_j \mu_j e_j$, ce qui prouve qu'on a bien une famille génératrice de E.
Montrons maintenant que c'est une famille libre et considérons pour cela des scalaires $\mu_1, \ldots, \mu_m, \lambda_1, \ldots, \lambda_n \in \mathbb{K}$ tels que $\sum_j \mu_j e_j + \sum_i \lambda_i g_i = 0_E$.
Prenant l'image par f, on trouve que

$$0_F = f\left(\sum_j \mu_j e_j + \sum_i \lambda_i g_i\right) = \sum_j \mu_j f(e_j) + \sum_i \lambda_i f(g_i) = \sum_i \lambda_i f_i$$

et comme les f_i forment une famille libre, on trouve que les λ_i sont tous nuls.
Par suite, on a $\sum_j \mu_j e_j = 0_E$ et comme les e_j forment une famille libre, les μ_j sont également nuls. □

5. La méthode du pivot de Gauss

Très souvent, on a besoin de résoudre des équations linéaires. La méthode suivante est un algorithme simple et efficace qui permet de le faire. Par exemple, essayons de voir si le vecteur $\begin{pmatrix} -4 \\ 13 \\ 2 \end{pmatrix}$ est combinaison linéaire de $\begin{pmatrix} 1 \\ -1 \\ 1 \end{pmatrix}$, $\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$ et $\begin{pmatrix} 1 \\ 5 \\ 6 \end{pmatrix}$.
On cherche donc $a, b, c \in \mathbb{R}$ tels que

$$a\begin{pmatrix} 1 \\ -1 \\ 1 \end{pmatrix} + b\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} + c\begin{pmatrix} 1 \\ 5 \\ 6 \end{pmatrix} = \begin{pmatrix} -4 \\ 13 \\ 2 \end{pmatrix}.$$

Cela équivaut à regarder le sysème

$$\left\{\begin{array}{rcrcrcl} a & + & b & + & c & = & -4 \\ -a & + & 2b & + & 5c & = & 13 \\ a & + & 3b & + & 6c & = & 2. \end{array}\right.$$

On cherche à éliminer certains termes pour se ramener à une forme triangulaire. Pour cela, on supprime tout les a des deux dernières lignes à l'aide de la première

$$\left\{\begin{array}{rcrcrcll} a & + & b & + & c & = & -4 & \\ & & 3b & + & 6c & = & 9 & L_2 \leftarrow L_2 + L_1 \\ & & 2b & + & 5c & = & 6 & L_3 \leftarrow -L_3 - L_1. \end{array}\right.$$

Ensuite, on essaye de supprimer les b dans la dernière ligne en utilisant la deuxième

$$\left\{\begin{array}{rcrcrcl} a & + & b & + & c & = & -4 \\ & & 3b & + & 6c & = & 9 \\ & & & & c & = & 0 \end{array}\right. \qquad L_3 \leftarrow L_3 - \tfrac{2}{3}L_1.$$

On peut alors trouver c, puis b, et enfin a :

$$\left\{\begin{array}{rcl} c & = & 0 \\ b & = & 3 \\ a & = & -7. \end{array}\right.$$

6. Structure d'espace vectoriel sur l'ensemble des matrices

Soient $\mathbb{K}$ un corps, $m, n \in \mathbb{N}$. Une matrice de type (m, n) à coefficients dans $\mathbb{K}$ est la donnée de mn éléments de $\mathbb{K}$. On représentera une matrice sous la forme d'un tableau

$$m \text{ lignes} \left\{ \overbrace{\begin{pmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,n} \\ \cdots & \cdots & & \cdots \\ a_{m,1} & a_{m,2} & \dots & a_{m,n} \end{pmatrix}}^{n \text{ colonnes}} \right.$$

Exemple 6.1 : la matrice $0_{m,n}$

$$m \text{ lignes} \left\{ \overbrace{\begin{pmatrix} 0 & 0 & \dots & 0 \\ \vdots & \dots & & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix}}^{n \text{ colonnes}} \right.$$

qui est appelée la matrice nulle.

Lorsque $m = n$, les matrices de type (m, n) seront appelées matrices carrées d'ordre n.

Exemple 6.2 : La matrice

$$I_n = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix}$$

appelée matrice identité.
Plus généralement, une matrice de la forme

$$\begin{pmatrix} \alpha_1 & 0 & 0 & \cdots & 0 \\ 0 & \alpha_2 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & \alpha_{n-1} & 0 \\ 0 & 0 & \cdots & 0 & \alpha_n \end{pmatrix}$$

est appelée matrice diagonale.

Encore plus généralement, une matrice de la forme

$$\begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} & \cdots & a_{1,n} \\ 0 & a_{2,2} & a_{2,3} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & a_{n-1,n-1} & a_{n-1,n} \\ 0 & 0 & \cdots & 0 & a_{n,n} \end{pmatrix}$$

est appelée matrice triangulaire supérieure.

Nous allons maintenant définir une addition et une multiplication par un scalaire sur l'ensemble $M_{m,n}(\mathbb{K})$ des matrices de type (m,n) à coefficients dans $\mathbb{K}$.

Soient A et B deux éléments de $M_{m,n}(\mathbb{K})$ et écrivons $A = (a_{i,j})_{1\leqslant i\leqslant m, 1\leqslant j\leqslant n}$ et $B = (b_{i,j})_{1\leqslant i\leqslant m, 1\leqslant j\leqslant n}$.
On définit $A+B$ comme étant la matrice

$$A + B = (a_{i,j} + b_{i,j})_{1\leqslant i\leqslant m, 1\leqslant j\leqslant n}.$$

Comme pour les vecteurs, on fait l'addition coordonnée par coordonnée. En particulier, il faut que les deux matrices aient même type !
Pour tout $\lambda \in \mathbb{K}$, on notera λA la matrice

$$\lambda.A = (\lambda a_{i,j})_{1\leqslant i\leqslant m, 1\leqslant j\leqslant n}.$$

On multiplie chaque coordonnées par λ.

Proposition 6.3

Le triplet $(M_{m,n}(\mathbb{K}), +, .)$ est un $\mathbb{K}$-espace vectoriel d'élément neutre la matrice nulle et de dimension mn.

Preuve : Exercice. □

7. Multiplication de matrices

Donnons-nous une matrice A de type (m,n) et une matrice B de type (n,p) : nous allons définir le produit $A.B$. Pour cela écrivons $A = (a_{i,j})_{1\leqslant i\leqslant m, 1\leqslant j\leqslant n}$ et $B = (b_{j,k})_{1\leqslant j\leqslant n, 1\leqslant k\leqslant p}$. On définit $A.B$ comme une matrice de type (m,p) égale $(c_{i,k})_{1\leqslant i\leqslant m, 1\leqslant k\leqslant p}$ avec

$$c_{i,k} = \sum_{j=1}^{n} a_{i,j}.b_{j,k}.$$

Formellement, on l'écrit sous la forme suivante :

$$\begin{pmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,n} \\ \dots & \dots & & \dots \\ \dots & \dots & & \dots \\ \dots & \dots & & \dots \\ \dots & \dots & & \dots \\ \dots & \dots & & \dots \\ a_{m,1} & a_{m,2} & \dots & a_{m,n} \end{pmatrix} \quad \begin{pmatrix} b_{1,1} & b_{1,2} & \dots & b_{1,p} \\ \dots & \dots & & \dots \\ b_{n,1} & b_{n,2} & \dots & b_{n,p} \end{pmatrix}$$

$$\begin{pmatrix} c_{1,1} & c_{1,2} & \dots & c_{1,p} \\ \dots & \dots & & \dots \\ \dots & \dots & & \dots \\ \dots & \dots & & \dots \\ \dots & \dots & & \dots \\ \dots & \dots & & \dots \\ c_{m,1} & c_{m,2} & \dots & c_{m,p}. \end{pmatrix}$$

Pour calculer $c_{1,1}$ on va utiliser les coefficients de A qui sont dans la même ligne, et les coefficients de B qui sont dans la même colonne, ainsi

$$c_{1,1} = a_{1,1}.b_{1,1} + a_{1,2}.b_{2,1} + a_{1,3}.b_{3,1} + \dots.$$

Exemple 7.1 :

$$\begin{pmatrix} 2 & 1 & 1 \\ -1 & -5 & 4 \end{pmatrix} \quad \begin{pmatrix} 3 & 4 & -2 & 1 \\ 4 & -2 & -1 & 0 \\ 0 & 1 & 2 & -1 \end{pmatrix}$$

$$\begin{pmatrix} 10 & 7 & -3 & 1 \\ -23 & 10 & 15 & -5 \end{pmatrix}$$

Proposition 7.2

La multiplication de matrices vérifie les propriétés suivantes

(1) Pour toute matrice A de type (m,n), toute matrice B de type (n,p) et tout scalaire λ on a
$$A.(\lambda B) = \lambda(AB) = (\lambda A)B.$$
(2) Pour toutes matrices A, B de type (m,n) et toute matrice C de type (n,p) on a $(A+B).C = A.C + B.C$ (distributivité à gauche).
(3) Pour toute matrice A de type (m,n) et toutes matrices B, C de type (n,p) on a $A.(B+C) = A.B + A.C$ (distributivité à droite).
(4) Pour toute matrice A de type (m,n), toute matrice B de type (n,p) et toute matrice C de type (p,q) on a $A.(B.C) = (A.B).C$ (associativité).
(5) Pour toute matrice A de type (m,n) on a $I_m.A = A.I_n = A$.

Preuve : : Exercice. □

Attention : Si on a une matrice A de type (m,n) et une matrice B de type (n,p) alors on peut parler de $A.B$ mais pas de $B.A$ en général. Pour cela, il faut que $p = n$.

Exemple 7.3 : Prenons $A = \begin{pmatrix} 3 & 4 & -2 & 1 \\ 4 & -2 & -1 & 0 \\ 0 & 1 & 2 & -1 \end{pmatrix}$ et $B = \begin{pmatrix} -1 & 2 & 4 \\ 4 & 0 & -1 \\ -1 & 0 & 1 \\ 2 & -7 & 2 \end{pmatrix}$.

Alors $A.B$ est une matrice de type $(3,3)$
$$A.B = \begin{pmatrix} 17 & -1 & 8 \\ -11 & 8 & 17 \\ 0 & 7 & -1 \end{pmatrix}$$
tandis que $B.A$ est une matrice de type $(4,4)$
$$AB = \begin{pmatrix} 5 & -4 & 8 & -5 \\ 12 & 15 & -10 & 5 \\ -3 & -3 & 4 & -2 \\ -22 & 24 & 7 & 0. \end{pmatrix}$$
Même lorsque $m = n = p$ (auquel cas $A.B$ et $B.A$ sont deux matrices de type (m,m), i.e. matrices carrées d'ordre m) on n'a pas égalité en général
Si $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ et $B = \begin{pmatrix} -1 & 2 \\ -3 & 1 \end{pmatrix}$ Alors $A.B = \begin{pmatrix} -7 & 4 \\ -15 & 10 \end{pmatrix}$ et $B.A = \begin{pmatrix} 5 & 6 \\ 0 & -2 \end{pmatrix}$.

---

8. Quelques objets associés à une matrice

Soit $M \in M_{m,n}(\mathbb{K})$. On définit une application linéaire $f_M : \mathbb{K}^n \to \mathbb{K}^m$ par
$$f_M(X) = MX.$$
Les propriétés du produit de matrices vues ci-dessus font que cette application est linéaire, le produit de matrice correspond alors à la composition des applications linéaires, i.e. pour toutes matrices M et N telles que le produit à un sens, on a $f_M \circ f_N = f_{MN}$.

Définissons maintenant un sous-ensemble de $\mathbb{K}^n$ par
$$K_M = \{X \in \mathbb{K}^n \mid MX = 0_{\mathbb{K}^m}\} = \ker f_M.$$

L'ensemble K_M est alors un sous-espace vectoriel de $\mathbb{K}^n$.

Exemple 8.1 : Si $M = (1, 2, 3)$ alors

$$K_M = \left\{ \begin{pmatrix} x \\ y \\ z \end{pmatrix} | x + 2y + 3z = 0 \right\}.$$

Une telle représentation d'un sous-espace vectoriel est appelée représentation implicite. L'avantage d'une telle représentation est qu'il est aisé de vérifier si un vecteur donné appartient à cet espace vectoriel (il suffit de le multiplier à gauche par la matrice M), il est toutefois plus compliqué de trouver de tels vecteurs car il faut résoudre un système linéaire.

Définissons maintenant un sous-ensemble de $\mathbb{K}^m$ par

$$I_M = \{Y \in \mathbb{K}^m \mid \exists X \in \mathbb{K}^n \text{ tel que } Y = MX\} = \mathrm{Im} f_M.$$

Utilisant de nouveau les propriétés du produit de matrices, on montre que cet ensemble est un sous-espace vectoriel.

Exemple 8.2 : Considérons la matrice

$$P = \begin{pmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{pmatrix}.$$

On a alors

$$I_M = \left\{ \begin{pmatrix} x + 4y \\ 2x + 5y \\ 3x + 6y \end{pmatrix}, x, y \in \mathbb{K} \right\}.$$

Une telle représentation est appellée représentation paramétrique. Avec une telle description, il est aisé de produire des vecteurs (remplacer les x, y par des valeurs) mais plus difficile de tester si un vecteur particulier est dans le sous-espace vectoriel.

Il peut donc être utile de passer d'une représentation à l'autre, ce qui peut se faire à l'aide du pivot de Gauss.

Exercice 8.3

Soit $M = \begin{pmatrix} 1 & 1 & 4 & 4 \\ 2 & 1 & 4 & 2 \end{pmatrix}$. *Donner une représentation paramétrique de* K_M.

Soit $P = \begin{pmatrix} 4 & 10 \\ -4 & -6 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}$. *Donner une représentation implicite de* I_P.

9. Inverse d'une matrice

Définition 9.1

Soit A une matrice carrée de type (n, n). On dira que A est inversible s'il existe une matrice carrée de type (n, n) telle que $B.A = A.B = I_n$. La matrice B est alors appelée l'inverse de A.

Proposition 9.2

Soit A une matrice carrée inversible de type (n,n) et M une matrice de type (n,m). Si $A.M = 0$ alors $M = 0$.

Preuve : Notons B l'inverse de A et multiplions à gauche par B. On a donc $B.A.M = 0$ (l'ordre dans lequel on multiplie ne change pas le résultat car la multiplication est associative).
Or $B.A = I_n$ et $I_n.M = M$, on trouve donc que $M = 0$. □

On prendra garde au fait que si A n'est pas inversible, alors ce résultat est faux

Exemple 9.3 :

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

Par contre, si le produit d'une matrice avec *tous* les vecteurs de la bonne taille est nul, alors la matrice elle-même est nulle.

Lemme 9.4

Soit A une matrice de type (m,n). supposons que, pour tout $X \in \mathbb{K}^n$ on a $MX = 0_{\mathbb{K}^m}$. Alors $M = 0$.

Preuve : Remplaçant X par les vecteurs de la base canonique, on trouve que les colonnes de M sont toutes nulles, et donc que M est nulle. □

Proposition 9.5

Soit A une matrice carrée d'ordre n. Notons $f_1, \dots, f_n$ les vecteurs obtenus à partir des colonnes de A. Alors la matrice A est inversible seulement si la famille $f_1, \dots, f_n$ est une base (ou, de manière équivalente, si $f_1, \dots, f_n$ est libre où génératrice).

Preuve : Dans les faits, si $e_1, \dots, e_n$ désigne la base canonique, on a $f_i = A.e_i$.
Supposons donc la matrice inversible. Nous allons montrer que la famille f_i est libre. Pour cela, supposons avoir une combinaison linéaire nulle $\sum_i \lambda_i f_i = 0$. Par définition, on a donc

$$0 = \sum_i \lambda_i A.e_i = \sum_i A.(\lambda_i e_i) = A.\left(\sum_i \lambda_i e_i\right).$$

D'après la proposition précédente, on trouve que $\sum_i \lambda_i e_i = 0$ mais comme les e_i forment une base (en particulier une famille libre) on trouve que pour tout i on a $\lambda_i = 0$. □

Nous verrons plus tard (lors de l'étude des matrices de changement de base) que la réciproque de cette proposition est vraie.

Soit $A = (a_{i,j})_{i,j}$ une matrice. Pour calculer un inverse (s'il existe) on procède de la manière suivante : si A possède un inverse B et qu'on a $AX = Y$ alors on aura $BY = BAX = X$. On prend donc un vecteur quelconque $X = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$ et un vecteur $Y = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix}$ et on cherche B tel que $BX = Y$. On essaie alors de résoudre $A.X = Y$ en utilisant le pivot de Gauss.

Au début, on aura donc

$$\begin{array}{rcl} a_{1,1}x_1 + a_{1,2}x_2 + \ldots + a_{1,n}x_n & = & y_1 \\ a_{2,1}x_2 + a_{2,2}x_2 + \ldots + a_{2,n}x_n & = & y_2 \\ \vdots & = & \vdots \\ a_{n,1}x_n + a_{n,2}x_2 + \ldots + a_{n,n}x_n & = & y_n \end{array}$$

Après l'avoir mis sous la forme triangulaire, on trouvera

$$\begin{array}{rrrcl} b_{1,1}x_1+ & b_{1,2}x_2+ & \ldots+ & b_{1,n}x_n & = & c_{1,1}y_1 + c_{1,2}y_2 + \ldots + c_{1,n}y_n \\ & b_{2,2}x_2+ & \ldots+ & b_{2,n}x_n & = & c_{2,1}y_1 + c_{2,2}y_2 + \ldots c_{2,n}y_n \\ & & \vdots & = & \vdots & \\ & & & b_{n,n}x_n & = & c_{n,1}y_1 + c_{n,2}y_2 + \ldots c_{n,n}y_n \end{array}$$

et si tous les éléments de la diagonale sont non nuls, alors on pourra résoudre. Si l'un des éléments de la diagonale est nul alors on ne pourra pas résoudre et donc la matrice n'est pas inversible.
On se place donc dans le cas ou tous les éléments diagonaux sont non nuls et on fini la résolution du système. On obtient donc finalement

$$\begin{array}{rcl} x_1 & = & d_{1,1}y_1 + d_{1,2}y_2 + \ldots + d_{1,n}y_n \\ x_2 & = & d_{2,1}y_1 + d_{2,2}y_2 + \ldots + d_{2,n}y_n \\ \vdots & = & \vdots \\ x_n & = & d_{n,1}y_n + d_{n,2}y_2 + \ldots + d_{n,n}y_n \end{array}$$

les $d_{i,j}$ sont alors les entrées de la matrice inverse de A.

Exercice 9.6
Calculer l'inverse de la matrice

$$\begin{pmatrix} 1 & 0 & -1 \\ 2 & -2 & 1 \\ -1 & -1 & 2 \end{pmatrix}$$

10. Matrice de passage

Soit E un espace vectoriel de dimension n sur $\mathbb{K}$. Considérons $e = (e_1, \ldots, e_n)$ et $f = (f_1, \ldots, f_n)$ deux bases de E. Tout vecteur $X \in E$ peut s'écrire sous la forme

$$X = \sum_i \lambda_i e_i = \sum_j \mu_j f_j.$$

Les (λ_i) s'apellent les coordonnées de X dans la base e et les μ_j sont les coordonnées de X dans la base f. Nous souhaitons voir comment passer des coordonnées dans la base e aux coordonnées dans la base f.

Pour cela écrivons, pour tout j, $f_j = \sum_i \alpha_{i,j} e_i$. On a alors

$$\begin{array}{rcll} X & = & \displaystyle\sum_j \mu_j f_j & (1) \\ & = & \displaystyle\sum_j \mu_j \sum_i \alpha_{i,j} e_i & (2) \\ & = & \displaystyle\sum_{i,j} \mu_j \alpha_{i,j} e_i & (3) \\ & = & \displaystyle\sum_i \left(\sum_j \alpha_{i,j}\mu_j \right) e_i & (4) \end{array}$$

Par unicité de la décomposition comme combinaison linéaire, on trouve que $\lambda_i = \sum_j \alpha_{i,j}\mu_j$.
On définit alors la matrice $P_{f,e}$ par $P_{f,e} = P = (\alpha_{i,j})_{1\leqslant i\leqslant n, 1\leqslant j\leqslant n}$. Ainsi, notant Λ le vecteur colonne de coordonnées λ_i et M le vecteur colonne de coordonnées μ_j on voit que

$$\Lambda = PM.$$

La matrice $P_{f,e}$ permet donc de passer des coordonnées dans la base f_j aux coordonnées dans la base e_i : c'est la matrice de passage de e à f (les colonnes de la matrice $P_{f,e}$ sont les coordonnées des f_j dans la base e).

