Rappels maths L3IF

Alice Pellet--Mary

18 octobre 2017

Table des matières

1 Surjection, Injection et Bijection

Notations 1. Dans toute cette partie, on utilisera les notations suivantes :

- X et Y sont des ensembles non vides quelconques (par exemple $\mathbb{R}$ ou $\mathbb{N}$, ...)
- f est une fonction de X dans Y, on note $f : X \to Y$.

Définition 1. *Une application $f : X \to Y$ est injective si pour tout $(a, b) \in X^2$, $a \neq b \implies f(a) \neq f(b)$. En d'autres termes, tout élément de Y est atteint par au plus un élément de X.*

Une application $f : X \to Y$ est surjective si pour tout $y \in Y$, il existe $x \in X$ tel que $f(x) = y$. En d'autres termes, tout élément de Y est atteint par au moins un élément de X.

Une application est bijective si elle est injective et surjective, i.e. tout élément de Y est atteint par exactement un élément de X. Ce qui s'écrit mathématiquement $\forall y \in Y, \exists! x \in X \quad t.q. \quad y = f(x)$.

Dessins.

Exercice 1. Dire si les fonctions suivantes sont des injections/surjection/bijections.

1. $f : \mathbb{R} \to \mathbb{R}$ tel que $f(x) = x^2$
2. $f : \mathbb{R} \to \mathbb{R}^+$ tel que $f(x) = x^2$
3. $f : \mathbb{R}^+ \to \mathbb{R}^+$ tel que $f(x) = x^2$
4. $f : \mathbb{R} \to \mathbb{R}$ tel que $f(x) = 2x + 1$
5. $f : \mathbb{R} \to \mathbb{R}$ tel que $f(n) = 5 * n^3 + 7$

Exercice 2. Trouver des bijections entre les ensembles suivants (et dessiner leur graphe).

de $\mathbb{R}$ dans $\mathbb{R}_+^*$ de $\mathbb{R}_+^*$ dans R de $]-\Pi, \Pi[$ dans $\mathbb{R}$

de $\mathbb{N} \times \mathbb{N}$ dans $\mathbb{N}$ de $\mathbb{N}$ dans $\mathbb{N} \times \mathbb{N}$

Remarque. Si on a $f : X \to Y$ et $g : Y \to X$ telles que $g \circ f$ soit l'identité sur X, alors f est injective et g est surjective.

Théorème 1. *Une application $f : X \to Y$ est injective si et seulement si il existe une application $g : Y \to X$ telle que $g \circ f$ soit égale à l'application identité sur X (on dit que f est inversible à gauche).*

Exemple 1. la fonction $f : x \mapsto x^2$ est injective de $\mathbb{R}^+$ dans $\mathbb{R}$ car la fonction $g : \mathbb{R} \to \mathbb{R}^+$ définie par $g(x) = \sqrt{x}$ si $x \geq 0$ et $g(x) = 0$ si $x < 0$ est une inverse à gauche pour f : on a $g \circ f = \mathrm{id}_{\mathbb{R}^+}$. Attention, g n'est pas l'inverse à droite de f car $f \circ g(x) = 0$ pour tout x négatif, donc $f \circ g$ n'est pas l'identité sur $\mathbb{R}$.

Théorème 2. *Une application $f : X \to Y$ est surjective si et seulement si il existe une application $g : Y \to X$ telle que $f \circ g$ soit égale à l'application identité sur X (f est inversible à droite).*

Exemple 2. la fonction $f : x \mapsto x^2$ est surjective de $\mathbb{R}$ dans $\mathbb{R}^+$ car la fonction $g : \mathbb{R}^+ \to \mathbb{R}$ définie par $g(x) = \sqrt{x}$ est une inverse à droite pour f : on a $f \circ g = \mathrm{id}_{\mathbb{R}^+}$. Attention, g n'est pas l'inverse à gauche de f car $g \circ f(x) = |x|$ (valeur absolue de x), qui n'est pas l'identité sur $\mathbb{R}$.

Théorème 3. *Une application $f : X \to Y$ est bijective si et seulement si elle est inversible, c'est à dire qu'il existe $g : Y \to X$ tel que $f \circ g$ et $g \circ f$ soient l'identité sur X et Y respectivement.*

Théorème 4 (Cantor-Bernstein)**.** *S'il existe des fonctions $g : Y \to X$ et $f : X \to Y$ injectives alors il existe une fonction $h : X \to Y$ bijective. On dit alors que X et Y sont en bijection.*

Exercice 3. Déterminer les ensembles qui sont en bijections dans la liste suivante (penser à utiliser Cantor-Bernstein) : $\mathbb{N}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{N} \times \mathbb{N}$, $\mathbb{R}^2$, $]0,1[$, $]0,1[\times]0,1[$, $]a,b[$ (pour $a < b$ dans $\mathbb{R}$), $\mathbb{Q}$, $\mathbb{N}^3$.

2 Trucs utiles pour les calculs de complexité

On regroupe dans cette partie plusieurs résultats utiles pour calculer des complexités.

2.1 Comportement asymptotique de fonctions

On définit ici les notations O, o, Θ... d'abord d'un point de vue mathématique, puis avec les mains.

Définition 2. *Soit une fonction $g : \mathbb{N} \to \mathbb{R}^+$, on note :*

- $O(g) = \{f :$ *il existe des constantes positives c, n_0 telles que $\forall n \geq n_0,\ 0 \leq f(n) \leq cg(n)$}$\}$
- $\Omega(g) = \{f :$ *il existe des constantes positives c, n_0 telles que $\forall n \geq n_0,\ 0 \leq cg(n) \leq f(n)$}$\}$
- $\Theta(g) = \{f :$ *il existe des constantes positives c_1, c_2, n_0 telles que $\forall n \geq n_0,\ 0 \leq c_1 g(n) \leq f(n) \leq c_2 g(n)$}$\}$
- $o(g) = \{f :$ *pour toute constante $c \geq 0$, il existe une constante n_0 telle que $\forall n \geq n_0,\ 0 \leq f(n) \leq cg(n)$}$\}$
- $\omega(g) = \{f :$ *pour toute constante $c \geq 0$, il existe une constante n_0 telle que $\forall n \geq n_0,\ 0 \leq cg(n) \leq f(n)$}$\}$

Remarque.

1. On pourrait élargir la définition précédente à $g : \mathbb{R} \to \mathbb{R}^+$ mais on ne s'en servira pas ici (il suffit de remplacer $n \in \mathbb{N}$ par $x \in \mathbb{R}$ qui tend vers $+\infty$).
2. Dans la pratique, si vous continuez en informatique, vous n'entendrez parler que du O, et parfois (rarement) du Ω et du Θ (vous pouvez oublier le reste, mais il faut maîtriser le O).

Interprétation (des notations O, Ω et Θ)**.**

- Dire que $f \in O(g)$ (ce qui s'écrit aussi $f = O(g)$ par abus de notation), c'est dire que f croit moins vite que g, à une constante près.
- Dire que $f \in \Omega(g)$ (ce qui s'écrit aussi $f = \Omega(g)$ par abus de notation), c'est dire que f croit plus vite que g, à une constante près.
- Dire que $f \in \Theta(g)$ (ce qui s'écrit aussi $f = \Theta(g)$ par abus de notation), c'est dire que f croit aussi vite que g, à une constante près.

Interprétation (des notations o et ω)**.**

Dire que $f \in o(g)$ (ce qui s'écrit aussi $f = o(g)$ par abus de notation), c'est dire que f croit beaucoup moins vite que g (un ordre de grandeur moins vite).

Dire que $f \in \omega(g)$ (ce qui s'écrit aussi $f = \omega(g)$ par abus de notation), c'est dire que f croit beaucoup plus vite que g.

Propriétés 1. *Si la fonction g ne s'annule pas sur $\mathbb{N}$, les définitions précédentes pour o et ω sont équivalentes aux définitions suivantes :*

- $o(g) = \{f : \lim_{n\to\infty} \frac{f(n)}{g(n)} = 0\}$

- $\omega(g) = \{f : \lim_{n\to\infty} \frac{g(n)}{f(n)} = 0\}$

Exercice 4. Donner les inclusions des ensembles $O(g)$, $\Omega(g)$, $\Theta(g)$, $o(g)$ et $\omega(g)$.

Propriétés 2 (manipuler les O)**.**

- *Si $f \in O(g)$ et c est une constante positive, alors $cf \in O(g)$*
- *Si $f_1, f_2 \in O(g)$, alors $f_1 + f_2 \in O(g)$*
- ***Attention**, si $f_1, f_2 \in O(g)$ on n'a **pas** forcément $f_1 f_2 \in O(g)$ (donner un contre-exemple)*

- *Si P et Q sont deux polynômes non nuls de degré d_P et d_Q, alors $\frac{P(n)}{Q(n)} = \Theta(n^{d_P - d_Q})$*

Exercice 5. Pour toutes les fonctions f et g ci-dessous, déterminer si $f = O(g)$, $f = \Omega(g)$, $f = \Theta(g)$, $f = o(g)$ ou $f = \omega(g)$.

- $f(n) = cos(n)$ et $g(n) = n$.
- $f(n) = n^2$ et $g(n) = n^5$.
- $f(n) = \sqrt{n}$ et $g(n) = n$.
- $f(n) = n^{7/9}$ et $g(n) = n^{11/13}$.
- $f(n) = log(n)$ et $g(n) = n$.
- $f(n) = nlog(n)$ et $g(n) = n/g(n) = n^{1+\varepsilon}$ pour un $\varepsilon > 0$.
- $f(n) = 2^n$ et $g(n) = n$.
- $f(n) = 2^n$ et $g(n) = 2^{n+1}/g(n) = 2^{2n}$.
- $f(n) = 2n + 7 + 5\log(n)$ et $g(n) = n$.
- $f(n) = \frac{n^2+\log n}{13+n}$ et $g(n) = n/g(n) = n^2$.
- $f(n) = 2^n + 5n$ et $g(n) = n^4 + 3n^2 + 9$.
- $f(n) = n!$ et $g(n) = exp(n)/g(n) = n^n$.

