4 Corps finis, applications en cryptographie et en théorie des codes correcteurs d'erreur

4.1 Introduction, premières propriétés

Un corps fini est... un corps fini (un corps dont l'ensemble sous-jacent est fini). On va élucider un peu la structure générale des corps finis, et expliquer comment on peut calculer concrètement dans les corps finis. On sait déjà que pour tout nombre p premier, l'anneau quotient $\mathbf{Z}/p\mathbf{Z}$, noté aussi $\mathbf{F}_p$, est un corps fini.

Proposition 1. *Soit* $\mathbf{K}$ *un corps fini et* $P \in \mathbf{K}[X]$ *un polynôme irréductible. Alors l'anneau quotient* $\mathbf{L} := \mathbf{K}[X]/\langle P\rangle$ *est un corps fini, de cardinal* $\mathrm{card}(K)^{\deg(P)}$.

Démonstration. L'anneau $\mathbf{L}$ est un corps d'après la proposition 30 et le théorème 58 du chapitre 2.

Par ailleurs, d'après le théorème 6 du chapitre 2, $\mathbf{L}$ est muni d'une structure naturelle de $\mathbf{K}$-espace vectoriel de dimension finie égale à $\deg(P)$. Un tel $\mathbf{K}$-espace vectoriel est en particulier en bijection avec $\mathbf{K}^{\deg(P)}$. Or ce dernier ensemble est fini, de cardinal $\mathrm{card}(K)^{\deg(P)}$. □

Remarque. En prenant $\mathbf{K} = \mathbf{F}_2$ et $P = X^2 + X + [1]_2$ on obtient ainsi un corps à quatre éléments. Un tel corps n'est donc isomorphe à aucun des corps $\mathbf{Z}/p\mathbf{Z}$ (p premier).

Proposition 2. *Tout anneau intègre fini est un corps fini.*

Démonstration. cf. l'exercice 1.11 ; indication : soit $a \in A \setminus \{0\}$; comme A est intègre, l'application $A \to A, \quad x \mapsto ax$ est injective, or A est fini, donc cette application est... □

4.2 Caractéristique et cardinal d'un corps fini

Théorème 3. *Soit* $\mathbf{K}$ *un corps fini. Alors la caractéristique de* $\mathbf{K}$ *est un nombre premier* p. *Il existe en particulier une unique structure de* $\mathbf{F}_p$*-algèbre sur* $\mathbf{K}$, *qui fait de* $\mathbf{K}$ *un* $\mathbf{F}_p$*-espace vectoriel de dimension finie. Si on note* n *cette dimension, le cardinal de* $\mathbf{K}$ *est* p^n.

En particulier le cardinal d'un corps fini est une puissance d'un nombre premier.

Démonstration. On sait que la caractéristique d'un corps est 0 ou un nombre premier (corollaire 60 du chapitre 2). Mais un corps de caractéristique 0 contient $\mathbf{Z}$, donc est infini. Donc $\mathbf{K}$ est de caractéristique un nombre premier p. L'unique structure de $\mathbf{F}_p$-algèbre sur $\mathbf{K}$ est alors donnée par la factorisation du morphisme $\mathbf{Z} \to \mathbf{K}$ par $\mathbf{Z}/p\mathbf{Z} \to \mathbf{K}$. En tant que $\mathbf{F}_p$-algèbre, $\mathbf{K}$ hérite d'une structure de $\mathbf{F}_p$-espace vectoriel (*cf.* la section 2.10 du chapitre 2). Comme $\mathbf{K}$ est fini, il admet une famille génératrice finie comme $\mathbf{F}_p$-espace vectoriel (prendre pour famille génératrice l'ensemble $\mathbf{K}$ lui-même !). C'est donc, par définition, un $\mathbf{F}_p$-espace vectoriel de dimension finie. Si n est sa dimension, on sait que $\mathbf{K}$ est isomorphe comme $\mathbf{F}_p$-espace vectoriel à $\mathbf{F}_p^n$. En particulier les ensembles $\mathbf{K}$ et $\mathbf{F}_p^n$ sont en bijection. Or $\mathbf{F}_p^n$ a pour cardinal p^n, ce qui conclut. □

En fait, l'un des résultat fondamentaux de la théorie des corps finis est le suifant : étant donnés un nombre premier p et un entier strictement positif n, il existe, à isomorphisme près, un unique corps fini de cardinal p^n. Nous allons démontrer ceci, et expliquer comment dans la pratique on peut décrire explicitement « le » corps fini de cardinal p^n.