Attention, $P_{f,e}$ multipliée par des coordonnées dans f donne des coordonnées dans e.

Proposition 10.1
Soient E un espace vectoriel de dimentsion n et e, f, g trois bases de E.

i) $P_{e,e} = I_n$
ii) $P_{f,g}P_{e,f} = P_{e,g}$
iii) $P_{e,f}P_{f,e} = I_n$ en particulier, $P_{e,f} = P_{f,e}^{-1}$.

Preuve : il suffit de considérer l'effet de la multiplication sur le vecteur des coordonnées dans la base e. □

Exemple 10.2 : Trouver les matrices de passage pour les bases $e_1 = \begin{pmatrix} 1 \\ 2 \\ 1 \end{pmatrix}, e_2 = \begin{pmatrix} 0 \\ -2 \\ -1 \end{pmatrix}, e_3 = \begin{pmatrix} -1 \\ 1 \\ 2 \end{pmatrix}$ et $f_1 = \begin{pmatrix} 3 \\ 1 \\ 2 \end{pmatrix}, f_2 = \begin{pmatrix} 5 \\ 1 \\ 3 \end{pmatrix}, f_3 = \begin{pmatrix} 4 \\ 1 \\ 2 \end{pmatrix}$
En calculant les décompositions des vecteurs f_i dans la base e on trouve

$$f_1 = 4e_1 + 4e_2 + e_3 \quad f_2 = \frac{20}{3}e_1 + 7e_2 + \frac{5}{3} \quad f_3 = 5e_1 + 5e_2 + e_3.$$

On peut donc écrire la matrice $P_{f,e} = \begin{pmatrix} 4 & 20/3 & 5 \\ 4 & 7 & 5 \\ 1 & 5/3 & 1 \end{pmatrix}$.
Si le vecteur $\begin{pmatrix} x \\ y \\ z \end{pmatrix}$ représente les coordonnées d'un vecteur u dans la base f alors $P_{f,e}\begin{pmatrix} x \\ y \\ z \end{pmatrix}$ représente les coordonnées de u dans la base e. Par exemple $P_{f,e}\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 4 \\ 4 \\ 1 \end{pmatrix}$ et ce sont les coordonnées de f_1 dans la base e.
En inversant la matrice, on trouve que $P_{f,e} = \begin{pmatrix} 4 & -5 & 5 \\ -3 & 3 & 0 \\ 1 & 0 & -4 \end{pmatrix}$

Et on a $P_{e,f}\begin{pmatrix}1\\0\\0\end{pmatrix} = \begin{pmatrix}4\\-3\\1\end{pmatrix}$ et $4f_1 - 3f_2 + f_3 = \begin{pmatrix}1\\2\\1\end{pmatrix}$ donc on a bien obtenu les coordonnées de e_1 dans la base f (sachant que $\begin{pmatrix}1\\0\\0\end{pmatrix}$ sont les coordonnées de e_1 dans la base e).

11. Transposée d'une matrice

Soit A une matrice de type (m,n), $A = (a_{i,j})_{1\leqslant i\leqslant m, 1\leqslant j\leqslant n}$. On appelle transposée de A et on note ${}^tA$ la matrice de type (n,m) définie par ${}^tA = (a_{i,j})_{1\leqslant j\leqslant n, 1\leqslant i\leqslant m}$.

Proposition 11.1

i) Soit A une matrice de type (m,n). alors ${}^{tt}A = A$.

ii) Pour toutes matrice A et B de type (m,n) on a
$$ {}^t(A+B) = {}^tA + {}^tB.$$

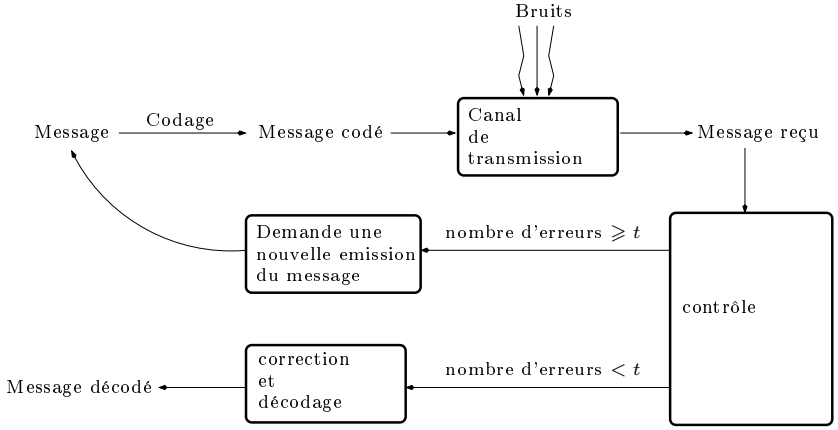
iii) Pour toute matrice A de type (m,n) et toute matrice B de type (n,p) on a ${}^t(AB) = {}^tB{}^tA$.

iv) Pour toute matrice carrée A d'ordre m on a ${}^t(A^{-1}) = ({}^tA)^{-1}$

Preuve : La première assertion est évidente. Passons à la deuxième $A = (a_{i,j})$, $B = (b_{j,k})$, $AB = (\sum_j a_{i,j}b_{j,k})$ et ${}^tB{}^tA = (\sum_j b_{k,j}a_{j,i})$.
Pour la dernière assertion, on remarque que ${}^tI_n = I_n$ et donc le résultat découle de l'assertion précédente.

12. Les codes correcteurs

Le but des codes correcteurs est d'assurer l'intégrité de l'information, ils doivent ainsi détecter et corriger si possible des erreurs dans un signal lors de sa transmission (la plupart des canaux ne sont pas complètement fiable, il arrive souvent qu'un signal soit perturbé et que sa réception ne soit pas fidèle au signal de d'origine, e.g. radio, fibre optique, ...) ou bien lors de son stockage (le matériau utilisé pour le stockage voit ses propriétés diminuer avec le temps, introduisant ainsi des erreurs, e.g. disque compact, RAM, ...).



Pour avoir une chance de corriger le message, il est nécessaire de connaître le nombre d'erreurs possibles pour un canal donné afin de pouvoir adapter le codage en fonction de la fiabilité.

On considère alors un ensemble de message non codé D, un ensemble de code C et une application $D \to C$ injective (l'injectivité est nécessaire pour ne pas perdre d'information, ce qui est tout de même le but premier de la théorie !).

12.1. Exemples et définitions. Nous ne considérerons ici que des codes binaires, ce qui suppose éventuellement une transformation préalable. Les deux ensembles D et C seront donc des sous-ensembles d'espaces vectoriels sur $\mathbb{F}_2$. De plus, C sera toujours (ici) un *code linéaire*, c'est-à-dire un sous-espace vectoriel de $\mathbb{F}_2^n$, pour un certain n. L'entier n sera appelé la *longueur* du code C et la *dimension* de C sera sa dimension en tant qu'espace vectoriel, le code C contient donc 2^k éléments.

Exemple 12.1: doublement de l'information : L'exemple le plus simple est le doublement de l'information, qui consiste simplement à répéter le message. Ainsi, les messages de 2 bits sont codés par des codes de longueur 4 et on a

$$\begin{array}{ccc} 00 & \to & 0000 \\ 01 & \to & 0101 \\ 10 & \to & 1010 \\ 11 & \to & 1111 \end{array}$$

Ce codage permet de détecter une erreur : recevant le code 1000, on sait qu'il y a automatiquement eu un problème. Par contre, on ne peut pas le réparer car il pourrait correspondre à 1010 ou bien à 0000, il est donc nécessaire de demander un renvoi du message.

Exemple 12.2: Checksum : Il est en fait possible d'être plus efficace pour un même résultat, et de coder des messages de 2 bits en des codes de longueurs 3 tout en gardant la même capacité de détection. Ceci est obtenu en ajoutant comme dernier bit la somme (dans $\mathbb{F}_2$) de tous les autres

$$\begin{array}{ccc} 00 & \to & 000 \\ 01 & \to & 011 \\ 10 & \to & 101 \\ 11 & \to & 110 \end{array}$$

Recevant le code 001, on sait alors qu'il y a une erreur mais on ne peut toujours pas le corriger.

Exemple 12.3: Triplement de l'information : Afin de pouvoir corriger d'éventuelles erreurs, il est nécessaire d'ajouter encore de l'information. L'exemple le plus simple de code *correcteur* est obtenu en triplant les messages

$$\begin{array}{ccc} 00 & \to & 000000 \\ 01 & \to & 010101 \\ 10 & \to & 101010 \\ 11 & \to & 111111 \end{array}$$

Supposant qu'il y a au plus une erreur dans la transmission du code 011101, on peut automatiquement le corriger en 010101 car les autres demanderaient au moins deux erreurs !

Ce dernier code permet *a priori* de détecter plus d'erreurs qu'il n'est possible d'en corriger et, pour savoir exactement combien, il convient d'introduire quelques concepts supplémentaires.

Définition 12.4: Distance de Hamming

Soit C un code de longueur n et x, y des éléments de C de sorte que $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n)$. La distance de Hamming de x à y, notée $d(x, y)$, est le nombre d'indices en lesquels x et y diffèrent, i.e.

$$d(x, y) = \operatorname{card}\{i \in \{1, \ldots, n\}, x_i \neq y_i\}.$$

La distance de Hamming du code C est le minimum des distances entre deux mots distincts

$$d = \min_{x,y \in C, x \neq y} d(x, y).$$

Définition 12.5: Type d'un code

Soit C un code. Le type de C est le triplet (n, k, d) composé de la longueur de C, de sa dimension et de sa distance de Hamming.

Proposition 12.6

La distance de Hamming vérifie les propriétés suivantes

i) pour tous $x, y \in C$ on a $d(x, y) = 0$ si et seulement si $x = y$,

ii) pour tous $x, y, z \in C$ on a $d(x, z) \leqslant d(x, y) + d(y, z)$,

iii) pour tous $x, y, z \in C$ on a $d(x, y) = d(x + z, y + z)$,

iv) on a $d = \min_{x \in C, x \neq 0} d(x, 0)$.

Exercice 12.7

Calculer la distance de Hamming des trois codes présentés ci-dessus.

Définition 12.8

Nous dirons qu'un code C est t-correcteur s'il permet de corriger au moins t erreurs.

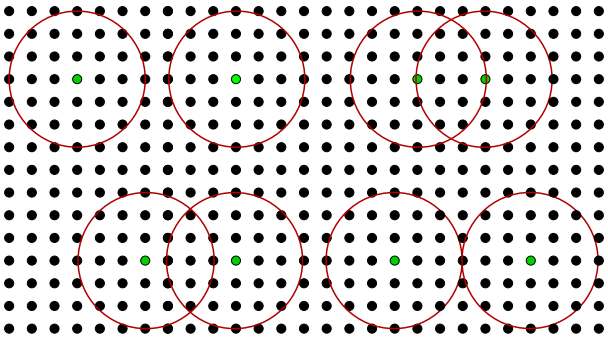
Théorème 12.9

Soit C un code de distance de Hamming d, alors C est t-correcteurs pour tout t vérifiant

$$d \geqslant 2t + 1$$

Si $t < d$, alors le code peut détecter t erreurs mais pas les corriger.

Preuve : La démonstration est en fait purement géométrique



Dans le premier cas, deux boules de rayon t centrées en des points distincts de C sont disjointes. Il est donc possible de corriger (partie en haut à gauche de la figure).

Si $d > t$ alors on peut détecter t erreurs car deux points de C ne sont jamais dans la même boule de rayon t (partie en bas à gauche de la figure).
Les autres figures représentent les cas limites : $t = d$ (en haut à droite) où on ne peut pas forcément détecter qu'il y a une erreur, ou bien $t = 2d$ (en bas à droite) où on ne peut pas forcément corriger les erreurs détectées. □

Théorème 12.10 (Borne de Singleton)

Pour tout code C de type (n, k, d) on a

$$d + k \leqslant n + 1$$

Preuve : Considérons l'application linéaire ϕ consistant à oublier les $n - k + 1$ dernières coordonnées. En particulier, $\dim \mathrm{Im}\phi = k - 1$, ce qui impose que $\dim \phi(C) \leqslant k - 1$.
D'après le théorème du rang, on a alors $\dim \ker \phi|_C \geqslant 1$, i.e. l'application ϕ n'est pas injective sur C. On en déduit alors qu'il y a au moins deux codes de C qui ont même image, c'est-à-dire qu'ils ont les mêmes $k - 1$ premières coordonnées et diffèrent donc au plus de $n - k + 1$ coordonnées, i.e. $d \leqslant n - k + 1$. □

Cette borne signifie que, à dimension du code fixé, on ne peut pas avoir une capacité de correction très élevée tout en conservant une petite longueur.

12.2. Matrice génératrice et décodage. Il est possible d'encoder toute l'information d'un code dans une matrice appelée *matrice génératrice*. En effet, étant donné un code linéaire C de type (n, k, d), choisissons une base $e_1, \ldots, e_k$ de C dans $\mathbb{F}_2^n$ (il y a ici vraiment un choix !) et considérons la matrice M dont les colonnes sont les coordonnées des e_i dans la base canonique de $\mathbb{F}_2^n$, elle est donc de type (n, k).
Pour le doublement de l'information, si on choisit la base $e_1 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}$ et $e_2 = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}$ alors on trouve la matrice

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

Cette matrice peut aussi servir pour l'encodage : si les messages sont les éléments de $\mathbb{F}_2^k$ alors on peut définir une application de codage

$$\begin{array}{rccc} f_M & : & \mathbb{F}_2^k & \to & \mathbb{F}_2^n \\ & & X & \mapsto & M.X \end{array}$$

Par définition, cette application est injective et son image est très exactement l'ensemble des codes de C et nous donne ainsi une représentation paramétrique de cet espace vectoriel.
Le calcul de la distance de Hamming demande un peu de travail car il faut tout d'abord décrire tous les codes de C.

Exemple 12.11: Code de Hamming $(7, 4)$: L'un des codes les plus importants (au moins historiquement) est le code de Hamming $(7, 4)$ inventé en 1950 par Richard Hamming dans les laboratoires Bell. Une matrice génératrice pour ce

code est

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

Exercice 12.12

Calculer la distance de Hamming du code de Hamming $(7, 4)$ *et déterminer*

i) son type,

ii) sa capacité de correction,

iii) sa capacité de détection d'erreurs,

iv) vérifier la borne de Singleton.

Proposition 12.13

Étant donné une matrice M de type (n, k) telle que f_M est injective. Il existe une matrice N de type (k, n) telle que $NM = I_k$.

Preuve : Exercice. □

Ainsi, si X est un mot du code C, on voit que NX est l'unique antécédent de X par l'application f_M. La matrice N permet ainsi le décodage du code X.

12.3. Matrice de contrôle et syndrome. Étant donné un code C, supposons avoir construit une matrice P telle que $K_P = C$: on a ainsi une description implicite de C. La matrice P est appelée *matrice de contrôle*, et elle permet de voir qu'un élément X de $\mathbb{F}_2^n$ est un code de C si et seulement si $PX = 0$. Si tel est le cas, on peut alors le décoder, sinon il faut essayer de le corriger (si possible) et renvoyer le code correspondant.
Supposons de plus que le code C est t-correcteur et donnons nous un message reçu X. Nous appellerons *syndrome* de X la quantité PX.
Si X est à une distance $\leqslant t$ d'un mot Y du code C, alors x doit être corrigé en Y. De plus, on a $P(X - Y) = PX - PY = PX$. Par suite, la quantité $e = X - Y$ est dans la boule $B \subset \mathbb{F}_2^n$ de centre 0 et de rayon t, et donc PX est dans l'image de B par la multiplication par P.

Considérons donc une table T contenant tout les couples (e, Pe) pour $e \in B$.
Cette table étant construite et recevant le message X, les étapes sont les suivantes

i) calculer le syndrome PX ;

ii) si $PX = 0$, alors il n'y a rien à corriger et le message est donné par NX ;

iii) si $PX \neq 0$, chercher dans la table T s'il existe $e \in \mathbb{F}_2^n$ tel que $Pe = PX$;

iv) si c'est le cas, alors le message d'origine est $N(X + e)$;

v) dans le cas contraire, il y a trop d'erreurs et on ne peut pas décoder.

12.4. Complexité. Dans le cas de code de petite longueur, la complexité n'a pas vraiment de sens car toutes les données sont de petite taille et il est possible de corriger très vite un code.
À l'opposé, lorsque la longueur du code augmente, on peut montrer que le problème devient NP-complet pour un code "générique" (très peu probable qu'il existe un algorithme permettant de trouver les solutions en temps polynomial en fonction des données du problème).

13. Retour sur la cryptographie

Il est possible de construire des méthodes d'encryptage en utilisant des codes correcteurs, c'est ce que nous allons voir avec l'algorithme de McEliece, proposé par Robert McEliece en 1978.

13.1. Principe et mise en oeuvre.

13.1.1. *Création des clefs.* Tout d'abord, Bob fixe des entiers k, n et t représentant la dimension, la longueur et la capacité de correction, et choisit une matrice G engendrant un code ayant ces caractéristiques. Nous supposerons de plus qu'il existe un algorithme efficace (en temps polynomial) pour décoder le code engendré par G (de tels algorithmes existent pour les codes de Golay, qui sont des exemples spécifiques de codes linéaires).
Finalement, choisissons deux matrices inversibles, S de taille $k \times k$, et P de taille $n \times n$, supposant de plus que P est une matrice de permutation (exactement un 1 sur chaque ligne).
Considérons finalement la matrice $\widehat{G} = PGS$. La clef publique est alors $(\widehat{G}, t)$ et la clef privée est (S, G, P).

13.1.2. *Encryptage et décryptage.* Pour envoyer un message à Bob, Alice décide d'abord de l'encoder sous forme d'un vecteur m de longueur k (éventuellement après une fonction de Hashage). Elle choisir ensuite un vecteur aléatoire z de longueur n possédant au plus t entrées à 1. Elle calcule finalement le vecteur $c = \widehat{G}m + z$ et l'envoi à Bob.
Recevant le message c, Bob calcule $\widehat{c} = P^{-1}c$. Comme P est une matrice de permutation, c'est aussi le cas de P^{-1}, et donc $P^{-1}z$ possède au plus t entrées à 1. en particulier, $\widehat{c}$ est obtenu d'un mot du code engendré par G en effectuant au plus t erreurs, et peut donc être corrigé *rapidement* grâce à l'algorithme efficace dont Bob dispose, et il obtient un code corrigé $\widehat{M}$, qu'il décode à l'aide d'un inverse à gauche de G en $\widehat{m}$. Il peut alors calculer $S^{-1}\widehat{m}$ qui est le message envoyé par Alice.

13.2. Sécurité. Dans les faits, il est bien sûr possible de corrigé directement le code $\widehat{c}$ à l'aide d'une table de Syndrôme, puis une attaque statistique pour calculer l'inverse de S (facile d'obtenir des données car on connaît $\widehat{G}$). Le problème est que résoudre à l'aide de la table des Syndrôme est très gourmand en temps (table de longueur au moins $\binom{t}{n}$), c'est même un problème NP-complet ! L'attaque statistique sur S demandant en plus un grand nombre (dépendant de k) de données, le cassage de l'algorithme de McElies est donc très long !
Dans les faits, afin que ce cryptosystème soit sûr, il semble nécessaire de prendre des clefs très grosses (par exemple, $n = 1024$, $t = 38$, et $k \geqslant 644$).
En raison de la taille des clefs, cet algorithmes a pendant longtemps été laissé de côté. Toutefois, il pourrait revenir sur le devant de la scène car, étant NP-complet, il ne semble pas attaquable par un ordinateur quantique[1].

1. assertion non prouvée à l'heure actuelle ! mais la plupart des scientifiques pensent que c'est vrai !

Chapitre 3

Étude de fonctions

Dans cette partie, on s'intéresse aux applications $f : \mathcal{D}_f \to \mathbb{R}$ où $\mathcal{D}_f$ est une partie de $\mathbb{R}$, on appelle $\mathcal{D}_f$ le domaine de définition de la fonction f, en général un intervalle ou une réunion d'intervalles.

1. Définitions et notations

Définition 1.1: Parité, imparité

Soit $\mathcal{D}_f$ une partie de $\mathbb{R}$ telle que $x \in \mathcal{D}_f \Rightarrow -x \in \mathcal{D}_f$. On dit que

i) f est *paire* si $f(-x) = f(x)$ quel que soit $x \in \mathcal{D}_f$;

ii) f est *impaire* si $f(-x) = -f(x)$ pour tout $x \in \mathcal{D}_f$.