Remarque (Lien avec les complexités)**.** Lorsqu'on cherche à estimer la complexité d'un algorithme, on essaye en général d'obtenir un résultat de la forme « l'algorithme toto effectue $O(f(n))$ opérations sur des bits/entiers/mots/... pour une entrée de taille n » (que l'on résume habituellement en « l'algorithme toto a une complexité en $O(f(n))$ », mais on perd de l'information en disant cela). Parfois, lorsque l'on veut être plus précis, on remplace le O par un Θ.

Exercice 6. Donner la complexité en nombre d'opération sur les entiers d'un algorithme pour calculer $n!$ (la complexité dépendra de n). Et pour calculer $n! + 2^n$? Et $2n! + n^2 + 5$?

2.2 Suites récurrentes

Définition 3. *Une suite $(u_n)_{n\in\mathbb{N}}$ est dite récurrente si elle vérifie une relation du type $u_{n+k} = f(u_{n+k-1}, \ldots, u_n)$ pour un certain k et une certaine fonction f de k variables (relation valable pour tout n). On dit alors que la suite est récurrente d'ordre k.*

Remarque. Les suites récurrentes apparaissent régulièrement lors des calculs de complexité de programmes récursifs.

Exemple 3. Considérons le programme `fact` qui calcul $n!$ de manière récursive en faisant $n \times \texttt{fact}(n-1)$. Si on note $T(n)$ le nombre d'opérations sur les entiers nécessaires pour calculer $\texttt{fact}(n)$ on a $T(n) = T(n-1) + 1$. $T(n)$ est une suite récurrente d'ordre 1, la fonction f de la définition précédente est alors $f(x) = x + 1$.

Dans l'exemple précédent, pour calculer la complexité de notre programme `fact`, on aimerait une expression exacte de $T(n)$. On voit ici facilement par récurrence que l'on a $T(n) = n - 1$, qu'en est-il dans les cas plus généraux ? On va voir dans la suite certaines classes de suites qui apparaissent régulièrement en complexité et que l'on sait calculer.

Théorème 5. *Soit une suite $(u_n)_{n\geq 0}$ vérifiant $\forall n$, $u_{n+1} = ru_n$ alors*

$$\forall n,\ u_n = u_0 r^n$$

La suite u_n est dite "récurrente linéaire d'ordre 1" ou encore "géométrique".

Théorème 6. *Soit une suite $(u_n)_{n\geq 0}$ vérifiant $\forall n$, $u_{n+1} = u_n + k$ alors*

$$\forall n,\ u_n = u_0 + nk$$

La suite u_n est dite "arithmétique".

Remarque. On retrouve le cas particulier de la fonction `fact` précédente.

Théorème 7. *Soit une suite $(u_n)_{n\geq 0}$ vérifiant $\forall n$, $u_{n+2} = bu_{n+1} + cu_n$. Pour calculer le terme général de cette suite, on cherche des solutions particulières en résolvant l'équation liée à la suite $X^2 = bX + c$. On distingue ensuite deux cas :*

- *Il y a deux racine λ_1, λ_2 : alors u_n est de la forme $u_n = c_1\lambda_1^n + c_2\lambda_2^n$ pour des constantes c_1 et c_2 à déterminer (on détermine c_1 et c_2 à partir de u_0 et u_1).*
- *Il y a une racine double λ : alors u_n est de la forme $u_n = (c_1 + c_2 n)\lambda^n$ (on détermine encore c_1 et c_2 à partir de u_0 et u_1).*

La suite u_n est dite récurrente linéaire d'ordre 2.

Exercice 7. Calculer u_n dans les cas suivants :

1. $u_n = u_{n-1} + 5$ et $u_0 = 2$.
2. $u_n = 4u_{n-1}$ et $u_0 = 7$.
3. $u_n = -u_{n-2}$ et $u_0 = 2, u_1 = -3$.
4. $u_n = 4u_{n-1} - 4u_{n-2}$ et $u_0 = 1, u_2 = 0$.
5. $u_n = 2u_{n-1} + 2^n$ et $u_0 = 1$ (*Indice :* diviser l'équation par 2^n pour se ramener à un cas connu).

Exercice 8. Calculer le nombre de façon de placer des dominos de taille 1×2 (on peut les tourner de 90 degrés) dans un rectangle de taille $2 \times n$.

2.3 Sommes et séries

Définition 4. *On définit* $a_0 + a_1 + \ldots + a_n = \sum_{i=0}^{n} a_i$
et $\sum_{i=0}^{\infty} a_i = \lim_{n\to\infty} \sum_{i=0}^{n} a_i$

Attention avec les sommes infinies. Avant d'écrire (et de manipuler) des sommes infinies, il faut vérifier que $\sum_{i=0}^{\infty} |a_i| < +\infty$ (où $|a_i|$ désigne la valeur absolue de a_i). On dit alors que la somme est absolument convergente. Dans le cas où la somme est absolument convergente, on peut manipuler les sommes infinies comme les sommes finies sans trop de risque : on peut

permuter les termes de la somme, on peut additionner des sommes... Par contre, dans le cas où la somme n'est pas absolument convergente, plein de choses bizarres peuvent arriver (par exemple, si on prend $\sum \frac{(-1)^n}{n}$, la somme converge vers zéro, mais si on permute les termes de la somme, on peut obtenir tout ce qu'on veut, comme Π, ou encore 42... C'est parce que cette somme n'est pas absolument convergente).

Propriétés 3 (règles de calcul)**.** *On a les propriétés suivantes :*

- $\sum_{i=0}^{n}(ca_i + b_i) = c\sum_{i=0}^{n} a_i + \sum_{i=0}^{n} b_i$
- $\sum_{i=0}^{n-1} a_{i+1} = \sum_{k=1}^{n} a_k$

La première propriété est aussi vraie pour des sommes infinies absolument convergentes.

2.3.1 Séries numériques classiques

Certaines sommes (finies ou infinies) apparaissent régulièrement dans des calculs, c'est bien de savoir les calculer (et d'avoir une idée de leur comportement asymptotique).

Exemple 4 (Sommes arithmétique et puissance)**.**

- $\sum_{i=0}^{n} i = \frac{n(n+1)}{2} = \Theta(n^2)$
- $\sum_{i=0}^{n} i^2 = \frac{n(n+1)(2n+1)}{6} = \Theta(n^3)$

Exemple 5 (Séries géométriques)**.**

- $\sum_{i=0}^{n} x^i = \frac{x^{n+1}-1}{x-1}$ si $x \neq 1$ et $\sum_{i=0}^{n} x^i = n$ si $x = 1$.
- $\sum_{i=0}^{\infty} x^i = \frac{1}{1-x}$ si $|x| < 1$ (si $|x| \geq 1$, on a $\sum_{i=0}^{n} |x^i| \geq n$ et cette somme n'est pas absolument convergente, donc on l'oublie).

Exemple 6 (Série harmonique)**.** $\sum_{i=0}^{n} \frac{1}{n} = \ln n + O(1)$

Exemple 7 (Somme téléscopique)**.** On appelle somme téléscopique une somme de la forme $\sum_{i=1}^{n}(a_i - a_{i-1})$, on peut alors simplifier cette somme en $\sum_{i=1}^{n}(a_i - a_{i-1}) = a_n - a_0$ (même si ça a l'air simple, ces sommes apparaissent régulièrement).

Exercice 9. Utiliser $\frac{1}{k(k+1)} = \frac{1}{k} - \frac{1}{k+1}$ pour calculer $\sum \frac{1}{k(k+1)}$.

2.3.2 Séries entières

Définition 5 (Série entière)**.** *Une série entière est une fonction de la forme* $x \mapsto \sum_{k=0}^{+\infty} a_k x^k$*. Cette fonction est définie pour les* $x \in \mathbb{R}$ *tels que la somme* $\sum_{k=0}^{+\infty} |a_k| \cdot |x|^k$ *est finie (sinon cette somme n'est pas absolument convergente et on n'en veux pas). Le plus grand réel* R *tel que* $x \mapsto \sum_{k=0}^{+\infty} |a_k| R^k$ *est finie est appelé rayon de convergence de la série entière. Cette série entière est alors définie pour tout* $x < R$ *(au moins).*

Exemple 8. La série entière $x \mapsto \sum_{k=0}^{+\infty} \frac{x^k}{k!}$ est définie pour tout x réel, c'est la fonction exponentielle. La série entière $x \mapsto \sum_{i=0}^{\infty} x^i$ a un rayon de convergence 1 et vaut $1/(1-x)$ pour tout $|x| < 1$ (c'est faux si $|x| \geq 1$, par exemple on trouverait $\sum_{i=0}^{\infty} (-1)^i = 1/2$

Propriétés 4. *Les séries entières se comportent bien sur leur espace de définition : on peut les sommer en sommant les* a_i *terme à terme, on peut dériver terme à terme...*

Exercice 10. Dériver la série entière $x \mapsto \sum_{i=0}^{\infty} x^i$ et en déduire la valeur de $\sum_{i=0}^{\infty} i(1/2)^i$

3 Ordres

Définition 6 (Relation d'ordre)**.** *Soit* E *un ensemble, alors* $\leq$ *est une relation d'ordre sur* E *si pour tout* x, y, z *dans* E *on a*

1. $x \leq x$ *(reflexivité)*
2. *si* $x \leq y$ *et* $y \leq x$ *alors* $x = y$ *(anti-symétrie)*
3. *si* $x \leq y$ *et* $y \leq z$ *alors* $x \leq z$ *(transitivité)*

La relation d'ordre est dite totale si pour tout x *et* y *dans* E*, on peut comparer* x *et* y*, c'est à dire qu'on a soit* $x \leq y$ *soit* $y \leq x$*.*

Dessins (ordre, ordre total et pas ordre)

Exemple 9. $\mathbb{R}$ muni de $\leq$ est une relation d'ordre totale.

Exercice 11. Dire si les relations suivantes sont des relations d'ordre, et si oui dire si elles sont totales.

