Agrégation 2024

Fiches

Document intégralement écrit par Hugo Delaunay.
Visitez `agreg.skyost.eu` pour plus de ressources et d'informations.

Une coquille ? Une correction à apporter ? Rendez-vous sur le dépôt Github "`Skyost/Agregation`" ou contactez-moi via mon site web personnel `skyost.eu`.

Table des matières

1 Autour de la compacité

En utilisant la compacité, on montre diverses propriétés des espaces métriques et des espaces vectoriels normés, notamment de dimension finie.

Proposition 1. Soient (E, d_E), (F, d_f) deux espaces métriques et $f : E \to F$ continue. Si E est compact, alors $f(E)$ est compact dans F.

Démonstration. Soit (y_n) une suite d'éléments de $f(E)$. On pose $\forall n \in \mathbb{N}$, $x_n = f(y_n)$. E est compact, donc il existe une extractrice $\varphi : \mathbb{N} \to \mathbb{N}$ telle que $x_{\varphi(n)} \longrightarrow_{n\to+\infty} x$ où $x \in E$. Par continuité,

$$y_{\varphi(n)} = f(x_{\varphi(n)}) \longrightarrow_{n\to+\infty} f(x) \in f(E)$$

$f(E)$ est ainsi séquentiellement compact, donc est compact. □

Proposition 2. Soit (E, d) un espace métrique. Si $A \subseteq E$ est compacte, alors A est fermée et bornée.

Démonstration.

— Fermée : Soit (a_n) une suite d'éléments de A qui converge vers $a \in E$. Par compacité, il existe une extractrice $\varphi : \mathbb{N} \to \mathbb{N}$ telle que $a_{\varphi(n)} \longrightarrow_{n\to+\infty} a'$ où $a' \in A$. Par unicité de la limite dans un espace métrique, $a' = a \in A$. Par la caractérisation séquentielle des fermés, A est bien fermée.

— Bornée : Soit $a \in A$. On pose $B = \{d(a, x) \mid x \in A\}$ et on suppose par l'absurde que B est non borné. Il existe une suite (a_n) telle que

$$\forall n \in \mathbb{N},\ d(a, a_n) \geq n$$

Par compacité, il existe une extractrice $\varphi : \mathbb{N} \to \mathbb{N}$ telle que $a_{\varphi(n)} \longrightarrow_{n\to+\infty} \ell$ où $\ell \in A$. Par continuité,

$$d(a, a_{\varphi(n)}) \longrightarrow_{n\to+\infty} d(a, \ell)$$

Mais, pour tout $n \in \mathbb{N}$, $d(a, a_{\varphi(n)}) \geq \varphi(n) \geq n$: absurde. Donc B est borné : il existe $r \geq 0$ tel que $d(a, x) \leq r$ pour tout $x \in A$.

□

Proposition 3. Soir E un espace vectoriel de dimension finie $n \geq 1$ muni d'une norme infinie $\|.\|_\infty$. Les compacts de cet espace vectoriel normé sont les parties fermées et bornées.

Démonstration. La Proposition 2 montre que les parties compactes sont fermées et bornées. Pour montrer la réciproque, prenons $r > 0$. Notons que l'intervalle $[-r, r]$ est compact : si (a_k) est une suite d'éléments de $[-r, r]$, on peut extraire une sous-suite monotone et bornée qui est alors convergente dans $[-r, r]$ car $[-r, r]$ est fermé. Le théorème de Tykhonov nous dit que le produit $[-r, r]^n$ est alors compact.

Posons

$$\varphi : \begin{array}{ccc} ([-r,r]^n, \|.\|_\infty) & \to & (E, \|.\|_\infty) \\ (\alpha_1, \dots, \alpha_n) & \mapsto & \sum_{k=1}^n \alpha_k e_k \end{array}$$

où $(e_1, \dots, e_n)$ désigne une base de E associée à la norme infinie $\|.\|_\infty$. Alors, par la Proposition 1, $\varphi([-r,r]^n) = \overline{B}(0,r)$ est compact.

Soit maintenant A une partie fermée bornée de E. Alors il existe $r > 0$ tel que $A \subseteq \overline{B}(0,r)$. Donc, si (a_n) est une suite d'éléments de A, par compacité de $\overline{B}(0,r)$, on a l'existence d'une sous-suite convergente vers $a \in \overline{B}(0,r)$. Comme A est fermée, $a \in A$. A est ainsi séquentiellement compacte, donc est compacte. □

Théorème 4. Un espace vectoriel normé E est de dimension finie $n \geq 1$ si et seulement si toutes ses normes sont équivalentes.

Démonstration. — $\Longleftarrow$: Soit $\|.\|$ une norme sur E et soit φ une forme linéaire quelconque sur E. On définit la norme suivante sur E :

$$\|.\|_\varphi : x \mapsto |\varphi(x)| + \|x\|$$

Alors, pour tout $x \in E$, $|\varphi(x)| = \|x\|_\varphi - \|x\| \leq \|x\|_\varphi$: φ est continue pour $\|.\|_\varphi$ donc pour $\|.\|$ aussi par équivalence des normes.

Supposons par l'absurde E de dimension infinie. Soit $(e_n)_{n\in\mathbb{N}}$ une suite infinie de vecteurs linéairement indépendantes. On pose $V = \text{Vect}(e_n)_{n\in\mathbb{N}}$. Soient W un supplémentaire de V dans E et $p : E \to V$ la projection sur V parallèlement à W. On définit ψ une forme linéaire sur V par $\forall n \in \mathbb{N}$, $\psi(e_n) = n\|e_n\|$. Alors, $\phi = \psi \circ p$ est une forme linéaire sur E qui n'est pas continue. En effet :

$$\sup_{x\neq 0} \frac{|\phi(x)|}{\|x\|} = +\infty$$

C'est absurde.

— $\Longrightarrow$:Soient $(e_1, \dots, e_n)$ une base de E et $x = \sum_{i=1}^n x_i e_i \in E$. Si $\|.\|$ est une norme sur E, on a :

$$\|x\| \leq \underbrace{\left(\sum_{i=1}^n \|e_i\|\right)}_{=\alpha} \|x\|_\infty$$

Donc $\|.\|_\infty$ est plus fine que $\|.\|$.

L'application $\|.\| : (E, \|.\|_\infty) \to (\mathbb{R}^+, |.|)$ est continue car lipschitzienne ($\forall x, y \in E$, $|\|x\| - \|y\|| \leq \|x-y\|$), donc est bornée et atteint ses bornes sur la sphère $S(0,1) = \{x \in E \mid \|x\|_\infty = 1\}$ (qui est fermée bornée, donc compacte par la Proposition 3). On note $x_0 \in E$ ce minimum :

$$\forall x \in E \text{ tel que } \|x\|_\infty = 1, \text{ on a } \|x\| \geq \underbrace{\|x_0\|}_{=\beta}$$

Ainsi,

$$\forall x \in E, \left\| \frac{x}{\|x\|_\infty} \right\| \geq \beta \text{ ie. } \|x\| \geq \beta \|x\|_\infty$$

Donc $\|.\|$ est plus fine que $\|.\|_\infty$: les normes $\|.\|$ et $\|.\|_\infty$ sont équivalentes. Comme la relation d'équivalence sur les normes d'un espace vectoriel est transitive, on en déduit que toutes les normes sur E sont équivalentes.

□

Corollaire 5. (i) Les parties compacts d'un espace vectoriel normé de dimension finie sont les parties fermées bornées.

(ii) Tout espace vectoriel normé de dimension finie est complet.

(iii) Tout sous-espace vectoriel de dimension finie d'un espace vectoriel normé est fermé.

(iv) Soient $(E, \|.\|_E)$ et $(E, \|.\|_F)$ deux espaces vectoriels avec E de dimension finie. Alors,

$$\mathscr{L}(E,F) = L(E,F)$$

ie. toute application linéaire de E dans F est continue.

Démonstration. (i) C'est une conséquence directe de la Proposition 3 et du Théorème 4.

(ii) Soit (x_n) une suite de Cauchy d'un espace vectoriel normé $(E, \|.\|)$. Notons que :

— (x_n) **est bornée.** En effet, il existe $N \in \mathbb{N}$ tel que $\forall p > q \geq N$, $\|x_p - x_q\| < 1$. Donc, $\forall p \geq N$, $\|x_p\| < 1 + \|x_N\|$. Ainsi,

$$M = \max(\|x_0\|, \dots, \|x_{N-1}\|, \|x_N\|)$$

majore la suite (x_n).

— (x_n) **admet au plus une valeur d'adhérence, et si c'est le cas, elle converge vers cette valeur d'adhérence.** En effet, si (x_n) converge, alors sa limite est son unique valeur d'adhérence. Soit maintenant x une valeur d'adhérence de (x_n). Soit $\epsilon > 0$,

$$\exists N \in \mathbb{N} \text{ tel que } \forall p > q \geq N,\ \|x_p - x_q\| < \frac{\epsilon}{2}$$

Soit $q \geq N$. Par définition de la valeur d'adhérence,

$$\exists p \geq q \text{ tel que } \|x_p - x\| < \frac{\epsilon}{2}$$

Donc :

$$\|x_q - x\| \leq \|x_p - x_q\| + \|x_p - x\| < \epsilon$$

ce que l'on voulait.

Supposons E de dimension finie. Par le premier point, (x_n) est bornée, donc incluse dans une boule fermée B, qui est compacte par le Point (i), donc elle admet une valeur d'adhérence $\ell \in B$. Par le second point, (x_n) converge vers ℓ.

(iii) Soient $(E, \|.\|)$ un espace vectoriel normé et F un sous-espace vectoriel de E de dimension finie. Soit (x_n) une suite de F qui converge vers $x \in E$. Notons que (x_n) **est de Cauchy.** En effet, soit $\epsilon > 0$,

$$\exists N \in \mathbb{N} \text{ tel que } \forall p > q \geq N,\ \|x_p - x_q\| < \frac{\epsilon}{2}$$

Soient $p > q \geq N$.

$$\begin{aligned}\|x_p - x_q\| &\leq \|x_p - x\| + \|x - x_q\| \\ &< \epsilon\end{aligned}$$

Donc (x_n) est une suite de Cauchy de F, qui est de dimension finie, donc complet par le Point (ii). (x_n) converge donc dans F, et par unicité de la limite, on a $x \in F$. Par la caractérisation séquentielle des fermés, F est bien fermé dans E.

(iv) Soit $f \in L(E,F)$. On définit une norme sur E par

$$\|.\| : x \mapsto \|x\|_E + \|f(x)\|_F$$

Or, $\forall x \in E$,

$$\begin{aligned}\|f(x)\|_F &= \|x\|_E - \|x\| \\ &\leq \|x\|_E - M\|x\|_E\end{aligned}$$

où $M > 0$, par le Théorème 4.Ainsi,

$$\|f(x)\|_F = (1-M)\|x\|_E$$

f est une application linéaire bornée, donc continue.

□

Application 6. $\forall M \in \mathcal{M}_n(\mathbb{C}), \exists P \in \mathbb{C}[X]$ tel que $\exp(M) = P(M)$.

Démonstration. Soit $M \in \mathcal{M}_n(\mathbb{C})$. L'ensemble $\mathbb{C}[M] = \{P(M) \mid P \in \mathbb{C}[X]\}$ est un sous-espace vectoriel de $\mathcal{M}_n(\mathbb{C})$ qui est de dimension finie, donc $\mathbb{C}[M]$ l'est aussi et est en particulier fermé par le Corollaire 5 Point (ii).

Pour tout $n \in \mathbb{N}$, on pose $P_n = \sum_{k=0}^{n} \frac{M^k}{k!} \in \mathbb{C}[M]$ de sorte que $P_n \longrightarrow_{n\to+\infty} \exp(M)$. Comme $\mathbb{C}[M]$ est fermé, on en déduit que $\exp(M) \in \mathbb{C}[M]$. Donc $\exists P \in \mathbb{C}[X]$ tel que $\exp(M) = P(M)$. □

2 Chiffrement RSA

On commence par récapituler toute l'arithmétique des entiers, connue depuis la L1, et sans faire appel à la théorie des groupes. On détaille ensuite un exemple pratique de chiffrement RSA, et on explique les mathématiques se trouvant derrière à l'aide de la première partie.

I - Arithmétique dans $\mathbb{Z}$

1. Divisibilité dans $\mathbb{Z}$

Définition 1. Soient a et b deux entiers relatifs. On dit que b **divise** a (ou que a est un **multiple** de b) s'il existe $k \in \mathbb{Z}$ tel que $a = kb$. On note ceci par $b \mid a$.

Exemple 2.
— $6 = 2 \times 3$ donc 2 et 3 sont des diviseurs de 6.Les diviseurs dans $\mathbb{N}$ de 6 sont : 1, 2, 3 et 6.
— $-52 = (-4) \times 13$ donc -4, 4, -13 et 13 sont des diviseurs de -52. Les diviseurs dans $\mathbb{Z}$ de -52 sont : -52, -26, -13, -4, -2, -1, 1, 2, 4, 13, 26 et 52.

Proposition 3.
(i) Tout entier relatif b divise 0 (car $0 = 0 \times b$).
(ii) 1 divise tout entier relatif a (car $a = a \times 1$).
(iii) Si $c \mid a$ et $c \mid b$ alors $c \mid (au + bv)$ pour tout $u, v \in \mathbb{Z}$.

Démonstration. Montrons le dernier point : il existe k, k' tels que $a = kc$ et $b = k'c$. Donc $ua + vb = ukc + vk'c = (uk + vk')c$. D'où $c \mid (au + bv)$. □

Définition 4. Un nombre entier $p \geq 2$ est dit **premier** si ses seuls diviseurs positifs sont 1 et lui-même.

Exemple 5. 2, 3, 5, 7, 11 et 13 sont des nombres premiers et il en existe une infinité.

2. Division euclidienne

Théorème 6 (Division euclidienne dans $\mathbb{Z}$)**.** Soient $a \in \mathbb{N}$ et $b \in \mathbb{N}^*$. On appelle **division euclidienne** de a par b, l'opération qui à (a, b), associe le couple d'entiers (q, r) tel que $a = bq + r$ où $0 \leq r < b$. Un tel couple existe forcément et est unique.