Définition 1.2: Périodicité

Soit $f : \mathbb{R} \to \mathbb{R}$ une fonction et soit T un nombre réel strictement positif. On dit que f est *périodique de période* T (ou encore T-*périodique*) si $f(x+T) = f(x)$ pour tout $x \in \mathbb{R}$.

La parité (resp. l'imparité) d'une fonction est une propriété de symétrie du graphe de cette fonction par rapport à l'axe des ordonnées (resp. à l'origine). Pour étudier une fonction paire ou impaire, il suffit de l'étudier sur $\mathcal{D}_f \cap \mathbb{R}_+$ puis de compléter par symétrie. La périodicité est une propriété de répétition. Pour étudier une fonction T-périodique, il suffit de s'intéresser à un intervalle de longueur T, puis de compléter par des translations.

Définition 1.3

Soit V une partie non vide de $\mathcal{D}_f$. La fonction f est *positive ou nulle sur* V (*resp. strictement positive sur* V) si $f(x) \geq 0$ (*resp.* $f(x) > 0$) pour tout $x \in V$.

On définit de même une fonction *négative ou nulle* ou une fonction *strictement négative* sur V. Si g est une fonction elle aussi définie sur $\mathcal{D}_f$, f est *inférieure ou égale à* g, et on note $f \leq g$, si on a $f(x) \leq g(x)$ pour tout $x \in \mathcal{D}_f$. On définit de même la relation *supérieure ou égale*. Deux nombres réels sont toujours comparables ($x \leq y$ ou $y \leq x$), mais il n'est pas toujours possible de comparer deux fonctions. On laisse le soin au lecteur de trouver des contre-exemples.

Définition 1.4

Soit V une partie non vide de $\mathcal{D}_f$. On dit que f est *croissante sur* V (*resp.* strictement croissante sur V) si pour tous x et y dans $\mathbb{R}$, $x \leq y \Rightarrow f(x) \leq f(y)$ (*resp.* $x < y \Rightarrow f(x) < f(y)$).

On définit de même une fonction décroissante et strictement décroissante sur V. Une fonction f est *monotone sur* V si elle est soit croissante, soit décroissante sur V, *strictement monotone* si elle est soit strictement décroissante, soit strictement

croissante sur V. On peut remarquer que f est décroissante si et seulement si $-f$ est croissante, et qu'une fonction est constante si et seulement si elle est croissante et décroissante. Il faut prendre soin de toujours préciser l'ensemble sur lequel il y a (ou non) monotonie d'une fonction.

Proposition 1.5

Soit V une partie non vide de $\mathcal{D}_f \cap \mathcal{D}_g$. Si f et g sont croissantes sur V,
- alors la somme $f+g$ est croissante sur V ;
- si, de plus, f et g sont positives ou nulles sur V, alors fg est croissante sur V.

Définition 1.6: Composition

Soient $f : \mathcal{D}_f \to \mathbb{R}$ et $g : \mathcal{D}_g \to \mathbb{R}$ deux fonctions telles que pour tout $x \in \mathcal{D}_f$, $f(x) \in \mathcal{D}_g$. La *composée de g par f* est la fonction $h : \mathcal{D}_f \to \mathbb{R}$ telle que pour tout $x \in \mathcal{D}_f$, $h(x) = g(f(x))$. On la note $g \circ f$.

La définition précédente n'est pas symétrique. La composée $g \circ f$ peut exister sans que $f \circ g$ existe. De plus, même si $g \circ f$ et $f \circ g$ existent, en général $g \circ f \neq f \circ g$.

Proposition 1.7

Si f et g sont toutes les deux croissantes ou toutes les deux décroissantes, alors leur composée, si elle existe, est croissante. Si l'une des fonctions f ou g est croissante, l'autre étant décroissante, alors leur composée est décroissante.

Définition 1.8

Soit $f : \mathcal{D}_f \to \mathbb{R}$. Un *majorant de f* (*resp.* un minorant de f) est un nombre réel M (*resp.* un nombre réel m) tel que $f(x) \leq M$ pour tout $x \in \mathcal{D}_f$ (*resp.* tel que $f(x) \geq m$ pour tout $x \in \mathcal{D}_f$). S'il existe un majorant M de f, f est *majorée* (par M).

La fonction est *bornée* si elle est majorée et minorée. En fait, une fonction est majorée (resp. minorée) si elle est inférieure (resp. supérieure) ou égale à une fonction constante.

Définition 1.9: Image

Si $f : \mathcal{D}_f \to \mathbb{R}$ est une fonction, *l'image de $\mathcal{D}_f$ par f*, notée $f(\mathcal{D}_f)$, est l'ensemble constitué de tous les $f(x)$ pour $x \in \mathcal{D}_f$. Autrement dit, c'est l'ensemble des nombres réels y pour lesquels il existe (au moins) un $x \in \mathcal{D}_f$ tel que $y = f(x)$.

Donc une fonction est majorée si et seulement si $f(\mathcal{D}_f)$ est une partie majorée de $\mathbb{R}$.
De plus une fonction f est majorée par M si et seulement si $-f$ est minorée par $-M$. Si f est minorée par un nombre réel $m > 0$, alors la fonction $1/f$ est majorée par $1/m$.

Proposition 1.10

Soient $f : \mathcal{D}_f \to \mathbb{R}$ et $g : \mathcal{D}_f \to \mathbb{R}$ deux fonctions.
- Si f et g sont majorées, alors la somme $f+g$ est majorée.
- Si f et g sont minorées, alors la somme $f+g$ est minorée.
- Supposons que f et g soient positives ou nulles. Alors si f et g sont majorées, leur produit fg est majorée.

Définition 1.11

Soit x un nombre réel. La *valeur absolue de* x est le nombre réel défini par

$$|x| = \begin{cases} x & \text{si } x \geq 0, \\ -x & \text{si } x \leq 0. \end{cases}$$

La *fonction valeur absolue* $x \mapsto |x|$ est définie sur $\mathbb{R}$.

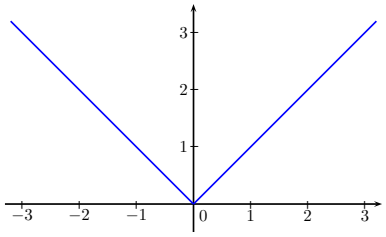


FIGURE 1. Fonction valeur absolue.

La valeur absolue d'un nombre x peut aussi être définie comme le plus grand des nombres x et $-x$. La fonction valeur absolue est donc *paire*. Rappelons quelques propriétés.

Proposition 1.12

Pour tous nombres réels x et y,

(1) $|x| \geq 0$, $-|x| \leq x \leq |x|$, $|-x| = |x|$
(2) $|x| > 0 \Leftrightarrow x \neq 0$.
(3) $\sqrt{x^2} = |x|$.
(4) $|xy| = |x||y|$ et si $x \neq 0$, $|1/x| = 1/|x|$.
(5) $|x + y| \leq |x| + |y|$ (inégalité triangulaire).
(6) $||x| - |y|| \leq |x - y|$.

Proposition 1.13

Soit $r > 0$. Pour tous les nombres réels a et x,

$$|x - a| < r \Leftrightarrow a - r < x < a + r.$$

Proposition 1.14

Soit f une fonction. La fonction f est bornée si et seulement si la fonction $|f| : x \mapsto |f(x)|$ est majorée.

2. Continuité

Soient $I \subset \mathcal{D}_f$ un intervalle, $f : I \to \mathbb{R}$ une fonction et $x_0 \in I$ ou x_0 est une extrémité de l'intervalle.

2.1. Limites et opérations sur les limites.

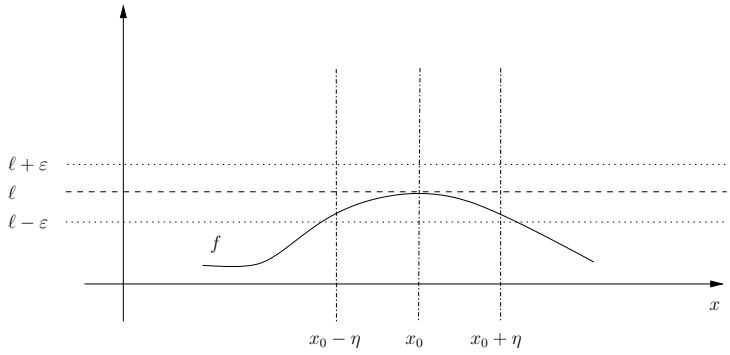


FIGURE 2. Limite de la fonction f en x_0.

Définition 2.1: Limite

Soit ℓ un nombre réel. On dit que f *a pour limite* ℓ *en* x_0, ou encore que $f(x)$ tend vers ℓ quand x tend vers x_0, si pour tout nombre $\varepsilon > 0$, il existe un nombre $\eta > 0$ ayant la propriété suivante :

$$(5) \qquad (x \in I, x \neq x_0, \quad \text{et} \quad |x - x_0| \leq \eta) \Longrightarrow |f(x) - \ell| < \varepsilon.$$

Si la fonction admet une limite, elle est unique et on la note

$$\lim_{x \to x_0} f(x) = \ell.$$

Intuitivement cette définition signifie que $f(x)$ est aussi près que l'on veut de ℓ à condition de choisir x assez près de x_0, mais différent de x_0.
Par définition il revient au même de dire que $f(x)$ tend vers ℓ ou que $f(x) - \ell$ tend vers 0 quand x tend vers x_0. On a ainsi les équivalences très utiles

$$\lim_{x \to x_0} f(x) = \ell \Longleftrightarrow \lim_{x \to x_0} (f(x) - \ell) = 0 \Longleftrightarrow \lim_{x \to x_0} |f(x) - \ell| = 0.$$

Définition 2.2: Limite infinie

— On dit que $f(x)$ *tend vers* $+\infty$ *quand* x *tend vers* x_0, et l'on note $\lim_{x\to x_0} f(x) = +\infty$, si pour tout nombre $A > 0$, il existe un nombre $\eta > 0$ ayant la propriété suivante :

$$(x \in I, x \neq x_0, \quad \text{et} \quad |x - x_0| < \eta) \Longrightarrow f(x) > A.$$

— Si I est l'un des intervalles $]-\infty, +\infty[$, $[a, +\infty[$ ou $]a, +\infty[$ où a est un nombre réel, on dit que $f(x)$ *tend vers* $+\infty$ *quand* x *tend vers* $+\infty$, et l'on note $\lim_{x\to+\infty} f(x) = +\infty$, si pour tout nombre $A > 0$, il existe un réel r tel que

$$x > r \Longrightarrow f(x) > A.$$

— Si I est l'un des intervalles $]-\infty, +\infty[$, $]-\infty, a]$ ou $]-\infty, a[$ où a est un nombre réel, on dit que $f(x)$ *tend vers* $+\infty$ *quand* x *tend vers* $-\infty$, et l'on note $\lim_{x\to-\infty} f(x) = +\infty$, si pour tout nombre $A > 0$, il existe un réel r tel que

$$x < r \Longrightarrow f(x) > A.$$

— On dit que $f(x)$ *tend vers* $-\infty$ *quand* x *tend vers* x_0 (ou bien *quand* x *tend vers* $+\infty$, ou bien *quand* x *tend vers* $-\infty$), si $-f(x)$ tend vers $+\infty$. Cette propriété se note $\lim_{x\to x_0} f(x) = -\infty$ dans le cas, par exemple, de la limite en x_0.

Dans ce paragraphe nous énonçons les propriétés pour la limite en $x_0 \in \mathbb{R}$, mais les résultats restent vrais si l'on remplace x_0 par $+\infty$ ou $-\infty$. Il est très important de bien comprendre et connaître ces résultats pour pouvoir les utiliser à bon escient.

Proposition 2.3

Soient f et g des fonctions et ℓ, ℓ' des nombres réels. Supposons $\lim_{x\to x_0} f(x) = \ell$ et $\lim_{x\to x_0} g(x) = \ell'$.

(1) On a $\lim_{x\to x_0} (f(x)+g(x)) = \ell+\ell'$, $\lim_{x\to x_0} (f(x)g(x)) = \ell\ell'$ et pour tout $\lambda \in \mathbb{R}$, $\lim_{x\to x_0} \lambda f(x) = \lambda\ell$.

(2) Si $\ell' \neq 0$, alors $\lim_{x\to x_0} \dfrac{f(x)}{g(x)} = \dfrac{\ell}{\ell'}$.

Proposition 2.4

Soient f et g des fonctions. Supposons $\lim_{x\to x_0} g(x) = +\infty$.

(1) On a $\lim_{x\to x_0} \dfrac{1}{g(x)} = 0$.

(2) Si f est minorée, alors $\lim_{x\to x_0} (f(x) + g(x)) = +\infty$.

(3) Si f est minorée par un nombre strictement positif, alors on a $\lim_{x\to x_0} f(x)g(x) = +\infty$.

(4) Si $\lim_{x\to x_0} f(x) = 0$ et $f(x) > 0$ pour tout x, alors $\lim_{x\to x_0} \dfrac{1}{f(x)} = +\infty$.

Corollaire 2.5
Soit ℓ un nombre réel strictement positif. Si $\lim\limits_{x\to x_0} f(x) = \ell$ et $\lim\limits_{x\to x_0} g(x) = +\infty$, alors $\lim\limits_{x\to x_0} f(x)g(x) = +\infty$.

Théorème 2.6

Soient f une fonction et ℓ un nombre réel. Si $f(x) \geq 0$ quel que soit x et si $\lim\limits_{x\to x_0} f(x) = \ell$, alors $\ell \geq 0$.

Corollaire 2.7: Passage à la limite dans les inégalités
Soient f et g des fonctions telles que $f \geq g$. Si $\lim\limits_{x\to x_0} f(x) = \ell$ et $\lim\limits_{x\to x_0} g(x) = \ell'$, alors $\ell \geq \ell'$.

Attention : même si $f > g$, on peut avoir $\ell = \ell'$!
Les énoncés suivants sont importants car ils permettent d'affirmer l'existence de la limite et de la calculer.

Théorème 2.8

Soit ℓ un nombre réel et soient f, g et h des fonctions.
- Si $f \leq g \leq h$ et $\lim\limits_{x\to x_0} f(x) = \lim\limits_{x\to x_0} h(x) = \ell$, alors $\lim\limits_{x\to x_0} g(x) = \ell$.
- Si $f \leq g$ et si $\lim\limits_{x\to x_0} f(x) = +\infty$, alors $\lim\limits_{x\to x_0} g(x) = +\infty$.

Corollaire 2.9
Soient f et g des fonctions. Si f est bornée et si $\lim\limits_{x\to x_0} g(x) = 0$, alors $\lim\limits_{x\to x_0} f(x)g(x) = 0$.

Voici un résultat sur certaines limites de fonctions composées.

Proposition 2.10
Soient f et g des fonctions. Si $\lim\limits_{x\to x_0} f(x) = +\infty$ et $\lim\limits_{x\to+\infty} g(x) = \ell$ (ou $+\infty$ ou $-\infty$), alors $\lim\limits_{x\to x_0} g\circ f(x) = \ell$ (ou $+\infty$ ou $-\infty$).

2.1.1. *Limite à droite, limite à gauche.* Soit $]a,b[$ un intervalle ouvert, soit $x_0 \in]a,b[$ et soit f une fonction définie sur la réunion $]a,x_0[\cup]x_0,b[$. Par exemple la fonction $x \mapsto \dfrac{\sqrt{2x}-x}{|x-2|}$ vérifie ces hypothèses si l'on choisit $x_0 = 2$, $a = 0$ et $b = 5$. Définissons les fonctions $g :]a,x_0[\to \mathbb{R}$ et $h :]x_0,b[\to \mathbb{R}$ en posant $g(x) = f(x)$ pour tout $x \in]a,x_0[$ et $h(x) = f(x)$ pour tout $x \in]x_0,b[$.

Définition 2.11

Si $\lim\limits_{x\to x_0} g(x) = \ell$ (ou $+\infty$ ou $-\infty$), on dit que $f(x)$ *tend vers* ℓ *(ou* $+\infty$ *ou* $-\infty$*) quand* x *tend vers* x_0 *à gauche* et l'on note $\lim\limits_{x\to x_0^-} f(x) = \ell$. On définit de même *la limite à droite en* x_0 : $\lim\limits_{x\to x_0^+} f(x) = \ell$ signifie $\lim\limits_{x\to x_0} h(x) = \ell$.

Bien remarquer le signe - ou + ajouté sous la limite !

2.1.2. *Formes indéterminées.* Toutes les propriétés précédentes ne permettent pas de calculer toutes les limites. Par exemple il n'y a pas de résultat général pour le produit d'une fonction qui tend vers zéro par une fonction qui tend vers $\pm\infty$: selon les cas, le résultat peut d'ailleurs être 0 ou $\pm\infty$ ou une limite finie non nulle, ou bien il n'y a pas de limite ; on dit que $0 \times \infty$ est une forme indéterminée.
Il existe d'autres formes indéterminées comme $\frac{\infty}{\infty}$, $\frac{0}{0}$, $(+\infty - \infty)$, 1^∞, ou ∞^0. Pour lever les indéterminations, c'est-à-dire pour voir si de telles expressions ont une limite et éventuellement calculer cette limite, il suffit parfois de transformer convenablement l'expression (ce qui n'est pas toujours simple) et de se ramener aux énoncés précédents. Souvent il faudra faire appel à des techniques que nous verrons progressivement (dérivabilité, développements limités, etc.).

2.2. Continuité d'une fonction. Soient I un intervalle et x_0 un élément de I. Dans la suite, les fonctions sont définies sur I.

Définition 2.12

Une fonction f est *continue en* x_0 si

$$\lim_{x \to x_0} f(x) = f(x_0).$$

La fonction f est *continue sur* I si, quel que soit $x \in I$, f est continue en x. En utilisant la définition de la limite en un point x_0 et en remarquant que si $x = x_0$, alors $f(x) - f(x_0) = 0$, on obtient que f est continue en x_0 si et seulement si pour tout $\varepsilon > 0$ il existe $\eta > 0$ tel que

$$(x \in I, \quad \text{et} \quad |x - x_0| < \eta) \Longrightarrow |f(x) - f(x_0)| < \varepsilon.$$

On peut enlever dans l'expression précédente $x \neq x_0$.

Exercice 2.13

- *Une fonction constante sur I est continue sur I.*
- *La fonction racine carrée est continue sur $[0, +\infty[$.*
- *La fonction valeur absolue est continue sur $\mathbb{R}$.*
- *La fonction partie entière est continue en tout point non entier et n'est pas continue (ou discontinue) en tout point entier.*

La proposition sur la limite d'une somme, d'un produit et d'un inverse permet de déduire que si f et g sont continues en $x_0 \in I$ alors,

- les fonctions $f + g$, fg et λf pour tout $\lambda \in \mathbb{R}$, sont continues en x_0 ;
- si $g(x_0) \neq 0$, alors la fonction $\frac{f}{g}$ est continue en x_0.

Une fonction polynomiale est continue sur $\mathbb{R}$. Ainsi, si f est une fonction rationnelle (quotient de deux fonctions polynômiales) définie sur un intervalle I, alors f est continue sur I.

Théorème 2.14

La composée de deux fonctions continues est continue.

Théorème 2.15 (Prolongement par continuité)

Soient a et b des nombres réels tels que $a < b$, $f :]a, b[\to \mathbb{R}$ une fonction et ℓ un nombre réel.
Supposons que l'on a $\lim_{x \to a} f(x) = \ell$ et définissons la fonction $g : [a, b[\to \mathbb{R}$ en posant

$$g(x) = \begin{cases} f(x) & \text{si } x \in]a, b[; \\ \ell & \text{si } x = a. \end{cases}$$

Nous avons $\lim_{x \to a} g(x) = \lim_{x \to a} f(x) = \ell$, donc $\lim_{x \to a} g(x) = \ell = g(a)$. Ainsi la fonction g est continue en a. La fonction g s'appelle *le prolongement par continuité de f en a.*

Parfois par abus de notation on confondra f et son prolongement en notant ce dernier également par f.

Théorème 2.16 (de la bijection)

Soient I un intervalle de $\mathbb{R}$ et $f : I \to \mathbb{R}$ une fonction continue et strictement monotone. Alors f induit une bijection de I sur $f(I)$.

3. Dérivabilité

La dérivée est l'outil principal pour étudier une fonction. Pour bien utiliser cette notion, il faut connaître parfaitement la définition et s'entraîner à calculer des dérivées rapidement et sans erreur. Ainsi pourra-t-on étudier le comportement d'une solution d'équation différentielle et même vérifier qu'une fonction est bien solution d'une équation différentielle données.