1. $\mathbb{N}$ muni de la relation $|$ (divisibilité : $a|b$ si a divise b).

2. $\mathbb{Z}^*$ muni de la relation $|$ (divisibilité : $a|b$ si a divise b).

3. E est un ensemble d'ensembles, et la relation est l'inclusion (si A et B sont dans E ont dit que A est plus petit que B si $A \subseteq B$).

Exercice 12. Sur $\mathbb{N} \times \mathbb{N}$ on définit l'ordre suivant : $(a, b) \leq_{\mathbb{N}^2} (c, d)$ ssi $a < c$ ou $a = c$ et $b \leq d$. Sinon on a $(c, d) \leq_{\mathbb{N}^2} (a, b)$. Pourquoi est-ce un ordre ? Est-il total ? Quel est son nom ?

4 Algèbre

4.1 Groupes, anneaux, corps

Définition 7 (Groupe)**.** $(G, \times)$ *est un groupe si :*

- *Pour tous a et b éléments de G, le résultat $a \times b$ est aussi dans G. (loi interne)*
- $(a \times b) \times c = a \times (b \times c)$ *(associativité)*
- *Il existe un élément e de G tel que, pour tout a dans G, $e \times a = a \times e = a$ (e est appelé élément neutre)*
- *Pour tout élément a de G, il existe b dans G tel que $a \times b = b \times a = e$ (b est appelé l'inverse de a, souvent noté a^{-1})*

Remarque.

1. Attention, on n'a pas forcément $a \times b = b \times a$ (penser aux matrices : $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$). Si pour tout a et b dans G on a $ab = ba$ alors on dit que le groupe est commutatif ou abélien.

2. La loi du groupe peut être notée multiplicativement (comme dans la définition précédente) ou additivement (on a alors la loi $+$, et on note $a+b$, l'élément neutre est noté 0 et l'inverse de a est noté $-a$). Pour éviter de faire des bêtises, on réserve la notation additive aux groupes commutatif (c'est quelque chose de classique en maths, dès que vous voyez un groupe $(G,+)$, c'est qu'il est commutatif, même si ce n'est pas dit explicitement).
3. Lorsque la loi est notée multiplicativement, l'élément neutre e est parfois noté 1 (par analogie avec $\mathbb{R}$).
4. Il faut parfois bien préciser la loi du groupe, par exemple $(\mathbb{R},+)$ et $(\mathbb{R}^*,\times)$ sont deux groupes différents. Dans un cas on ne fait qu'additionner les éléments et dans l'autre cas on ne fait que les multiplier.

Exercice 13. Déterminer si les ensembles suivants sont des groupes ou non, et dans le cas où ce ne sont pas des groupes expliquer pourquoi. Parmi les groupes, préciser ceux qui sont commutatifs.

- $(\mathbb{N},+)$
- $(\mathbb{Z},+)$
- $(\mathbb{R},+)$
- $(\mathbb{Z}/n\mathbb{Z},+)$
- $(\mathbb{Z},\times)$
- $(\mathbb{R},\times)$
- $(\mathbb{R}^*,\times)$
- $(\mathbb{Q}^*,\times)$
- On note M_2 l'ensemble des matrices 2×2 sur $\mathbb{R}$ et GL_2 l'ensemble des matrices 2×2 inversibles. Que dire de $(M_2,+)$, et de $(GL_2,\times)$?

Exemple 10. Encore un exemple de groupe non commutatif : les bijections de $\mathbb{R}$ dans $\mathbb{R}$ muni de la composition comme loi de groupe (c'est-à-dire que $fg = f\circ g$ ou $\circ$ désigne la composition des deux fonctions). Ne pas oublier de se restreindre aux bijections si on veux que nos fonctions soient inversibles.

Définition 8 (Anneau (unitaire))**.** *On dit que $(A,+,\times)$ est un anneau (unitaire) s'il existe des éléments $0,1\in A$ tels que pour tout $a,b,c\in A$, on a :*

- $(a+b)+c = a+(b+c)$
- $a+b=b+a$
- $a+0=0+a=a$
- *pour tout $a\in A$, $\exists b$, $a+b=b+a=0$*
- $(a\times b)\times c = a\times(b\times c)$ *(associativité de $\times$)*

- $a \times (b + c) = a \times b + a \times c$ *(distributivité de* $\times$ *sur* $+$*)*
- $(b + c) \times a = b \times a + c \times a$ *(distributivité de* $+$ *sur* $\times$*)*
- $a \times 1 = 1 \times a = a$ *(élément neutre pour* $\times$*)*

Remarque.
1. Un anneau est un groupe commutatif $(A, +)$ (c'est ce que disent les 4 premières propriétés), auquel on a rajouté une loi de multiplication $\times$ qui doit vérifier quelques propriétés sympatiques (associativité, distributivité...).
2. Attention, $(A, \times)$ n'est pas forcément un groupe, même si on retire l'élément 0 de A (qui n'est jamais inversible), on peut avoir des éléments qui n'ont pas d'inverse pour la loi $\times$. C'est justement lorsque tous les éléments de A sont inversibles sauf zéro qu'on dira que A est un corps (voir après).
3. Si $a \times b = b \times a$ pour tout a et b alors l'anneau est dit commutatif.

Exercice 14. Déterminer si les ensembles suivants sont des anneaux (commutatifs ?).

- $(\mathbb{N}, +, \times)$
- $(\mathbb{Z}, +, \times)$
- $(\mathbb{Z}/n\mathbb{Z}, +, \times)$
- $(\mathbb{Q}, +, \times)$
- $(\mathbb{R}, +, \times)$
- $(\mathbb{R}[X], +, \times)$, où $\mathbb{R}[X]$ désigne l'ensemble des polynômes à coefficients dans $\mathbb{R}$

Définition 9 (Corps)**.** $(K, +, \times)$ *est un corps si c'est un anneau commutatif et que tout élément différent de* 0 *possède un inverse pour la loi* $\times$*.*

Remarque.
1. Remarquez les notations classiques : G pour groupe, A pour anneau et K pour korps (le matheux n'est pas très bon en orthographe).
2. $(K^*, \times)$ est un groupe (où K^* désigne $K \setminus \{0\}$) : tous les éléments non nuls ont un inverse pour la loi $\times$.
3. Remarquez qu'un corps est un anneau qui est toujours commutatif par définition. Certains vieux matheux s'amusent à parler de "corps commutatifs" et à définir les corps comme n'étant pas forcément commutatifs, mais il n'y a qu'au 4ème étage de l'ENS qu'ils s'embêtent avec ça. Pour tout le reste du monde un corps est commutatif par définition (et il n'y a donc pas besoin de préciser "commutatif").

Exercice 15. Déterminer si les ensembles suivants sont des corps ou non.

- $(\mathbb{Z}, +, \times)$
- $(\mathbb{Q}, +, \times)$
- $(\mathbb{R}, +, \times)$
- $(\mathbb{R}[X], +, \times)$

Le cas de $\mathbb{Z}/n\mathbb{Z}$

Définition 10 (Rappel : $\mathbb{Z}/n\mathbb{Z}$)**.** *Soit n un entier supérieur à 2. On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble $\{0, 1, \ldots, n-1\}$ muni des lois $+$ et $\times$ qui consistent à faire les opérations modulo n.*

Exercice 16. Dans $\mathbb{Z}/8\mathbb{Z}$, calculer $2 \times 5 + 3 - 27$.

Remarque. Lorsque l'on dit que 9 est dans $\mathbb{Z}/7\mathbb{Z}$, c'est que l'on réduit 9 mod $7 = 2$ pour obtenir un élément de $\{0, 1, \ldots, 6\}$.

Théorème 8. *Soit n un entier supérieur à 2, alors $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau. C'est un corps si et seulement si n est un nombre premier.*

Exercice 17 ($\mathbb{Z}/p\mathbb{Z}$)**.** Montrer que $\mathbb{Z}/4\mathbb{Z}$ n'est pas un corps (trouver un élément non inversible). Essayer de voir pourquoi plus généralement $\mathbb{Z}/nm\mathbb{Z}$ n'est pas un corps (n et m sont des entiers quelconques supérieurs ou égaux à 2).

Les anneaux $\mathbb{Z}/n\mathbb{Z}$ interviennent très souvent en informatique car c'est ce que manipulent les ordinateurs. En général, les ordinateurs utilisent des entiers de 64 bits : on ne peut pas stocker des entiers aussi grand qu'on veut, la mémoire de l'ordinateur n'est pas infinie. On a donc décidé que la taille maximal d'un entier était 64 bits, c'est à dire que les entiers sont compris

entre 0 et $2^{64}-1$. Que faire alors lorsqu'un entier dépasse 2^{64} (suite à une addition ou une multiplication par exemple) ? Le choix qui a été fait est de revenir à zéro (oublier les bits qui devraient apparaître à gauche après le 64ème), c'est à dire que les ordinateurs calculent modulo 2^{64}. Les éléments manipulés par les ordinateurs ne sont donc pas des entiers de $\mathbb{Z}$ mais des éléments de $\mathbb{Z}/2^{64}\mathbb{Z}$. D'où l'intérêt de bien comprendre ces anneaux $\mathbb{Z}/n\mathbb{Z}$ (et ne pas hésiter à me poser des questions si ce n'est pas clair).

En plus, les anneaux $\mathbb{Z}/n\mathbb{Z}$ apparaissent aussi beaucoup en calcul formel, cryptographie, et tout ce qui est arithmétique en général.

4.2 Espace vectoriel

Définition 11 (Espace vectoriel)**.** *E est un espace vectoriel sur un corps K pour les opérations $+$ et $\cdot$ si :*

*$(E,+)$ est un **groupe commutatif** et pour tous vecteurs u, v de E et tous scalaires λ, μ dans K, on a :*

- $\lambda \cdot (u+v) = (\lambda \cdot u) + (\lambda \cdot v)$
- $(\lambda + \mu) \cdot u = (\lambda \cdot u) + (\mu \cdot u)$
- $(\lambda\mu) \cdot u = \lambda \cdot (\mu \cdot u)$
- $1 \cdot u = u$

Remarque.