Démonstration. Si $a < b$, alors il suffit de prendre $q = 0$ et $r = a$. Nous supposerons donc dans la suite $a \geq b$.

— Existence : On note S l'ensemble des entiers naturels s qui s'écrivent $s = a - tb$ où $t \in \mathbb{N}$. Cet ensemble est non vide (car il contient a) et comme c'est un sous-ensemble de $\mathbb{N}$, il admet un plus petit élément $r = a - qb$. On a forcément $r < b$ (sinon $a-(q+1)b$ serait dans S et serait plus petit que r). Donc $0 \leq a - qb < b$ et ce couple (q, r) vérifie les conditions données par le théorème.

— Unicité : On suppose qu'il existe un deuxième couple (q', r') vérifiant les conditions du théorème. On a $a = bq + r = bq' + r'$, donc $b(q - q') = r - r'$. Comme $0 \leq r < b$ alors $-b < -r \leq 0$. De plus $0 \leq r' < b$, donc en additionnant les inégalités on a $-b < r' - r < b$. Comme $b \mid r - r'$ on a $r - r' = 0$ (i.e. $r = r'$) et donc $q = q'$. D'où $(q', r') = (q, r)$.

□

Définition 7. En reprenant les notations du théorème, a s'appelle le **dividende**, b le **diviseur**, q le **quotient** et r le **reste** de la division euclidienne.

Remarque 8. Il est possible d'étendre le principe de la division euclidienne aux entiers relatifs. La condition pour le reste r devient alors $0 \leq r < |b|$.

Exemple 9. On souhaite effectuer la division euclidienne de 314 par 7. Détaillons étape par étape :

— On cherche combien de fois 7 est contenu dans 31 (cela ne sert à rien de commencer par 3 car $3 < 7$). On a $4 \times 7 = 28$ et $5 \times 7 = 35$ donc, on écrit 4 sous le diviseur et le reste $31 - 28 = 3$. Puis, on abaisse le chiffre des unités qui est 4.

— On recommence : combien de fois 7 est-il contenu dans 34 ? Comme $4 \times 7 = 28$ et $5 \times 7 = 35$, 7 est contenu 4 fois dans 34 et il reste $34 - 28 = 6$.

— Comme $6 < 7$, la division euclidienne est terminée : on a $314 = 7 \times 44 + 6$.

Donnons, pour finir, une propriété qui nous sera utile dans la sous-section suivante.

Proposition 10. Soit $n \in \mathbb{N}^*$. Deux entiers relatifs a et b ont le même reste dans la division euclidienne par n si et seulement si $a - b$ est un multiple de n.

Démonstration. Supposons que a et b ont le même reste dans la division euclidienne par n i.e. $a = qn + r$ et $b = q'n + r$. Alors par différence, $a - b = (q - q')n$ donc $a - b$ est un multiple de n.

Réciproquement, si $a - b$ est un multiple de n alors il existe k tel que $a - b = kn$. En effectuant la division euclidienne de a par n, on a $a = qn + r$, d'où $nq + r - b = kn$. Ainsi, $b = (q - k)n + r$ avec $0 \leq r < q - k$, ce que l'on voulait. □

Voici également un énoncé qui sera utilisé par la suite. C'est un corollaire du théorème de théorème de Bézout.

Proposition 11 (Corollaire du théorème de Bézout)**.** Soient a et b deux entiers naturels non nuls premiers entre eux. Alors, il existe $u, v \in \mathbb{Z}$ tels que $au + bv = 1$.

Démonstration. On note par S l'ensemble des entiers naturels strictement positifs s qui s'écrivent $s = na + mb$ où $n, m \in \mathbb{Z}$. Cet ensemble est non-vide (car il contient a) et comme c'est un sous-ensemble de $\mathbb{N}$, il admet un plus petit élément $d = au + bv > 0$.

— On a $1 \mid d$ (car $1 \mid a$ et $1 \mid b$) donc $1 \leq d$.

— Faisons la division euclidienne de a par d : on a $a = dq + r \iff r = a - dq = a - (au + bv)q = a(1 - uq) + b(-vq)$ donc $r = 0$ (car sinon on aurait $r \in S$ mais $r < d$ et d est le plus petit élément de S). Donc d divise a et par le même raisonnement, d divise b. Donc d divise leur plus grand diviseur commun positif qui est 1. Donc $d \leq 1$.

D'où finalement $d = 1$. □

Remarque 12. Il est possible de trouver de tels entiers u et v en effectuant la division euclidienne de a par b, puis de b par le reste de la division précédente, etc…et en remontant. Il s'agit de la remontée de **l'algorithme d'Euclide**.

Corollaire 13. Soient a et b deux entiers naturels non nuls premiers entre eux. Soit $c \in \mathbb{Z}$ tel que $a \mid c$ et $b \mid c$. Alors $ab \mid c$.

Démonstration. On écrit $c = ka$ et $c = k'b$. De plus, par le Proposition 11, il existe u et v tels que $au + bv = 1$. En multipliant l'égalité par c, on obtient $c = auc + bvc = au(k'b) + bv(ka) = ab(k'u + kv)$. D'où le résultat. □

Lemme 14 (Euclide)**.** Soit p un nombre premier et a et b deux entiers. Si $p \mid ab$ alors $p \mid a$ ou $p \mid b$.

Démonstration. Soit p un nombre premier tel que $p \mid ab$. Supposons que p ne divise pas a. Alors comme p est premier, ses seuls diviseurs sont 1 et p. Comme a n'est pas divisible par p, le plus grand diviseur commun positif à a et p est 1. Donc par le Proposition 11 il existe $u, v \in \mathbb{Z}$ tels que $au + pv = 1$. En multipliant par b on obtient $\underbrace{abu}_{\text{Multiple de } p} + \underbrace{pbv}_{\text{Multiple de } p} = b$. Ainsi $p \mid b$. □

3. Congruences dans $\mathbb{Z}$

Dans toute cette sous-section, on fixe un entier naturel $n \geq 2$.

Définition 15. On dit que deux entiers relatifs a et b sont **congrus** modulo n si a et b ont le même reste dans la division euclidienne par n. On note alors $a \equiv b \mod n$.

Remarque 16. On remarque que a est un multiple de n si et seulement si $a \equiv 0 \mod n$.

On signale que la congruence est une **relation d'équivalence**.

Proposition 17. Pour tout $a, b, c \in \mathbb{Z}$:

(i) $a \equiv a \mod n$ (**réflexivité**)

(ii) Si $a \equiv b \mod n$, alors $b \equiv a \mod n$ (**symétrie**)

(iii) Si $a \equiv b \mod n$, et si $b \equiv c \mod n$, alors $a \equiv c \mod n$ (**transitivité**)

De plus, le congruence est compatible avec les opérations usuelles sur les entiers relatifs.

Théorème 18. Soient a, b, c et $d \in \mathbb{Z}$ tels que $a \equiv b \mod n$ et $c \equiv d \mod n$. Alors on a la compatibilité avec :

(i) L'**addition** : $a + c \equiv b + d \mod n$.

(ii) La **multiplication** : $ac \equiv bd \mod n$.

(iii) Les **puissances** : pour tout $k \in \mathbb{N}$, $a^k \equiv b^k \mod n$.

Démonstration. (i) Comme $a \equiv b \mod n$, et $c \equiv d \mod n$, alors $(a-b)$ et $(c-d)$ sont des multiples de n. Donc il existe deux entiers relatifs k et k' tels que $a - b = kn$ et $c - d = k'n$. En additionnant ces deux égalités on trouve que $(a+c) - (b+d) = (k+k')n$. Donc par la Remarque 16, $a + c \equiv b + d \mod n$.

(ii) Comme précédemment, on a $a - b = kn$ et $c - d = k'n$. En multipliant les deux égalités on trouve que $ac = (b+kn)(d+k'n) = bd + (k'b + kd + kk'n)n$. Donc par la Remarque 16, $ac \equiv bd \mod n$.

(iii) On utilise la compatibilité avec la multiplication : $a \equiv b \mod n$ et $a \equiv b \mod n$ donc $a^2 \equiv b^2 \mod n$. De même, on a $a^3 \equiv b^3 \mod n$. Il suffit de répéter l'opération k fois et on a $a^k \equiv b^k \mod n$.

□

Exemple 19. Comme $7 \equiv 3 \mod 4$, et $5 \equiv 1 \mod 4$, on a $35 = 5 \times 7 \equiv 1 \times 5 \mod 4$.

Nous utiliserons le résultat suivant dans la sous-section suivante.

Théorème 20 (Petit théorème de Fermat)**.** Soit p un nombre premier et a un entier quelconque. Alors $a^p \equiv a \mod p$.

Démonstration. Soit p un nombre premier et soit a tel que p ne divise pas a. Notons :

— $N = a \times 2a \times 3a \times \cdots \times (p-1)a$.

— r_k le reste de la division euclidienne de ka par p pour tout $k \in \mathbb{N}$ tel que $1 \leq k \leq p-1$.

— $(p-1)! = 1 \times 2 \times \ldots \times p-1$.

Montrons que $N = (p-1)!a^{p-1}$. Il suffit en fait de réordonner les facteurs de N :

$$N = a \times 2a \times \cdots \times (p-1)a = 1 \times 2 \times 3 \times \cdots \times (p-1) \times a \times a \times \cdots \times a = (p-1)!a^{p-1} \qquad (*)$$

De plus, r_k est le reste de la division euclidienne de ka par p donc $ka \equiv r_k \mod p$. Par $(*)$, $N = a \times 2a \times \cdots \times (p-1)a \equiv r_1 r_2 \ldots r_{p-1} \mod p$. $0 \leq k \leq p-1 < p$, donc k ne peut pas être

divisible par p. Ainsi, par le Lemme 14, ka n'est pas divisible par p et donc $r_k \neq 0$.

Soit i tel que $1 \leq i \leq p-1$ et $r_i = r_k$. Montrons que $(i-k)a$ est divisible par p. Comme r_i et r_k sont respectivement le reste de la division euclidienne de ia et ka par p, on a $r_i - r_k = 0 \equiv (i-k)a \mod p$ donc $(i-k)a$ est divisible par p. Comme p ne divise pas a, par le Lemme 14, on a $i-j$ divise p. Et comme $-p < i-j < p$, on en déduit que $i = j$.

Pour tout k, on a $1 \leq r_k \leq p-1$. De plus, par ce qui précède, on a $p-1$ r_k qui sont tous différents les uns des autres. Donc $\{r_1, r_2, \dots, r_{p-1}\} = \{1, 2, \dots, p-1\}$ Ainsi, $r_1 r_2 \dots r_{p-1} = (p-1)!$.

Enfin, on a $N = (p-1)!a^{p-1} = a \times 2a \times \cdots \times (p-1)a \equiv r_1 r_2 \dots r_{p-1} \mod p$ et $r_1 r_2 \dots r_{p-1} \equiv (p-1)! \mod p$, donc, on a $N \equiv (p-1)! \mod p$. De par la définition des congruences modulo p, on a $N-(p-1)!$ divisible par p et $N-(p-1)! = (p-1)!(a^{p-1}-1)$. Comme p divise $(p-1)!(a^{p-1}-1)$ mais que pour tout $k \in \mathbb{N}$ tel que $1 \leq k \leq p-1$, p ne divise pas k, alors, en appliquant le Lemme 14 à chaque facteur de $(p-1)!$, il en résulte que p divise $a^{p-1}-1$.

Pour conclure, comme $a^{p-1} - 1 \equiv 0 \mod p$ alors $a^{p-1} \equiv 1 \mod p$ et donc $a^p \equiv a \mod p$. Nous venons de montrer que pour tout a non divisible par p, on a $a^p \equiv a \mod p$. Soit maintenant b un entier divisible par p. Alors $b \equiv 0 \mod p$ et donc $b^p \equiv 0^p \equiv 0 \mod p$. D'où $b^p \equiv b \mod p$. □

Exemple 21. Cherchons le reste de la division euclidienne de 2019^5 par 5.

Posons $a = 2019$ et $p = 5$. En faisant la division euclidienne de a par p, on a $a = 403p + 4$ donc $a \equiv 4 \mod p$. Donc $a^p \equiv a \equiv 4 \mod p$.

II - RSA par un exemple

1. Calcul de le clé publique et de la clé privée

Alice souhaite envoyer un code à Bob et uniquement à lui à travers un groupe de messagerie. Pour éviter de communiquer son code à tous les autres membres du groupe de messagerie, ils cherchent donc un moyen pour que seul Bob soit capable de le lire et de le déchiffrer : ils vont employer la méthode de chiffrement **RSA**.

Ce chiffrement se base sur le choix de deux nombres premiers p et q distincts. On pose alors $n = pq$ et $N = (p-1)(q-1)$, puis on choisit $e < N$ premier avec N.

Définition 22. Le couple (n, e) est la **clé publique** de ce chiffrement et est utilisée pour chiffrer des nombres, des caractères, des mots, ...

Pour déchiffrer un nombre, on détermine deux entiers u et v vérifiant $ue + vN = 1$ (ils existent par le Proposition 11). On pose d comme le reste de la division euclidienne de u par N.

Définition 23. Le triplet (p, q, d) est la **clé privée** du chiffrement.

Dans notre exemple, c'est Bob qui va générer la clé publique et la clé privée. Ainsi, il choisit $p = 5$, $q = 7$ (donc $n = 35$ et $N = 24$) et $e = 5$. Comme $5e - N = 1$, alors $d = u = 5$.

Il communique sa clé publique (qui est $(35,5)$) dans la conversation et garde bien précieusement sa clé privée (qui est $(5,7,5)$).