3.1. Dérivée en un point et fonction dérivée. Soient I un intervalle et x_0 un élément de I. Dans la suite, les fonctions sont définies sur I.

Définition 3.1

On dit que f est *dérivable en x_0* si

$$\frac{f(x) - f(x_0)}{x - x_0}$$

a une limite finie quand x tend vers x_0. La limite

$$\lim_{x \to x_0} \frac{f(x) - f(x_0)}{x - x_0}$$

est notée $f'(x_0)$ et s'appelle le *nombre dérivé de f en x_0*.

Supposons f dérivable en x_0 et définissons une fonction ε en posant

$$\varepsilon(x) = \frac{f(x) - f(x_0)}{x - x_0} - f'(x_0) \quad \text{si } x \neq x_0 \text{et } \varepsilon(x_0) = 0.$$

Pour tout nombre $x \neq x_0$, on a

$$f(x) = f(x_0) + (x - x_0)f'(x_0) + (x - x_0)\varepsilon(x)$$

et cette égalité est encore vraie si $x = x_0$ car dans ce cas les deux membres sont égaux à $f(x_0)$. Par ailleurs

$$\lim_{x \to x_0} \varepsilon(x) = \lim_{x \to x_0} \frac{f(x) - f(x_0)}{x - x_0} - f'(x_0) = f'(x_0) - f'(x_0) = 0 = \varepsilon(x_0),$$

donc la fonction ε est continue en x_0.

Finalement si f est dérivable en x_0, il existe une fonction ε continue en x_0 telle que $\varepsilon(x_0) = 0$ et

$$f(x) = f(x_0) + (x - x_0)f'(x_0) + (x - x_0)\varepsilon(x) \quad \text{quel que soit } x \in I.$$

Cette propriété caractérise les fonctions dérivables en x_0.

Corollaire 3.2
Si f est dérivable en x_0, alors elle est continue en x_0.

On dit que f est *dérivable sur* I si quel que soit $x_0 \in I$, f est dérivable en x_0. Dans ce cas, la fonction $f' : I \to \mathbb{R}$ qui à x associe $f'(x)$ s'appelle la *dérivée de* f.
L'ensemble des fonction dérivables sur I est noté $D(I)$.

3.2. Monotonie et dérivée.

Lemme 3.3
Soient I un intervalle ouvert et $f : I \to \mathbb{R}$ une fonction dérivable sur I.
- Si f est croissante sur I, alors pour tout $x \in I$ on a $f'(x) \geq 0$.
- Si f est décroissante sur I, alors pour tout $x \in I$ on a $f'(x) \leq 0$.

3.2.1. *Tangente au graphe de* f. Soit $\mathcal{C}$ le graphe de la fonction f dans le plan. Notons M_0 le point $(x_0, f(x_0))$ et si $x \in I$, $x \neq x_0$, notons M le point $(x, f(x))$; par définition les points M_0 et M appartiennent à $\mathcal{C}$.
Le rapport $\dfrac{f(x) - f(x_0)}{x - x_0}$ est la *pente* de la droite passant par M_0 et M. Supposons que f est dérivable en x_0. Alors intuitivement, quand x tend vers x_0, la droite (M_0M) a pour position limite la droite passant par M_0 et de pente $f'(x_0)$. Par définition cette droite s'appelle la *tangente à* $\mathcal{C}$ *au point* M_0. Ainsi :

Proposition 3.4
Si f est dérivable en $x_0 \in I$, la courbe $\mathcal{C}$ a pour tangente au point M_0 la droite d'équation $y = (x - x_0)f'(x_0) + f(x_0)$.

3.2.2. *Dérivée à gauche, dérivée à droite.* Soient I un intervalle et $f : I \to \mathbb{R}$ une fonction. Soit x_0 un élément de I.

Définition 3.5

On dit que f est *dérivable à droite en* x_0 si $\dfrac{f(x) - f(x_0)}{x - x_0}$ a une limite à droite quand x tend vers x_0. La limite $\lim\limits_{x \to x_0^+} \dfrac{f(x) - f(x_0)}{x - x_0}$ est notée $f'_d(x_0)$.
De même, si $\dfrac{f(x) - f(x_0)}{x - x_0}$ a une limite à gauche quand x tend vers x_0, on dit que f est *dérivable à gauche en* x_0 et la limite $\lim\limits_{x \to x_0^-} \dfrac{f(x) - f(x_0)}{x - x_0}$ est notée $f'_g(x_0)$.

Distinguons quatre cas :
- Cas 1 : si x_0 n'est pas une extrémité de I. La fonction f est dérivable en x_0 si et seulement si f est dérivable à droite et à gauche en x_0 et si l'on a $f'_d(x_0) = f'_g(x_0)$; dans ce cas le nombre dérivé de f en x_0 est $f'(x_0) = f'_d(x_0) = f'_g(x_0)$. Si f est dérivable à droite (ou à gauche) en x_0, on dit que le graphe de f admet une *demi-tangente* de pente $f'_d(x_0)$ (ou $f'_g(x_0)$) au point d'abscisse x_0.

— Cas 2 : $x_0 = \max I$ (extrémité droite). Alors f est dérivable en x_0 si et seulement si f est dérivable à gauche en x_0.
— Cas 3 : $x_0 = \min I$ (extrémité gauche). Alors f est dérivable en x_0 si et seulement si f est dérivable à droite en x_0.
— Cas 4 : f n'est pas dérivable (à gauche ou à droite) en un point, au sens où une des limites vaut $\pm\infty$. Dans ce cas le graphe de f admet en ce point une (demie) tangente verticale. C'est le cas par exemple de la fonction racine.

Prenons par exemple la fonction f définie par $f(x) = |x|$. Le rapport $\dfrac{|x| - |0|}{x - 0} = \dfrac{|x|}{x}$ est égal à $x/x = 1$ si $x > 0$ et à $-x/x = -1$ si $x < 0$. On a donc $f'_d(0) = 1$ et $f'_g(0) = -1$. La fonction valeur absolue est donc dérivable à gauche et à droite en 0, mais n'est pas dérivable en 0.

3.3. Calcul des dérivées. Dérivée d'une somme et du produit par une constante. Si f et g sont deux fonctions dérivables en x_0, alors les fonctions $f + g$ et λf pour tout $\lambda \in \mathbb{R}$, sont dérivables en x_0 et

$$(f + g)'(x_0) = f'(x_0) + g'(x_0), \qquad (\lambda f)'(x_0) = \lambda f'(x_0).$$

Dérivée d'un produit. Si f et g sont deux fonctions dérivables en x_0, alors la fonction fg est dérivable en x_0 et

$$(fg)'(x_0) = f'(x_0)g(x_0) + f(x_0)g'(x_0).$$

Dérivée d'une fonction constante. Une fonction constante a une dérivée nulle en tout point.

Dérivée d'une composée. Soient f et g deux fonctions telles que la composée $g \circ f$ est définie. Si f est dérivable en x_0 et si g est dérivable en $f(x_0)$, alors la fonction $g \circ f$ est dérivable en x_0 et

$$(g \circ f)'(x_0) = g'(f(x_0))f'(x_0).$$

Dérivée de l'inverse. Soit f dérivable en x_0. Si $f(x_0) \neq 0$, alors la fonction $1/f$ est dérivable en x_0 et

$$\left(\frac{1}{f}\right)'(x_0) = -\frac{f'(x_0)}{f(x_0)^2}.$$

En utilisant les formules donnant la dérivée d'un produit et d'un inverse, on obtient que si f et g sont des fonctions dérivables en x_0 et si $g(x_0) \neq 0$, alors la fonction f/g est dérivable en x_0 et

$$\left(\frac{f}{g}\right)'(x_0) = \frac{f'(x_0)g(x_0) - f(x_0)g'(x_0)}{(g(x_0))^2}.$$

En conséquence on peut montrer que
— une fonction polynôme est dérivable sur $\mathbb{R}$ et la fonction dérivée est une fonction polynôme,
— une fonction rationnelle est dérivable sur son domaine de définition et la fonction dérivée est une fonction rationnelle.

Dérivée d'une fonction réciproque. Soient I un intervalle ouvert et f une fonction dérivable et strictement monotone sur I. Posons $J = f(I)$ et notons $f^{-1} : J \to I$ la bijection réciproque de $f : I \to J$. Si l'on a $f'(x) \neq 0$ pour tout $x \in I$, alors f^{-1} est dérivable sur J et l'on a pour tout $x \in J$:

$$(f^{-1})'(x) = \frac{1}{f'(f^{-1}(x))}.$$

3.4. Dérivées successives. Soient I un intervalle ouvert et $f : I \to \mathbb{R}$ une fonction dérivable ; par définition cela signifie que f est dérivable en tout point de I. Nous avons alors défini la fonction dérivée $f' : I \to \mathbb{R}$ qui à tout x appartenant à I associe le nombre dérivé $f'(x)$.
Si la fonction f' est à son tour dérivable en tout point de I, alors la fonction $(f')'$ dérivée de f' est définie sur I ; cette fonction se note f'' et s'appelle la *dérivée seconde de* f. Plus généralement si n est un entier positif ou nul, on définit, si elle existe, la *dérivée n-ième de f* en posant $f^{(0)} = f$ par convention et

$$f^{(p)} = \left(f^{(p-1)}\right)' \text{ pour tout entier } p \text{ tel que } 1 \leq p \leq n.$$

Si la dérivée n-ième de f existe, on dit que f est n fois dérivable.

Définition 3.6

Soient $f : I \to \mathbb{R}$ et $p \in \mathbb{N}$. On dit que f *est de classe C^p sur I* si et seulement si f est (au moins) p fois dérivable et la dérivée p-ième $f^{(p)}$ est continue sur I.
On dit que f *est de classe C^∞ sur I* si et seulement si f est indéfiniment dérivable sur I (ou de classe C^p pour tout $p \in \mathbb{N}$). Pour $p \in \mathbb{N} \cup \{\infty\}$, on note $C^p(I)$ l'ensemble des fonctions de classe C^p sur I.

Si f est de classe C^p sur I, alors $f^{(p)}$ est continue sur I et $f, f', \ldots, f^{(p-1)}$ sont aussi continues car dérivables. Si $f \in C^\infty$ sur I, alors pour tout $p \in \mathbb{N}$, $f^{(p)}$ est continue sur I. En particulier $C^0(I) = C(I)$ est l'ensemble des fonctions continues sur I. Les fonctions dans $C^1(I)$ sont dites *continuement dérivables*. Enfin on a les inclusions suivantes (toutes strictes) :

$$C^\infty(I) \subset \ldots \subset C^{p+1}(I) \subset C^p(I) \subset \ldots \subset C^1(I) \subset D(I) \subset C(I).$$

Exemple 3.7 : Soit $n \in \mathbb{N}$. On définit la fonction $e_n : \mathbb{R} \to \mathbb{R}$ par $e_n(x) = x^n$. Alors e_n est de classe C^∞ sur $\mathbb{R}$ et si $0 \leq p \leq n$, pour tout $x \in \mathbb{R}$,

$$e_n^{(p)}(x) = n(n-1)\ldots(n-p-1)x^{n-p} = \frac{n!}{(n-p)!}x^{n-p}.$$

En particulier on a $e_n^{(n)}(x) = n!$ et si $p \geq n+1$, $e_n^{(p)}(x) = 0$ pour tout $x \in \mathbb{R}$.

3.5. Somme, produit et composée de fonctions dans $C^p(I)$.

Proposition 3.8

Soit $p \in \mathbb{N} \cup \{\infty\}$. Si f et g sont dans $C^p(I)$ et si $\lambda \in \mathbb{R}$, alors $f+g$ et λf sont dans $C^p(I)$ et

$$(f+g)^{(p)} = f^{(p)} + g^{(p)}, \qquad (\lambda f)^{(p)} = \lambda f^{(p)}.$$

Proposition 3.9: Formule de Leibniz

Soit $p \in \mathbb{N} \cup \{\infty\}$. Si f et g sont dans $C^p(I)$, alors fg appartient à $C^p(I)$ et

$$(fg)^{(p)} = \sum_{k=0}^{p} C_p^k f^{(k)} g^{(p-k)}.$$

Pour $n = 1$, on retrouve $(fg)' = f'g + fg'$.

Théorème 3.10

Soit $p \in \mathbb{N} \cup \{\infty\}$. Si f est dans $C^p(I)$, g dans $C^p(J)$ avec $f(I) \subset J$, alors $g \circ f$ est de classe C^p sur I.

Corollaire 3.11

Si f et g sont de classe C^p sur I et si g ne s'annule pas sur I, alors f/g est de classe C^p sur I (pour $p \in \mathbb{N} \cup \{\infty\}$).

Théorème 3.12

Soit $f : I \to \mathbb{R}$ de classe C^p sur I avec $p \in \mathbb{N}^* \cup \{\infty\}$ strictement monotone et telle que f' ne s'annule pas sur I. Si $J = f(I)$ et si $g : J \to \mathbb{R}$ est la bijection réciproque de f, alors g est de classe C^p sur J.

3.6. Extremum local d'une fonction.

Définition 3.13

Soient I un intervalle et $f : I \to \mathbb{R}$ une fonction. Si $x_0 \in I$, on dit que
- f *a un maximum local en* x_0 s'il existe un intervalle ouvert J de centre x_0 et contenu dans I, tel que $f(x) \leq f(x_0)$ pour tout nombre x appartenant à J ;
- f *a un minimum local en* x_0 s'il existe un intervalle ouvert J de centre x_0 et contenu dans I, tel que $f(x) \geq f(x_0)$ pour tout nombre x appartenant à J ;
- f *a un extremum local en* x_0 si f a un maximum local ou un minimum local en x_0.

Si une fonction $f :]a, b[\to \mathbb{R}$ a un maximum (ou un minimum) en un point $x_0 \in]a, b[$, alors f a aussi un maximum local (ou un minimum local) en x_0.

Exemple 3.14 : Considérons la fonction $f : \mathbb{R} \to \mathbb{R}$ définie par $f(x) = |1 - x^2|$. Si $x \in]-1, 1[$, on a $x^2 < 1$, donc $f(x) = 1 - x^2$. On en déduit que si $x \in]-1, 1[$, alors $f(x) \leq 1$, c'est-à-dire $f(x) \leq f(0)$. La fonction f a donc un maximum local en 0. Hors de cet intervalle, la fonction f peut prendre des valeurs supérieures à 1 : ainsi $f(4) = 15$.
Pour tout $x \in \mathbb{R}$, $f(x) \geq 0$ et $f(1) = f(-1) = 0$. Donc la fonction f atteint son minimum global (par opposition à local) en 1 et -1. En ces points f a aussi un minimum local.

La fonction $g : [0, +\infty[\to \mathbb{R}$ définie par $g(x) = |1 - x^2|$ a encore un minimum local (et global) en 1, mais n'a pas de maximum local en 0.

Lorsqu'une fonction f est dérivable, le théorème suivant donne une condition nécessaire pour que f ait un extremum local en un point.

Théorème 3.15

Soient I un intervalle ouvert et $f : I \to \mathbb{R}$ une fonction. Supposons que f a un extremum local en un point $x_0 \in I$ et que f est dérivable en x_0. Alors $f'(x_0) = 0$.

Théorème 3.16 (de Rolle)

Soient a et b des nombres réels tels que $a < b$ et soit $f : [a, b] \to \mathbb{R}$ une fonction telle que :

(1) f est continue sur $[a, b]$,

(2) f est dérivable sur $]a, b[$,

(3) $f(a) = f(b) = 0$.

Alors il existe un nombre $c \in]a, b[$ tel que $f'(c) = 0$.

Le principe de la démonstration consiste à prouver qu'il existe un maximum (ou un minimum) local strictement positif (ou négatif).

3.7. Le théorème des accroissements finis.

Théorème 3.17 (des accroissements finis])

Soient a et b des nombres réels tels que $a < b$ et soit $f : [a, b] \to \mathbb{R}$ une fonction continue sur $[a, b]$ et dérivable sur $]a, b[$. Il existe un nombre $c \in]a, b[$ tel que $f(b) - f(a) = (b - a)f'(c)$.

Le nombre $p = \dfrac{f(b) - f(a)}{b - a}$ est la pente de la droite passant par les points $(a, f(a))$ et $(b, f(b))$. D'après le théorème des accroissements finis, il existe donc un point $(c, f(c))$ du graphe de f où la tangente est parallèle à cette droite.

Corollaire 3.18

Soient a et b des nombres réels tels que $a < b$ et soit $f : [a, b] \to \mathbb{R}$ une fonction continue sur $[a, b]$ et dérivable sur $]a, b[$.

- Si $f'(x) = 0$ pour tout $x \in]a, b[$, alors f est constante sur $[a, b]$.
- Si $f'(x) \geq 0$ (resp. $f'(x) \leq 0$) pour tout $x \in]a, b[$, alors f est croissante (resp. décroissante) sur $[a, b]$.
- Si $f'(x) > 0$ (resp. $f'(x) < 0$) pour tout $x \in]a, b[$, alors f est strictement croissante (resp. décroissante) sur $[a, b]$.

On peut même préciser que les deux premières assertions sont des équivalences (voir lemme 3.2). Pour la troisième on a :

Proposition 3.19

Soit Z l'ensemble des points x de $]a, b[$ tels que $f'(x) = 0$. f est strictement croissante (resp. décroissante) sur $[a, b]$ si et seulement si pour tout $x \in]a, b[$, $f'(x) \geq 0$ (resp. $f'(x) \leq 0$) et Z ne contient aucun intervalle ouvert $]u, v[$ avec $u < v$.

Le théorème suivant affirme qu'une fonction dérivable, à dérivée bornée ne peut avoir de grande variation, on dit qu'elle est lipschitzienne.

Théorème 3.20 (Inégalité des accroissements finis])

Soient I un intervalle ouvert et $f : I \to \mathbb{R}$ une fonction dérivable. Supposons qu'il existe un nombre $K > 0$ tel que $|f'(t)| \leq K$ pour tout $t \in I$. On a alors $|f(x) - f(y)| \leq K|x - y|$ quels que soient les nombres x et y appartenant à I.

On prendra garde que la réciproque est fausse : la fonction valeur absolue est lipschitzienne sur $\mathbb{R}$, sans être dérivable sur $\mathbb{R}$.

Méthode : pour encadrer une expression de la forme $f(x) - f(y)$, pensez au théorème et à l'inégalité des accroissements finis.

4. Fonctions usuelles

Dans cette section, nous allons redonner les principales propriétés de fonctions usuelles telles que le logarithme, l'exponentielle, les fonctions puissances et les fonctions trigonométriques.

4.1. Fonctions polynomiales, fractions rationnelles. Les fonctions polynômiales sont les fonctions définies sur $\mathbb{R}$ de la forme

$$x \longmapsto a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n = \sum_{k=0}^{n} a_k x^k,$$

où n est un entier naturel et les a_i, $i = 0, \ldots, n$, sont des nombres réels. Si tous les a_i sont nuls, cette fonction constante égale à zéro a pour degré $-\infty$; si $a_n \neq 0$, l'entier n est le *degré du polynôme*.

Exemple 4.1 : Les fonctions $x \longmapsto 1 + 2x$, $x \longmapsto x^2 - 3x^5$ sont des fonctions polynomiales de degré respectif 1 et 5.

Toutes les fonctions polynomiales sont de classe C^∞ sur $\mathbb{R}$ avec pour dérivée

$$x \mapsto a_1 + 2a_2 x + \ldots + n a_n x^{n-1} = \sum_{k=0}^{n-1} (k+1) a_{k+1} x^k.$$

On rappelle qu'en dehors des polynômes constants, les limites en $+\infty$ et $-\infty$ d'une fonction polynomiale sont $\pm\infty$, suivant la parité de n et le signe de $a_n \neq 0$.

Les fractions rationnelles sont des fonctions de la forme

$$x \mapsto \frac{P(x)}{Q(x)} = \frac{a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n}{b_0 + b_1 x + b_2 x^2 + \ldots + b_m x^m},$$

la fonction Q devant être non nulle. En général ces fonctions ne sont pas définies sur $\mathbb{R}$ tout entier, mais uniquement sur $\mathbb{R}$ privé des racines (ou des zéros) de Q, c'est-à-dire des nombres réels x tels que $Q(x) = 0$.