1. Les éléments de E sont appelés des vecteurs et les éléments de K sont appelés des scalaires.
2. En pratique, le seul espace vectoriel que vous risquez de rencontrer est $\mathbb{R}^n$ (et donc le corps K sera presque toujours $\mathbb{R}$). La théorie des espaces vectoriels n'est pas très intéressante en info (vous pouvez oublier ce qu'il y a au dessus), mais ça permet de définir proprement les matrices, qui elles sont des objets importants.

Exercice 18. Déterminer si les ensembles ci-dessous sont des $\mathbb{R}$-espaces vectoriels, et si c'est le cas, trouver un isomorphisme ($\approx$ une bijection) avec $\mathbb{R}^n$ pour un certain n.

- $\mathbb{R}$
- $\mathbb{R}^n$
- $\mathbb{Z}$
- $\mathbb{R}_m[X]$ (c'est-à-dire les polynômes à coefficients dans $\mathbb{R}$ et de degré inférieur ou égal à m).

Définition 12 (Famille libre)**.** *Soit E un K-espace vectoriel et $F = (v_1, \ldots, v_n) \in E$, F est une famille libre si pour tout i, v_i n'est pas une combinaison lineaire des autres v_j. C'est à dire que pour tout $a_1, \ldots, a_n$ dans K on a $\sum_{i=1}^{n} a_i v_i = 0 \Rightarrow a_1 = \cdots = a_n = 0$.*

Remarque. En général, pour montrer qu'une famille est libre, on suppose qu'on a des a_i tels que $\sum_{i=1}^{n} a_i v_i = 0$ et on essaye de montrer qu'alors les a_i sont nécessairement tous nuls.

Définition 13 (Famille génératrice)**.** *Soit E un K-espace vectoriel et $F = (v_1, \ldots, v_n) \in E$, F est une famille génératrice si pour tout $v \in E$, il existe $a_1, \ldots, a_n$ dans K tels que $v = a_1 v_1 + \cdots + a_n v_n$.*

Définition 14 (Base)**.** *Une base est une famille génératrice libre.*

Théorème 9. *Soit E un K-ev alors toutes les bases de E ont le même cardinal, qu'on appelle dimension de E noté $dim(E)$.*

Remarque. Pour montrer qu'une famille $(v_1, \ldots, v_n)$ est une base, on montre en général qu'elle est libre en utilisant la remarque ci-dessus, puis on montre qu'elle est génératrice en utilisant la définition. Si on sait déjà que la dimension de l'espace vectoriel est n, il suffit de faire l'une des 2 vérifications (celle qui semble la plus facile, en général c'est vérifier que la famille est libre).

Théorème 10 (base incomplète)**.** *Soit E un espace vectoriel :*

- *toute famille libre de vecteurs peut être complétée en une base de E ;*
- *de toute famille génératrice de E on peut extraire une base de E.*

Exercice 19. Quelle est la dimension des $\mathbb{R}$-espaces vectoriels suivants ? Donner une base de ces espaces vectoriels.

1. $\mathbb{R}^n$

2. $\mathbb{R}_n[X]$ (ensemble des polynômes de degré inférieur ou égal à n).

Exercice 20. Avec $E = \mathbb{R}^3$: quelles sont les familles libres/génératrices et les bases ?

- $(1,0,0)$, $(0,1,0)$, $(0,0,1)$?
- $(0,0,1)$, $(0,4,0)$?
- $(3,0,1)$, $(0,0,1)$, $(0,4,0)$?
- $(1,0,1)$, $(1,0,0)$, $(0,0,1)$?

4.3 Matrices

Définition 15. *L'espace des matrices de taille $n \times m$ à coefficients dans un corps K est noté $M_{n,m}(K)$. Si $m = n$ on raccourcis la notation en $M_n(K)$.*

Propriétés 5 (multiplication de matrices)**.** *Si $M = (m_{i,j})_{1 \leq i,j \leq n}$ et $N = (n_{i,j})_{1 \leq i,j \leq n}$ sont deux matrices de taille n, leur produit est $MN = (q_{i,j})_{1 \leq i,j \leq n}$ ou $q_{i,j} = \sum_{k=1}^{n} m_{i,k} n_{k,j}$. On dit qu'on multiplie "ligne par colonne".*

Exercice 21. Calculer $\begin{pmatrix} 1 & 7 \\ -3 & 5 \end{pmatrix} \begin{pmatrix} 4 & 3 \\ 0 & 1 \end{pmatrix}$

Le multiplication de matrices est-elle commutative ?

Définition 16. *Une matrice M est inversible s'il existe une matrice M^{-1} telle que $MM^{-1} = M^{-1}M = Id$.*

Définition 17 (déterminant)**.** *Le déterminant d'une matrice $M \in M_n(k)$ est*

$$det(M) = \sum_{\sigma \in S_n} \varepsilon(\sigma) m_{1,\sigma(1)} m_{2,\sigma(2)} \dots m_{n,\sigma(n)}$$

où $m_{i,j}$ désignent les coefficients de M et $\varepsilon(\sigma)$ désigne la signature de la permutation σ.

Rappel : Si la permutation σ se décompose en cycles disjoints $c_1, \dots, c_k$ alors la signature de σ est $\varepsilon(\sigma) = (-1)^{\sum_{i=1}^{k} e_i}$ ou $e_i = 1$ si le cycle c_i est de longueur paire, et $e_i = 0$ sinon.

Remarque. Pour calculer un déterminant, on n'utilise presque jamais la formule du dessus. En général, si on fait le calcul à la main on développe par rapport à une ligne ou une colonne. Et si on a un ordinateur, on fait un pivot de Gauss. Le pivot de Gauss a une complexité $O(n^3)$ alors que développer par rapport à une ligne ou une colonne a une complexité $O(n!)$ donc le pivot de Gauss est beaucoup plus efficace. Mais à la main, si on a de petites matrices, c'est souvent plus pratique de développer par rapport à une ligne ou une colonne.

Propriétés 6. *Une matrice $M \in M_n(K)$ est inversible ssi son déterminant est non nul. C'est la méthode la plus simple qu'on utilise en général pour vérifier qu'une matrice est inversible.*

Exercice 22. Calculer le déterminant des matrices suivantes et dire si elles sont inversibles

$$\det \begin{bmatrix} 1 & 7 \\ -3 & 5 \end{bmatrix} =$$

$$\det \begin{bmatrix} 1 & 7 & 4 \\ -3 & 5 & 1 \\ 0 & 2 & -5 \end{bmatrix} =$$

Propriétés 7. *On a pour toute matrices A et B dans $M_n(K)$, on a* $\det(AB) = \det(A)\det(B)$.

4.3.1 "Le pivot c'est beau"

On a dit plus haut que le pivot de Gauss pouvait être utilisé pour calculer le déterminant. Dans les cours de maths, on l'introduit aussi souvent pour résoudre des systèmes linéaires. En fait le pivot de Gauss permet de faire énormément de choses en algèbre linéaire : résoudre un système linéaire, calculer le déterminant, calculer l'inverse d'une matrice, calculer le noyau d'une matrice (les vecteurs v tels que $Mv = 0$), extraire une base à partir d'une famille génératrice, trouver un système d'équations pour décrire un sous-espace vectoriel... Bref, presque tout ce que vous pouvez vouloir faire en algèbre linéaire peut se faire avec un pivot de Gauss (sauf calculer les valeurs propres d'une matrice, ça c'est une autre histoire). Et en plus le pivot de Gauss se calcule bien avec un ordinateur (en $O(n^3)$ opérations dans K, c'est polynomial).
Conclusion : Ne pas hésiter à se servir du pivot de Gauss.

Le pivot de Gauss qu'est-ce que c'est ? En général, on appelle pivot de Gauss des opérations élémentaires faites sur les lignes et les colonnes d'une matrice pour se ramener à une forme de matrice plus simple (par exemple triangulaire, ou diagonale, ou carrément l'identité selon ce qu'on veut obtenir). Il y a trois types d'opérations élémentaires sur les lignes :

(1) Échanger les lignes i et j. Cela revient à multiplier à gauche par la matrice $\begin{pmatrix} 1 & & & & & \\ & 1 & & & & \\ & & 0 & 1 & & \\ & & 1 & 0 & & \\ & & & & \ddots & \\ & & & & & 1 \end{pmatrix}$, ou les deux 1 qui ne sont pas sur la diagonale correspondent aux lignes et colonnes i et j. Cette matrice est appelée matrice de permutation.

(2) Ajouter un multiple de la ligne j à la ligne i (ce que l'on note parfois $L_i \leftarrow L_i + aL_j$). Cela revient à multiplier à gauche par la matrice

$\begin{pmatrix} 1 & & & & & \\ & 1 & & & & \\ & & \ddots & & & \\ & & & 1 & a & \\ & & & & \ddots & \\ & & & & & 1 \end{pmatrix}$, où le a se trouve sur la ième ligne et jème colonne. Cette matrice s'appelle matrice de transvection.

(3) Multiplier la ligne i par une constante a. Cela revient à multiplier à gauche par la matrice $\begin{pmatrix} 1 & & & & & \\ & 1 & & & & \\ & & \ddots & & & \\ & & & a & & \\ & & & & \ddots & \\ & & & & & 1 \end{pmatrix}$, où le a se trouve sur la ième ligne et ième colonne. Cette matrice est appelée matrice de dilatation.

Remarque.

- Pour retrouver la matrice à laquelle correspond une opération, on fait cette opération sur la matrice identité et on renvoie la matrice obtenue.
- Bien sûr on peut faire les même opérations élémentaires sur les colonnes, en multipliant pas des matrices de permutation/transvection/dilatation à droite cette fois et plus à gauche.