2. Chiffrement du code

Le code d'Alice est 2743, elle le décompose en chacun de ses chiffres : $a_0 = 2$, $a_1 = 7$, $a_3 = 4$ et $a_4 = 3$. Pour tout k, elle calcule ensuite b_k qui est le reste de la division euclidienne de a_k^e par n. Ainsi, elle obtient :

a_k	2	7	4	3
b_k	32	7	9	33

Par conséquent, elle écrit dans la conversation :

32 7 9 33

À titre d'exemple, pour calculer b_1, il s'agit de calculer le reste de la division euclidienne de $a_1^5 = 7^5$ par $n = 35$. On peut, par exemple, procéder comme ceci :

— $7^2 = 49 \equiv 14 \mod 35$

— $7^3 = 7^2 \times 7 \equiv 28 \equiv -7 \mod 35$

— $7^5 = 7^3 \times 7^2 \equiv -98 \equiv 7 \mod 35$

3. Déchiffrement du code

Bob a donc reçu, une suite de quatre nombres (b_k) avec $b_0 = 32$, $b_1 = 7$, $b_2 = 9$ et $b_3 = 33$. Pour déchiffrer la suite (b_k) en une suite (a_k), il s'agit alors pour tout k, de calculer le reste de la division euclidienne de b_k^d par n. Ce reste est a_k. Ainsi, dans le cadre de notre exemple, cela nous donne :

b_k	32	7	9	33
a_k	2	7	4	3

Le code déchiffré est donc :

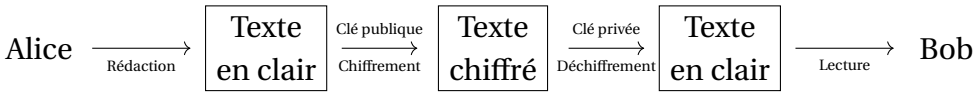
2 7 4 3

Ce qui correspond bien au code qu'Alice a voulu transmettre. De plus, seul Bob connaît le nombre d qui permet de déchiffrer le code. Leur objectif est donc atteint.

L'algorithme RSA est dit "asymétrique" car pour chiffrer un message, il suffit de connaître la clé publique (n,e). Cependant, pour déchiffrer un message, il faut connaître n et d. Or, d se calcule à partir de e et n en trouvant les nombres premiers p et q qui divisent n. Donc finalement, pour déchiffrer un message, il faut connaître la clé privée (p,q,d).

Dans cet exemple, les nombres p et q ont été choisis petits de manière à simplifier les calculs, mais si on souhaitait mettre en place cet algorithme de chiffrement dans un cadre plus sécuritaire, il faudrait ainsi choisir des nombres p et q beaucoup plus grands.

Le chiffrement demande donc de pouvoir vérifier que de très grands nombres sont des nombres premiers, pour pouvoir trouver p et q, mais aussi que le produit de ces deux très grands nombres, ne soit pas factorisable pratiquement. En effet les algorithmes efficaces connus qui permettent de vérifier qu'un nombre n'est pas premier ne fournissent pas de factorisation.



III - Explication mathématique

Soient p et $q \geq 2$ des nombres premiers distincts.

Notation 24. On note $n = pq$ et $N = \varphi(n) = (p-1)(q-1)$.

Prouvons tout d'abord l'existence de la clé publique ainsi que l'existence de la clé privée.

Proposition 25. Soit e un entier premier avec N soit 1. Alors il existe $d < N$ tel que $de \equiv 1 \mod N$.

Démonstration. En effet, par le Proposition 11, il existe u et $v \in \mathbb{Z}$ tels que $ue + vN = 1$. Donc, on a $ue = 1 - vN$ et ainsi $ue \equiv 1 - vN \equiv 1 \mod N$. Il suffit alors de poser d le reste de la division euclidienne de u par N. □

Montrons enfin que ce chiffrement est valide.

Proposition 26. Soit M un entier naturel strictement inférieur à n que nous souhaitons (dé-)chiffrer. On pose C le reste de la division euclidienne de M^e par n. Alors, $M \equiv C^d \mod n$.

Démonstration. On a $C^d \equiv (M^e)^d \equiv M^{ed} \mod n$ et $ed \equiv 1 \mod N$ donc il existe k tel que $ed = Nk + 1$. Comme p et q sont deux nombres premiers, alors par le Théorème 20, on a $M^{p-1} \equiv 1 \mod p$ et $M^{q-1} \equiv 1 \mod q$. Donc $M^{ed} = M^{Nk+1} = M(M^{p-1})^{k(q-1)} \equiv M \mod p$. En faisant le même raisonnement, on a $M^{ed} \equiv M \mod q$. Ainsi, $M^{ed} - M$ est un multiple de p et de q (deux premiers distincts), donc aussi de n par le Corollaire 13. On conclue que $M \equiv M^{ed} \equiv C^d \mod n$. □

3 Codes correcteurs d'erreurs

Petite fiche résumant ce qu'il faut savoir sur les codes correcteurs d'erreurs pour l'agrégation.

Pour tout le document, on fixe p un nombre premier, k et n deux entiers non nuls et $q = p^k$.

I - Théorie générale

Il s'agit, dans un premier temps, de choisir le corps $\mathbb{F}_q$ en fonction de l'information que l'on cherche à coder. Par exemple, le choix de $\mathbb{F}_2$ semble le plus naturel pour représenter la manière dont est stockée l'information dans un ordinateur, tandis que $\mathbb{F}_4$ serait plus approprié vis-à-vis de l'ADN.

Définition 1. On appelle **mot** un vecteur à coefficients dans $\mathbb{F}_q$.

Après avoir choisi $\mathbb{F}_q$ comme alphabet, il reste à choisir l'ensemble des mots $\mathscr{C}$ du code. Plus précisément :

Définition 2. On appelle **code correcteur** (ou simplement **code**) de taille n un sous-ensemble de $\mathbb{F}_q^n$.

Remarque 3. Le code correcteur $\mathscr{C}$ est l'ensemble des mots que l'on est en mesure de produire par codage : il ne peut pas occuper l'espace $\mathbb{F}_q^n$ entier, sinon tous les mots seraient valides !

Si l'on reçoit un mot qui n'est pas dans le code, on est donc sûr qu'il y a eu une erreur de transmission. L'opération de codage "ajoute" une information pour distinguer les mots valides des autres. C'est uniquement lors du décodage que l'on va pouvoir réparer une ou plusieurs erreurs. Le procédé général étant le suivant :

1. on transforme un message m en un mot c du code (c'est le processus de **codage**) ;
2. pendant la transmission, c est altéré en c' (c'est le processus de **transmission**) ;
3. on essaye de déterminer si c' est un mot du code (c'est le processus de **détection d'erreur**) ;
4. on essaye de retrouver c à partir de c' (c'est le processus de **correction d'erreur**) ;
5. on retrouve le message m à partir de c (c'est le processus de **décodage**).

Exemple 4 (Bit de parité)**.** Dans un ordinateur, chaque mot est coupé en "sous-mots" de 7 bits, c'est-à-dire, en vecteurs formés de 7 éléments de $\mathbb{F}_2$. Lors du codage de chaque vecteur, on ajoute un bit dit "de parité".

Ainsi, soit $b_1, \dots, b_7$ une suite de 7 bits. On calcule :

$$b_8 = b_1 + \cdots + b_7 \mod 2$$

Si le nombre de bits égaux à 1 est pair, $b_8 = 0$, sinon, $b_8 = 1$. Ainsi, le mot $(b_1, \dots, b_8)$ a toujours

un nombre de bits égaux à 1 qui est pair. On peut alors détecter, à la lecteur d'un mot, si une erreur a eu lieu lors de sa réception : il y aura un nombre impair de bits égaux à 1.

Dans le cadre d'un mot de taille 2, on peut représenter la situation par un cube. Sur cette illustration, nous voyons en turquoise l'ensemble des mots $\mathscr{C}$ du code. Une unique erreur correspond à un déplacement sur le cube le long d'une arête. Dans ce cas, le récepteur reçoit un point noir dont la somme de toutes les lettres est un entier impair. En revanche, un tel point est toujours à proximité de trois points turquoise, le récepteur ne dispose donc d'aucun moyen pour une correction automatique.

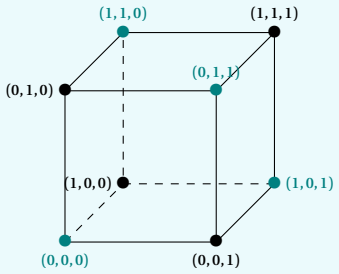


FIGURE 1 – Mots de $\mathbb{F}_2$ de longueur 2 avec un bit de parité.

Ainsi, ce code, a deux inconvénients :

— il est impossible de détecter où l'erreur a eu lieu, et donc, de la corriger ;

— si deux erreurs ont lieu, il est impossible de les détecter (car alors, le nombre de bits égaux à 1 reste pair).

L'exemple précédent montre bien qu'il est nécessaire de pouvoir évaluer les propriétés qualitatives d'un code. Ainsi :

Définition 5. Soient x et y deux mots de $\mathbb{F}_q$ de taille n.

— Le **poids** de x, noté $\omega(x)$, est le nombre de coefficients non nuls dans x.

— La **distance de Hamming** entre x et y, notée $d_H(x,y)$ est définie par

$$d_H(x,y) = \omega(x-y)$$

Proposition 6. (i) d_H correspond aux nombres de coefficients qui diffèrent entre x et y.

(ii) d_H est une distance sur $\mathbb{F}_q^n$.

Démonstration. (i) Soient $x, y \in \mathbb{F}_q^n$. Par définition, $\omega(x-y)$ est égal au nombre de coefficients non nuls de $x-y$, soit au nombre de coefficients qui diffèrent entre x et y.

(ii) Soient $x, y, z \in \mathbb{F}_q^n$.

(a) On a $d_H(x,y) \geq 0$ par positivité de ω et $d_H(x,y) = 0$ si et seulement s'il y a 0 coefficients qui diffèrent entre x et y ie. $x = y$.

(b) Le nombre de coefficients non nuls de $x-y$ est égal au nombre de coefficients non nuls de $y-x$. Donc,

$$d_H(x,y) = \omega(x-y) = \omega(y-x) = d_H(y,x)$$

(c) On note $(x_i)_{i\in[\![1,n]\!]}$, $(y_i)_{i\in[\![1,n]\!]}$ et $(z_i)_{i\in[\![1,n]\!]}$ les coefficients respectifs de x, y et z. Soient $\mathscr{A} = \{k \in [\![1,n]\!] \mid x_k = y_k\}$, $\mathscr{B} = \{k \in [\![1,n]\!] \mid y_k = z_k\}$ et $\mathscr{C} = \{k \in [\![1,n]\!] \mid x_k = z_k\}$. On a,

$$(\mathscr{A} \cap \mathscr{B}) \subseteq \mathscr{C}$$

En passant au complémentaire,

$${}^c\mathscr{C} \subseteq {}^c(\mathscr{A} \cap \mathscr{B}) = {}^c\mathscr{A} \cup {}^c\mathscr{B}$$

D'où,

$$\underbrace{d(x,z)}_{|{}^c\mathscr{C}|} \leq \underbrace{d(x,y)}_{|{}^c\mathscr{A}|} + \underbrace{d(y,z)}_{|{}^c\mathscr{B}|}$$

□

La distance d_H permet de quantifier la notion de "mot le plus proche". Avec elle, on peut donner la définition suivante.

Définition 7. Soit $\mathscr{C}$ un code. On appelle **distance minimale** de $\mathscr{C}$, l'entier suivant :

$$\min_{x,y\in\mathscr{C}} \{d_H(x,y) \mid x \neq y\}$$

Plus la distance minimale d'un code est grande, plus les mots vont être "espacés" les uns des autres. En ne prenant en compte que la plus petite des distances, on va pouvoir s'assurer que le code est en mesure de corriger une erreur sous certaines conditions.

Définition 8. Un code $\mathscr{C}$ est dit t-**correcteur** s'il peut corriger au maximum t erreurs.

Remarque 9. Cela signifie que, si $x \in \mathscr{C}$ désigne un mot codé et $x' \in \mathbb{F}_q^n$ le mot réceptionné, alors on est en mesure de retrouver le mot x original si $d(x,x') \leq t$.

Proposition 10. Soit $\mathscr{C}$ un code de distance minimale d. On suppose $d \geq 2t+1$. Alors, $\mathscr{C}$ est t-correcteur.

Démonstration. Soient $x, y \in \mathscr{C}$ deux mots distincts du code. Alors,

$$d_H(x,y) \geq 2t+1$$

les boules $B(x,t)$ et $B(y,t)$ sont disjointes.Ainsi, soient $a \in \mathscr{C}$ un mot codé émis et $a' \in \mathbb{F}_q^n$ le mot réceptionné. Si $d(a,a') \leq t$, alors $a' \in B(a,t)$ et n'appartient pas à une autre boule de centre un mot du code et de rayon inférieur ou égal à t : on peut corriger a'. □

Remarque 11. Notons qu'alors

$$t \leq \frac{d-1}{2} \implies t = \left\lfloor \frac{d-1}{2} \right\rfloor$$

II - Codes linéaires

Nous allons maintenant observer ce qui se passe en imposant une structure sur le code.

Définition 12. Un **code linéaire** $\mathscr{C}$ de taille n et de dimension m sur $\mathbb{F}_q$ est un sous-espace vectoriel de dimension m de $\mathbb{F}_q^n$.

Soit alors une base de $\mathscr{C}$. On considère G une matrice dont les colonnes sont les vecteurs de cette base. On dit que G est une **matrice génératrice** de $\mathscr{C}$.

Proposition 13. Soit $\mathscr{C}$ un code linéaire de taille n et de dimension m sur $\mathbb{F}_q$. Soit G une matrice génératrice de $\mathscr{C}$. On a,

$$\mathscr{C} = \{Gx \mid x \in \mathbb{F}_q^n\}$$

Démonstration. Soit $(v_1, \dots, v_m)$ une base de $\mathscr{C}$. On considère la matrice génératrice de $\mathscr{C}$ associée, que l'on note G.