Exercice 4.2

- *La fonction* $x \mapsto \dfrac{x+1}{x^2+x+1}$ *est une fraction rationnelle définie sur* $\mathbb{R}$ *tout entier, car* $x^2+x+1 > 0$ *pour tout* $x \in \mathbb{R}$ *(discriminant strictement négatif).*
- *La fonction* $x \mapsto \dfrac{2x^3 - 7x}{x^3 - 5x^2 + 6x}$ *est une fraction rationnelle définie sur* $\mathbb{R}$ *privé des points 0, 2 et 3 car* $x^3 - 5x^2 + 6x = x(x-2)(x-3)$.

Il faut parfois faire attention toutefois à ce qu'un zéro du dénominateur peut aussi être un zéro du numérateur, auquel cas il peut y avoir un prolongement par continuité.

Exercice 4.3

Ainsi la fraction rationnelle définie par $x \mapsto \dfrac{x^3-x^2-2x}{x^2-4x}$ *a pour ensemble de définition* $\mathbb{R}$ *privé de 4. En effet on a* $x^3-x^2-2x = x(x^2-x-2) = x(x-2)(x+1)$ *et* $x^2-4x = x(x-4)$*, d'où une simplification possible par* x*.*

Sur leur ensemble de définition, les fractions rationnelles sont de classe C^∞. Pour déterminer leurs limites en $-\infty$ et $+\infty$, il y a une indétermination qu'on lève en mettant en facteur les termes de plus haut degré au numérateur et au dénominateur et en effectuant les simplifications adéquates pour se trouver avec une puissance de x multipliée par une fraction dont le comportement à l'infini ne pose pas de problème. Ainsi

$$\frac{x+1}{x^2+x+1} = \frac{x(1+(1/x))}{x^2(1+(1/x)+(1/x^2))} = \frac{1}{x} \times \frac{1+(1/x)}{1+(1/x)+(1/x^2)},$$

$$\frac{2x^3-7x}{x^3-5x^2+6x} = \frac{x^3(2-(7/x^2))}{x^3(1-(5/x)+(6/x^2))} = x^0 \times \frac{2-(7/x^2)}{1-(5/x)+(6/x^2)},$$

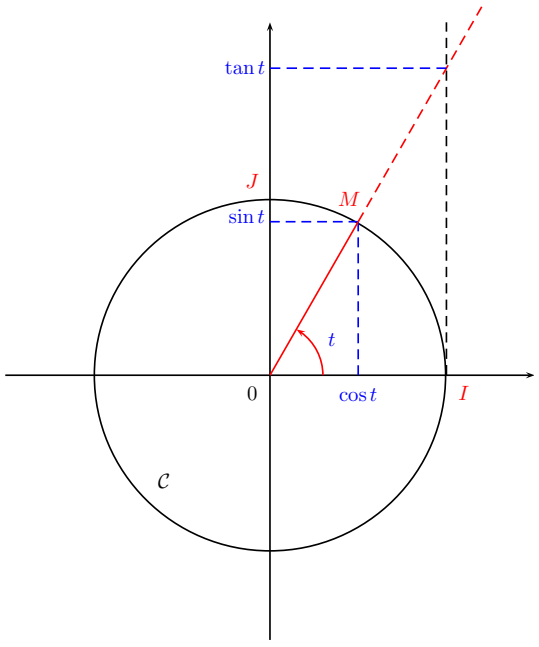
$$\frac{x^3-x^2-2x}{x^2-4x} = \frac{x^3(1-(1/x)-(2/x^2))}{x^2(1-(4/x))} = x \times \frac{1-(1/x)-(2/x^2)}{1-(4/x)}.$$

On rappelle ensuite

Lemme 4.4

$$\lim_{x\to+\infty} x^n = \begin{cases} +\infty & \text{si } n \geq 1, \\ 1 & \text{si } n = 0, \\ 0 & \text{si } n \leq -1. \end{cases} \qquad \text{et} \quad \lim_{x\to-\infty} x^n = \begin{cases} +\infty & \text{si } n \geq 1 \text{ et } n \text{ pair}, \\ -\infty & \text{si } n \geq 1 \text{ et } n \text{ impair}, \\ 1 & \text{si } n = 0, \\ 0 & \text{si } n \leq -1. \end{cases}$$

4.2. Sinus, Cosinus. Dans un repère orthonormal direct $(O, \vec{\imath}, \vec{\jmath})$ du plan, on note $I(1,0)$ et $J(0,1)$. $\mathcal{C}$ désigne le cercle trigonométrique, de centre O et de rayon 1. Pour tout $t \in \mathbb{R}$, on note M le point de $\mathcal{C}$ tel que $(\overrightarrow{OI}, \overrightarrow{OM}) \equiv t[2\pi]$ (l'angle entre les vecteurs vaut t).



Définition 4.5

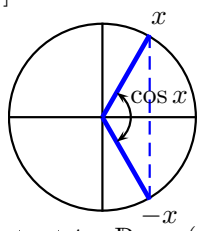
On appelle *cosinus de* t, noté $\cos(t)$, l'abscisse de M et *sinus de* t, noté $\sin(t)$, l'ordonnée de M.

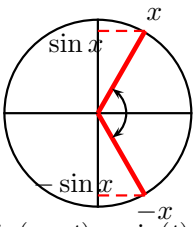
On note N le point d'intersection de la droite (OM) et de la tangente en I au cercle $\mathcal{C}$ (droite verticale passant par I).
Les fonctions cos et sin sont définies, continues sur $\mathbb{R}$, à valeurs dans $[-1,1]$. Ce sont des fonctions 2π- périodiques, c'est-à-dire

$$\forall x \in \mathbb{R}, \qquad \cos(x+2\pi) = \cos(x), \ \sin(x+2\pi) = \sin(x).$$

Quelques propriétés pour étudier ces fonctions :

- l'étude sur un intervalle de longueur 2π est donc suffisante. On complète ensuite par des translations de vecteurs $n2\pi\overrightarrow{\imath}$;
- cos est paire, sin impaire, on peut donc encore réduire l'intervalle d'étude à $[0,\pi]$





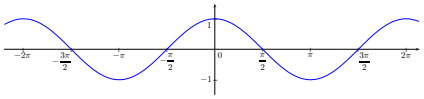
- pour tout $t \in \mathbb{R}$, $\cos(\pi - t) = -\cos(t)$ et $\sin(\pi - t) = \sin(t)$. La courbe de cos est donc symétrique par rapport au point de coordonnées $(\pi/2, 0)$ et celle de sin est symétrique par rapport à la droite d'équation $x = \pi/2$. On peut donc réduire l'intervalle d'étude à $[0, \pi/2]$ et compléter par symétrie.

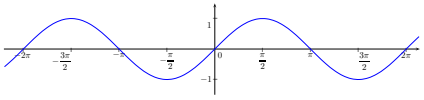
Proposition 4.6

Les fonctions cos et sin sont dérivables sur $\mathbb{R}$ avec

$$\forall x \in \mathbb{R}, \qquad \cos'(x) = -\sin(x), \quad \sin'(x) = \cos(x).$$

La fonction cos est strictement décroissante sur $[0, \pi/2]$; sin est strictement croissante sur $[0, \pi/2]$.



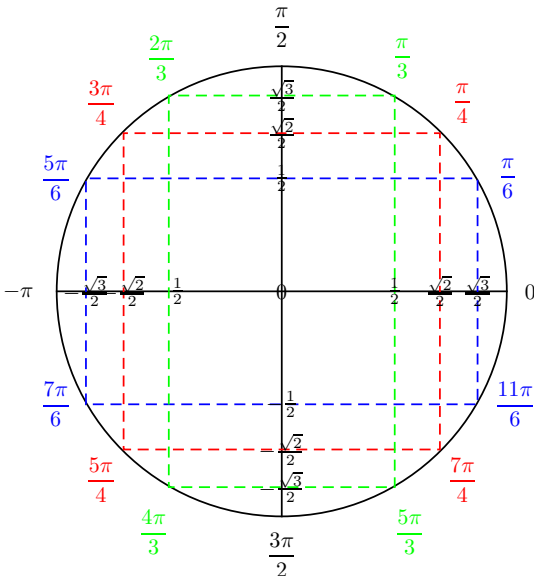


x	0		$\frac{\pi}{2}$		π
$\cos' x = -\sin x$	0	$-$	-1	$-$	0
$\cos x$	1	↘	0	↘	-1

x	0		$\frac{\pi}{2}$		π
$\sin' x = \cos x$		$+$	0	$-$	
$\sin x$	0	↗	1	↘	0

Pour terminer remarquons que comme pour tout $t \in \mathbb{R}$, $\sin(t + \pi/2) = \cos(t)$, la courbe de sinus est image de celle de cosinus par la translation de vecteur $(\pi/2)\overrightarrow{\imath}$.

Citons enfin, pour finir, quelques valeurs remarquables du cosinus et du sinus



4.3. Tangente.

Définition 4.7

On appelle *tangente de t*, noté $\tan t$, l'ordonnée de N.

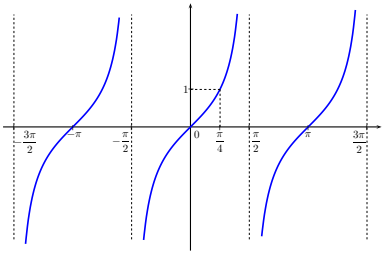
En appliquant le théorème de Thalès, on a : $\tan t = \dfrac{\sin t}{\cos t}$ pour $t \not\equiv \frac{\pi}{2}\ [\pi]$. En effet, les angles pour lesquels le cosinus s'annule sont $\pi/2$ et $-\pi/2$, auxquels cas les droites (OM) et la tangente n'ont pas d'intersection.

Proposition 4.8

La fonction tangente est continue et dérivable sur son ensemble de définition D, où D est la réunion des intervalles $]-\pi/2+k\pi, \pi/2+k\pi[$ avec $k \in \mathbb{Z}$. De plus pour tout $x \in D$,

$$\tan'(x) = 1 + \tan^2(x) = \frac{1}{\cos^2(x)}.$$

De plus cette fonction est π-périodique et impaire.



x	$-\frac{\pi}{2}$		0		$\frac{\pi}{2}$
$\tan' x = 1+\tan^2 x$	$+\infty$	$+$	1	$+$	$+\infty$
$\tan x$	$-\infty$	↗	0	↗	$+\infty$

On a donc les relations suivantes :

- $\tan(-x) = -\tan x$ (*imparité*).
- $\tan(x+\pi) = \tan x$ (π-*périodicité*).

Quelques valeurs particulières :

$$\tan 0 = 0, \qquad \tan\frac{\pi}{6} = \frac{1}{\sqrt{3}}, \qquad \tan\frac{\pi}{4} = 1, \qquad \tan\frac{\pi}{3} = \sqrt{3}.$$

4.4. La fonction logarithme.

Définition 4.9

On appelle *logarithme népérien*, que l'on note ln, l'unique fonction définie sur $]0,+\infty[$ et à valeurs dans $\mathbb{R}$ telle que

$$\forall x \in]0,+\infty[, \quad \ln'(x) = \frac{1}{x}, \quad \text{et} \quad \ln(1) = 0.$$

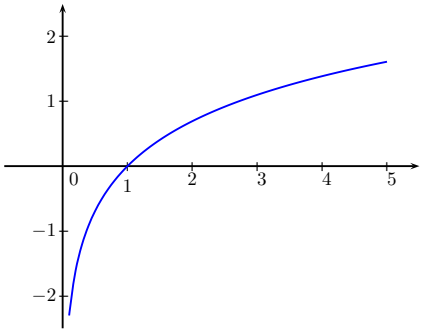
On peut montrer l'existence et l'unicité d'une telle fonction en utilisant la théorie de l'intégration : $\ln(x) = \displaystyle\int_1^x \frac{1}{t} dt$. Souvent on l'appelle simplement logarithme. Voici ces principales propriétés :

Proposition 4.10

C'est une fonction continue (et de classe C^∞ sur $]0,+\infty[$) et strictement croissante sur $]0,+\infty[$. De plus

(1) pour tout x et y strictement positifs,
   (a) $\ln(xy) = \ln(x) + \ln(y)$
   (b) $\ln(1/x) = -\ln(x)$
   (c) $\ln(x/y) = \ln(x) - \ln(y)$
   (d) $\ln(x^\alpha) = \alpha \ln(x)$ pour tout $\alpha \in \mathbb{R}$.

(2) Enfin pour tout $x > 0$, $\ln(x) \leq x - 1$.



x	0		1		$+\infty$
$\ln' x = 1/x$		$+$	1	$+$	
$\ln x$	$-\infty$	↗	0	↗	$+\infty$

Rappelons également quelques limites usuelles du logarithme :

Proposition 4.11

(1) $\displaystyle\lim_{x\to 0} \ln(x) = -\infty$ et $\displaystyle\lim_{x\to+\infty} \ln(x) = +\infty$.

(2) $\displaystyle\lim_{x\to 0} x \ln x = 0$, $\displaystyle\lim_{x\to 0} \frac{\ln(1+x)}{x} = 1$.

(3) $\displaystyle\lim_{x\to+\infty} \frac{\ln(x)}{x} = 0$.

Remarque 4.12

La fonction $x \mapsto \ln(|x|)$ est définie sur $\mathbb{R}^* = \mathbb{R}\backslash\{0\}$. On vérifiera que cette fonction est dérivable et a pour dérivée $1/x$ pour tout $x \in \mathbb{R}^*$.

Terminons ce paragraphe par le logarithme *de base a*.

Définition 4.13

Soit $a \in]0,1[\cup]1,+\infty[$. On appelle *logarithme de base a* l'application définie sur $]0,+\infty[$ par

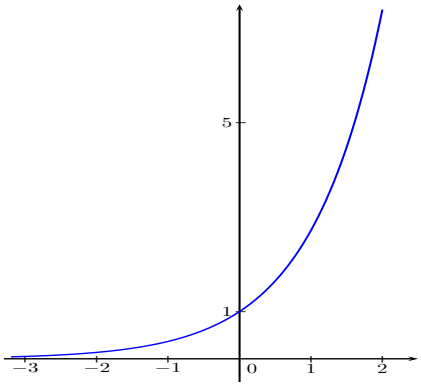
$$\forall x > 0, \quad \log_a(x) = \frac{\ln(x)}{\ln(a)}.$$

Notons que pour tout a, $\log_a(1) = 0$ et par définition $\log_a(a) = 1$. En physique on utilise fréquemment le logarithme de base 10. Il vérifie notamment, pour tout $n \in \mathbb{Z}$, $\log_{10}(10^n) = n$.

4.5. La fonction exponentielle. En rassemblant les propriétés de la fonction ln et en utilisant le théorème 2.2, cette fonction est donc une bijection de $]0,+\infty[$ sur $\mathbb{R}$.

Définition 4.14

La bijection réciproque de la fonction ln est la *fonction exponentielle*, notée exp. Elle est définie sur $\mathbb{R}$ et à valeurs dans $]0,+\infty[$.



x	$-\infty$		0		$+\infty$
$\exp' x = \exp x$		$+$	1	$+$	
$\exp x$	0	↗	1	↗	$+\infty$

Ainsi on a

$$\forall x > 0, \quad \exp(\ln x) = x, \qquad \text{et } \forall x \in \mathbb{R}, \quad \ln(\exp x) = x.$$

On en déduit également les propriétés suivantes :

Proposition 4.15

La fonction exp est continue et strictement croissante sur $\mathbb{R}$, dérivable avec $\exp'(x) = \exp(x)$ pour tout $x \in \mathbb{R}$. De plus pour tout x et y dans $\mathbb{R}$:

- $\exp(x+y) = \exp(x)\exp(y)$, d'où $\exp(nx) = (\exp(x))^n$ pour tout $n \in \mathbb{N}$,
- $\exp(-x) = 1/\exp(x)$,
- $\exp(x-y) = \exp(x)/\exp(y)$,
- pour tout $\alpha \in \mathbb{Q}$, $\exp(\alpha x) = (\exp(x))^\alpha$.

Concernant les limites usuelles concernant cette fonction, on obtient :

Proposition 4.16

(1) $\lim\limits_{x\to-\infty} \exp(x) = 0$ et $\lim\limits_{x\to+\infty} \exp(x) = +\infty$.

(2) $\lim\limits_{x\to-\infty} x\exp(x) = 0$, $\lim\limits_{x\to0} \dfrac{\exp(x)-1}{x} = 1$.

(3) $\lim\limits_{x\to+\infty} \dfrac{\exp(x)}{x} = +\infty$.

Notation. Le nombre réel $\exp(1)$ se note e ; on a donc $\ln(e) = 1$. Puisque la fonction exponentielle est strictement croissante, il vient $\exp(1) > \exp(0)$, donc $e > 1$.

4.6. Fonctions puissance et racine n-ième. Vous connaissez déjà les fonctions puissances définies pour les entiers $n \in \mathbb{N}$. En effet si n est un entier positif

$$\forall x \in \mathbb{R}, \qquad x^n = \underbrace{x \times \ldots \times x}_{n \text{ fois}}$$

avec par convention $x^0 = 1$ pour tout $x \in \mathbb{R}$.
Soit n un entier supérieur ou égal à 2. La fonction $x \mapsto x^n$ est continue et strictement croissante sur l'intervalle $[0, +\infty[$. La valeur en 0 est 0 et l'on a $\lim\limits_{x \to +\infty} x^n = +\infty$. D'après le théorème 2.2, la fonction $x \mapsto x^n$ définit une bijection de $[0, +\infty[$ sur $[0, +\infty[$.
Si l'entier n est impair, la fonction $x \to x^n$ est continue et strictement croissante sur $\mathbb{R}$, et l'on a $\lim\limits_{x \to -\infty} x^n = -\infty$. Dans ce cas la fonction $x \to x^n$ est une bijection de $\mathbb{R}$ sur $\mathbb{R}$.

Définition 4.17

La bijection réciproque d'une des bijections précédentes s'appelle la fonction *racine n-ième* et se note $x \mapsto \sqrt[n]{x}$. Si $n = 2$, c'est la fonction *racine carrée* que l'on note simplement $x \mapsto \sqrt{x}$.

La fonction racine n-ième est donc définie sur $[0, +\infty[$ si n est un entier pair et elle est définie sur $\mathbb{R}$ si n est un entier impair. C'est une fonction continue et strictement croissante. De plus

- pour tout x et y positifs ou nuls, $y = x^n \Leftrightarrow x = \sqrt[n]{y}$;
- si $x \in [0, 1]$, alors $x^n \leq x$ et en prenant la racine n-ième, on obtient $x \leq \sqrt[n]{x}$;
- si $x \geq 1$, alors $x \leq x^n$, donc $\sqrt[n]{x} \leq x$;
- si n est impair, la fonction $x \mapsto x^n$ est impaire et la fonction racine n-ième aussi.

Par composition, on peut définir les fonctions puissance pour $\alpha \in \mathbb{Q} \cap]0, +\infty[$. En effet si α est un nombre rationnel strictement positif, alors il existe deux uniques entiers n et m premiers entre eux tels que $\alpha = n/m$. La fonction puissance α est définie sur $[0, +\infty[$ par

$$\forall x \geq 0, \qquad x^\alpha = \sqrt[m]{x^n}.$$

Enfin si n est strictement négatif, alors

$$\forall x \neq 0, \qquad x^n = \left(\frac{1}{x}\right)^{-n}.$$

De même si $\alpha = -n/m \in \mathbb{Q} \cap]-\infty, 0[$ avec n et m entiers positifs premiers entre eux, alors $x \mapsto x^\alpha$ est définie sur $]0, +\infty[$ par

$$\forall x > 0, \qquad x^\alpha = \sqrt[m]{\left(\frac{1}{x}\right)^n}.$$

Remarque 4.18

Pour les fonctions puissance, on est certain de ne pas se tromper si on prend comme ensemble de définition l'ensemble $]0, +\infty[$. Dans certains cas, il est possible de l'étendre (mais il faut faire alors très attention).

4.7. Fonctions puissance (suite). Soit a un nombre réel strictement positif.

- Pour tout entier $n \in \mathbb{Z}$, $\exp(n \ln a) = (\exp(\ln a))^n = a^n$.

— Supposons que n est un entier positif au moins égal à 2 et posons $y = \exp\left(\frac{1}{n}\ln a\right)$. On a $y^n = \exp(n(1/n)\ln a) = a$. Puisque y est strictement positif, on en déduit $y = \sqrt[n]{a}$ par définition de la racine n-ième. On a donc

$$\sqrt[n]{a} = \exp\left(\frac{1}{n}\ln a\right), \text{ pour tout } a > 0.$$

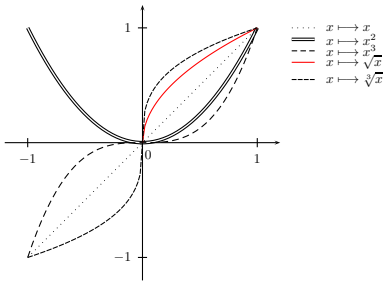


FIGURE 3. Fonctions puissance

Plus généralement

Définition 4.19

Soit a un nombre strictement positif et soit $b \in \mathbb{R}$. On définit le nombre réel a^b, appelé *a puissance b*, en posant

$$a^b = \exp(b\ln a).$$

On peut donc élever un nombre **strictement positif** à une puissance réelle quelconque. Les règles de calcul sont ensuite celles dont on a l'habitude.