Calculer le déterminant

Propriétés 8. *Les matrices de transvection on un déterminant égal à* 1 *et les matrices de permutation ont un déterminant égal à* -1 *(car ici on n'échange les lignes que deux par deux). Donc si on ne fait que des opérations élémentaires de type (1) et (2) on multiplie le déterminant de notre matrice par* ± 1*. Pour obtenir le bon déterminant à la fin, il suffit de compter le nombre* m *de matrices de permutation qu'on a utilisées et multiplier le déterminant par* $(-1)^m$*.*

Remarque. En ne faisant que des opérations du type (1) et (2), on peut mettre notre matrice sous forme diagonale sans changer son déterminant. On peut ensuite calculer le déterminant d'une matrice diagonale facilement (en prenant le produit des éléments diagonaux).

Exercice 23. Utiliser le pivot de Gauss pour calculer le déterminant de la matrice suivante

$$\begin{bmatrix} 1 & 7 & 4 \\ -3 & 5 & 1 \\ 0 & 2 & -5 \end{bmatrix}$$

Résoudre un système linéaire

On veut résoudre un système linéaire représenté sous forme matricielle par $Ax = b$ (où les lignes de A correspondent aux différentes équations linéaires, b et x sont des vecteurs colonne et x est le vecteur des inconnues). Avec le pivot de Gauss, en ne faisant des opérations que sur les lignes (c'est à dire en ne multipliant que par des matrices à gauche), on peut trouver une matrice R, produit de matrices de permutation/transvection/dilatation, telle que RA soit triangulaire. La matrice R est forcément inversible car les matrices de permutation/transvection/dilatation le sont, donc le système $Ax = b$ est équivalent à $(RA)x = Rb$. Mais maintenant RA est une matrice triangulaire, donc on sait résoudre le système "en remontant" (cf exercice).

Remarque. On n'a pas besoin de connaître la matrice R, on peut se contenter de faire les opérations sur les lignes de A et faire les même opérations sur b en parallèle (ce qui revient à multiplier b à gauche par R).

Exercice 24. Résoudre le système linéaire

$$\begin{aligned} 3x_1 + 2x_2 - 1 &= 0 \\ -x_1 + 5x_2 + 2x_3 - 2 &= 0 \\ x_1 + x_2 + x_3 &= 0 \end{aligned}$$

4.4 Arithmétique

Définition 18 (PGCD)**.** *Soient a et b deux entiers, on appelle PGCD de a et b et on note $d = pgcd(a, b)$ (parfois aussi notés $a \wedge b$ ou encore (a, b)) le plus grand entier (au sens de la division) qui divise à la fois a et b.*

Remarque. Au sens de la division, a et $-a$ sont aussi grand l'un que l'autre (ils se divisent tous les deux). Deux entiers a et b ont donc toujours deux PGCD dans $\mathbb{Z}$: d et $-d$. On parle quand même souvent "du" PGCD par abus (alors qu'il y en a deux), parce que le signe importe peu en général (on peut supposer que le PGCD est toujours positif par exemple, auquel cas il n'y en a qu'un).

Propriétés 9. *Pour calculer le PGCD de a et b on fait des divisions euclidiennes successives jusqu'à obtenir un reste nul. Si les entiers sont petits, on peut aussi les décomposer en produit de nombre premiers et s'en servir pour calculer le PGCD, mais c'est une méthode à oublier quand les entiers sont grands : factoriser un grand nombre c'est très difficile.*

Exercice 25. Calculer le PGCD de 412 et 327 en utilisant des divisions successives puis en factorisant les entiers.

Théorème 11 (Bezout)**.** *Soient a et b des entiers relatifs et d leur PGCD, alors il existe u et v dans $\mathbb{Z}$ tels que $au + bv = d$.*

Remarque.

- Réciproquement, si on a u et v tels que $av + bv = c$ alors c est un multiple de d (on note $d|c$).
- Les entiers u et v ne sont pas uniques, on a même une infinité de couples (u, v) qui satisfont le théorème.

Remarque. Pour calculer u et v on utilise un algorithme appelé "PGCD étendu", c'est à dire qu'on calcule le PGCD pas divisions successives comme précédemment puis on remonte les égalités pour calculer u et v.

Exercice 26. Calculer u et v tels que $412u + 327v = \text{pgcd}(412, 327)$.

Définition 19. *On dit que deux entiers a et b sont premiers entre eux si leur PGCD vaut 1.*

Théorème 12 (Théorème chinois)**.** *Soient p et q premiers entre eux et a et b deux entiers, alors il existe un entier c tel que $c \equiv a \mod p$ et $c \equiv b \mod q$.*

Interprétation. Ce théorème apparait pour la première fois au 3ème siècle, dans un livre de l'auteur chinois Sun Zi pour résoudre le problème suivant : "Soient des objets en nombre inconnu. Si on les range par 3 il en reste 2. Si on les range par 5, il en reste 3 et si on les range par 7, il en reste 2. Combien a-t-on d'objets ?" (ref Wikipédia).

Les problèmes faciles en arithmétique

Les problèmes suivants sont faciles à résoudre avec un ordinateur (c'est à dire qu'on a des algorithmes en temps polynomial) :

- Étant donné a et n des entiers premiers entre eux, calculer b tel que $ab = 1 \mod n$ (c'est à dire calculer l'inverse de a dans l'anneau $\mathbb{Z}/n\mathbb{Z}$). Ce calcul se fait avec le théorème de Bezout : on calcule u et v tels que $au + vn = 1$, on a alors que $au = 1 - vn \equiv 1 \mod n$ donc u convient.
- Calculer le c du théorème chinois. Là encore on utilise le théorème de Bezout. On commence par chercher c_1 tel que $c_1 \equiv 1 \mod p$ et $c_1 \equiv 0 \mod q$. Comme p et q sont premiers entre eux le théorème de Bezout nous donne u et v tels que $pu + qv = 1$. Donc $c_1 = qv$ convient. De même, $c_2 = pu$ vérifie $c_2 \equiv 0 \mod p$ et $c_2 \equiv 1 \mod q$. Il ne reste ensuite plus qu'à prendre $c = ac_1 + bc_2$.
- Tester si un nombre n est premier (l'algorithme pour résoudre ce problème est compliqué et ne date que de 2003). Attention, savoir si un nombre est premier ou non est facile, mais même si on sait que notre nombre n'est pas premier, on ne peut pas le factoriser facilement. L'algorithme qui permet de tester si un nombre est premier ou non ne calcule pas de facteur de ce nombre.

Les problèmes difficiles en arithmétique

Pour les problèmes suivants, on n'a pas actuellement d'algorithme polynomial, ce qui ne veux pas dire qu'il n'en existe pas, seulement qu'on ne les a pas trouvé pour l'instant :

- Factoriser un entier n. C'est sur ce problème que repose le cryptosystème RSA.
- Étant donné un grand nombre n, un élément g de $\mathbb{Z}/n\mathbb{Z}$ et $g^a \mod n$, retrouver a. Ce problème est appelé logarithme discret et est utilisé dans le chiffrement de El Gamal.

4.5 Polynômes

Définition 20 (Polynômes)**.** *Soit K un corps, on définit $K[X]$ l'anneau des polynômes à une indéterminée sur K par*

$$K[X] = \{a_0 + a_1X + \cdots + a_nX^n, \text{ pour un certain } n \in \mathbb{N}, a_i \in K\}$$

Les éléments de $K[X]$ sont appelés polynômes à coefficients dans K et n est le degré du polynôme (si $a_n \neq 0$).

Propriétés 10 (Racines d'un polynôme)**.**

- *Un polynôme de degré n a au plus n racines.*
- *Si $K = \mathbb{C}$ alors un polynôme de degré n a exactement n racines (comptées avec multiplicité). C'est faux dans $\mathbb{R}$ (trouver un contre exemple).*

Remarque. $K[X]$ est un anneau. C'est même un anneau très proche de $\mathbb{Z}$: on peut faire des divisions euclidiennes, factoriser des polynômes, parler de PGCD de polynômes...

Les problèmes liés aux polynômes sont en général plus simples qu'avec les entiers (il n'y a pas de retenue lorsqu'on fait une addition par exemple, et factoriser des polynômes est facile si K est un corps fini...).

Globalement, ce qu'il faut retenir, c'est qu'il y a beaucoup d'analogies entre les polynômes et les entiers, et que les problèmes sont en général aussi faciles voire plus faciles pour les polynômes que pour les entiers.

Propriétés 11 (Division euclidienne de polynômes)**.** *Soient P_1 et P_2 deux polynômes non nuls. Alors il existe des polynômes Q et R tels que*

$$P_1 = P_2 Q + R$$

et $\deg(R) < \deg(P_2)$.

Exercice 27. Calculer les divisions euclidiennes des polynômes suivants (à coefficients dans $\mathbb{R}$) :

- $P_1 = X$ et $P_2 = X^2$
- $P_1 = X^2$ et $P_2 = X$
- $P_1 = X^4 + 3X^2 - X + 2$ et $P_2 = X^2 + 3$

Définition 21. *Si $R = 0$ dans la division euclidienne, on dit que P_2 divise P_1. Dans ce cas, toutes les racines de P_2 sont aussi des racines de P_1.*

Définition 22. *Soient P et Q deux polynômes, on appelle PGCD de P et Q le plus grand polynôme (au sens de la divisibilité) qui divise P et Q.*

Remarque. Comme précédemment, le PGCD n'est pas unique : si on le multiplie par un élément de K on a toujours un PGCD. Mais abusivement on parle souvent "du" PGCD.

Propriétés 12. *On peut calculer le PGCD de deux polynômes comme pour les entiers, en faisant des divisions euclidiennes successives et en gardant le dernier reste non nul.*

Exercice 28. Calculer le PGCD de $P_1 = X^4 + 3X^2 - X + 2$ et $P_2 = X^2 + 3$.

Propriétés 13. *Si $K = \mathbb{C}$, alors P et Q ont un PGCD différent de 1 si et seulement si ils ont une racine commune (on dit qu'ils sont premiers entre eux si leur PGCD vaut 1).*

Exercice 29. Les polynômes $X^2 - 1$ et $X^2 - 2X + 1$ sont-ils premiers entre eux ?

Définition 23. *Un polynôme P de $K[X]$ est dit irréductible si pour tous Q et R tels que $P = QR$, on a Q ou R qui est de degré 0. C'est l'équivalent des nombres premiers pour les entiers.*

Exercice 30.