Alors, $\forall i \in [\![1, m]\!]$, en notant e_i le i-ième vecteur de la base canonique de $\mathbb{F}_q^n$, on a $Me_i = v_i$. Donc, par linéarité, $\{Gx \mid x \in \mathbb{F}_q^n\} \subseteq \mathscr{C}$.Et comme $v_i = Me_i$, on a bien l'inclusion réciproque. □

Remarque 14. Dans le cadre d'un code linéaire $\mathscr{C}$, la distance minimale d s'exprime alors

$$d = \min_{x,y \in \mathscr{C}} \{d_H(x,y) \mid x \neq y\} = \min_{x \in \mathscr{C}} \{\omega(x) \mid x \neq 0\}$$

Proposition 15. Soit $\mathscr{C}$ un code linéaire de taille n et de dimension m sur $\mathbb{F}_q$. Il existe une matrice $H \in \mathscr{M}_{n-m,n}(\mathbb{F}_q)$ telle que

$$\forall x \in \mathbb{F}_q^n,\ x \in \mathscr{C} \iff Hx = 0$$

Démonstration. On considère le produit scalaire canonique sur $\mathbb{F}_q^n$:

$$\langle .,. \rangle : ((x_1, \dots, x_n), (y_1, \dots, y_n)) \mapsto \sum_{i=1}^{n} x_i y_i$$

et $\mathscr{C}^\perp$ l'orthogonal de $\mathscr{C}$ pour ce produit scalaire. $\mathscr{C}^\perp$ est un sous-espace vectoriel de $\mathbb{F}_q^n$ de dimension $n-m$, dont on note $(v_1, \dots, v_{n-m})$ une base. Définissons H comme étant la matrice

dont la i-ième ligne est v_i pour tout $i \in [\![1, n-m]\!]$. Soit $x \in \mathbb{F}_q^n$. Alors, on a

$$\begin{aligned} Hx = 0 &\iff \forall i \in [\![1, n-m]\!], \langle v_i, x\rangle = 0 \\ &\iff x \in (\mathscr{C}^\perp)^\perp \\ &\iff x \in \mathscr{C} \end{aligned}$$

On aurait aussi pu se contenter de considérer le noyau à gauche de la matrice génératrice (c'est une caractérisation plus commode à implémenter en algorithmique). □

Définition 16. En reprenant les notations précédentes, H est appelée **matrice de contrôle** du code $\mathscr{C}$.

Il s'agit là d'un critère extrêmement pratique pour permettre de tester l'appartenance d'un mot au code.

Exemple 17 (Code de répétition)**.** On se place sur le corps $\mathbb{F}_2$. L'idée est d'envoyer plusieurs copies de chaque bit à être transmis. Ainsi, sur $\mathbb{F}_2^4$, le code $\mathscr{C}$ est composé de deux mots :

$$(0,0,0,0) \text{ et } (1,1,1,1)$$

Des matrices génératrices G et de contrôle H sont données par

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

On corrige en remplaçant un message reçu reconnu erroné par le message émis potentiel le plus proche (c'est-à-dire avec le moins de bits différents). Par conséquent, le codage par répétition permet de corriger correctement une erreur portant sur un seul bit mais ne permet pas de corriger correctement une erreur portant sur deux bits.

Proposition 18 (Borne de Singleton)**.** Soit $\mathscr{C}$ un code linéaire de taille n, de dimension m et de distance minimale d sur $\mathbb{F}_q$. Alors,

$$d \leq n - m + 1$$

Démonstration. Pour prouver ceci, exhibons un mot x de $\mathscr{C}$ de poids inférieur ou égal à $n-m+1$ (car alors, on aura $d \leq \omega(x) \leq n-m+1$). Soit F, le sous-espace vectoriel de $\mathbb{F}_q^n$ constitué des vecteurs dont les $m-1$ dernières coordonnées sont nulles. C'est un espace de dimension $n-m+1$,

et la formule de Grassmann donne :

$$\begin{aligned}\dim(\mathscr{C} \cap F) &= \dim(\mathscr{C}) + \dim(F) - \dim(\mathscr{C} + F)\\ &= m + n - m + 1 - \dim(\mathscr{C} + F)\\ &= n + 1 - \dim(\mathscr{C} + F)\\ &\geq n + 1 - n\\ &= 1\end{aligned}$$

Il existe donc $x \neq 0$ dans $\mathscr{C} \cap F$, et ce mot a un poids inférieur ou égal à $n - m + 1$. □

Ce dernier résultat illustre le choix à faire entre capacité de correction, et redondance de l'information transmise.Terminons cette sous-section par la méthode pratique permettant de corriger un mot reçu. Pour cela, on a besoin d'une dernière définition.

Définition 19. Soit $\mathscr{C}$ un code linéaire de taille n et de dimension m sur $\mathbb{F}_q$. Soit H une matrice de contrôle de $\mathscr{C}$. On appelle **syndrome** d'un mot $x \in \mathbb{F}_q^m$ le vecteur Hx.

Imaginons maintenant que l'on réceptionne un mot $a' \in \mathbb{F}_q^m$. On calcule son syndrome via une matrice de contrôle H et on a deux cas :

— Le syndrome est nul : $a' \in \mathscr{C}$: on considère alors qu'il n'y a pas d'erreur.

— Le syndrome est non nul : il existe $a \in \mathscr{C}$ (le mot d'origine) et $e \in \mathbb{F}_q^n$ (l'erreur) tels que $a' = a + e$. Alors,

$$Ha' = H(a + e) = Ha + He = He$$

En notant h_j le j-ième vecteur colonne de H et e_j la j-ième coordonnée de e :

$$Ha' = \sum_{j \text{ tel que } e_j \neq 0} h_j e_j \qquad (*)$$

On en déduit e en résolvant le système $(*)$. Il est possible que ce système n'ait pas de solution, s'il y a trop d'erreurs par exemple. S'il y a une solution, elle est unique et on peut effectuer la correction : $a = a' - e$.

III - Codes cycliques

Nous avons vu dans la section précédente qu'imposer une structure d'espace vectoriel sur un code rendait le codage de l'information beaucoup plus simple via les matrices génératrices. Renforçons davantage la structure de notre code et observons les conséquences.

Définition 20. Soit $\mathscr{C}$ un code linéaire de taille n et de dimension m sur $\mathbb{F}_q$. $\mathscr{C}$ est dit **cyclique** s'il est stable par décalage circulaire, ie.

$$(a_0, a_1, \ldots, a_{m-1}) \in \mathscr{C} \implies (a_1, \ldots, a_{m-1}, a_0) \in \mathscr{C}$$

Notons maintenant

$$\varphi : \begin{array}{ccc} \mathbb{F}_q^n & \to & \mathbb{F}_q[X]/(X^n-1) \\ (a_0,\dots,a_{n-1}) & \mapsto & \overline{\sum_{i=0}^{n-1} a_i X^i} \end{array}$$

Lemme 21. φ est un isomorphisme d'espaces vectoriels.

Démonstration. On sait (par la théorie des corps), que $\mathbb{F}_q[X]/(X^n-1)$ est un espace vectoriel sur $\mathbb{F}_q$ de dimension n. En effet, en notant $\overline{X}$ la classe de X dans $\mathbb{F}_q[X]/(X^n-1)$:

— La famille $(\overline{1},\dots,\overline{X}^{n-1})$ est libre. Soient $\lambda_0,\dots,\lambda_{n-1} \in \mathbb{K}$ tels que

$$\sum_{i=0}^{n-1} \lambda_i \overline{X}^i = \overline{\sum_{i=0}^{n-1} \lambda_i X^i} = 0$$

Alors, le polynôme $\sum_{i=0}^{n-1} \lambda_i X^i$ est dans l'idéal (X^n-1), mais est de degré strictement inférieur à n. Donc ses coefficients sont nuls : on a $\forall i \in [\![1,n]\!]$, $\lambda_i = 0$.

— La famille $(\overline{1},\dots,\overline{X}^{n-1})$ est génératrice. Soit $\overline{P} \in \mathbb{F}_q[X]/(X^n-1)$. On fait la division euclidienne de P par X^n-1 dans $\mathbb{F}_q[X]$:

$$\exists (Q,R) \in \mathbb{F}_q[X] \text{ tel que } P = Q(X^n-1)+R \text{ avec } \deg(R) < n \text{ ou } R = 0$$

En repassant modulo (X^n-1), on a bien

$$\overline{P} = \overline{R}$$

de degré inférieur à n, donc appartenant à l'espace vectoriel engendré par $(\overline{1},\dots,\overline{X}^{n-1})$.

Ainsi, $\mathbb{F}_q^n$ et $\mathbb{F}_q[X]/(X^n-1)$ sont isomorphes en tant qu'espaces vectoriels de même dimension sur $\mathbb{F}_q$. L'application φ étant surjective et linéaire (par définition), on a bien un isomorphisme. □

À l'aide de cet isomorphisme, nous allons pouvoir identifier un code linéaire de taille n sur $\mathbb{F}_q$ à un sous-espace vectoriel $\widetilde{\mathscr{C}} = \varphi(\mathscr{C})$ de $\mathbb{F}_q[X]/(X^n-1)$. Ce raisonnement va nous permettre de caractériser les codes cycliques.

Proposition 22. Soit $\mathscr{C}$ un code linéaire de taille n. Alors, $\mathscr{C}$ est cyclique si et seulement si $\widetilde{\mathscr{C}} = \varphi(\mathscr{C})$ est un idéal de $\mathbb{F}_q[X]/(X^n-1)$.

Démonstration. Soient $a = (a_0, a_1, \dots, a_{n-1}) \in \mathscr{C}$ et $a' = (a_{n-1}, a_0, \dots, a_{n-2})$. Remarquons que,

$$\begin{aligned}\varphi(a') &= \overline{a_{n-1} + \sum_{i=0}^{n-2} a_i X^{i+1}} \\ &= a_{n-1}(\overline{1} - \overline{1} + \overline{X}^n) + \sum_{i=0}^{n-2} a_i \overline{X}^{i+1} \\ &= \sum_{i=0}^{n-1} a_i \overline{X}^{i+1} \\ &= \overline{X} \sum_{i=0}^{n-1} a_i \overline{X}^{i} \\ &= \overline{X}\varphi(a)\end{aligned}$$

— Supposons $\mathscr{C}$ cyclique. Alors, par ce qu'on vient de dire, $\widetilde{\mathscr{C}}$ est stable par multiplication par X. Mais $\widetilde{\mathscr{C}}$ est un sous-espace vectoriel de $\mathbb{F}_q[X]/(X^n-1)$, donc il est aussi stable par addition et par multiplication par un scalaire. Finalement, $\widetilde{\mathscr{C}}$ est bien un idéal de $\mathbb{F}_q[X]/(X^n-1)$.

— Supposons $\widetilde{\mathscr{C}}$ idéal de $\mathbb{F}_q[X]/(X^n-1)$. Alors, $\widetilde{\mathscr{C}}$ est stable par multiplication par X. Donc par le raisonnement précédent, $\mathscr{C}$ est clairement cyclique.

□

Nous arrivons au théorème suivant qui nous indique que, pour fabriquer un code cyclique de dimension m, il suffit de savoir factoriser $X^m - 1$ dans $\mathbb{F}_q[X]$ (ce qui peut se faire par l'algorithme de Berlekamp).

Théorème 23 (Structure des codes cycliques)**.** Soit $m \in [\![0, n]\!]$.

(i) Soit $P = \sum_{i=0}^{n-m} a_i X^i$ un diviseur unitaire de $X^n - 1$ dans $\mathbb{F}_q[X]$. Soit $a = \varphi^{-1}(\overline{P})$ le mot correspondant à P. Alors, en notant $\sigma : \mathbb{F}_q^n \to \mathbb{F}_q^n$ l'application de "permutation circulaire",

$$\mathscr{C} = \mathrm{Vect}(\sigma^i(a))_{i \in [\![0, m-1]\!]} \qquad (*)$$

forme un code cyclique de dimension m.

(ii) Réciproquement, si $\mathscr{C}$ est un code cyclique de dimension m sur $\mathbb{F}_q^n$, il existe un polynôme $P \in \mathbb{F}_q[X]$ diviseur de $X^n - 1$ vérifiant $(*)$ pour $\mathscr{C}$.

Démonstration. (i) Clairement, $\mathscr{C} = \mathrm{Vect}(\sigma^i(x))_{i \in [\![0, m-1]\!]}$ est un sous-espace vectoriel de $\mathbb{F}_q^n[X]$ de dimension m : c'est un code linéaire. Reste à montrer qu'il est cyclique. Soit $b = \sum_{i=0}^{m-1} b_i \sigma^i(a)$ un mot de $\mathscr{C}$. Il s'agit de montrer que $\sigma(b) \in \mathscr{C}$. Or,

$$\sigma(b) = \sum_{i=0}^{m-1} b_i \sigma^{i+1}(a) = b_{m-1}\sigma^m(a) + \sum_{i=1}^{m-1} b_{i-1}\sigma^i(m)$$

et, d'après la base choisie pour $\mathscr{C}$, $\sum_{i=1}^{m-1} b_{i-1}\sigma^i(m) \in \mathscr{C}$. Reste à montrer que $b_{m-1}\sigma^m(a) \in \mathscr{C}$.

On a,

$$\begin{aligned}\varphi(b_{m-1}\sigma^m(a)) &= b_{m-1}\overline{X}^m\varphi(a)\\ &= b_{m-1}\overline{X}^m\overline{P}\end{aligned}$$

Or, P est de degré $n-m$, unitaire et divise X^n-1, donc il existe $Q\in\mathbb{F}_q[X]$ unitaire de degré m tel que $X^n-1=PQ$. D'où,

$$\begin{aligned}\varphi(b_{m-1}\sigma^m(a)) &= b_{m-1}(\overline{X}^m-\overline{Q})\overline{P}+b_{m-1}\overline{QP}\\ &= b_{m-1}(\overline{X}^m-\overline{Q})\overline{P}\end{aligned}$$

Comme $b_{m-1}(X^m-Q)$ est de degré au plus $m-1$, on peut l'écrire $\sum_{i=0}^{m-1}c_iX^i$. Ainsi,

$$\begin{aligned}\varphi(b_{m-1}\sigma^m(a)) &= \sum_{i=0}^{m-1}c_i\overline{X}^i\overline{P}\\ &= \sum_{i=0}^{m-1}c_i\varphi(\sigma^i(a))\\ &= \varphi\left(\sum_{i=0}^{m-1}c_i\sigma^i(a)\right)\\ &\in \varphi(\mathscr{C})\end{aligned}$$

D'où $b_{m-1}\sigma^m(a)\in\mathscr{C}$: on a bien ce qu'on voulait.