4.3 Un exemple de calcul dans un corps fini qui n'est pas un quotient de Z

Soit p un nombre premier et n un entier strictement positif. Pour construire un corps fini de cardinal p^n et calculer explicitement dans ce corps, il « suffit » d'exhiber un polynôme irréductible de degré n à coefficients dans $\mathbf{F}_p$. On verra ci-dessous qu'un tel polynôme existe toujours. Pour en exhiber un, on peut procéder par énumération exhaustive des polynômes irréductibles de degré donné, ce qui reste relativement efficace si p et n ne sont pas trop grands. On peut aussi étudier les facteurs irréductibles de $X^{p^n} - X$ (*cf.* le théorème 13 ci-dessous pour la justification théorique) ; il se trouve qu'il existe des méthodes efficaces pour déterminer la factorisation d'un polynôme sur un corps fini, sur lesquelles nous reviendrons au dernier chapitre.

Remarquons que si p est un nombre premier impair et $a \in \mathbf{F}_p$ n'est pas un carré dans $\mathbf{F}_p$, un corps à p^2 élément est donné par $\mathbf{F}_p[X]/\langle X^2 - a\rangle$. En particulier, si p est congru à 3 modulo 4, $\mathbf{F}_p[X]/\langle X^2 + [1]_p\rangle$ est un corps à p^2 élément.

Détaillons à présent le calcul des tables d'addition et de multiplication du corps fini de cardinal non premier le plus petit possible. qui soit, à savoir le corps à quatre éléments.

Avertissement : pour alléger l'écriture, on note désormais, pour tout $n \in \mathbf{Z}$, n en lieu et place de $[n]_2$. Comme on l'a déjà évoqué, c'est un abus de notation pratique mais potentiellement dangereux.

Le polynôme $X^2 + X + 1 \in \mathbf{F}_2[X]$ est de degré 2 et n'a pas de racines dans $\mathbf{F}_2$ (on calcule ses valeurs en 0 et 1), il est donc irréductible sur $\mathbf{F}_2$. Soit $\mathbf{K} \overset{\text{déf}}{=} \mathbf{F}_2[X]/\langle X^2 + X + 1\rangle$, $\pi\colon \mathbf{F}_2[X] \to \mathbf{K}$ le morphisme quotient et $\alpha := \pi(X)$. En particulier $\mathbf{K}$ est un $\mathbf{F}_2$-espace vectoriel de base $\{1, \alpha\}$. L'ensemble des éléments de $\mathbf{K}$ est donc

$$\{a + b\,\alpha, \quad (a, b) \in \mathbf{F}_2^2\} = \{0, 1, \alpha, 1 + \alpha\}.$$

On obtient aussitôt la table d'addition :

$+$	0	1	α	$1+\alpha$
0	0	1	α	$1+\alpha$
1	1	0	$1+\alpha$	α
α	α	$1+\alpha$	0	1
$1+\alpha$	$1+\alpha$	α	1	0

Pour la table de multiplication, calculons les coordonnées de α^2 dans la base $\{1, \alpha\}$ en remarquant que $0 = \pi(X^2+X+1) = \alpha^2+\alpha+1$, d'où $\alpha^2 = -\alpha-1$, soit finalement $\alpha^2 = \alpha+1$ car le corps des coefficients est $\mathbf{F}_2$ (avec notre notation, on a $-1 = 1$). On en déduit alors le calcul de $\alpha.(1+\alpha) = \alpha + \alpha^2 = 1 + 2\,\alpha = 1$ et de $(1+\alpha)^2 = 1 + 2\,\alpha + \alpha^2 = 1 + 1 + \alpha = \alpha$.