- $X^2 + 1$ est-il irréductible sur $\mathbb{C}$? Et sur $\mathbb{R}$?
- Quels sont les polynômes irréductibles sur $\mathbb{C}$?
- Quels sont les polynômes irréductibles sur $\mathbb{R}$?

Propriétés 14. *soit P un polynôme, alors P s'écrit de façon unique (à permutation près des termes et multiplication par une constante) comme un produit de polynômes irréductibles. C'est l'analogue de la décomposition en facteurs premiers pour les entiers.*

Exercice 31. Décomposer $X^4 - 1$ en facteurs irréductibles dans $\mathbb{C}$ et dans $\mathbb{R}$.

Remarque. On peut aussi considérer des polynômes avec des coefficients dans un anneau au lieu d'un corps, mais dans ce cas là, beaucoup des résultats précédents ne sont plus vrais (on n'a plus de division euclidienne, plus forcément de factorisation, on n'a plus forcément non plus le fait que le nombre de racines est inférieur au degré...). De façon générale, il vaut mieux éviter de manipuler des polynômes à coefficients dans un anneau tant que vous n'avez pas bien réfléchis à la question. On peut facilement faire des bêtises.

Remarque. $K[X]$ n'est jamais un corps. En effet, $\deg(PQ) = \deg(P) + \deg(Q)$, donc X n'est jamais inversible (et tous les polynômes de degré non nul ne sont jamais inversibles) car si on avait P tel que $XP = 1$ alors $\deg(P) + 1 = 0$ ce qui contredit le fait que $\deg(P)$ est positif.

Définition 24 (Fractions rationnelles)**.** *On définit le corps des fractions rationnelles sur K par*

$$K(X) = \{P/Q, avecP, Q \in K[X]\}$$

Les éléments de $K(X)$ sont appelés fractions rationnelles à coefficients dans K.

Remarque. Contrairement à $K[X]$, on a que $K(X)$ est un corps. C'est l'analogue de $\mathbb{Q}$.

5 Probabilités

5.1 Dénombrement

Exercice 32.

1. Soit A un alphabet contenant n lettres. Combien peut-on former de mots de taille l avec des lettres de A.

2. J'ai un ensemble de n boules différentes. J'en pioche k (l'ordre ne compte pas), combien de sous-ensembles de taille k différents puis-je obtenir ?

3. J'ai n boules différentes, de combien de façon est-ce que je peux les ordonner ?

Propriétés 15. *Souvent, lorsque l'on fait des probas discrètes, on peut calculer des probabilités grâce au dénombrement. Si j'ai un ensemble d'événements E qui sont tous équiprobables et que A est un sous-ensemble de E, alors on a $\mathbb{P}(A) = |A|/|E|$ (où $|A|$ désigne le nombre d'éléments de A).*

Remarque. Attention, pour que cette méthode marche il faut bien que tous les événements soient équiprobables.

Exercice 33.

1. J'ai un dé non pipé, quelle est la probabilité de faire un 1 ? Et de faire un nombre pair ? Et si le dé est pipé ?

2. J'ai n nombres différents, triés par ordre croissant. Je les mélange (en utilisant une permutation tirée uniformément). Quelle est la probabilité que le premier élément soit toujours le plus petit ?

3. Je tire deux cartes d'un jeu de 52 cartes. Quelle est la probabilité que j'obtienne une paire de rois ?

4. J'ai deux boules bleues et une boule rouge. J'en pioche deux, quelle est la probabilité que j'ai pioché les deux bleues ?

5.2 Événements disjoints / indépendants

Propriétés 16. *Soit E un ensemble d'événements et A et B deux sous-ensembles de E disjoints, alors on a $\mathbb{P}(A \cup B) = \mathbb{P}(A) + \mathbb{P}(B)$.*

Remarque. Cette formule, qui dit qu'on peut sommer les probabilités si les événements sont disjoints, est souvent très utile en probabilités. Elle admet la généralisation suivante (qui est aussi souvent utile).

Propriétés 17 (formule du crible)**.** *Soit E un ensemble d'événements et A et B deux sous-ensembles de E (par forcément disjoints), alors on a $\mathbb{P}(A \cup B) = \mathbb{P}(A) + \mathbb{P}(B) - \mathbb{P}(A \cap B)$.*

Dessin

Exercice 34.

1. J'ai un dé pipé qui renvoie 1 avec probabilité 1/2 et les autres numéros avec probabilité 1/10. Quelle est la probabilité d'obtenir un numéro inférieur ou égal à 2 ? et à 3 ?

2. J'ai n entiers différents, triés par ordre croissants. J'applique une permutation choisie uniformément à ces entiers. Quelle est la probabilité que le premier ou le deuxième entier n'ait pas bougé ?

Définition 25. *Soient A et B deux événements. Si $\mathbb{P}(B)$ est non nul, on définit la probabilité conditionnelle de A sachant B par $\mathbb{P}(A|B) = \frac{\mathbb{P}(A \cap B)}{\mathbb{P}(B)}$.*

Interprétation. Comme son nom l'indique, la probabilité de A sachant B est la probabilité que A ait lieu, si on sait déjà que B a eu lieu.

Exercice 35. J'ai un dé non pipé. Calculer les probabilités conditionnelles suivantes :

1. Probabilité d'avoir 1 sachant que j'ai un nombre pair.

2. Probabilité d'avoir 1 sachant que j'ai un nombre impair.

3. Probabilité d'avoir un nombre impair sachant que j'ai 1.

Définition 26. *On dit que A et B sont indépendants si $\mathbb{P}(A|B) = \mathbb{P}(A)$.*

Remarque. La notion d'indépendance porte assez bien son nom : deux événements sont indépendants si avoir des infos sur l'un ne donne pas d'informations sur l'autre. Attention par contre, on peut avoir deux événements qui dépendent l'un de l'autre mais qui sont indépendants quand même (voir exo 36).

Propriétés 18. *Si $\mathbb{P}(B) \neq 0$, alors A et B sont indépendants si et seulement si $\mathbb{P}(A \cap B) = \mathbb{P}(A)\mathbb{P}(B)$.*

Exercice 36. Déterminer si les événements suivants sont indépendants (j'ai toujours un dé non pipé que je lance).

1. $A =$ " mon dé renvoie un nombre pair" et $B =$ " mon dé renvoie 1".

2. J'ai maintenant deux dés non pipés, $A =$ " le premier dé renvoie un nombre pair" et $B =$ " le deuxième dé renvoie 1".

3. J'ai deux pièces non truquées que je lance, $A =$ " la première pièce renvoie pile" et $B =$ " les deux pièces renvoient la même chose".

Exercice 37. Calculer les probabilités suivantes.

1. J'ai deux dés non pipés. Quelle est la probabilité qu'ils renvoient 1 tous les deux ?

2. J'ai deux dés non pipés, quelle est la probabilité qu'au moins un des deux renvoie un nombre pair ?

3. J'ai 5 pièces non truquées, je dit que les pièces renvoient 1 pour face et 0 pour pile. Quelle est la probabilité que mes 5 pièces me donnent le tirage 01100 ?

5.3 Variables aléatoires

Définition 27 (Avec les mains)**.** *Une variable aléatoire X à valeur dans χ est une variable qui prend les valeurs de χ avec une certaine probabilité.*

Exemple 11.

1. J'ai un dé non pipé. Alors la variable X qui prend la même valeur que le dé est une variable aléatoire.

2. Je lance une pièce deux fois. Soit X qui vaut a si j'ai deux fois pile, b si j'ai deux fois face et c sinon. Alors X est une variable aléatoire.
3. Soit X qui vaut tout le temps 1, c'est une variable aléatoire.

5.3.1 Lois classiques

On donne ici les lois discrètes classiques.

Définition 28 (Loi de Bernoulli)**.** *Une variable aléatoire X suit une loi de Bernoulli de paramètre p (avec $0 < p < 1$) si elle vaut 1 avec probabilité p et 0 avec probabilité $1 - p$. On note $X \sim B(p)$.*

Exemple 12. Si on lance une pièce non truquée et que X vaut 1 si la pièce fait pile et 0 sinon, alors X suit une loi de Bernoulli de paramètre $1/2$. Si la pièce est truquée, X suit une loi de Bernoulli de paramètre p pour un certain p.

Définition 29 (Loi binomiale)**.** *Soient $X_1, \ldots, X_n$ des variables de Bernoulli indépendantes, de même paramètre p. Alors $Y = \sum_{k=i}^{n} X_k$ suit une loi binomiale de paramètres n et p. On note $Y \sim Binom(n, p)$. On a alors, si $0 \leq k \leq n$*

$$\mathbb{P}(Y = k) = \binom{n}{k} p^k (1-p)^{n-k}$$

et si $k < 0$ ou $k > n$ on a $\mathbb{P}(Y = k) = 0$.

Exemple 13. Si on lance n fois une pièce et que l'on note Y le nombre de fois que l'on a observé un pile, alors Y suit une loi binomiale de paramètres n et $1/2$.

Définition 30 (Loi géométrique)**.** *Soient $X_1, X_2, \ldots$ une suite infinie de variables de Bernoulli indépendantes de même paramètre p. On note Y le premier indice pour lequel un X_i vaut 1, c'est-à-dire $Y = \min\{i, X_i = 1\}$. On dit alors que Y suit une loi géométrique de paramètre p. On note $Y \sim Geom(p)$. On a alors, pour tout $k \geq 1$*

$$\mathbb{P}(Y = k) = (1-p)^{k-1} p$$

et si $k \leq 0$ on a $\mathbb{P}(Y = k) = 0$.

Exemple 14. On lance une pièce non truquée jusqu'à obtenir un pile. On note Y le nombre de fois qu'on a du lancer la pièce pour obtenir notre pile, alors Y suit une loi géométrique de paramètre $1/2$.