Proposition 4.20

Pour tous nombres réels b et c :

— $1^b = 1$.
— $x^{b+c} = x^b x^c$ et $(x^b)^c = x^{(bc)}$ pour tout $x > 0$;
— si $x > 0$ et $y > 0$, alors $(xy)^c = x^c y^c$;
— si $x > 0$, alors $x^{-c} = 1/(x^c)$.

Méthode. Pour étudier une expression de la forme a^b où b n'est pas un entier, revenez à la définition : $a^b = \exp(b\ln a)$.

Définition 4.21

Soit α un nombre réel. La fonction $f :]0, +\infty[\to \mathbb{R}$ définie par $f(x) = x^\alpha$ s'appelle la *fonction puissance d'exposant α*.

Proposition 4.22

Pour $\alpha \in \mathbb{R}^*$, la fonction puissance d'exposant α

(1) est une application continue sur $]0, +\infty[$, strictement monotone (croissante si $\alpha > 0$ et décroissante si $\alpha < 0$),
(2) est une bijection de $]0, +\infty[$ sur $]0, +\infty[$,
(3) elle est dérivable sur $]0, +\infty[$ avec pour dérivée la fonction $x \mapsto \alpha x^{\alpha-1}$.

Concernant les limites on a

Proposition 4.23

(1) $$\lim_{x\to+\infty} x^\alpha = \begin{cases} 0 & \text{si } \alpha < 0, \\ 1 & \text{si } \alpha = 0, \\ +\infty & \text{si } \alpha > 0. \end{cases}$$

(2) $$\lim_{x\to 0} x^\alpha = \begin{cases} +\infty & \text{si } \alpha < 0, \\ 1 & \text{si } \alpha = 0, \\ 0 & \text{si } \alpha > 0. \end{cases}$$

4.8. Fonction exponentielle de base a.

Définition 4.24

Soit a un nombre réel strictement positif. La fonction $f : \mathbb{R} \to \mathbb{R}$ définie par $f(x) = a^x$ s'appelle la *fonction exponentielle de base a*.

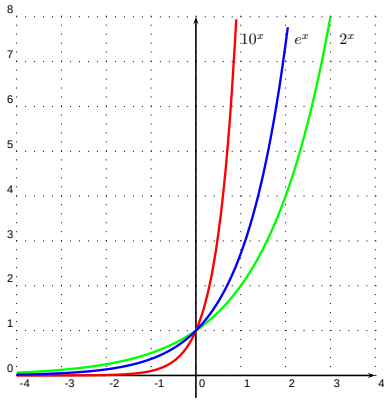


FIGURE 4. Fonctions exponentielles de base a

En voici quelques propriétés.

Proposition 4.25

Si $a \neq 1$, la fonction $x \mapsto a^x$ est une bijection continue de $\mathbb{R}$ sur $]0, +\infty[$. Si $a > 1$ cette bijection est strictement croissante ; si $a < 1$ elle est strictement décroissante. De plus elle est dérivable sur $\mathbb{R}$ avec pour dérivée $x \mapsto (\ln a)a^x$.

Remarquons que si $a = e = \exp(1)$, alors pour tout $x \in \mathbb{R}$, $\exp(x) = e^x$. La fonction exponentielle de base e est donc l'exponentielle ordinaire. On utilisera par la suite indifféremment les deux notations. Enfin pour tout $x > 0$:

$$\forall x \in \mathbb{R},\ \log_a(a^x) = x \quad \text{et} \quad \forall x > 0,\ a^{\log_a(x)} = x.$$

Autrement dit l'exponentielle en base a est la bijection réciproque du logarithme en base a.

4.9. Relations de comparaison. Il est important de s'en rappeler et de savoir les utiliser.

Théorème 4.26 (Croissances comparées)

(1) Si α et β sont deux nombres réels et si $\alpha < \beta$, alors
$$\lim_{x\to 0^+} \frac{x^\beta}{x^\alpha} = 0, \qquad \lim_{x\to+\infty} \frac{x^\beta}{x^\alpha} = +\infty.$$
(2) Si $\alpha > 0$ et $\beta \in \mathbb{R}$,
$$\lim_{x\to 0^+} x^\alpha |\ln x|^\beta = 0.$$
(3) Si $\alpha > 0$ et $\beta \in \mathbb{R}$, au voisinage de $+\infty$,
$$\lim_{x\to+\infty} x^\beta \exp(-\alpha x) = 0, \qquad \lim_{x\to+\infty} x^\beta \exp(\alpha x) = +\infty.$$
(4) Si $\alpha > 0$ et $\beta \in \mathbb{R}$,
$$\lim_{x\to+\infty} \frac{(\ln x)^\beta}{x^\alpha} = 0.$$

5. Suites

5.1. Définition. Une suite $u = (u_n)_{n\in\mathbb{N}}$ à valeurs réelles peut être vue comme une application de $\mathbb{N}$ dans $\mathbb{R}$. On définit la somme de deux suites, $u+v = (u_n + v_n)_{n\in\mathbb{N}}$, et le produit d'une suite et d'un scalaire $\lambda \in \mathbb{R}$, $\lambda u = (\lambda u_n)_{n\in\mathbb{N}}$. Ces opérations confèrent à l'ensemble des suites à valeurs réelles la structure de $\mathbb{R}$-espace vectoriel. Il y a principalement deux manières de définir le terme général d'une suite $(u_n)_{n\in\mathbb{N}}$ de nombres réels :

i) Par une formule explicite de la forme
$$u_n = f(n)$$
où f est une fonction donnée définie sur les entiers et à valeurs réelles, avec laquelle on peut calculer n'importe quel terme de la suite en fonction de l'indice n. On pourra avoir à l'esprit les exemples de suites définies par les termes généraux suivants : $\sin(n)$, $(-1)^n$, $\frac{1}{n+1}$, $\frac{n}{n+1}$, n, a^n avec $a \in \mathbb{R}$ et $\ln(n+1)$.

ii) Par la donnée de premiers termes et d'une formule de récurrence, par exemple
$$\begin{cases} u_0, u_1, \dots, u_{p-1} \text{ fixés,} \\ u_n = g(u_{n-1}, u_{n-2}, \dots, u_{n-p}) \end{cases}$$
où g est une fonction de $\mathbb{R}^p$ dans $\mathbb{R}$. On pourra retenir les exemples de suites arithmétiques définies par la relation de récurrence $u_{n+1} = u_n + b$, $n \geq 0$ et $b \in \mathbb{R}$, et la donnée initiale u_0, les suites géométriques définies par $u_{n+1} = au_n$ et les suites linéaires d'ordre 1 $u_{n+1} = au_n + b$.

Une suite à valeurs réelles est majorée (resp. minorée) s'il existe $M \in \mathbb{R}$ (resp. $m \in \mathbb{R}$) tel que pour tout $n \in \mathbb{N}$, $u_n \leq M$ (resp. $u_n \geq m$). Une suite est bornée si

$$\exists M \in \mathbb{R}\,,\ \forall n \in \mathbb{N}\,,\ |u_n| \leq M\,. \tag{6}$$

Une suite à valeurs réelles est croissante (resp. décroissante) si pour tout $n \in \mathbb{N}$, $u_n \leq u_{n+1}$ (resp. $u_n \geq u_{n+1}$). Une suite est monotone si elle est soit croissante, soit décroissante. On parle aussi de suite croissante (décroisante, monotone, *etc.*) à partir d'un certain rang, i.e.

$$\exists N_0 \in \mathbb{N}\,,\ \forall n \geq N_0\,,\ u_n \leq u_{n+1}\,.$$

Une suite à valeurs réelles converge vers $\ell \in \mathbb{R}$ si

$$\forall \varepsilon > 0\,,\ \exists N \in \mathbb{N}\,,\ \forall n \geq N\,,\ |u_n - \ell| < \varepsilon\,. \tag{7}$$

et diverge dans tous les autres cas. Cette limite, quand elle existe, est unique et notée $\ell = \lim_{n\to+\infty} u_n$.

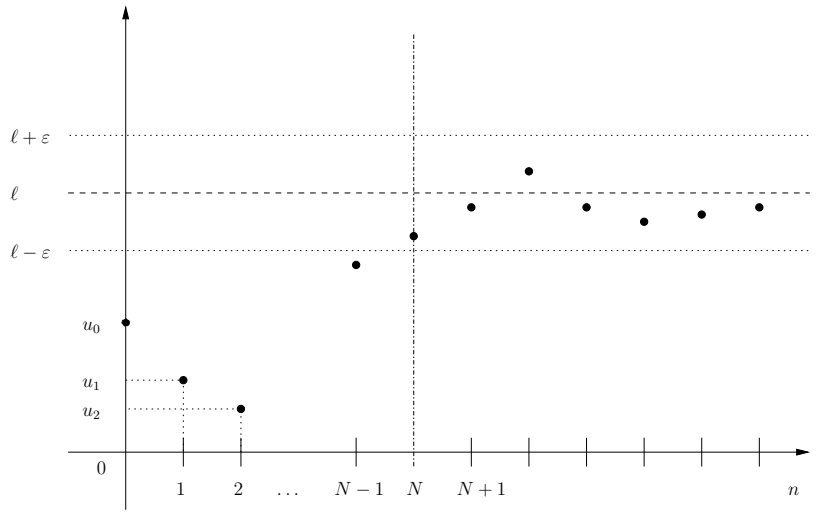


FIGURE 5. Convergence d'une suite à valeurs réelles.

DÉMONSTRATION. Par l'absurde, supposons qu'il y ait deux limites ℓ_1 et ℓ_2 distinctes. Pour $0 < \varepsilon < |\ell_1 - \ell_2|/3$, il existe $N_1 \in \mathbb{N}$ et $N_2 \in \mathbb{N}$ tels que, pour tout $n \geq \max(N_1, N_2)$, $|u_n - \ell_1| < \varepsilon$ et $|u_n - \ell_2| < \varepsilon$. Alors

$$|\ell_1 - \ell_2| \leq |u_n - \ell_1| + |u_n - \ell_2| < 2\varepsilon < \frac{2|\ell_1 - \ell_2|}{3}$$

qui amène à une contradiction. □

Une suite à valeurs réelles tend vers $+\infty$ (resp. $-\infty$) si

$$\forall A > 0,\ \exists N \in \mathbb{N},\ \forall n \geq N,\ u_n \geq A \quad (\text{resp.} u_n \leq -A).$$

Il est possible pour une suite de diverger sans tendre vers un infini ; c'est le cas, par exemple, de la suite explicite $u_n = (-1)^n$.

Exemple 5.1: Suite de Fibonnacci : Considérons la suite définie par récurrence par $F_0 = 0$, $F_1 = 1$ et, pour tout $n \geqslant 2$, $F_{n+1} = F_n + F_{n-1}$.
On montre alors par récurrence que, notant $\varphi = \frac{1+\sqrt{5}}{2} (\approx 1.618)$, on a

$$F_n = \frac{1}{\sqrt{5}} \left(\varphi^n - \frac{1}{\varphi^n} \right)$$

et on a donc $\lim_{n\to\infty} \dfrac{F_n}{\varphi^n} = \dfrac{1}{\sqrt{5}}$.

5.2. Comparaison, équivalence. Nous souhaitons pouvoir comparer des suites, et en particulier dire quand une suite est négligeable (i.e. très petite) par rapport à une autre, ou bien quand elles sont du même ordre.

5.2.1. *Négligeabilité.*

Définition 5.2

Une suite de nombres réels $(u_n)_{n\in\mathbb{N}}$ est dite négligeable devant une suite réelle $(v_n)_{n\in\mathbb{N}}$ lorsque pour tout $\varepsilon > 0$, il existe $n_0 \in \mathbb{N}$ tel que pour tout $n \geqslant n_0$ on a $|u_n| \leqslant \varepsilon |v_n|$.
On note alors $u_n = o(v_n)$ et on dit que la suite (u_n) est un petit o de la suite (v_n).

Exemple 5.3 : La suite de terme général $u_n = n$ est négligeable par rapport à la suite $v_n = n^2$.

La plupart du temps pour montrer qu'une suite est négligeable par rapport à une autre nous utiliserons le critère suivant

Proposition 5.4

Soient $(u_n)_{n\in\mathbb{N}}$ et $(v_n)_{n\in\mathbb{N}}$ deux suites réelles et supposons que v_n est non nul pour n assez grand.
Alors $u_n = o(v_n)$ si et seulement si on a $\lim\limits_{n\to\infty} \dfrac{u_n}{v_n} = 0$.

Preuve : C'est exactement la définition de la négligeabilité. □

Proposition 5.5

Soient $(u_n)_{n\in\mathbb{N}}$, $(v_n)_{n\in\mathbb{N}}$ et $(w_n)_{n\in\mathbb{N}}$ trois suites réelles. Alors

i) si $u_n = o(v_n)$ et $v_n = o(w_n)$ alors $u_n = o(w_n)$;
ii) si $u_n = o(w_n)$ et $v_n = o(w_n)$ alors pour tout $\lambda \in \mathbb{R}$ on a $u_n + \lambda v_n = o(w_n)$;
iii) si $u_n = o(w_n)$ et que v_n est bornée, alors $u_n v_n = o(w_n)$.

Preuve : Exercice. □

Les règles de comparaison entre les fonctions classiques permettent alors de voir que

i) si α et β sont deux réels tels que $\alpha < \beta$ alors $n^\alpha = o(n^\beta)$,
ii) si $\alpha > 0$ et $\beta \in \mathbb{R}$ alors $|\ln(n)|^\beta = o(n^\alpha)$,
iii) si $\alpha > 0$ et $\beta \in \mathbb{R}$ alors $n^\beta = o(\exp(\alpha n))$,
iv) si $\alpha < 0$ et $\beta \in \mathbb{R}$ alors $\exp(\alpha n) = o(n^\beta)$.

Proposition 5.6

Soient $(u_n)_{n\in\mathbb{N}}$, $(v_n)_{n\in\mathbb{N}}$ des suites à valeurs réelles telles que $u_n = o(v_n)$. Alors

i) si $u_n = o(v_n)$ et que u_n est non nul à partir d'un certain rang, alors $\frac{1}{v_n} = o(\frac{1}{u_n})$,
ii) pour tout $a > 0$ on a $u_n^a = o(v_n^a)$.

Preuve : Exercice. □

Remarque 5.7

Attention, avec les hypothèeses ci-dessus on n'a pas, en général,

i) $\ln u_n = o(\ln v_n)$, *si* u_n *est positif. Par exemple, on a* $\frac{1}{n} = o(1)$ *mais* $-\ln(n) \neq o(0)$ *! Il faut donc, en général, faire une étude dépendant des suites.*

ii) $\exp u_n = o(\exp(v_n))$. *Par exemple, si* $u_n = 0$ *et* $v_n = 1$, *on n'a pas* $1 = o(e)$.

5.2.2. *Domination.*

Définition 5.8

soient $(u_n)_{n\in\mathbb{N}}$ et $(v_n)_{n\in\mathbb{N}}$ deux suites réelles. On dit que (u_n) est dominées par (v_n) s'il existe un $n_0 \in \mathbb{N}$ et une constance C telle que pour tout $n \geqslant n_0$ on a $|u_n| \leqslant C|v_n|$.
On écrit alors $u_n = O(v_n)$ et on dit que u_n est un grand O de v_n.

En particulier, si $u_n = o(v_n)$ alors on a aussi $u_n = O(v_n)$, mais ces deux notions ne sont pas équivalentes. En effet, on a $1 = O(2)$ mais $1 \neq o(2)$.

6. Application à la complexité

La théorie de la complexité a pour but d'exprimer l'ordre de grandeur des temps de calcul des algorithmes en fonction des données initiales. Par exemple, étant donné un nombre entier n, on peut se demander quel est le temps de calcul nécessaire pour déterminer sa décomposition en facteur premier.
En général, le but n'est pas de connaître exactement le temps de calcul mais plus une majoration (parfois très fine ou très grossière selon nos besoins ou nos capacités) ou même l'ordre de grandeur de ce temps de calcul lorsque les données initiales deviennent grandes.
On peut ainsi montrer que, lorsque n devient très grand, le temps de calcul nécessaire à la factorisation de n est un $O(e^\ell)$ où ℓ est le nombre de bits de n, qui est lui-même de l'ordre de $\log_2(n)$.

6.0.1. *Exponentiation.* Pour un nombre réel a fixé et un entier $n \in \mathbb{N}$ lde calcul de a^n par l'algorithme naïf (par la formule de récurrence $a^{\ell+1} = a^\ell.a$) demande n multiplication.
L'algorithme introduit dans ce cours demande exactement $\log_2 n$ calculs de carré (les nombres a, a^2, $(a^2)^2, \ldots$) et au plus $\log_2 n$ multiplication. On a donc un temps de calcul au plus égal à $2\log_2 n$, i.e. $O(\log(n))$

6.0.2. *L'algorithme d'Euclide.* L'étude de la complexité de l'algorithme d'Euclide a été entreprise par Gabriel Lamé en 1844 qui a ainsi inventé la théorie de la complexité. Le but en est précisément le suivant : étant donné deux entiers a et b, b étant non nul, borner le nombre d'étapes nécessaires au calcul du pgcd de a et b en fonction de la grandeur de ces deux nombres.

Pour cela, notons $T(a, b)$ le nombre d'étapes nécessaire pour calculer le pgcd de a et b.
Ce nombre ne dépend en fait vraiment que de a et b, et pas seulement de leur grandeur. En effet, si ℓ est un entier, le détail de l'algorithme d'Euclide montre que $T(a, b) = T(\ell a, \ell b)$.
À l'opposé, il n'y a aucun lien entre $T(a, b)$ et $T(a, b + 1)$, alors que les nombres rentrant en jeux sont de taille comparable.
Ainsi, nous n'allons pas essayer de trouver une formule exacte pour $T(a, b)$ en fonction de leur taille, mais plus une majoration en étudiant le pire des cas.
Reprenant tout d'abord l'algorithme d'Euclide, on a $a = q_0 b + r_0$ puis, tant que l'algorithme n'est pas terminé, $r_{n-2} = q_n r_{n-1} + r_n$ et on voit que

$$T(a, b) = T(b, r_0) + 1 = T(r_0, r_1) + 2 = \ldots = T(r_{n-2}, r_{n-1}) + n + 1.$$

avec $T(\ell, 0) = 0$ pour tout ℓ : c'est le critère de fin de l'algorithme.

Nous allons maintenant montrer que le cas qui demande le plus de calcul est atteint pour les nombres de la suite de Fibonacci. Plus précisément, nous allon montrer par récurrence que si $a > b$ et $T(a, b) = N$ alors $a \geqslant F_{N+2}$ et $b \geqslant F_{N+1}$.

Si $N = 1$ alors $b|a$. On a donc $b \geqslant 1 = F_2$ et $a \geqslant 2 = F_3$.
Supposons le résultat démontré au rang $N-1$. Comme on a $a = q_0 b + r_0$ et par $N = T(a,b) = T(b,r_0) + 1$ on trouve que $T(b,r_0) = N-1$ et, par hypothèse de récurrence, $b \geqslant F_{N+1}$ et $r_0 \geqslant F_N$.Comme $a > b$ et que $b > r_0$, on a $q_0 > 0$ et donc $a \geqslant b + r_0 \geqslant F_{N+1} + F_N$, ce qui prouve que $a \geqslant F_{N+2}$.
Prenant la contraposée, on trouve que si $a \leqslant F_{N+2}$ ou $b \leqslant F_{N+1}$ alors $T(a,b) \leqslant N$.
Or on a vu précédemment que $F_N = \frac{1}{\sqrt{5}}(\varphi^N - \varphi^{-N})$.
Or si $a \geqslant F_{n+2}$ si et seulement si $\sqrt{5}a \leqslant \varphi^{N+2} - \varphi^{-(N+2)}$, ce qui équivaut à

$$\sqrt{5}a \leqslant \varphi^{N+2} - 1$$

car $\varphi^{-1} \approx 0.61$ et que a est un entier.
Par suite, cela équivaut à

$$\ln_\varphi(\sqrt{5}a + 1) \leqslant N + 2$$

Finalement, on trouve que

$$T(a,b) \leqslant \max\left(\ln_\varphi(\sqrt{5}a+1) - 2, \ln_\varphi(\sqrt{5}b+1) - 1\right)$$

ce qui implique que, de manière asymptotique, on a $T(a,b) = O(\max(\ln a, \ln b))$.