$\times$	0	1	α	$1+\alpha$
0	0	0	0	0
1	0	1	α	$1+\alpha$
α	0	α	$1+\alpha$	1
$1+\alpha$	0	$1+\alpha$	1	α

On verra un peu plus tard que le groupe multiplicatif $\mathbf{K}^\times$ est cyclique d'ordre 3, il est donc engendré par n'importe quel élément différent de 1. De fait on vérifie facilement que α et $1+\alpha$ sont des éléments d'ordre 3 de $\mathbf{K}^\times$.

4.4 Le morphisme de Frobenius

Théorème 4. *Soit p un nombre premier et A un anneau de caractéristique p. Alors l'application $A \to A$, $F_A \colon x \mapsto x^p$ est un morphisme d'anneaux.*

En particulier si $\mathbf{K}$ est un corps fini, $F_{\mathbf{K}}$ est un isomorphisme de corps.

Démonstration. (esquisse) La compatibilité à la multiplication se vérifie aussitôt, de même que la relation $F_A(1_A) = 1_A$. Le point délicat est la compatibilité à l'addition. Elle se déduit de la formule du binôme de Newton (proposition 3 du chapitre 2) et du résultat élémentaire d'arithmétique suivant : comme p est un nombre premier, pour tout $1 \leqslant n \leqslant p-1$, p divise $\binom{p}{n}$; en particulier $\binom{p}{n} \cdot a = 0$ pour tout $a \in A$.

Soit $\mathbf{K}$ un corps fini de caractérisitique p. Le noyau du morphisme $F_{\mathbf{K}}$, qui est un idéal de $\mathbf{K}$, est soit $\{0\}$, soit $\mathbf{K}$ (proposition 57 du chapitre 2). Ça ne peut pas être $\mathbf{K}$, car $F_{\mathbf{K}}(1_{\mathbf{K}}) = 1_{\mathbf{K}} \neq 0$; donc $F_{\mathbf{K}}$ est injectif (en fait cet argument montre que si $\mathbf{K}$ est un corps quelconque et A est un anneau non nul, tout élément de $\mathrm{Hom}_{\text{anneaux}}(\mathbf{K}, A)$ est automatiquement injectif). Comme $F_{\mathbf{K}}$ est une application de l'ensemble fini $\mathbf{K}$ dans lui-même, $F_{\mathbf{K}}$ est alors surjectif. Ainsi $F_{\mathbf{K}}$ est un morphisme d'anneaux bijectif de $\mathbf{K}$ sur lui-même, ce qui conclut. □

4.5 Le groupe des éléments inversibles d'un corps fini est cyclique

On va démontrer le résultat énoncé dans le titre de la section.

Commençons par quelques notations et rappels.

Pour tout entier strictement positif d, on note $\varphi(d)$ le cardinal de $(\mathbf{Z}/d\mathbf{Z})^\times$. D'après le théorème 1 du chapitre 3, $\varphi(d)$ est aussi le cardinal de l'ensemble des entiers e tels que $1 \leqslant e \leqslant d$ et e et d sont premiers entre eux.

Soit G un groupe et d un entier strictement positif. Soit $\Delta_d(G) := \{x \in G, \quad x^d = e\}$, $\Omega_d(G) \subset \Delta_d(G)$ l'ensemble des éléments de G d'ordre d et $\omega_d(G) := \mathrm{card}(\Omega_d(G))$.

En particulier, d'après le théorème de Lagrange, si G est fini d'ordre n et si d est un entier positif qui ne divise pas n, on a $\omega_d(G) = 0$. Ainsi $\{\Omega_d(G)\}_{d \text{ diviseur positif de } n}$ est une partition de G, et on en déduit la relation

$$\sum_{d \text{ diviseur positif de } n} \omega_d(G) = n. \tag{4.1}$$

Par ailleurs, rappelons que l'on montre que si G est cyclique d'ordre n et si d est un diviseur positif de n, on a $\mathrm{card}(\Delta_d(G)) = d$ et $\omega_d(G) = \varphi(d)$. Comme il existe des groupes cycliques d'ordre n (par exemple $G = \mathbf{Z}/n\mathbf{Z}$), (4.1) montre la relation

$$\sum_{d \text{ diviseur positif de } n} \varphi(d) = n. \tag{4.2}$$

On démontre d'abord un critère général de cyclicité.