Remarque. La loi géométrique est une loi sans mémoire, c'est à dire que $\mathbb{P}(Y = n + k \mid Y \geq n) = \mathbb{P}(Y = k)$. Elle modélise la désintégration d'une particule radioactive : si on sait que la particule n'est pas désintégrée au bout de n années, elle a autant de chance de se désintégrer pendant la $(n+1)$-ème année qu'elle n'en avait au début de se désintégrer dans la première année.

Définition 31 (Loi de Poisson)**.** *On dit que Y suit une loi de Poisson de paramètre λ si pour tout $k \in \mathbb{N}$ on a*

$$\mathbb{P}(Y = k) = e^{-\lambda}\frac{\lambda^k}{k!}$$

et $\mathbb{P}(Y = k) = 0$ pour les autres valeurs de k.

Remarque. La loi de Poisson modélise le nombre d'événements qui arrivent dans un laps de temps donné, si les événements sont indépendants des précédents. Par exemple, dans une boutique, on suppose que l'arrivée des clients ne dépend pas des clients déjà arrivés. Si le nombre moyen de clients qui entrent dans la boutique en une heure est λ, alors la probabilité qu'en une heure k clients entrent dans la boutique vaut $\mathbb{P}(Y = k)$, où Y suit une loi de Poisson de paramètre λ.

En remplaçant la boutique et les clients par un serveur et des paquets, on peut modéliser de la même manière le nombre de paquets qui arrivent à un serveur wifi par unité de temps (il y a un cours de M1 qui parle de ça, et qui utilise plein de variables aléatoires de Poisson).

5.3.2 Espérance et Variance de variables aléatoires

Définition 32 (Espérance)**.** *On définit l'espérance d'une variable aléatoire X à valeurs dans $\chi \subset \mathbb{R}$ par*

$$\mathbb{E}[X] = \sum_{x\in\chi} x\mathbb{P}(X = x)$$

Remarque. Attention, certaines variables aléatoires peuvent ne pas avoir d'espérance. Par exemple si X est à valeur dans $\mathbb{N}^*$ et que pour tout $k \in \mathbb{N}^*$ on a

$$\mathbb{P}(X = k) = \frac{\alpha}{k^2},$$

avec $\alpha = 6/\pi^2$. On a alors

$$\mathbb{E}[X] = \sum_{k\in\mathbb{N}} k\mathbb{P}(X = k) = \sum_{k\in\mathbb{N}} \frac{\alpha}{k} = +\infty$$

On dit alors que la variable aléatoire X n'a pas d'espérance. Dans toute la suite, quand on parle d'une variable X et de son espérance, on suppose sans le dire qu'on prend une variable X qui a une espérance (finie).

Propriétés 19. *Soient X et Y deux variables aléatoires réelles et $a \in \mathbb{R}$, alors on a*

- $\mathbb{E}[aX] = a\mathbb{E}[X]$
- $\mathbb{E}[X + Y] = \mathbb{E}[X] = \mathbb{E}[Y]$
- *Si X et Y sont **indépendantes** alors* $\mathbb{E}[XY] = \mathbb{E}[X]\mathbb{E}[Y]$

Remarque. Attention aux hypothèses, on peut toujours additionner des espérances, mais pour pouvoir les multiplier il faut bien que les variables soient indépendantes (voir exo 39).

Exercice 38. Calcules les espérances des variables aléatoires classiques.

1. X suit une loi de Bernoulli de paramètre p.

2. X suit une loi binomiale de paramètres n et p.

3. X suit une loi géométrique de paramètre p.

4. X suit une loi de Poisson de paramètre λ.

Exercice 39.

1. Soient X et Y deux variables de Bernoulli de paramètre p indépendantes, calculer $\mathbb{E}[XY]$.

2. Soit X une variable de Bernoulli de paramètre p et $Y = 1 - X$. Calculer $\mathbb{E}[XY]$ et $\mathbb{E}[X]\mathbb{E}[Y]$.

Définition 33 (Variance)**.** *Soit X une variable aléatoire à valeurs dans $\chi \subset \mathbb{R}$. On définit la variance de X par*

$$Var[X] = \mathbb{E}[(X - \mathbb{E}[X])^2] = \mathbb{E}[X^2] - \mathbb{E}[X]^2$$

On définit aussi l'écart type de X comme étant $\sigma = \sqrt{Var(X)}$.

Remarque. Ici encore, certaines variables aléatoires peuvent avoir une espérance mais ne pas avoir de variance (finie). Dans la suite, quand on

parle de variance d'une variable aléatoire, c'est qu'on a implicitement supposé que notre variable aléatoire avait une variance.

Propriétés 20. *Si X et Y sont des variables aléatoires* ***indépendantes****, alors $Var(X+Y) = Var(X) + Var(Y)$.*

Remarque. Attention, contrairement à l'espérance, on ne peut plus ajouter les variances tout le temps, il faut que les variables soient indépendantes. Et on ne peut rien dire en général sur la variance d'un produit (même si les variables sont indépendantes).

Attention aussi, on peut sommer les variances (quand les variables sont indépendantes), mais pas les écarts type.

Exercice 40. Calculer les variances des variables aléatoires classiques.

1. X suit une loi de Bernoulli de paramètre p.

2. X suit une loi binomiale de paramètres n et p.

3. X suit une loi géométrique de paramètre p.

4. X suit une loi de Poisson de paramètre λ.

Exercice 41. Soit X une variable de Bernoulli de paramètre p et $Y = 1-X$. Calculer $\mathrm{Var}[X+Y]$ et $\mathrm{Var}[X] + \mathrm{Var}[Y]$.

5.3.3 Inégalités de Markov et Tchebychev

Théorème 13 (Inégalité de Markov)**.** *Soit X une variable aléatoire positive (qui a une espérance) et $a > 0$, alors on a*

$$\mathbb{P}(X \geq a) \leq \frac{\mathbb{E}[X]}{a}$$

Remarque.

- Cette inégalité et son corollaire (inégalité de Tchebychev) sont très utiles en probas.
- Attention, pour l'inégalité de Markov il faut bien vérifier que X est positive.
- Ce n'est pas nécessaire d'apprendre la formule par cœur, elle se retrouve facilement. Il faut juste être capable de la retrouver assez rapidement.

Preuve.

Théorème 14 (Inégalité de (Bienaymé-)Tchebychev)**.** *Soit X une variable aléatoire réelle (qui a une espérance et une variance) et $a > 0$, alors on a*

$$\mathbb{P}(|X - \mathbb{E}[X]| \geq a) \leq \frac{Var[X]}{a^2}$$

Preuve.

Remarque.

- Là encore il ne faut pas apprendre la formule par cœur, elle se déduit facilement de l'inégalité de Markov.
- Ici il n'y a plus besoin d'avoir X positif. Mais il faut qu'il ait une espérance et une variance.
- Cette inégalité est très pratique en proba quand on veut montrer que la moyenne empirique (obtenue par l'expérience) converge vers la moyenne théorique (cf exo).

Exercice 42. J'ai une pièce biaisée, qui renvoie pile avec probabilité p et face avec probabilité $1-p$, mais je ne connais pas p. Comment connaître p ?

6 Analyse

6.1 dérivée

Définition 34. *On appelle dérivée de f la fonction f' définie par*

$$f'(x) = \lim_{\substack{h \to 0 \\ h \neq 0}} \frac{f(x+h) - f(x)}{h}$$

La dérivée n'existe que si cette limite est bien définie et est égale à droite et à gauche.

Exemple 15. La fonction $x \mapsto \sqrt{x}$ n'est pas dérivable en zéro car $\frac{\sqrt{0+h}-\sqrt{0}}{h} = \frac{1}{\sqrt{h}}$ n'a pas de limite finie quand h tend vers 0. Cela s'explique par le fait que la tangente à la courbe en zéro est verticale (donc de pente infinie). Faire un dessin.

Interprétation. La dérivée d'une fonction f en x_0 donne la pente de la tangente à la courbe en x_0. En particulier, si $f'(x_0) > 0$, la pente est positive,

donc la fonction est croissante au voisinage de x_0, si $f'(x_0) < 0$ la fonction est décroissante au voisinage de x_0 et si $f'(x_0) = 0$ la tangente est horizontale et on ne peut rien dire de la croissance de la fonction (par exemple la fonction $x \mapsto x^3$ a une dérivée nulle en 0 mais elle est strictement croissante).

Propriétés 21 (Opérations sur les dérivées)**.**

f	f'
$u + \lambda v$	$u' + \lambda v'$
$u \circ v$	$v' \times u' \circ v$
$u \times v$	$u' \times v + u \times v'$
f^{-1}	$\frac{1}{f'(f^{-1}(x))}$

Exemple 16 (Dérivées usuelles)**.**

domaine de définition de f	f	f'
$\mathbb{R}$	x^n, $n \in \mathbb{Z}^*$	nx^{n-1}
$\mathbb{R}_+^*$	x^α, $\alpha \in \mathbb{R}^*$	$\alpha x^{\alpha-1}$
$\mathbb{R}_+^*$	$\ln(x)$	$1/x$
$\mathbb{R}$	e^x	e^x
$\mathbb{R}$	$\cos(x)$	$-\sin(x)$
$\mathbb{R}$	$\sin(x)$	$\cos(x)$
$]-\Pi/2;\Pi/2[$	$\tan(x)$	$\frac{1}{\cos^2(x)} = 1 + \tan^2(x)$
$\mathbb{R}$	$\arctan(x)$	$1/(1+x^2)$

Remarque. En info, quand on dérive une fonction, c'est en général pour calculer son maximum ou son minimum. On fait alors comme au lycée : si on cherche le maximum de f, on calcule f', on regarde où f' est strictement positive, on en déduit le tableau de variation de f et on connaît alors les points extrémaux de f.

Exercice 43. Calculer la valeur de $p \in [0;1]$ qui maximise $p(1-p)$.