(ii) Soient $\mathscr{C}$ un code cyclique de dimension m sur $\mathbb{F}_q^n$ et $\pi=\pi_{(X^n-1)}$ la projection de $\mathbb{F}_q[X]$ sur le quotient $\mathbb{F}_q[X]/(X^n-1)$. Alors, d'après la Proposition 22, $\varphi(\mathscr{C})=\widetilde{\mathscr{C}}$ est un idéal de $\mathbb{F}_q[X]/(X^n-1)$, donc $\pi^{-1}(\widetilde{\mathscr{C}})$ est un idéal de $\mathbb{F}_q[X]$, qui est principal par principalité de $\mathbb{F}_q[X]$. On peut noter P le générateur unitaire. Montrons que $P\mid X^n-1$.

$\widetilde{\mathscr{C}}$ est un idéal de $\mathbb{F}_q[X]/(X^n-1)$, donc $\overline{0}\in\widetilde{\mathscr{C}}$, donc $X^n-1\in\pi^{-1}(\widetilde{\mathscr{C}})$: il existe $Q\in\mathbb{F}_q[X]$ tel que $X^n-1=QP$. On a bien $P\mid X^n-1$.

Il s'agit maintenant de montrer que P est bien de degré $n-m$. Notons $k=\deg(P)$. Soit

$$E=\{h\in\mathbb{F}_q[X]\mid \deg(h)\in[\![0,n-k-1\}$$

On a,

$$\pi(P\cdot E)=\{\overline{Ph}\in\mathbb{F}_q[X]/(X^n-1)\mid \deg(h)\in[\![0,n-k-1\}$$

et $P\cdot E\subseteq\pi^{-1}(\widetilde{\mathscr{C}})\implies\pi(P\cdot E)\subseteq\widetilde{\mathscr{C}}$.

Soit $R\in\pi^{-1}(\widetilde{\mathscr{C}})$. Par définition de P, il existe $S\in\mathbb{F}_q[X]$ tel que $R=PS$. On effectue la division euclidienne de S par Q :

$$\exists(T,U)\in\mathbb{F}_q[X]\text{ tel que }S=QT+U\text{ avec }\deg(U)<n-k\text{ ou }U=0$$

d'où :

$$\begin{aligned} R &= P(QT+U) \\ &= T(X^n-1)+PU \\ \implies \pi(R) &= \pi(PU) \\ &\in \pi(P\cdot E) \end{aligned}$$

Ainsi, on a $\widetilde{\mathscr{C}} \subseteq \pi(P\cdot E)$. On a alors montré que $\widetilde{\mathscr{C}} = \pi(P\cdot E)$. Or, $|\pi(P\cdot E)| = q^{n-k}$ et $\mathscr{C}$ est un sous-espace vectoriel de $\mathbb{F}_q^n$ de dimension m. Par isomorphisme, on a donc :

$$|\mathscr{C}| = q^m = |\widetilde{\mathscr{C}}|$$

ce qui permet de conclure que $m = n-k$.

Pour terminer, on écrit $P = \sum_{i=0}^{n-m} a_i X^i$ et on considère $a = (a_0, \dots, a_{m-1}) \in \mathbb{F}_q^m$. Comme $\widetilde{\mathscr{C}}$ est un idéal de $\mathbb{F}_q[X]/(X^n-1)$,

$$\forall i \in [\![0, m-1]\!], \overline{X}^i\overline{P} \in \widetilde{\mathscr{C}} \implies \forall i \in [\![0, m-1]\!], \sigma(a)^i \in \mathscr{C}$$

Et $(\sigma^i(a))_{i\in[\![0,m-1]\!]}$ est une famille libre de cardinal m, donc est bien une base de $\mathscr{C}$.

□

IV - Étude d'un code de Hamming

D'après Wikipédia, un code de Hamming est un code correcteur linéaire. Il permet la détection et la correction automatique d'une erreur si elle ne porte que sur une lettre du message. Un code de Hamming est parfait : pour une longueur de code donnée il n'existe pas d'autre code plus compact ayant la même capacité de correction. En ce sens son rendement est maximal. Il existe une famille de codes de Hamming; le plus célèbre et le plus simple après le code de répétition binaire de dimension 3 et de longueur 1 est sans doute le code binaire de longueur 7, de dimension 4 et de distance minimale 3 : ça tombe bien, il est au programme de l'option C de modélisation !

Définition 24. Le code Hamming $\mathscr{C}_H$ de longueur 7 permet de coder un mot de longueur 4 en un mot de code de longueur 7. C'est un code linéaire, dont une matrice génératrice est

$$G_H = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \in \mathscr{M}_{7,4}(\mathbb{F}_2)$$

Exemple 25. On souhaite coder le mot $(1,0,0,1)$. On calcule :

$$G_H \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}$$

Le mot codé est donc $(1,1,0,0,1,0,1)$.

On peut en fait expliciter les mots de ce code : il y en a $2^4 = 16$.

Mot	**Mot codé**	**Poids**	**Mot**	**Mot codé**	**Poids**
$(0,0,0,0)$	$(0,0,0,0,0,0,0)$	0	$(1,0,0,0)$	$(1,1,0,1,0,0,0)$	3
$(0,0,0,1)$	$(0,0,0,1,1,0,1)$	3	$(1,0,0,1)$	$(1,1,0,0,1,0,1)$	4
$(0,0,1,0)$	$(0,0,1,1,0,1,0)$	3	$(1,0,1,0)$	$(1,1,1,0,0,1,0)$	4
$(0,0,1,1)$	$(0,0,1,0,1,1,1)$	4	$(1,0,1,1)$	$(1,1,1,1,1,1,1)$	7
$(0,1,0,0)$	$(0,1,1,0,1,0,0)$	3	$(1,1,0,0)$	$(1,0,1,1,1,0,0)$	4
$(0,1,0,1)$	$(0,1,1,1,0,0,1)$	4	$(1,1,0,1)$	$(1,0,1,0,0,0,1)$	3
$(0,1,1,0)$	$(0,1,0,1,1,1,0)$	4	$(1,1,1,0)$	$(1,0,0,0,1,1,0)$	3
$(0,1,1,1)$	$(0,1,0,0,0,1,1)$	3	$(1,1,1,1)$	$(1,0,0,1,0,1,1)$	4

Proposition 26. (i) $\mathscr{C}_H$ a une distance minimale de 3.

(ii) $\mathscr{C}_H$ est 1-correcteur.

(iii) $H = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$ est une matrice de contrôle de ce code.

Démonstration. (i) Le minimum des poids est bien 3 d'après le tableau précédent.

(ii) D'après la Remarque 11, la capacité de correction du code est égale à

$$\left\lfloor \frac{3-1}{2} \right\rfloor = 1$$

(iii) Soit $x \in \mathbb{F}_2^7$. On note $(v_0, \dots, v_3)$ la base de $\mathscr{C}_H$ associée à G_H. Alors,

$$\begin{aligned} x \in \mathscr{C}^\perp &\iff \forall i \in [\![0,3]\!], \langle x, v_i \rangle = 0 \\ &\iff x = ah_1 + bh_2 + ch_3 \text{ pour } a,b,c \in \mathbb{F}_2 \end{aligned}$$

où $h_1 = (1,0,0,1,0,1,1)$, $h_2 = (0,1,0,1,1,1,0)$ et $h_3 = (0,0,1,0,1,1,1)$. Donc (h_1, h_2, h_3) est une base de $\mathscr{C}^\perp$, ce qui mène au résultat voulu.

□

Proposition 27. Le code de Hamming est cyclique, engendré par $P = X^3 + X + 1$.

Démonstration. Les 4 vecteurs colonnes de la matrice G_H se déduisent les uns des autres par permutation circulaire. Par conséquent, l'ensemble du code est invariant par permutation circulaire : $\mathscr{C}_H$ est bien cyclique. Et le polynôme P correspond au mot $(1,1,0,1,0,0,0)$ qui est le premier vecteur colonne de la matrice G_H. □

En pratique, le code de Hamming se manipule de la manière suivante :

1. On a un mot $x \in \mathbb{F}_2^4$. On calcule
$$a = G_H x$$
et on envoie a.
2. Le receveur reçoit a'. Il calcule le syndrome $s = Ha'$. Si s est nul, il pose $a = a'$. Sinon, il pose $a = a' + e_j$ où pour $j \in [\![1,7]\!]$, $s = He_j$.
3. Le receveur résout $G_H x = a$.

4 Conseils généraux

Dans cette fiche un peu différente, je liste quelques conseils de préparation qui ont fonctionné pour moi.

Avant de commencer la lecture de ce document, je tiens à avertir tous ses lecteurs : les conseils qui vont suivre sont très personnels. Je les rédige en toute modestie ici avec l'expérience acquise au cours de cette année de préparation et je ne pourrai résumer à quelques phrases tout ce que j'ai appris. Bref, c'est à vous de trouver les méthodes de travail qui marchent le mieux pour vous. Ci-dessous ne sont listés que de modestes exemples...

Je précise également que j'ai obtenu l'agrégation en deux fois : admissible en 2021, puis admis en 2024 en "candidat libre". J'ai continué à étudier parallèlement à mon travail d'enseignant en mathématiques, et j'ai donc dû adapter mon plan de travail en conséquence.

I - Conseils pour la préparation pendant l'année

1. Travail de l'écrit

À mon sens, il faut commencer à travailler les écrits dès la rentrée. Personnellement, j'ai commencé par des petits exercices très ciblés, puis j'ai assez vite enchaîné sur des sujets d'agrégation. Un travail de l'ordre d'un sujet par semaine ; pas tout d'un coup, mais étalé sur les sept jours. Environ deux mois avant les oraux, je me suis imposé un écrit blanc par semaine : six heures de suite le mercredi à la bibliothèque universitaire, puis correction dans la foulée.

L'idée pour les écrits était de bien faire environ la moitié du sujet, le reste serait du bonus étant donné que je ne vise aucun classement.

2. Travail de l'oral

Mes développements étant déjà rédigés suite à mon parcours de 2021, je n'avais "que" les leçons à retravailler et à rerédiger.

Ma méthode était assez simple : un plan de leçon par semaine jusqu'aux écrits, puis un plan par jour sur cinq jours de la semaine jusqu'à avoir terminé. Je me suis autorisé trois impasses : deux en algèbre et une en analyse. Je conçois que la seconde moitié de cette préparation est assez lourde, j'aurais sans doute dû équilibrer un peu mieux au cours de l'année. Une fois mes plans terminés, j'ai fait des révisions thématiques (groupes, anneaux, séries entières, probabilités, etc.) notamment à l'aide des retours d'oraux disponibles sur le site agreg-maths.fr. Je ne peux que vous conseiller d'en faire de même, certaines questions sont très classiques et il y a de grandes chances que vous les retrouviez le jour J.

Pour mémoriser mes plans, j'ai utilisé le logiciel Anki. Cela fonctionne très bien, et j'ai pu tout apprendre en un mois et demi environ.

En ce qui concerne le contenu des plans, il me semble inutile et même contreproductif d'inclure des résultats non maîtrisés. Le jury interroge en priorité sur les résultats qui figurent dans le plan.

À mon avis, il vaut mieux un plan simple d'un niveau moindre mais dont on est sûr du contenu, qu'un plan trop ambitieux.

II - Conseils pour le jour J

1. Pour les écrits

Déjà, un point simple mais essentiel : rester pendant les six heures d'épreuve et tout donner jusqu'à la fin. Il n'y a rien de plus frustrant que de rater l'admission à un point, il faut mettre toutes les chances de son côté.

Ensuite, on le lit partout et les rapports du jury le confirme, mais il faut soigner au maximum le début de sa copie. Les premières questions servent régulièrement de discriminant entre les candidats, il convient d'être du bon côté.

Dernier détail ; les copies sont numérisées, puis corrigées sur ordinateur. Donc il vaut mieux écrire avec un stylo à encre foncée.

2. Pour les oraux

J'ai organisé mes préparations de la manière suivante :

— une heure et demi consacrée à l'écriture du plan ;

— le reste pour apprendre mes développements et travailler les résultats qui figurent dans mon plan selon le temps restant.

Cela ne peut fonctionner que si les développements ont été travaillés et appris en amont. Pour les oraux de 2024, nous avions réellement trois heures de préparation et nous disposions d'une petite minute pour relire le développement choisi par le jury. Pour cette raison, il convient de l'avoir rédigé proprement sur une des feuilles de brouillon.

Je n'ai pas de conseil à donner pour la défense du plan autre qu'il faut indiquer ses développements et motiver leur place dans la leçon choisie.

Pour le développement, il ne faut faire ni trop court ni trop long. Je pense qu'un développement n'est jamais trop court : on peut mettre à profit le temps superflu en faisant un plan de la preuve au tableau, en prenant le temps de se retourner vers le jury pour expliquer son raisonnement, en appliquant le résultat démontré à un exemple, etc. Le jury attend une certaine aisance à l'oral, et faire preuve de qualités pédagogiques dans un tel contexte ne peut être que valorisé.

À ce sujet, je vous conseille de porter une montre digitale le jour de l'oral (on peut en trouver des très bonnes pour une quinzaine d'euros dans un magasin de sport très connu), et de lancer le chronomètre, que ce soit pour la défense du plan ou pour le développement. Cela aide vraiment dans la gestion du temps. Ce conseil vaut d'autant plus pour l'épreuve de modélisation où la partie orale en autonomie dure tout de même 35 minutes.

Ensuite, pour les questions, les notes réalisées pendant la préparation sont autorisées. Donc il ne faut pas hésiter à noter quelques éléments de preuve de résultats non triviaux. Et, je vais sûrement me répéter, mais il faut maîtriser son plan car le jury peut interroger sur tous les éléments qui s'y

trouvent.