6.0.3. *Exemples divers.* Nous donnons dans le tableau ci-dessous des exemples d'algorithmes ainsi que leur complexité.

Comparaison	Complexité	Problème exemple
$O(1)$	constante	Accès tableaux
$O(\log(n))$	logarithmique	Dichotomie
$O(n)$	linéaire	Parcours d'une liste de longueur n
$O(n\log(n))$	linéarithmique	Tris d'une liste de longueur n (ex. Tri fusion ou le Tri rapide)
$O(n^2)$	quadratique	Parcours tableaux 2D de taille $n \times n$
$O(n^3)$	cubique	Parcours tableaux 3D de taille $n \times n \times n$
$O(e^n)$	exponentielle	Décomposition en produit de facteurs premiers d'un nombre de n bits
$O(n!)$	factorielle	Problème du voyageur de commerce pour n villes
$O(2^{2^n})$	doublement exponentielle	Décision de l'arithmétique de Presburger pour un énoncé de longueur n
$O(n\log(\log n))$		Crible d'Eratosthène donnant tous les nombres premiers $\leqslant n$.

Annexe A

Promenade cryptographique

Les systèmes cryptographiques détaillés dans le chapitre 1 sont essentiellement numériques et relativement récents : ce sont des système de cryptographie asymétrique à clef publique. Le but de cette annexe est de détailler des algorithmes plus simples et plus anciens et qui feront l'objet du premier TP. Ils sont en général basés sur une clef qui doit être échangée avec le destinataire selon un canal différent de celui utilisé pour le message.
Cette promenade ne prétend pas être exhaustive, mais seulement de donner des exemples de différentes méthodes.

1. Le scytale

Le scytale était utilisé par les armées spartiates pour communiquer. Il est basé sur la permutation des lettres d'un message de manière précise et est composé physiquement de deux parties : un bâton d'un diamètre donné (appelé scytale), et d'un ruban sur lequel est écrit le message.
Pour coder, on enroule le ruban sur le bâton et on écrit le message sur le ruban dans la longueur du bâton. Une fois déroulé, le message écrit sur le ruban est incompréhensible car les lettres sont mélangées. Pour décoder le message, il est nécessaire d'avoir le ruban, ainsi que le bâton, celui-ci jouant donc le rôle de clef.
Ainsi, si le périmètre du rouleau permet d'écrire 5 caractères, la phrase

```
Que j'aime à faire apprendre un nombre utile aux sages!
```

devient

```
Q' ipdnbtaauaàrpr riugei erenelxe mf e o e sjeaanumu s!
```

Il est toutefois relativement simple de décoder le message si on connaît le principe du codage : il suffit d'essayer tout les diamètres de bâton possibles.

2. Le code de César

Le code de césar est le premier exemple de code monoalphabétique, dans lesquels chaque lettre est remplacée par une autre lettre de l'alphabet. Ainsi, pour le code le code de César, chaque lettre est décalée de 3 places dans l'alphabet, le "a" devient donc "c", le "b" devient "d", ... et le "z" devient "b".
La phrase

```
Que j'aime à faire apprendre un nombre utile aux sages!
```

devient donc

```
Swg l'ckog à hcktg crrtgpftg wp pqodtg wvkng cwz ucigu!
```

Pour décoder le code de César, il suffit de décaler chaque lettre du code de 3 places dans l'autre sens... La clef est donc le nombre de décalage dans l'alphabet.
Il est toutefois relativement simple de décoder le code de César à l'aide d'attaques statistiques, cf. 6.2.

3. La substitution

Généralisation du code de César, et également code monoalphabétique, l'idée de la substitution est de remplacer un alphabet par un autre (ou bien par n'importe quelle permutation des lettres de l'alphabet latin). Un tel codage a été utilisé par Conan Doyle et ses aventures de Sherlock Holmes dans la nouvelles "Les hommes dansants".
Le codage par substitution se prête beaucoup moins bien aux attaques statistiques, mais il est parfois possible de s'en sortir en y ajoutant un peu de déduction, en regardant par exemple les mots d'une lettres (qui sont rares), de deux lettres, ...

4. Le code de vigenère

Le code de Vigenère a été décrit par Blaise de Vigenère au XVIème siècle et est un exemple de code polyalphabétique. C'est une généralisation du code de César qui dépend d'un mot M qui sert de clef :
Pour coder la première lettre du message, on utilise un codage de César qui translate le "a" vers la première lettre du mot M, pour la deuxième lettre, on procède de même mais en translatant le "a" vers la deuxième lettre de M. On répète ensuite sur toute la longueur du mot M pour revenir au début une fois atteinte la fin de celui-ci.
Ainsi, si la clef est "maths", la phrase

```
Que j'aime à faire apprendre un nombre utile aux sages!
```

et codée en

```
Cux q'sumx à msurx hhbrxuvde nu famuyw gtbsw muq zssel!
```

On voit en particulier que si la clef est au moins de la longueur du message, et que celui-ci est suffisamment bien choisit, il sera impossible de décoder le message sans la clef.
Par contre, lorsque la clef est suffisamment courtes par rapport à la taille du message, l'indice de coïncidence, cf. 6.3, permet souvent de trouver la taille de la clef M. Une fois celle-ci obtenue, il est alors possible d'utiliser l'analyse fréquentielle sur les parties du message *modulo* la longueur de M.

5. La stéganographie

La stéganographie consiste en fait plus en une dissimulation car elle "cache" les messages en pleine lumière. Le message peut être caché dans tous type de support, dont nous ne donnons ici que quelques exemples parlant.

5.1. Dans un texte. En ne considérant que certaines lettres d'un texte plus long, par exemple ici le premier de chaque ligne

> Antique clef de France,
> Necteté de souffrance,
> Garant contre ennemys,
> Estappe d'asseurance,
> Recours de secourance,
> Seccurité d'amys.

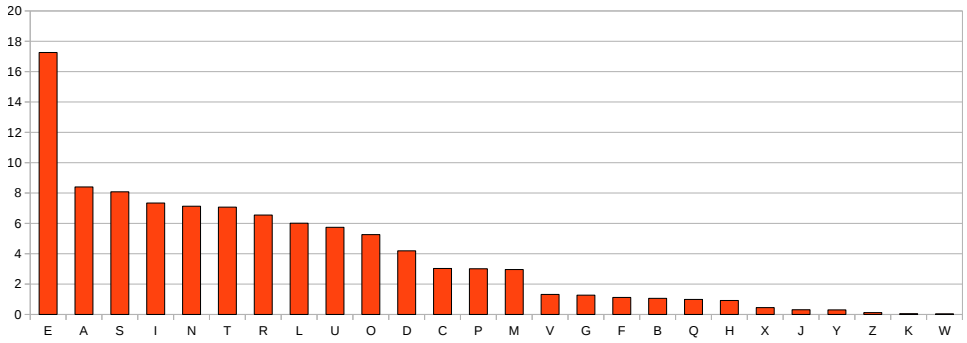
5.2. Dans une image. Étant donné une image et un message sous forme numérique, la technique classique est d'utiliser le bit de poids faible de chaque couleur de chaque pixel de l'image pour coder le message. Étant donné que seul les bits de poids faible sont changés, il est difficile de détecter visuellement un changement.
Il convient toutefois de préciser que cette méthode ne peut être utilisée qu'avec des formats d'image non compressées, ou du moins sans perte, et donc pas de jpeg (par exemple).

6. Élements de cryptanalyse

La cryptanalyse est la science du décodage des messages cryptés. L'une des hypothèses que nous utiliserons ici, et qui est potentiellement l'un des plus gros problème, est que nous connaissons l'algorithme qui a servi à coder le message. Dans le cas contraire, il peut être impossible de décoder le texte. À titre d'exemple, le manuscrit de Voynich, écrit au XVème siècle, n'est toujours pas décodé alors que de nombreux chercheurs se sont penchés dessus.
L'histoire de la cryptanalyse est assez ancienne : son premier traité fut écrit par Al-Kindi mathématicien de Bagdad du IXème siècle. On peut toutefois penser qu'elle a été inventée peu de temps après la cryptographie...

6.1. La force brute. Il est parfois possible de recourir à la force brute, et d'essayer toutes les possibilités (par exemple, pour le scytale, on peut essayer tous les diamètres pour le rouleau). Toutefois, il convient de pouvoir tester si une de ces possibilités est effectivement le bon codage, ce qui peut nécessiter l'intervention d'un être humain et ralenti donc énormément le procédé.
La pluspart du temps, la force brute est inenvisageable !

6.2. Analyse fréquentielle. L'analyse fréquentielle repose sur un constat simple : dans un texte en français, la lettre la plus fréquente sera le "e", tandis que le "w" apparaitra très peu.
Il faut toutefois prendre garde que ce constat est parfois mis en défaut : il faut que le texte soit suffisamment long pour que le calcul des fréquences ait du sens, et que le texte n'ai pas été écrit dans l'intention de mettre ce constat en défaut (cf. "La disparition", de Georges Perec).
Cette mise en garde étant faite, il est possible de calculer les fréquences d'apparition des lettres dans un texte français "au hasard" et "suffisamment long" :



Par suite, étant donné un texte français dont on sait qu'il est codé avec un code monoalphabétique, la lettre dont la fréquence est la plus haute était probablement un "e" avant le codage.

6.3. Indice de coïncidence. Dans le cas du codage de Vigenère, et plus généralement des codes polyalphabétiques, l'analyse fréquentielle est malheureusement inutile tant que la longueur de la clef n'est pas connue. Pour cela, on peut avoir recourt à l'indice de coïncidence de Friedman, qui est une généralisation des travaux de Charles Babbage.
L'idée est la suivante, pour un texte donné, on peut calculer la probabilité que deux lettres choisies aux hasard soient égales : cette probabilité est l'indice de coïncidence du texte.
Or il se trouve que pour beaucoup de textes français suffisamment long, cette probabilité est de l'ordre de $0,0746$, alors que pour un texte créé de manière aléatoire, elle serait de $26.\left(\frac{1}{26}\right)^2 \approx 0,0385$.

Pour un texte de longueur N, et dont la fréquence d'apparition de la lettre α est notée N_α, l'indice de coïncidence du texte est calculée par

$$I_c = \sum_{\alpha \in \{a,b,\cdots,z\}} \frac{N_\alpha(N_\alpha - 1)}{N(N-1)}.$$

Par suite, étant donné un texte T dont on sait qu'il a été codé avec un code de Vigenère et une clef M (inconnue pour l'instant). Le but est de trouver la longueur n de la clef. Pour cela, on regarde l'indice de coïncidence du texte T_i obtenu de T en ne gardant que les lettres en position $i \mod n$ pour chaque $i \in \{0, \cdots, n-1\}$.
Si les textes T_i ont un indice de coïncidence proche de $0,0746$, alors ils sont probablement extrait d'un texte français (modulo un codage de César dont on peut trouve la clef par analyse fréquentielle), et la longueur de la clef est probablement n. Il suffit donc d'effectuer ce test pour n variant de 1 à N afin de trouver la longueur de la clef M.
Comme pour l'analyse fréquentielle, l'indice de coïncidence de certains textes français peut être très différent de $0,0746$.

Exercices d'arithmétiques

1. La division euclidienne

Exercice 1. Calculer les pgcd et trouver une décomposition de Bézout pour les couples suivants : $(19, 3)$, $(18, 3)$, $(101, 37)$, $(501, 2)$, $(501, 9)$.

Exercice 2. Soient $a, b, c, d \in \mathbb{Z}$. Montrer les implications suivantes :

(1) Si $c \neq 0$, $(\text{pgcd}(a, b) = d) \Leftrightarrow (\text{pgcd}(ac, bc) = dc)$.

(2) $(\text{pgcd}(a, b) = 1$ et $\text{pgcd}(a, c) = 1) \Rightarrow \text{pgcd}(a, bc) = 1$.

(3) $\text{pgcd}(a, b) = 1 \Rightarrow (\forall m \geqslant 1, \forall n \geqslant 1, \text{pgcd}(a^m, b^n) = 1)$.

(4) $\text{pgcd}(a, b) = d \Rightarrow (\forall n \geqslant 2, \text{pgcd}(a^n, b^n) = d^n)$.

(5) $\text{pgcd}(a, b) = 1 \Rightarrow \text{pgcd}(a + b, ab) = 1$.

Exercice 3. Soient $a, b, c, d \in \mathbb{Z}$ tels que $ad - bc = 1$. Soient $m, n \in \mathbb{Z}$. Montrer que $\text{pgcd}(am + bn, cm + dn) = \text{pgcd}(m, n)$.

Exercice 4. Soit $n \in \mathbb{Z}$. Montrer que $\text{pgcd}(21n + 4, 14n + 3) = 1$ et que $\text{pgcd}(n^3 + 2n, n^4 + 3n^2 + 1) = 1$.

Exercice 5. Soient a et b deux entiers. Le but de cet exercice est de décrire toutes les décompositions de Bézout de a et b. Pour cela, on s'en fixe une $au_0 + bv_0 = d$ où $d = \text{pgcd}(a, b)$.

(1) Écrivons $a = da'$ et $b = db'$. Quel vaut $\text{pgcd}(a', b')$?

(2) En déduire une décomposition de Bézout de a' et b'.

(3) Donnons nous une autre décomposition de Bézout $a'u + b'v = 1$. Montrer que $a'(u_0 - u) = b'(v - v_0)$.

(4) En déduire que $a'|v - v_0$ et que $b'|u_0 - u$ (utiliser le lemme de Gauss).

(5) Montrer qu'il existe une entier k tel que $v = v_0 + ka'$ et $u = u_0 - kb'$.

(6) En déduire la forme des autres décompositions de Bézout de a et b.

Exercice 6. Donner toutes les solutions dans $\mathbb{Z}^2$ de l'équation $5x - 18y = 4$.

Exercice 7. Donner toutes les solutions dans $\mathbb{Z}^2$ de l'équation $6x + 15y = 28$.

Exercice 8 (Étude du ppcm)**.** Pour tout cet exo, on fixe deux entiers p et q.
Un entier a sera dit un être un multiple commun de p et q si $p|a$ et $q|a$. Montrer qu'il existe au moins un multiple commun à p et q. Nous noterons $\text{ppcm}(p, q)$ le plus petit commun multiple à p et q.

i) Soient a et b deux multiples communs de p et q. Montrer que pour tout $u, v \in \mathbb{Z}$ l'entier $au + bv$ est un multiple commun de p et q.

ii) Notons $c = \text{pgcd}(a, b)$. Montrer que c'est un multiple de p et q.

iii) Supposons $a = \text{ppcm}(p, q)$. Montrer que $a \leqslant c$ puis que $c \leqslant a$.

iv) En déduire que $a = c$ et que $\text{ppcm}(p, q)|b$.

On suppose désormais que p et q sont positifs et on veux montrer que

$$\mathrm{pgcd}(p,q)\cdot \mathrm{ppcm}(p,q) = pq.$$

i) Notons $d = \frac{pq}{\mathrm{pgcd}(p,q)}$. Montrer que d est un entier.

ii) Montrer que d est un multiple commun de p et de q.

iii) En déduire que d est un multiple de $\mathrm{ppcm}(p,q)$.

iv) On note $d = \alpha\cdot \mathrm{ppcm}(p,q)$, montrer que $\alpha\cdot \mathrm{ppcm}(p,q)\cdot \mathrm{pgcd}(p,q) = pq$.

v) Montrer que $\alpha\cdot \mathrm{pgcd}(p,q)$ est un diviseur commun de p et de q.

vi) En déduire que $\alpha = 1$.

Exercice 9. Résoudre dans $\mathbb{N}^2$ le système

$$\begin{cases} x+y = 56 \\ \mathrm{ppcm}(x,y) = 105 \end{cases}$$

2. Les nombres premiers

Exercice 10. Donner les nombres premiers $\leqslant 100$.

Exercice 11. Calculer les décompositions en facteurs premiers des nombres suivants : $3, 9, 21, 50, 99, 10, 47, 62$.

Pour chaque couple de nombres a, b dans la liste précédente, calculer $\mathrm{pgcd}(a,b)$.

Exercice 12. Soient $a, n \in \mathbb{N}$ avec $a, n \geqslant 2$.

i) Montrer que si $a^n - 1$ est premier alors $a = 2$ et n est premier.

ii) Montrer que si $a^n + 1$ est premier alors a est pair et n est une puissance de 2.

Exercice 13. Dire si les nombres suivants sont des nombres premiers : 101, 307, 1000, 1001.

3. Calcul dans $\mathbb{Z}/n\mathbb{Z}$

Exercice 14. Écrire les tables d'addition et de multiplication dans $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z}$ et $\mathbb{Z}/6\mathbb{Z}$.

Exercice 15. Calculer les inverses des nombres suivants dans $\mathbb{Z}/307\mathbb{Z}$: 2, 10, 154, 211, 306.

Exercice 16. Montrer que $\forall n \in \mathbb{Z}$ on a $6 | 5n^3 + n$, $9 | n^3 + (n+1)^3 + (n+2)^3$.

Exercice 17. Montrez que pour tout $n \in \mathbb{N}$ on a $7 | (3^{2n+1} + 2^{n+2})$, $7 | (4^{2^n} + 2^{2^n} + 1)$, $9 | (2^{2n} + 15n - 1)$, $11 | (2^{6n-5} + 3^{2n})$, $17 | (3\cdot 5^{2n-1} + 2^{3n-2})$.

Exercice 18. Montrez que pour tout $a, b \in \mathbb{Z}$, si $7 | a^2 + b^2$ alors $7 | a$ ou $7 | b$.

Exercice 19. Montrez que pour tout $n \in \mathbb{N}$ on a $7 \nmid 2^n + 3^n + 5^n$.

Exercice 20. Calculer la dernière décimale de 2792^{217}.

Exercice 21. Montrez que les équations

$$x^3 + y^3 + z^3 = 94 \text{ et } x^3 + y^3 + z^3 = 95$$

n'ont pas de solutions dans $\mathbb{Z}$ (on pourra raisonner modulo 9).

Exercice 22. Montrez que pour tout $a \in \mathbb{Z}$ impair et tout $n \geqslant 3$ on a $a^{2^{n-2}} \equiv 1 \mod 2^n$.

Exercice 23. Montrez que pour $a, b, c \in \mathbb{Z}^3$, si $9|a^3 + b^3 + c^3$ alors $3|a$ ou $3|b$ ou $3|c$.

3.1. Théorème chinois.

Exercice 24. Déterminer la plus petite solution positive du système

$$\begin{cases} x \equiv 3 \text{ dans } \mathbb{Z}/5\mathbb{Z} \\ x \equiv 1 \text{ dans } \mathbb{Z}/12\mathbb{Z}. \end{cases}$$

Même question avec le système

$$\begin{cases} x \equiv 9 \text{ dans } \mathbb{Z}/14\mathbb{Z} \\ x \equiv 13 \text{ dans } \mathbb{Z}/31\mathbb{Z}. \end{cases}$$

3.2. Ordre d'éléments.

Exercice 25. Calculer les ordres de tous les éléments de $(\mathbb{Z}/6\mathbb{Z})^*$.

Exercice 26. Calculer les ordres de tous les éléments de $(\mathbb{Z}/7\mathbb{Z})^*$.

Exercice 27. Calculer les ordres de tous les éléments de $(\mathbb{Z}/15\mathbb{Z})^*$.

Exercice 28. Calculer l'ordre de 2 dans $(\mathbb{Z}/n\mathbb{Z})^*$ pour tous les entiers n impairs inférieurs à 19.

Exercice 29. Sachant que 19 est premier et 2 est d'ordre 18 dans $(\mathbb{Z}/19\mathbb{Z})^*$, calculer les logarithmes en base 2 de 3, 5, 9, 17, 18 dans $(\mathbb{Z}/19\mathbb{Z})^*$.

Exercice 30. Montrer que 2 est un générateur de $(\mathbb{Z}/307\mathbb{Z})^*$.

4. Cryptographie

4.1. RSA.

Exercice 31. Soient $p = 5$, $q = 7$, $d = 5$. Calculer les clefs publique et privée pour l'algorithme RSA.
Coder puis décoder les messages $m = 9$, $m = 15$ et $m = 2$.

Exercice 32. Soient $p = 3$, $q = 5$, $d = 7$. Calculer les clefs publique et privée pour l'algorithme RSA.
Coder puis décoder les messages $m = 9$, $m = 15$ et $m = 2$.