6.2 integration

Définition 35. *On note* $\int_a^b f(x)\,\mathrm{d}x$ *l'intégrale de* f *entre* a *et* b*.*
On note $\int_a^\infty f(x)\,\mathrm{d}x = \lim_{b\to\infty}(\int_a^b f(x)\,\mathrm{d}x)$ *si la limite existe.*

Remarque. Comme pour les séries, quand les intégrales ont des bornes infinies, il vaut mieux qu'elles soient absolument convergentes, c'est à dire

que $\lim_{b\to\infty}(\int_a^b |f(x)|\,\mathrm{d}x)$ soit finie. Si cette condition est vérifiée, on dit que l'intégrale est absolument convergente et tout se passera bien normalement. En revanche, si $\lim_{b\to\infty}(\int_a^b |f(x)|\,\mathrm{d}x)$ est infinie mais que la limite $\lim_{b\to\infty}(\int_a^b f(x)\,\mathrm{d}x)$ existe, on dit que l'intégrale est semi-convergente, mais c'est un abus de langage. Ce n'est pas vraiment une intégrale, juste une limite d'intégrale. Il faut donc se méfier (on n'a plus forcément Chasles, ...).

Comme pour les séries, il vaut mieux ne manipuler que des intégrales absolument convergentes.

Définition 36 (primitive)**.** *La primitive d'une fonction f est une fonction dérivable, dont la dérivée vaut f.*

Interprétation. $\int_a^b f(x)\,\mathrm{d}x$ peut s'interpréter de plusieurs façons.

- L'interprétation géométrique est que $\int_a^b f(x)\,\mathrm{d}x$ est l'aire de la surface sous la courbe entre a et b (faire un dessin).

- si f est continue, $\int_a^b f(x)\,\mathrm{d}x$ nous donne aussi une primitive de f (voir théorème 15).

Théorème 15. *Soit une fonction f continue sur $[a,b]$. On définit, pour $x \in [a,b]$*

$$F(x) = \int_a^x f(t)\,\mathrm{d}t$$

Alors F est une primitive de f.

Théorème 16.

- *Deux primitives d'une même fonction sont égales à une constante additive près. En utilisant ce résultat et le théorème précédent, on en déduit que si f est continue et si F est une primitive de f, alors on a*
$$\int_a^b f(x)\,\mathrm{d}x = F(b) - F(a)$$
- $\int_a^a f(x)\,\mathrm{d}x = 0$
- $\int_a^b f(x)\,\mathrm{d}x + \int_b^c f(x)\,\mathrm{d}x = \int_a^c f(x)\,\mathrm{d}x$ *(relation de Chasles)*
- $\int_a^b (g(x) + \lambda f(x))\,\mathrm{d}x = \int_a^b g(x) + \lambda \int_a^b f(x)\,\mathrm{d}x$ *(linéarité de l'intégrale)*

Remarque. La formule $\int_a^b f(x)\,\mathrm{d}x = F(b) - F(a)$ si f est continue et F est une primitive de f est très utile pour calculer des intégrales. C'est la première méthode à appliquer quand on essaye de calculer une intégrale : connaît-on une primitive ? Si on sait calculer directement une primitive de f, on peut calculer l'intégrale. Sinon on peut utiliser les règles de calcul

données dans les points suivants (linéarité, Chasles, ...) pour essayer de se ramener à des primitives qu'on connaît.

Si les opérations de base ci-dessus ne suffisent pas à se ramener à des primitives connues, on peut utiliser les techniques ci-dessous (intégration par partie et changement de variable).

Théorème 17.

- $\int_a^b u(x)v'(x)\,\mathrm{d}x = [uv]_a^b - \int_a^b u'(x)v(x)\,\mathrm{d}x$ *(intégration pas partie).*
- *Si f est une bijection dérivable, de dérivée continue et dont la réciproque est aussi dérivable et de dérivée continue (ça a l'air compliqué comme ça mais la plupart des bijections gentilles vérifient ces conditions), alors on a*
$$\int_a^b f\circ\phi(x)\phi'(x)\,\mathrm{d}x = \int_{\phi(a)}^{\phi(b)} f(x)\,\mathrm{d}x$$

Remarque. Ces deux formules sont souvent utiles pour calculer des intégrales. Attention pour le changement de variable à ne pas se tromper de sens, et à ne pas oublier de changer les bornes. Un bon moyen de faire (pas très rigoureux mais au moins ça évite de se planter de sens) c'est d'écrire à coté de l'intégrale $u = \phi(x)$, et après calculer $\mathrm{d}u$ en fonction de $\mathrm{d}x$ et de changer les bornes en se disant "quand $x = a$, que vaut u ?"

Exemple 17 (primitives usuelles)**.**

domaine de définition de f	f	F, une primitive de f
$\mathbb{R}$	x^n, $n\in\mathbb{Z}, n\neq -1$	$x^{n+1}/(n+1)$
$\mathbb{R}_+^*$	$1/x$	$\ln(x)$
$\mathbb{R}_+^*$	$\ln(x)$	$x\ln(x)-x$
$\mathbb{R}$	e^x	e^x
$\mathbb{R}$	$\cos(x)$	$\sin(x)$
$\mathbb{R}$	$\sin(x)$	$-\cos(x)$
$\mathbb{R}$	$1/(1+x^2)$	$\arctan(x)$

Remarque. La technique classique pour calculer des intégrales est donc la suivante : essayer de reconnaître une fonction dont on connaît une primitive, et si on n'y arrive pas, effectuer un changement de variable ou une intégration par partie pour essayer de se ramener à quelque chose qu'on sait intégrer.

Exercice 44. Calculer les intégrales suivantes :

1. $\int_0^1 \arctan(x)\,\mathrm{d}x$ (indication : on pourra poser $u'(x) = 1$, $v(x) = \arctan(x)$ et faire une intégration par partie).

2. $\int_0^{1/2} \frac{x}{\sqrt{1-x^2}}\,\mathrm{d}x$ (indication : on pourra poser $u = \sqrt{1-x^2}$ et faire un changement de variable).

7 Géométrie en dimension 3

7.1 Produit scalaire

Définition 37. *Soient* $u = \begin{pmatrix} u_1 \\ u_2 \\ u_3 \end{pmatrix}$ *et* $v = \begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix}$ *deux vecteurs de* $\mathbb{R}^3$. *On définit le produit scalaire de* u *et* v *par* $u.v = u_1v_1 + u_2v_2 + u_3v_3$. *On note aussi parfois le produit scalaire* $< u, v >$ *ou* (u, v).

Remarque. Le produit scalaire ne dépend que des vecteurs, on peut les déplacer. Par exemple, lorsqu'on fait de la géométrie et que l'on a des points A, B, C, si on note $D = C + \overrightarrow{AB}$ alors les vecteurs $\overrightarrow{AB}$ et $\overrightarrow{CD}$ sont les mêmes. En particulier, si on a quatre points de l'espace A, B, C, D et que l'on veut calculer $< \overrightarrow{AB}, \overrightarrow{CD} >$ on peut déplacer le vecteur $\overrightarrow{CD}$ pour que son point d'origine soit A et on se ramène à un produit scalaire de la forme $< \overrightarrow{AB}, \overrightarrow{AE} >$ pour un certain point E (faire un dessin).

Interprétation. D'un point de vue géométrique, on a une formule équivalente pour le produit scalaire :

$$< \overrightarrow{AB}, \overrightarrow{AC} >= \cos(\widehat{BAC})|AB||AC|$$

Plus les vecteurs sont alignés, plus le produit scalaire sera grand (en norme), et plus les vecteurs sont proches de former un angle droit, plus leur produit scalaire est proche de zéro. Le produit scalaire indique aussi si les vecteurs pointent dans la même direction (s'il est positif) ou dans des directions opposées (s'il est négatif).

Cas particulier du résultat précédent : $< \overrightarrow{AB}, \overrightarrow{AB} >= |AB|^2$.

Dessin

7.2 Produit vectoriel

Définition 38 (produit vectoriel)**.** *Dans $\mathbb{R}^3$ le produit vectoriel de deux vecteurs $\overrightarrow{u}$ et $\overrightarrow{v}$ non-colinéaires est le vecteur $\overrightarrow{w}$ tel que :*

- *$\overrightarrow{w}$ est orthogonal à $\overrightarrow{u}$ et $\overrightarrow{v}$,*
- *$(\overrightarrow{u}, \overrightarrow{v}, \overrightarrow{w})$ est de sens direct (règle de la main droite : on peut mettre $\overrightarrow{u}$ sur le pouce, $\overrightarrow{v}$ sur l'index et $\overrightarrow{w}$ sur le majeur)*
- $||\overrightarrow{w}|| = ||\overrightarrow{u}||.||\overrightarrow{v}|| \sin(\widehat{\overrightarrow{u}\,\overrightarrow{v}})$

Le produit vectoriel est noté $\overrightarrow{u} \wedge \overrightarrow{v}$.

Remarque. Attention, pour le produit scalaire on avait $< \overrightarrow{u}, \overrightarrow{v} >=< \overrightarrow{v}, \overrightarrow{u} >$ mais pour le produit vectoriel ce n'est plus vrai : $\overrightarrow{u} \wedge \overrightarrow{v} = -\overrightarrow{v} \wedge \overrightarrow{u}$.

Théorème 18.

$$\begin{pmatrix} u_1 \\ u_2 \\ u_3 \end{pmatrix} \wedge \begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix} = \begin{pmatrix} u_2v_3 - u_3v_2 \\ u_3v_1 - u_1v_3 \\ u_1v_2 - u_2v_1 \end{pmatrix}$$

Remarque. Le produit vectoriel de deux vecteurs est nul ssi les deux vecteurs sont colinéaires.

Interprétation. Si $\overrightarrow{u}$ et $\overrightarrow{v}$ sont deux vecteurs orthogonaux de norme 1, alors $\overrightarrow{u} \wedge \overrightarrow{v}$ est l'unique vecteur qui permet de compléter $(\overrightarrow{u}, \overrightarrow{v})$ en une base orthonormale (ie avec des vecteurs de norme 1 et orthogonaux) directe.

On a aussi que $||\overrightarrow{u} \wedge \overrightarrow{v}||$ est l'aire du parallélogramme engendré par $\overrightarrow{u}$ et $\overrightarrow{v}$.