En ce qui concerne l'attitude des membres du jury, de mon expérience, ils sont généralement bienveillants. Les questions servent à tester le degré de maîtrise du sujet par le candidat. À ce titre, il faut être honnête et ne pas tenter d'entourloupes (les membres du jury sauront de toute manière le détecter, et le restant de l'heure pourra vite tourner au clavaire).

Dernier conseil, plus personnel, mais il ne faut pas se décourager. Un tirage défavorable, ça existe. Deux tirages défavorables, aussi. Ce fut mon cas cette année, et je confirme que la préparation est d'autant plus stressante que de savoir que nous allons rester une heure devant des spécialistes de leur domaine pour parler d'un sujet que nous ne maîtrisons pas. Même dans ce cas là, n'oubliez pas que vous savez des choses, même si elles sont simples, et le jury saura (aussi) le mettre en valeur. Et même si vous n'arrivez à rien, une mauvaise note ça arrive et cela ne vous disqualifie pas d'office. Il ne faut pas se décourager et donner le maximum les autres jours en pensant à tout le chemin parcouru dans l'année pour en arriver là où vous êtes...

5 Extrema liés

Rédaction "propre" et la plus détaillée possible de l'existence et l'unicité des multiplicateurs de Lagrange liant les différentielles de plusieurs fonctions sous certaines hypothèses.

Théorème 1 (Extrema liés)**.** Soit U un ouvert de $\mathbb{R}^n$ et soient $f, g_1, \dots, g_r : U \to \mathbb{R}$ des fonctions de classe $\mathscr{C}^1$. On note $\Gamma = \{x \in U \mid g_1(x) = \cdots = g_r(x) = 0\}$. Si $f_{|\Gamma}$ admet un extremum relatif en $a \in \Gamma$ et si les formes linéaires $\mathrm{d}(g_1)_a, \dots, \mathrm{d}(g_r)_a$ sont linéairement indépendantes, alors il existe des uniques $\lambda_1, \dots, \lambda_r$ appelés **multiplicateurs de Lagrange** tels que

$$\mathrm{d}f_a = \lambda_1 \mathrm{d}(g_1)_a + \cdots + \lambda_r \mathrm{d}(g_r)_a$$

[GOU20] p. 337

Démonstration. Soit $s = n - r$. Identifions $\mathbb{R}^n$ à $\mathbb{R}^s \times \mathbb{R}^r$ et écrivons les éléments (x, y) de $\mathbb{R}^n$ sous la forme $(x, y) = (x_1, \dots, x_s, y_1, \dots, y_r)$. On notera également par la suite $a = (\alpha, \beta)$ avec $\alpha \in \mathbb{R}^s$ et $\beta \in \mathbb{R}^r$. On a déjà plusieurs informations : p. 347

— Déjà, $r \leq n$, car les formes linéaires $\mathrm{d}(g_i)_a$ forment une famille libre de $(\mathbb{R}^n)^*$, qui est de dimension n.

— De plus, si $r = n$, la démonstration est triviale car $(\mathrm{d}(g_i)_a)_{i \in [\![1,n]\!]}$ est alors une base de $(\mathbb{R}^n)^*$.

Pour ces raisons, nous supposerons dans la suite $r \leq n - 1$ (ie. $s \geq 1$).

Comme $(\mathrm{d}(g_i)_a)_{i \in [\![1,r]\!]}$ est une famille libre, la matrice

$$\left(\left(\frac{\partial g_i}{\partial x_j}(a) \right)_{\substack{i \in [\![1,r]\!] \\ j \in [\![1,s]\!]}} \quad \left(\frac{\partial g_i}{\partial y_j}(a) \right)_{\substack{i \in [\![1,r]\!] \\ j \in [\![1,r]\!]}} \right)$$

est de rang r. On peut donc extraire une sous-matrice de taille $r \times r$ inversible. Quitte à changer le nom des variables, on peut supposer que c'est la sous-matrice de droite, ie.

$$\det \left(\left(\frac{\partial g_i}{\partial y_j}(a) \right)_{i,j \in [\![1,r]\!]} \right) \neq 0 \qquad (*)$$

On va appliquer le théorème des fonctions implicites à la fonction $g = (g_1, \dots, g_r)$. Pour cela, on vérifie les hypothèses :

— g est de classe $\mathscr{C}^1$.

— $g(\alpha, \beta) = 0$ car $(\alpha, \beta) = a \in \Gamma$.

— La différentielle partielle $\mathrm{d}_y g_a$ est inversible par $(*)$.

Ainsi, il existe :

— U' voisinage de α dans $\mathbb{R}^s$.

— V' voisinage de β dans $\mathbb{R}^r$.

— $\varphi : U' \to V'$ de classe $\mathscr{C}^1$ telle que $\varphi(\alpha) = \beta$ et $\forall (x, y) \in U' \times V'$, $(x, y) \in \Gamma \iff g(x, y) = 0 \iff y = \varphi(x)$.

En d'autres termes, sur un voisinage de a, les éléments de Γ s'écrivent $(x, \varphi(x))$. On pose maintenant $u : x \mapsto (x, \varphi(x))$ et $h = f \circ u$. Par composition, h est différentiable en α et

$$0 \overset{\alpha \text{ extremum de } h}{=} \mathrm{d}h_\alpha = \mathrm{d}(f \circ u)_\alpha = \mathrm{d}f_{u(\alpha)} \circ \mathrm{d}u_\alpha = \mathrm{d}f_a \circ \mathrm{d}u_\alpha$$

En termes de matrices, cela donne :

$$\begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} = \left(\left(\frac{\partial f}{\partial x_j}(a) \right)_{j \in [\![1,s]\!]} \quad \left(\frac{\partial f}{\partial y_j}(a) \right)_{j \in [\![1,r]\!]} \right) \begin{pmatrix} I_s \\ \left(\frac{\partial \varphi_i}{\partial x_j}(\alpha) \right)_{\substack{i \in [\![1,r]\!] \\ j \in [\![1,s]\!]}} \end{pmatrix}$$
$$= \begin{pmatrix} \frac{\partial f}{\partial x_1}(a) + \sum_{k=1}^{r} \frac{\partial f}{\partial y_k}(a) \frac{\partial \varphi_k}{\partial x_1}(\alpha) \\ \vdots \\ \frac{\partial f}{\partial x_s}(a) + \sum_{k=1}^{r} \frac{\partial f}{\partial y_k}(a) \frac{\partial \varphi_k}{\partial x_s}(\alpha) \end{pmatrix}$$

On aboutit à la relation suivante :

$$\forall i \in [\![1,s]\!], \frac{\partial f}{\partial x_i}(a) + \sum_{k=1}^{r} \frac{\partial f}{\partial y_k}(a) \frac{\partial \varphi_k}{\partial x_i}(\alpha) = 0 \qquad (**)$$

Comme $\forall j \in [\![1,r]\!]$, $g_j(\alpha, \varphi(\alpha)) = g_j(a) = 0$, on peut aboutir de la même manière à la relation suivante :

$$\forall i \in [\![1,s]\!], \forall j \in [\![1,r]\!], \frac{\partial g_j}{\partial x_i}(a) + \sum_{k=1}^{r} \frac{\partial g_j}{\partial y_k}(a) \frac{\partial \varphi_k}{\partial x_i}(\alpha) = 0 \qquad (***)$$

On considère maintenant la matrice M suivante :

$$M = \begin{pmatrix} \left(\frac{\partial f}{\partial x_j}(a) \right)_{j \in [\![1,s]\!]} & \left(\frac{\partial f}{\partial y_j}(a) \right)_{j \in [\![1,r]\!]} \\ \left(\frac{\partial g_i}{\partial x_j}(a) \right)_{\substack{i \in [\![1,r]\!] \\ j \in [\![1,s]\!]}} & \left(\frac{\partial g_i}{\partial y_j}(a) \right)_{\substack{i \in [\![1,r]\!] \\ j \in [\![1,r]\!]}} \end{pmatrix}$$

Par $(**)$ et $(***)$, les s premiers vecteurs colonnes de cette matrice s'expriment linéairement en fonction de ses r derniers. Donc $\mathrm{rang}(M) \leq r$. Mais, le rang des vecteurs lignes d'une matrice est égal au rang de ses vecteurs colonnes. Donc les $r+1$ vecteurs lignes de M forment une famille liée. Mais par hypothèse, les r dernières lignes sont libres. Donc la première ligne est combinaison linéaire des r dernières, ce qui se réécrit :

$$\exists \lambda_1, \ldots, \lambda_r \in \mathbb{R} \text{ tels que } \mathrm{d}f_a = \lambda_1 \mathrm{d}(g_1)_a + \cdots + \lambda_r \mathrm{d}(g_r)_a$$

L'unicité est claire car $(\mathrm{d}(g_i)_a)_{i \in [\![1,r]\!]}$ est une famille libre. □

Attention à la rigueur et à la propreté dans cette démonstration. On peut très vite se perdre si l'on va trop vite ou si l'on ne prend pas le temps de bien écrire chaque donnée.

Remarque 2. Il paraît que le jury n'aime pas beaucoup cette démonstration. Si vous la proposez en développement, soyez sûr de pouvoir en donner une interprétation géométrique : grâce à la condition d'indépendance des $\mathrm{d}(g_i)_a$, Γ est une sous-variété de $\mathbb{R}^n$ autour du

[BMP] p. 20

point a. D'autre part,

$$\mathrm{d}f_a = \lambda_1 \mathrm{d}(g_1)_a + \cdots + \lambda_r \mathrm{d}(g_r)_a \iff \bigcap_{i=1}^{r} \mathrm{Ker}(\mathrm{d}(g_i)_a) \subseteq \mathrm{Ker}(\mathrm{d}f_a) \qquad (*)$$

En particulier, $\mathrm{d}f_a$ est nulle sur $\bigcap_{i=1}^{r} \mathrm{Ker}(\mathrm{d}(g_i)_a)$. Or, l'espace tangent en a à la sous-variété $\{x \text{ proche de } a \mid g_1(x) = \cdots = g_r(x) = 0\}$ est justement $\{h \in \mathbb{R}^n \mid \mathrm{d}(g_1)_a(h) = \cdots = \mathrm{d}(g_r)_a(h) = 0\}$.

Bref, la condition $(*)$ exprime que $\mathrm{d}f_a$ est nulle sur le plan tangent à Γ en a. Ceci équivaut aussi à ce que ∇f_a soit orthogonal à l'espace tangent à Γ en a. Ainsi, la seule manière de rendre f plus petit serait de "sortir de Γ".

6 Invariants de similitude

Nous montrons l'existence et l'unicité des invariants de similitude d'un endomorphisme d'un espace de dimension finie en utilisant la dualité.

Soit E un espace vectoriel de dimension finie $n \geq 1$ sur un corps commutatif $\mathbb{K}$. Soit $f \in \mathscr{L}(E)$. **[GOU21]** p. 398

Notation 1. Soit $x \in E$. On note P_x le polynôme unitaire engendrant l'idéal $\{P \in \mathbb{K}[X] \mid P(f)(x) = 0\}$ (un tel polynôme existe car $\mathbb{K}[X]$ est principal et cet idéal est non réduit à $\{0\}$) et $E_x = \{P(f)(x) \mid P \in \mathbb{K}[X]\}$.

Lemme 2. (i) Si $k = \deg(\pi_f)$, alors $\mathbb{K}[f]$ est un sous-espace vectoriel de $\mathscr{L}(E)$ de dimension k, dont une base est $(f^i)_{i \in [\![0,k-1]\!]}$.

(ii) Soit $x \in E$. Si $l = \deg(P_x)$, alors E_x est un sous-espace vectoriel de E de dimension l, dont une base est $(f^i(x))_{i \in [\![0,l-1]\!]}$.

Démonstration. (i) Montrons que la famille $(f^i)_{i \in [\![0,k-1]\!]}$ est à la fois libre et génératrice. p. 61

— Soit $P(f) \in \mathbb{K}[f]$. On fait la division euclidienne de P par π_f dans $\mathbb{K}[X]$ pour écrire $P = \pi_f Q + R$ avec $Q, R \in \mathbb{K}[X]$ et $\deg(R) < k = \deg(\pi_f)$. En évaluant en f, cela donne $P(f) = R(f) \in \mathrm{Vect}(\mathrm{id}_E, \dots, f^{k-1})$. Donc la famille est génératrice.

— Si $\sum_{i=0}^{k-1} \lambda_i f^i = 0$, alors le polynôme $P = \sum_{i=0}^{k-1} \lambda_i X^i$ vérifie $P(f) = 0$. Donc $\pi_f \mid P$, et comme $\deg(P) < \deg(\pi_f)$, on a $P = 0$. Donc $\lambda_0 = \cdots = \lambda_{k-1} = 0$. Donc la famille est libre.

(ii) La deuxième assertion se montre sensiblement de la même manière.

□

Lemme 3. Il existe $x \in E$ tel que $P_x = \pi_f$. p. 290

La démonstration est un peu trop longue pour être incluse ici : c'est un résultat qui demande du temps pour le démontrer (et pourrait constituer un vrai développement à part entière). Nous vous renvoyons vers **[GOU21]** p. 178 pour la démonstration.

Théorème 4 (Frobenius)**.** Il existe des sous-espaces vectoriels $F_1, \dots, F_r$ de E tous stables par f tels que :

(i) $E = \bigoplus_{i=1}^{r} F_i$.

(ii) $\forall i \in [\![1, r]\!]$, la restriction $f_i = f_{|F_i}$ est un endomorphisme cyclique de F_i.

(iii) Si $P_i = \pi_{f_i}$ est le polynôme minimal de f_i, on a $P_{i+1} \mid P_i$ $\forall i \in [\![1, r-1]\!]$.

La suite $(P_i)_{i \in [\![1,r]\!]}$ ne dépend que de f et non du choix de la décomposition (elle est donc unique). On l'appelle **suite des invariants de** f.