Exercice 33. Reprendre les exercices précédents et procéder à une authentification au lieu d'un envoi de message.

Exercice 34. Considérons la clef publique $(35, 25)$ et supposons avoir intercepté le message $M = 32$. Quel est le code original ?

Exercice 35. Considérons la clef publique $(247, 11)$ et supposons avoir intercepté le message $M = 54$. Quel est le code original ?

4.2. El Gamal.

Exercice 36. Notons $p = 19$, $g = 3$, $x = 6$. Calculer les clefs privée et publique pour l'algorithme El Gamal.
Coder puis décoder le message $m = 11$.

Exercice 37. Notons $p = 307$, $g = 2$, $x = 35$. Calculer les clefs privée et publique pour l'algorithme El Gamal.
Coder puis décoder le message $m = 111$.

Exercice 38. Considérons la clef publique $(29, 3, 4)$ et supposons avoir intercepté le message $(10, 15)$. Quel est le code original ?

Exercices d'algèbres linéaires

1. Espaces vectoriel

Exercice 39. Dites si les ensembles suivants sont des sous-espaces vectoriels de $\mathbb{R}^3$:

i) L'ensemble $\left\{ \begin{pmatrix} x \\ y \end{pmatrix} z \in \mathbb{R}^3 \text{ tels que } z = 0 \right\}$

ii) L'ensemble $\left\{ \begin{pmatrix} x \\ y \end{pmatrix} z \in \mathbb{R}^3 \text{ tels que } z = 1 \right\}$

iii) L'ensemble $\left\{ \begin{pmatrix} x \\ y \end{pmatrix} z \in \mathbb{R}^3 \text{ tels que } x + y - 2z = 0 \right\}$

Exercice 40. Dans $\mathbb{R}^3$, la famille $\left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix} 1, \begin{pmatrix} 1 \\ 3 \end{pmatrix} 1, \begin{pmatrix} -2 \\ 1 \end{pmatrix} 3 \right\}$ est-elle libre ? Est-elle génératrice ?
Même questions pour la famille $\left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix} 3, \begin{pmatrix} 0 \\ 1 \end{pmatrix} 2, \begin{pmatrix} 2 \\ -3 \end{pmatrix} 0 \right\}$

Exercice 41. Déterminer une base de l'espace vectoriel engendré par les vecteurs $\begin{pmatrix} 1 \\ 2 \end{pmatrix} 3, \begin{pmatrix} 2 \\ 3 \end{pmatrix} 4, \begin{pmatrix} 3 \\ 5 \end{pmatrix} 7$ dans $\mathbb{R}^3$.

Exercice 42. Reprendre l'exercice 39 et donner des bases des ensembles qui sont des espaces vectoriels.

Exercice 43. Soient E un espace vectoriel, F et G deux sous-espaces vectoriels de E.

(1) Montrer que $F \cap G$ est un sous-espace vectoriel de E.

(2) Montrer que si $F \cup G = E$ alors $F = E$ ou bien $G = E$.

(3) Montrer que si $F \cup G$ est un sous-espace vectoriel de E alors $F \subset G$ ou bien $G \subset F$.

Exercice 44. Discuter selon les valeurs de α la dimension du sous-espace vectoriel de $\mathbb{R}^3$ engendré par les vecteurs $\begin{pmatrix} \alpha \\ 1 \end{pmatrix} 1, \begin{pmatrix} 1 \\ \alpha \end{pmatrix} 1, \begin{pmatrix} 1 \\ 1 \end{pmatrix} \alpha$.

Exercice 45. On considère, dans $\mathbb{R}^3$, les vecteurs $e = \begin{pmatrix} 1 \\ 1 \end{pmatrix} -1$, $f = \begin{pmatrix} 2 \\ 1 \end{pmatrix} 1$, $g = \begin{pmatrix} 1 \\ 1 \end{pmatrix} 3$ et $h = \begin{pmatrix} 1 \\ 1 \end{pmatrix} 1$. Notons $E = \langle \{e, f\} \rangle$ et $F = \langle \{g, h\} \rangle$.
Donner une base de $E \cap F$.

2. Applications linéaires

Exercice 46. Dire si les applications suivantes sont linéraires :

$$\begin{array}{ccc}\mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & x^2\end{array} \qquad \begin{array}{ccc}\mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & 0\end{array}$$

$$\begin{array}{ccc}\mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & 1\end{array} \qquad \begin{array}{ccc}\mathbb{R}^2 & \to & \mathbb{R} \\ \begin{pmatrix} x \\ y \end{pmatrix} & \mapsto & x-y+1\end{array}$$

$$\begin{array}{ccc}\mathbb{R}^2 & \to & \mathbb{R} \\ \begin{pmatrix} x \\ y \end{pmatrix} & \mapsto & e^x - y\end{array} \qquad \begin{array}{ccc}\mathbb{R} & \to & \mathbb{R}^2 \\ x & \mapsto & \begin{pmatrix} x \\ 3x \end{pmatrix}\end{array}$$

$$\begin{array}{ccc}\mathbb{R} & \to & \mathbb{R}^2 \\ x & \mapsto & \begin{pmatrix} x \\ 0 \end{pmatrix}\end{array} \qquad \begin{array}{ccc}\mathbb{R} & \to & \mathbb{R}^2 \\ \begin{pmatrix} x \\ y \end{pmatrix} & \mapsto & \begin{pmatrix} 5x-3y \\ 12x+4y \end{pmatrix}\end{array}$$

Exercice 47. Soit $f\colon E \to F$ une application entre deux espaces vectoriels. Montrer que f est linéaire si et seulement si $\forall u, v \in E$ et $\forall \lambda, \mu \in \mathbb{K}$ on a

$$f(\lambda u + \mu v) = \lambda f(u) + \mu f(v).$$

Exercice 48. Soit $f\colon E \to F$ une application linéaire. Notons

$$\ker(f) = \{u \in E \mid f(u) = 0_F\}.$$

Montrer que $N(f)$ est un sous espace vectoriel de E.

Exercice 49. Soit $f\colon E \to F$ une application linéaire. Notons

$$\mathrm{Im}(f) = \{f(u), u \in E\}.$$

Montrer que $\mathrm{Im}(f)$ est un sous espace vectoriel de F. Donner en une famille génératrice.

Exercice 50. Soit $f\colon E \to F$ une application linéaire. Montrer que f est injective si et seulement si $\ker f = \{0_E\}$.

Exercice 51. Soient $f\colon E \to F$ une application linéaire et $e_1, \ldots, e_n$ une base de E. Montrer que f est injective si et seulement si la famille $f(e_1), \ldots, f(e_n)$ est libre.

Exercice 52. Soient $f\colon E \to F$ une application linéaire et $e_1, \ldots, e_n$ une base de E. Montrer que f est surjective si et seulement si la famille $f(e_1), \ldots, f(e_n)$ est génératrice.

3. Matrices

Exercice 53. Dans l'ensemble $M_{2,3}(\mathbb{R})$ des matrices à deux lignes et trois colonnes, résoudre l'équation

$$\begin{pmatrix} 1 & 1 & -3 \\ 2 & -1 & 2 \end{pmatrix} - X = \begin{pmatrix} 0 & 2 & -4 \\ -1 & 0 & -1 \end{pmatrix}$$

Exercice 54. Déterminer dans $M_{2,2}(\mathbb{R})$ les matrices X et Y vérifiant

$$X + Y = \begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix} \quad \text{et} \quad X - Y = \begin{pmatrix} 1 & -4 \\ -1 & 5 \end{pmatrix}$$

Exercice 55. Calculer les produits suivants lorsque cela est possible

$$\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 3 & 0 \\ 2 & -1 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 5 & 0 \\ i & -1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 4 \\ -1 & -1 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & -1 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 1 & -4 & 0 \\ 5 & -1 & 2 \end{pmatrix}$$

Exercice 56. On considère les matrices suivantes
$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 2 & -5 \\ 1 & -1 & 2 \end{pmatrix}, B = \begin{pmatrix} 2 & 4 \\ 3 & 1 \\ -1 & -2 \end{pmatrix}, C = \begin{pmatrix} -1 & 2 & 5 \\ -6 & -2 & -1 \end{pmatrix}, D = \begin{pmatrix} 2 & 3 & 1 \end{pmatrix},$
$E = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$.
Comment doit on choisir X et Y dans $\{A, B, C, D, E\}$ pour que $X + Y$ soit défini ? Et pour que XY soit défini ? Calculer dans chacun des cas $X + Y$ ou XY.

Exercice 57. Calculer

$$\begin{pmatrix} 1 & 2 & 1 \\ 2 & 1 & 2 \\ 1 & 2 & 3 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix} - \begin{pmatrix} 2 & 1 & 2 \\ 1 & 2 & 3 \\ 1 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 1 \end{pmatrix}$$

Exercice 58. On considère les matrices $T := \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$ et $A := \begin{pmatrix} 1 & -2 & 1 \\ 2 & -3 & 3 \\ 1 & 4 & -1 \end{pmatrix}$

a) Calculer TA et AT. Si $X \in M_{3,3}(\mathbb{R})$, comment obtient-on TX à partir de X ? et XT à partir de X ? Calculer T^2.

b) Pour $E = \begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ calculer EA et AE. Si $X \in M_{3,3}(\mathbb{R})$, comment obtient-on EX à partir de X ? et XE à partir de X ?

Exercice 59. Soit $A := \begin{pmatrix} 2 & 1 & 1 \\ 1 & 4 & -1 \\ 4 & 9 & -1 \end{pmatrix}$

a) On note K_A l'ensemble des vecteurs $X = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$ tels que $AX = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$. Montrer que K_A est un sous-espace vectoriel de $\mathbb{R}^3$ et déterminer une base de K_A.

b) On pose $C_1 = A \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, C_2 = A \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, C_1 = A \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$. La famille (C_1, C_2, C_3) est-elle libre ? Déterminer une base de sous-espace vectoriel I_A de $\mathbb{R}^3$ engendré par C_1, C_2, C_3.

c) Déterminer une base de l'espace vectoriel engendré par $K_A \cup I_A$. Que peut-on dire de $K_A \cap I_A$?

Exercice 60. Déterminer les matrices $A \in M_{2,2}(\mathbb{C})$ telles que $A^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

Exercice 61. Soient $A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$ et $a, b, c \in \mathbb{R}$. Résoudre en x, y, z le système d'équations

$$\begin{cases} x + y = a \\ y + z = b \\ x + z = c. \end{cases}$$

En déduire la matrice inverse de A.

Exercice 62. Trouver les inverses des matrices suivantes (quand cela est possible)

$$\begin{pmatrix} 2 & 4 & 3 \\ 0 & 1 & 1 \\ 2 & 2 & -1 \end{pmatrix} \quad \begin{pmatrix} 1 & 1 & 2 \\ -1 & -2 & 1 \\ -1 & 2 & -8 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 \\ -1 & 4 & 7 \\ 0 & 0 & 1 \end{pmatrix} \quad \begin{pmatrix} -1 & 0 & 5 \\ -1 & 2 & 0 \\ -1 & -1 & 1 \end{pmatrix}$$

Exercice 63. Soit $M = \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix}$. Calculer M^2. En déduire que M a un inverse et donner M^{-1}.

Exercice 64. Soit $M = \begin{pmatrix} 1 & 3 \\ 1 & 1 \end{pmatrix}$. Calculer $M^2 - 2M - 2I_2$. En déduire que M a un inverse et calculer M^{-1}.

Exercice 65. Soient $A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}$ deux matrices à coefficients réels.

i) Déterminer l'ensemble E des matrices B vérifiant $AB = BA$.
ii) Prouver que E est un sous-espace vectoriel de $M_{3,3}(\mathbb{R})$.
iii) Donner une base de ce sous-espace.

Exercice 66. Soient $n \in \mathbb{N}$ et $A, B \in M_{n,n}(\mathbb{R})$. Supposons que A et B sont inversibles. Montrer que $(AB)^{-1} = B^{-1}A^{-1}$.
Soient $A = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ et $B = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$. Calculer $A^{-1}B^{-1}$, $B^{-1}A^{-1}$, $(AB)^{-1}$ et $(BA)^{-1}$.

4. Codes correcteurs

Exercice 67. Considérons la matrice

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

- Décrire les mots du code correspondant.
- Calculer la distance minimale de ce code, qu'elle est la capacité de correction ?
- Écrire une matrice de contrôle pour ce code.
- Écrire une matrice de décodage.
- Construire la table des syndromes possibles.
- Vérifier si les mots suivants sont des codes et les corriger si nécessaire

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

On voit que chaque colonne est obtenue de la première par un décalage. Des codes possédants cette propriétés sont appelés des codes cycliques.

Exercice 68. Considérons la matrice

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

- Décrire les mots du code correspondant.
- Calculer la distance minimale de ce code, qu'elle est la capacité de correction ?
- Écrire une matrice de contrôle pour ce code.
- Écrire une matrice de décodage.
- Construire la table des syndromes possibles.

Exercices sur les fonctions et la complexité

1. Études de fonctions

Exercice 69. Trouver le domaine de définition des fonctions suivantes :

i) $x \longmapsto (x-1)(x+1)$,
ii) $x \longmapsto \frac{1}{3x^2-7x-2}$,
iii) $x \longmapsto \sqrt{x^2+mx+1}$, $m \in \mathrm{R}$,
iv) $x \longmapsto \ln(3x^3-10x^2+5x+2)$.

Exercice 70. Donner le plus petit intervalle permettant d'étudier complètement les fonctions suivantes :

i) $x \longmapsto \frac{x^4+3x^2+1}{2x^2-1}$,
ii) $x \longmapsto \sin(x^3)$.

Exercice 71. Les fonctions suivantes sont-elles minorées, majorées, bornées ?

i) $x \longmapsto x^3$,
ii) $x \longmapsto 1-x^2$,
iii) $x \longmapsto \sin(x^2)$,
iv) $x \longmapsto \tan(x)$.

Exercice 72. Tracer le graphe des fonctions suivantes :

i) $x \longmapsto 2x-1$,
ii) $x \longmapsto |2x-1|$,
iii) $x \longmapsto |x^2-1|$,
iv) $x \longmapsto ||2x-1|-1|$,
v) $x \longmapsto 3x+2-\ln(x)$
vi) $x \longmapsto \frac{e^x-2}{e^x+1}$
vii) $x \longmapsto \frac{2\ln(x)-1}{x}$
viii) $x \longmapsto \frac{x^2}{x+2}e^{1/x}$
ix) $x \longmapsto \exp\left(\frac{x+3}{x^2-1}\right)$

Exercice 73. Étudier les fonctions suivantes et tracer leur graphe :

i) ($\star$) $x \longmapsto \frac{e^x-1}{e^x+1}$,
ii) $x \longmapsto x\ln(x)$,
iii) $x \longmapsto \frac{x+1}{x^2-x-1}$,
iv) $x \longmapsto \frac{\sin(x)}{x}$.

Exercice 74. Étudier la fonction $f(x) = \dfrac{x^2}{x+2}\, e^{\frac{1}{x}}$ et tracer sa courbe représentative.

2. Relation de comparaisons

Exercice 75. Trouver des relations de comparaisons entre les suites suivantes

i) n^a, $a > 0$
ii) n^{-a}, $a > 0$
iii) $\ln(n)^b$, $b > 0$
iv) $\ln(n)^{-b}$, $b > 0$
v) $\exp(cn)$, $c > 0$
vi) $\exp(-cn)$, $c > 0$

Exercice 76. Démontrer les relations de comparaisons suivantes :

$$\frac{\ln n}{n} = o(\frac{1}{\sqrt{n}}) , \quad \frac{n^2 \ln n}{2^n} = o(\frac{1}{n^4}) , \quad \frac{10^n}{n!} = o((3/2)^{-n}) .$$

$$10^n = o(\frac{\sqrt{n!}}{(4/3)^n}) , \quad n^4 2^{n^2} = o((6/5)^{n^3}) , \quad (\ln n)^4 \sqrt{n} = o(n^2 \ln(\ln n)) .$$

Exercice 77. Démontrer les relations de comparaisons suivantes :

$$\frac{\ln(n^2+n)}{n} = O(\frac{\ln(n)}{n}) , \quad \frac{n^2+\ln(n^2)}{(2n+1)^3} = O(\frac{1}{n}) , \quad \frac{3}{2^{2n+1}+n^4} = O(4^{-n}) .$$

$$\frac{2n+\sqrt{n}}{\sqrt[3]{2n+3}} = O(n^{2/3}) , \quad \ln(n^2+2n+3) = O(\ln(n)) , \quad \frac{4n^2+3n\cos(n)}{5n-\sin(n+3)} = O(n) .$$

Exercice 78. Démontrer les relations de comparaisons suivantes :

$$\frac{4n^3-\sqrt{n^5+3n^4}}{(\sqrt{2}n+\sqrt{n})^4} \sim \frac{1}{n} , \quad \frac{\ln(2^{n+\sqrt{n}})}{\ln(2^{n\sqrt{n}})} \sim \frac{1}{\sqrt{n}} , \quad \frac{\sqrt[3]{n^2+2n\cos(n)}}{\sqrt{n^3+n^2\sin(n)}} \sim n^{-5/6} .$$

$$\frac{2n+\ln(n^3)}{\sqrt{4n+5}} \sim \sqrt{n} , \quad \frac{\ln(2^{n^2+3n})}{\ln(2^{n\sqrt{n}})} \sim \sqrt{n} , \quad \frac{\sqrt[3]{n^2+2n\cos(n)}}{\sqrt{n+\sin(n)}} \sim \sqrt[6]{n} .$$

Exercice 79. Soit N fixé, montrer que

$$\sum_{n=1}^{N} \frac{1}{n} \sim \ln(N).$$

On pourra pour cela se ramener à comparer la série à une intégrale.

Exercice 80. Soit N fixé, montrer que

$$\ln(N!) \sim N\ln(N) - N.$$

On pourra pour cela se ramener à comparer la série à une intégrale.
On peut en fait montrer que

$$N! \sim N^N e^{-N} \sqrt{2_p i N}.$$

C'est la formule de Stirling.

3. Complexité

Exercice 81. Étant donné des entiers n et ℓ, donner le temps de calcul pour le calcul de la puissance n^ℓ par

i) l'algorithme naïf
ii) l'algorithme rapide vu en cours.

Exercice 82 (Evaluation d'un polynôme)**.** Considérons un polynôme $P(x) = a_0 + a_1 x + \ldots + a_n x^n$ et un réel α.

i) Calculer le nombre d'opération nécessaire à l'évaluation du polynôme P en α par une méthode naïve.

ii) Décomposons le polynôme P sous la forme

$$P(\alpha) = a_0 + \alpha(a_1 + \alpha(a_2 + \alpha(\ldots +)))$$

Donner le temps de cacul par cette méthode (c'est la méthode de Horner).

Exercice 83. Considérons la suite de Fibonacci définie par $u_0 = 1$, $u_1 = 1$ puis $u_{n+1} = u_n + u_{n-1}$.

(1) Construire un algorithme récursif pour le calcul de u_n (i.e. à l'aide d'une fonction `F` qui appellera `F(n)` et `F(n-1)` pour calculer `F(n+1)`). Quel est le temps de calcul ?

(2) Construire un algorithme itératif pour le calcul de u_n. Quel est le temps de calcul ?

Comparer les temps de calculs pour les deux implémentations.

Exercice 84. Considérons un tableau T de longueur n et un élément x. La question est de savoir si x est dans la table, et de renvoyer sa position dans la table si on l'y trouve.

i) Donner une majoration du temps de calcul pour la recherche de la position de x dans la table.

ii) Dans le cas où le tableau est ordonné (i.e. $T(i) < T(i+1)$ pour tout i) il est possible d'utiliser l'algorithme de dichotomie. Donner dans ce cas le temps de calcul pour la recherhce de la position de x.

Exercice 85. Étant donné un entier n, donner une majoration du temps de calcul pour la recherche des nombres premiers $\leqslant n$ par la méthode du crible d'Eratosthène sous la forme simplifiée suivante

```
T(1:n) = 1
pour tout i de 2 à sqrt(n)
   pour tout j de 2 à floor(n/i)
      T(j*i) = 0
   end
end
```

Exercice 86. Étant donné un entier n, donner une majoration du temps de calcul pour le décomposer en produit de facteurs premiers.

Exercice 87. Étant donnés une matrice A de taille $n \times n$ et un vecteur b de K^n, donner le temps de calcul nécessaire à la résolution du système

$$Ax = b$$

par l'algorithme du pivot de Gauss.