Démonstration. — Existence : Soit $k = \deg(\pi_f)$. Par le Lemme 3, il existe $x \in E$ tel que $P_x = \pi_f$. Par le Lemme 2, le sous-espace $F = E_x$ est de dimension k et est stable par f et comme $\deg(P_x) = k$, la famille de vecteurs

$$(\underbrace{x}_{=e_1}, \dots, \underbrace{f^{k-1}(x)}_{=e_k})$$

forme une base de F. Complétons cette base en une base $(e_1, \dots, e_n)$ de E. En désignant par $(e_1^*, \dots, e_n^*)$ la base duale associée et en notant $\Gamma = \{e_k^* \circ f^i \mid i \in \mathbb{N}\}$, on pose

$$\begin{aligned} G &= \Gamma^\circ \\ &= \{x \in E \mid \forall i \in \mathbb{N}, (e_k^* \circ f^i)(x) = 0\} \end{aligned}$$

Ainsi, G est l'ensemble des $x \in E$ tel que la k-ième coordonnée de $f^i(x)$ (dans la base $(e_1, \dots, e_n)$) est nulle $\forall i \in \mathbb{N}$; G est donc un sous-espace de E stable par f. Montrons que $F \oplus G = E$.

Montrons que $F \cap G = \{0\}$. Soit $y \in F \cap G$. Si $y \neq 0$, on peut écrire $y = \lambda_1 e_1 + \dots + \lambda_p e_p$ avec $\lambda_p \neq 0$ et $p \leq k$. En composant par $e_k^* \circ f^{k-p}$, on obtient

$$\begin{aligned} 0 &\underset{y \in G}{=} e_k^* \circ f^{k-p}(y) \\ &= e_k^*(\lambda_1 f^{k-p}(e_1) + \dots + \lambda_p f^{k-p}(e_p)) \\ &= e_k^*(\lambda_1 f^{k-p}(x) + \dots + \lambda_p f^{k-p}(x)) \\ &= \lambda_p \end{aligned}$$

Ce qui est absurde.

Montrons que $\dim(F) + \dim(G) = n$. Cela revient à montrer que $\dim(G) = n - k$. On sait que $G = \Gamma^\circ = (\mathrm{Vect}(\Gamma))^\circ$ et $\dim(\mathrm{Vect}(\Gamma)) + \dim(\mathrm{Vect}(\Gamma)^\circ) = n$. Montrons donc que $\dim(\mathrm{Vect}(\Gamma)) = k$. Posons

$$\varphi : \begin{array}{ccc} \mathbb{K}[f] & \to & \mathrm{Vect}(\Gamma) \\ g & \mapsto & e_k^* \circ g \end{array}$$

Par définition de Γ, φ est surjective. Soit $g \in \mathrm{Ker}(\varphi)$. On a alors $e_k^* \circ g = 0$, et comme $g \in \mathbb{K}[f]$,

$$g = \lambda_1 \mathrm{id} + \dots \lambda_p f^{p-1} \text{ avec } \lambda_p \neq 0 \text{ et } p \leq k$$

On a donc $0 = e_k^* \circ g(f^{k-p}(x)) = \lambda_p \neq 0$. Ainsi, $g = 0$ et ϕ est un isomorphisme. Donc $\dim(\mathrm{Vect}(\Gamma)) = \dim(\mathbb{K}[f]) = k$ par le Lemme 2, ce que l'on voulait.

Soit P_1 le polynôme minimal de $f_{|F}$ (qui est le polynôme minimal de f car $P_1 = \pi_{f_{|F}} \underset{\pi_f = P_x}{=} \pi_f$). Soit P_2 le polynôme minimal de $f_{|G}$. Comme G est stable par f, on a $P_1(f_{|G}) = \pi_f(f_{|G}) = 0$, donc $P_2 \mid P_1$. Il suffit alors de réitérer en remplaçant f par $f_{|G}$ et E par G pour obtenir la décomposition voulu.

— Unicité : Soient $F_1, \dots, F_r$ et $G_1, \dots G_s$ des sous-espaces vectoriels stables par f qui vérifient le Point (i), le Point (ii) et le Point (iii). On note pour tout i, $P_i = \pi_{f_{|F_i}}$ et $Q_i = \pi_{f_{|G_i}}$. On suppose par l'absurde $(P_1, \dots, P_r) \neq (Q_1, \dots, Q_s)$. Soit $j = \min\{i \mid P_i \neq Q_i\}$.Comme $E = \bigoplus_{i=1}^r F_i$ (où

$\forall i \in [\![1,r]\!]$, F_i est stable par f et $\forall k \geq j \geq 1$, $P_j(f)(F_k) = 0$) :

$$P_j(f)(F_1) \oplus \cdots \oplus P_j(f)(F_{j-1}) = P_j(f)(E) \qquad (*)$$

De même,

$$P_j(f)(G_1) \oplus \cdots \oplus P_j(f)(G_{j-1}) \oplus P_j(f)(G_j) \oplus \cdots \oplus P_j(f)(G_s) = P_j(f)(E) \qquad (**)$$

Notons que l'on a $\forall i \in [\![1, j-1]\!]$, $\dim(P_j(f)(F_i)) = \dim(P_j(f)(G_i))$. En effet, on peut trouver une base $\mathscr{B}_i$ de F_i et une base $\mathscr{B}'_i$ de G_i telles que $\mathrm{Mat}(f_{|F_i}, \mathscr{B}_i) = \mathrm{Mat}(f_{|G_i}, \mathscr{B}'_i)$ par cyclicité de $f_{|F_i}$ et $f_{|G_i}$. En prenant les dimensions dans $(*)$ et $(**)$, on en déduit :

$$0 = \dim(P_j(f)(G_j)) = \cdots = \dim(P_j(f)(G_s)) \implies Q_j \mid P_j$$

Par symétrie, on a de même $P_j \mid Q_j$. D'où $P_j = Q_j$: absurde.

□

7 Lemme des noyaux

On montre par récurrence le lemme des noyaux pour un endomorphisme d'un espace vectoriel de dimension finie, et on applique ce résultat pour obtenir un critère de diagonalisation.

Soit E un espace vectoriel de dimension finie $n \geq 1$ sur un corps commutatif $\mathbb{K}$.

[GOU21] p. 185

Théorème 1 (Lemme des noyaux)**.** Soient $f \in \mathscr{L}(E)$ et $P = P_1 \dots P_k \in \mathbb{K}[X]$ (les P_i étant supposés premiers entre eux deux-à-deux). Alors,

$$\operatorname{Ker}(P(f)) = \bigoplus_{i=1}^{k} \operatorname{Ker}(P_i(f))$$

Démonstration. On procède par récurrence sur $k \geq 2$.

— Pour $k = 2$: par le théorème de Bézout, il existe $U, V \in \mathbb{K}[X]$ tels que $UP_1 + VP_2 = 1$. Donc,

$$\forall x \in E,\ (UP_1 + VP_2)(f)(x) = (U(f) \circ P_1(f))(x) + (V(f) \circ P_2(f))(x) = x \qquad (*)$$

Soit $x \in \operatorname{Ker}(P_1(f)) \cap \operatorname{Ker}(P_2(f))$. On a :

$$x \overset{(*)}{=} (U(f) \circ P_1(f))(x) + (V(f) \circ P_2(f))(x) \overset{x \in \operatorname{Ker}(P_1(f)) \cap \operatorname{Ker}(P_2(f))}{=} 0$$

Donc $\operatorname{Ker}(P_1(f)) \cap \operatorname{Ker}(P_2(f)) = \{0\}$: la somme est directe.

Soit maintenant $x \in \operatorname{Ker}(P(f))$. Par calcul,

$$P_2(f)(UP_1(f)(x)) = (UP_1P_2)(f)(x) = (U(f) \circ P(f))(x) = 0$$

ie. $UP_1(f)(x) \in \operatorname{Ker}(P_2(f))$. De même, $VP_2(f)(x) \in \operatorname{Ker}(P_1(f))$. Par $(*)$, $x \in \operatorname{Ker}(P_1(f)) + \operatorname{Ker}(P_2(f))$. Donc $\operatorname{Ker}(P(f)) \subseteq \operatorname{Ker}(P_1(f)) \oplus \operatorname{Ker}(P_2(f))$.

Et si $x \in \operatorname{Ker}(P_1(f))$,

$$P(f)(x) = (P_1(f) \circ P_2(f))(x) = (P_2(f) \circ P_1(f))(x) = 0$$

donc $x \in \operatorname{Ker}(P(f))$ et $\operatorname{Ker}(P_1)(f) \subseteq \operatorname{Ker}(P(f))$. De même, on montre que $\operatorname{Ker}(P_2)(f) \subseteq \operatorname{Ker}(P(f))$. Comme $\operatorname{Ker}(P(f))$ est un espace vectoriel, on a bien l'inclusion réciproque.

— On suppose le résultat vrai à un rang $k \geq 2$. Montrons qu'il reste vrai au rang $k+1$. Écrivons

$$P = Q_1 Q_2 \text{ avec } Q_1 = P_1 \dots P_k, Q_2 = P_{k+1}$$

Les polynômes Q_1 et Q_2 sont premiers entre eux, donc le cas $k=2$ permet d'obtenir :

$$\begin{aligned}\operatorname{Ker}(P(f)) &= \operatorname{Ker}(Q_1(f)) \oplus \operatorname{Ker}(Q_2(f)) \\ &= \left(\bigoplus_{i=1}^{k} \operatorname{Ker}(P_i(f))\right) \oplus \operatorname{Ker}(P_{k+1}(f)) \text{ par hypothèse de récurrence} \\ &= \bigoplus_{i=1}^{k+1} \operatorname{Ker}(P_i(f))\end{aligned}$$

ce que l'on voulait.

□

Application 2. Soit $f \in \mathscr{L}(E)$. Alors f est diagonalisable si et seulement s'il existe $P \in \mathbb{K}[X]$ scindé sur $\mathbb{K}$ à racines simples tel que $P(f)=0$.

Démonstration. Sens direct : Soient $\lambda_1, \dots, \lambda_k$ les valeurs propres distinctes de f et $E_{\lambda_1}, \dots, E_{\lambda_k}$ les sous-espaces propres correspondants. On pose

$$P = (X-\lambda_1)\dots(X-\lambda_k) \in \mathbb{K}[X]$$

On peut appliquer le Théorème 1 :

$$\begin{aligned}\operatorname{Ker}(P(f)) &= \bigoplus_{i=1}^{k} \operatorname{Ker}(f-\lambda_i \operatorname{id}_E) \\ &= \bigoplus_{i=1}^{k} E_{\lambda_i} \\ &\overset{f \text{ diagonalisable}}{=} E\end{aligned}$$

donc $P(f)=0$ (et P est bien scindé à racines simples).

Réciproque : On écrit

$$P = \alpha(X-\lambda_1)\dots(X-\lambda_k)$$

avec les $\lambda_i \in \mathbb{K}$ distincts et $\alpha \neq 0$. On peut encore appliquer Théorème 1 :

$$\begin{aligned}E &= \operatorname{Ker}(P(f)) \\ &= \bigoplus_{i=1}^{k} \operatorname{Ker}(f-\lambda_i \operatorname{id}_E) \qquad (*)\end{aligned}$$

Notons $I = \{i \in [\![1,k]\!] \mid \operatorname{Ker}(f-\lambda_i \operatorname{id}_E) \neq \{0\}\}$. $\forall i \in I$, λ_i est valeur propre de f et $E_{\lambda_i} = \operatorname{Ker}(f-\lambda_i \operatorname{id}_E)$ n'est autre que le sous-espace propre correspondant. Par $(*)$,

$$E = \bigoplus_{i \in I} E_{\lambda_i}$$

donc f est diagonalisable. □

8 Transformée de Fourier discrète

On dispose en mathématiques de quatre opérations dites "élémentaires" : l'addition, la soustraction, la division et donc la multiplication. On sait tous multiplier deux entiers en base 10 *: il suffit de faire la multiplication de chaque chiffre du multiplicateur par chaque chiffre du multiplicande, puis d'additionner le tout. Pour deux nombres de taille n, cela donne un algorithme de complexité $O(n^2)$. Mais dès que l'on veut multiplier de très grands chiffres (en informatique par exemple), cet algorithme montre très vite ses limites. Nous allons étudier ici le cas des polynômes en donnant un algorithme de multiplication utilisant la transformée de Fourier rapide.*

I - Transformée de Fourier discrète sur $\mathbb{C}$

1. Définitions

L'idée va être d'identifier les polynômes de degré inférieur à $n-1$ de la forme $\sum_{k=0}^{n-1} a_k x^k$ au vecteur de $\mathbb{C}^n$ $(a_0, \dots, a_{n-1})$. On fixe, pour toute la suite, ω une racine primitive n-ième de l'unité.

Définition 1. On appelle **transformée de Fourier discrète** l'application

$$\begin{array}{rccc} \mathrm{DFT}_\omega : & \mathbb{C}^n & \to & \mathbb{C}^n \\ & (f_0, \dots, f_{n-1}) & \mapsto & (\sum_{k=0}^{n-1} f_k, \sum_{k=0}^{n-1} f_k \omega^k, \dots, \sum_{k=0}^{n-1} f_k \omega^{(n-1)k}) \end{array}$$

Remarque 2. Si F est le polynôme associé au vecteur $f = (f_0, \dots, f_{n-1})$, on a

$$\mathrm{DFT}_\omega(f) = (F(1), \dots, F(\omega^{n-1}))$$

fait que nous utiliserons plusieurs fois dans la suite.

Dans un premier temps, on peut écrire l'algorithme de calcul suivant.

Algorithme 3.

```
# Exponentiation rapide. Calcul x^n.
def power(x, n):
    if n == 0:
        return 1
    if n == 1:
        return x
    if n % 2 == 0:
        return power(x*x, n//2)
    return x * power(x*x, (n-1)//2)

# Algorithme naïf pour calculer la transformée de Fourier rapide de f.
def naive_dft(f, omega):
    n = len(f)
    return [sum(f[k] * power(omega, i*k) for k in range(n)) for i in range
```

```
    (n)]
```

Définition 4. Le **produit de convolution** de deux vecteurs $f = (f_0, \dots, f_{n-1})$ et $g = (g_0, \dots, g_{n-1})$ de $\mathbb{C}^n$ est le vecteur de $\mathbb{C}^n$ noté $f *_n g$ défini par

$$f *_n g = \left(\sum_{i+j \equiv k \mod n} f_i g_j \right)_{k \in [\![0, n-1]\!]}$$

Exemple 5. $\mathrm{DFT}_{-1}(1,3) = (4,-2)$ et $(1,3) *_2 (1,3) = (1+9, 3+3) = (10,6)$.

2. Propriétés

Proposition 6. Soient $f = (f_0, \dots, f_{n-1})$, $g = (g_0, \dots, g_{n-1})$ deux vecteurs de $\mathbb{C}^n$. On pose $h = f *_n g = (h_0, \dots, h_{n-1})$ ainsi que F, G et H les polynômes associés respectivement à f, g et h. Modulo $X^n - 1$, on a :

$$\overline{H} = \overline{FG}$$

Démonstration. Écrivons :

$$H = \sum_{k=0}^{n-1} \left(\sum_{i+j \equiv k \mod n} f_i g_j \right) X^k$$

Comme H est au plus de degré $n-1$, on a $H = \overline{H}$ (par abus de notation). Maintenant avec $F = \sum_{k=0}^{n-1} f_k X^k$ et $G = \sum_{k=0}^{n-1} g_k X^k$, on a :

$$\begin{aligned} FG &= \sum_{k=0}^{2n-2} \left(\sum_{i+j=k} f_i g_{k-i} \right) X^k \\ &= \sum_{k=0}^{n-1} \left(\sum_{i+j=k} f_i g_{k-i} \right) X^k + \sum_{k=n}^{2n-2} \left(\sum_{i+j=k} f_i g_{k-i} \right) X^k \\ &= \sum_{k=0}^{n-1} \left(\sum_{i+j=k} f_i g_{k-i} \right) X^k + X^n \left(\sum_{k=0}^{n-2} \left(\sum_{i+j=n+k} f_i g_{k-i} \right) X^k \right) \end{aligned}$$

En passant modulo $X^n - 1$,

$$\begin{aligned}
\overline{FG} &= \overline{F}\,\overline{G} \\
&= \sum_{k=0}^{n-1}\left(\sum_{i=0}^{k} f_i g_{k-i}\right)\overline{X^k} + \sum_{k=n}^{2n-2}\left(\sum_{i=0}^{k} f_i g_{k-i}\right)\overline{X^k} \\
&\overset{\overline{X^n}=\overline{1}}{=} \sum_{k=0}^{n-1}\left(\sum_{i=0}^{k} f_i g_{k-i}\right)\overline{X^k} + \sum_{k=0}^{n-2}\left(\sum_{i+j=n+k} f_i g_{k-i}\right)\overline{X^k} \\
&= \sum_{k=0}^{n-1}\left(\sum_{i+j\equiv k \bmod n} f_i g_j\right)\overline{X^k} \\
&= \overline{H}
\end{aligned}$$

□

Théorème 7. DFT_ω est un isomorphisme d'algèbres entre $(\mathbb{C}^n, +, *_n)$ et $(\mathbb{C}^n, +, \cdot)$ dont la matrice dans la base canonique est la matrice de Vandermonde :

$$V_\omega = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \omega & \omega^2 & \dots & \omega^{n-1} \\ 1 & \omega^2 & \omega^4 & \dots & \omega^{2(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{n-1} & \omega^{2(n-1)} & \dots & \omega^{(n-1)^2} \end{pmatrix}$$

(où $\cdot$ est le produit sur $\mathbb{C}^n$ effectué composante par composante.)

Démonstration. Soient $f = (f_0, \dots, f_{n-1})$ et $g = (g_0, \dots, g_{n-1})$ deux vecteurs de $\mathbb{C}^n$.

— $\forall \lambda \in \mathbb{C}$,

$$\begin{aligned}
\mathrm{DFT}_\omega(\lambda f + g) &= \left(\sum_{k=0}^{n-1} \lambda f_k + g_k, \dots, \sum_{k=0}^{n-1} (\lambda f_k + g_k)\omega^{(n-1)k}\right) \\
&= \lambda\left(\sum_{k=0}^{n-1} f_k, \dots, \sum_{k=0}^{n-1} f_k \omega^{(n-1)k}\right) + \left(\sum_{k=0}^{n-1} g_k, \dots, \sum_{k=0}^{n-1} g_k \omega^{(n-1)k}\right) \\
&= \lambda\,\mathrm{DFT}_\omega(f) + \mathrm{DFT}_\omega(g)
\end{aligned}$$

DFT_ω est bien une application linéaire.

— Soit $h = f *_n g$. On note F, G et H les polynômes respectivement associés à f, g et h.
Soit $i \in [\![0, n-1]\!]$. Par la Proposition 6, on a $H = FG + Q(X^n - 1)$. Ainsi,

$$H(\omega^i) = (FG)(\omega^i) + Q(\omega^i)((\omega^i)^n - 1) = (FG)(\omega^i)$$

Or, le $(i+1)$-ième coefficient de $\mathrm{DFT}_\omega(f) \cdot \mathrm{DFT}_\omega(g)$ est

$$F(\omega^i)G(\omega^i) = (FG)(\omega^i) = H(\omega^i)$$

Donc $\mathrm{DFT}_\omega(f) \cdot \mathrm{DFT}_\omega(g) = \mathrm{DFT}_\omega(h)$, et ainsi, DFT_ω est bien un morphisme d'algèbres.

— Clairement,
$$\mathrm{DFT}_\omega(f_0,\dots,f_{n-1}) = V_\omega\,{}^t(f_0,\dots,f_{n-1})$$
donc la matrice dans la base canonique de DFT_ω est V_ω. Or, les ω^k sont distincts deux-à-deux, donc V_ω est inversible (car de déterminant non nul, en vertu de la formule de Vandermonde).

□

Proposition 8. L'inverse de DFT_ω est donné par $\frac{1}{n}\mathrm{DFT}_{\omega^{-1}}$.

Démonstration. Déjà, remarquons que si ω est une racine primitive n-ième de l'unité, alors ω^{-1} aussi :

— $(\omega^{-1})^n = (\omega^n)^{-1} = 1$.

— Et si on a $m < n$ tel que $(\omega^{-1})^m = (\omega^m)^{-1} = 1$, alors $\omega^m = 1$, ce qui est absurde.

Il suffit donc de montrer que $V_\omega V_{\omega^{-1}} = nI_n$. Soient $i,j \in [\![1,n]\!]$. En notant $c_{i,j}$ le coefficient à la i-ième ligne et à la j-ième colonne de $V_\omega V_{\omega^{-1}}$, on a :
$$c_{i,j} = \sum_{k=1}^{n} \omega^{(i-1)(k-1)}\omega^{(1-j)(k-1)} = \sum_{k=0}^{n-1} \omega^{(i-j)k} = \begin{cases} n & \text{si } i=j \\ \frac{1-\omega^{(i-j)n}}{1-\omega^{i-j}} \overset{\omega^n=1}{=} 0 & \text{sinon} \end{cases}$$

Ce qu'on voulait. □

3. Application à la multiplication de polynômes

Notre but ici va être de trouver un moyen de calculer la transformée de Fourier discrète d'un polynôme de manière efficace, puis d'en déduire un algorithme de multiplication de deux polynômes.

Proposition 9. Soit $n = 2^k$, soit ω une racine n-ième de l'unité et soit $F \in \mathbb{C}[x]$ de degré inférieur ou égal à n. On suppose qu'il existe F_0 et F_1 tels que $F = F_1X^{\frac{n}{2}} + F_0$ et on pose $R_0 = F_0 + F_1$ et $R_1 = F_0 - F_1$. Alors
$$\forall k \in [\![0, \frac{n}{2}]\!],\ F(\omega^{2k}) = R_0(\omega^{2k}) \text{ et } F(\omega^{2k+1}) = R_1(\omega^{2k+1})$$

Démonstration. Écrivons $F = F_1X^{\frac{n}{2}} + F_0$. On a donc
$$F - F_0 - F_1 = F_1(x^{\frac{n}{2}} - 1) \iff F = F_1(x^{\frac{n}{2}} - 1) + R_0$$

Soit $k \in [\![0, \frac{n}{2}]\!]$, on évalue en ω^{2k} :
$$F(\omega^{2k}) = F_1(\omega^{2k})(\omega^{nk} - 1) + R_0(\omega^{2k}) = R_0(\omega^{2k})$$

et la deuxième égalité s'obtient par un calcul similaire (en utilisant le fait que $\omega^{\frac{n}{2}} = -1$). □

Proposition 10. Si ω est une racine primitive n-ième de l'unité, alors ω^2 est une racine primitive $\frac{n}{2}$-ième de l'unité.

Démonstration. Clairement, ω^2 est une racine $\frac{n}{2}$-ième de l'unité. Maintenant, si $d \mid \frac{n}{2}$, alors

$$(\omega^2)^d = 1 \iff \omega^{2d} = 1 \iff 2d = n \iff d = \frac{n}{2}$$

□

On déduit de la Proposition 9 et de la Proposition 10 un algorithme récursif de calcul de DFT_ω qui a une complexité de $O(n\ln(n))$.

Algorithme 11.

```
# Renvoie les indices impairs d'une liste.
def odd_indices(l):
  return [l[2*k+1] for k in range(len(l)//2)]

# Fusionne deux listes de longueur égale en alternant les termes.
def alternate_merge(l1, l2):
  return [val for pair in zip(l1, l2) for val in pair]

# Calcule et renvoie les puissances successives de la racine primitive n-
    ième omega.
def primitive_root_powers(omega, n):
  return [power(omega, k) for k in range(n)]

# Cette fonction renvoie la transformée de Fourier discrète de F en omega.
    La liste l demandée est la liste des puissances de omega.
def fft(F, m, l):
  n = m + 1
  if n == 1:
    return [0] if F == 0 else [F.list()[0]]
  (F1, F0) = F.quo_rem(X^(n/2))
  R0 = F0+F1
  R1 = F0-F1
  l2 = odd_indices(l)
  return alternate_merge(fft(R0, n/2-1, l2), fft(R1.substitute(X=l[1]*X),
    n/2-1, l2))
```

Théorème 12. Soient F et G deux polynômes de degré strictement inférieur à $\frac{n}{2}$ dont on note f et g les vecteurs de $\mathbb{C}^n$ associés. Alors

$$FG = H$$

où H est le polynôme associé au vecteur $\frac{1}{n}\mathrm{DFT}_{\omega^{-1}}(\mathrm{DFT}_\omega(f)\cdot\mathrm{DFT}_\omega(g))$.

Démonstration. Comme $\deg(FG) < n$, on a $FG = H = \sum_{i=1}^{n} h_k X^k$ où $h = (h_0, \dots, h_{n-1}) = f *_n g$ par la Proposition 6. Par le Théorème 7, on a

$$\mathrm{DFT}_\omega(h) = \mathrm{DFT}_\omega(f *_n g) = \mathrm{DFT}_\omega(f) \cdot \mathrm{DFT}_\omega(g)$$

Et $\mathrm{DFT}_\omega^{-1} = \frac{1}{n}\mathrm{DFT}_{\omega^{-1}}$ par la Proposition 8. On obtient le résultat voulu. □

En utilisant l'algorithme écrit précédemment, on peut donc écrire un nouvel algorithme permettant de calculer le produit de deux polynômes de degré strictement inférieur à $\frac{n}{2}$ en $O(n\ln(n))$.

Algorithme 13.

```
# Multiplie deux polynômes de degré n.
def fast_polynomial_multiply(F, G, n, omega):
    l1 = primitive_root_powers(omega, n)
    l2 = primitive_root_powers(power(omega, n-1), n)
    prod = [fft(F, n-1, l1)[i] * fft(G, n-1, l1)[i] for i in range(n)]
    h = fft(sum(prod[k] * X^k for k in range(len(prod))), n-1, l2)
    return sum(1/n * h[k] * X^k for k in range(len(h)))
```

Remarque 14. On pourrait imaginer un algorithme calculant le produit de deux polynômes de degrés quelconques n et m sur le même modèle en considérant F et G comme des polynômes de degré 2^k où k est tel que $2^{(k-1)} \leq \max(n, m) \leq 2^k$. Il suffit ensuite de choisir ω racine primitive 2^k-ième de l'unité.

Bibliographie

Objectif agrégation **[BMP]**

Vincent Beck, Jérome Malick et Gabriel Peyré. *Objectif agrégation*. 2e éd. H&K, 22 août 2005. https://objectifagregation.github.io.

Mathématiques pour l'agrégation **[DAN]**

Jean-François Dantzer. *Mathématiques pour l'agrégation. Analyse et probabilités*. De Boeck Supérieur, 20 avr. 2021. https://www.deboecksuperieur.com/ouvrage/9782807332904-mathematiques-pour-l-agregation-analyse-et-probabilites.

Les maths en tête **[GOU20]**

Xavier Gourdon. *Les maths en tête. Analyse*. 3e éd. Ellipses, 21 avr. 2020. https://www.editions-ellipses.fr/accueil/10446-les-maths-en-tete-analyse-3e-edition-9782340038561.html.

Les maths en tête **[GOU21]**

Xavier Gourdon. *Les maths en tête. Algèbre et probabilités*. 3e éd. Ellipses, 13 juill. 2021. https://www.editions-ellipses.fr/accueil/13722-25266-les-maths-en-tete-algebre-et-probabilites-3e-edition-9782340056763.html.

Algèbre et calcul formel **[FFN]**

Loïc Foissy Odile Fleury et Alain Ninet. *Algèbre et calcul formel. Agrégation de Mathématiques Option C*. 2e éd. Ellipses, 9 mai 2023. https://www.editions-ellipses.fr/accueil/14799-algebre-et-calcul-formel-agregation-de-mathematiques-option-c-2e-edition-9782340078567.html.

L'algèbre discrète de la transformée de Fourier **[PEY]**

Gabriel Peyré. *L'algèbre discrète de la transformée de Fourier. Niveau M1*. Ellipses, 15 jan. 2004. https://adtf-livre.github.io.