Théorème 5. *Soit n un entier strictement positif et G un groupe fini d'ordre n. Les assertions suivantes sont équivalentes :*

1. *G est cyclique ;*
2. *pour tout diviseur positif d de n, on a $\mathrm{card}(\Delta_d(G)) \leqslant d$;*
3. *pour tout diviseur positif d de n, $\omega_d(G) \leqslant \varphi(d)$.*

Démonstration. (1)⇒(2) : Les rappels ci-dessus montrent qu'on peut même conclure que $\mathrm{card}(\Delta_d(G)) = d$.

(3)⇒(1) : L'hypothèse permet d'écrire

$$\sum_{d \text{ diviseur positif de } n} \omega_d(G) \leqslant \sum_{d \text{ diviseur positif de } n} \varphi(d).$$

D'après (4.1) et (4.2), cette inégalité est une égalité. Donc nécessairement pour *tout* diviseur positif d de n on doit avoir $\omega_d(G) = \varphi(d)$. En particulier $\omega_n(G) = \varphi(n)$ est strictement positif. Donc G contient un élément d'ordre n et est donc cyclique.

(2)⇒ (3) : Soit d un diviseur positif de n. Si $\omega_d(G) = 0$, la majoration est évidemment vérifiée. Si $\omega_d(G) > 0$, il existe un élément x de G d'ordre d. Prenons un tel élément x et soit H le sous-groupe engendré par x. C'est un groupe cyclique d'ordre d. En particulier tout élément de H a un ordre qui divise d, et on a donc $H \subset \Delta_d(G)$. L'hypothèse $\mathrm{card}(\Delta_d(G)) \leqslant d$ assure donc que $H = \Delta_d(G)$. Ainsi on a $\Omega_d(G) = \Omega_d(H)$. Donc $\omega_d(G) = \omega_d(H) = \varphi(d)$. □

On applique ce critère au cas du groupe des inversibles d'un corps fini.

Théorème 6. *Soit* $\mathbf{K}$ *un corps fini. Alors le groupe* $\mathbf{K}^\times$ *est un groupe cyclique.*

Démonstration. On veut appliquer le théorème précédent avec $G = \mathbf{K}^\times$. Remarquons que pour tout diviseur positif d de $\mathrm{card}(G)$, $\Delta_d(G)$ est l'ensemble des racines dans $\mathbf{K}$ du polynôme $X^d - 1_{\mathbf{K}}$. Comme $\mathbf{K}$, en tant que corps, est un anneau intègre, d'après le corollaire 43 du chapitre 2, on a $\mathrm{card}(\Delta_d(G)) \leqslant d$. Ainsi le théorème précédent s'applique et $\mathbf{K}^\times$ est bien un groupe cyclique. □

Remarque. L'exercice 3.16 propose une autre démonstration du théorème précédent, basée sur le théorème de structure des groupes abéliens finis. Le corollaire 43 du chapitre 2 reste un argument clef.

Voici une conséquence importante du théorème 6.

Théorème 7. *Soit* $\mathbf{K}$ *un corps fini et* p *sa caractéristique. Alors il existe un élément* $P \in \mathbf{F}_p[X]$ *irréductible tel que* $\mathbf{K}$ *est isomorphe à l'anneau quotient* $\mathbf{F}_p[X]/\langle P\rangle$.

Démonstration. Rappelons que $\mathbf{K}$ est naturellement muni d'une structure de $\mathbf{F}_p$-algèbre. Soit x un générateur du groupe cycliqe $\mathbf{K}^*$. Soit $\varphi\colon \mathbf{F}_p[X] \to \mathbf{K}$ l'unique morphisme de $\mathbf{F}_p$-algèbre qui envoie X sur x. Par définition de x, on a $\mathbf{K} = \{0\} \cup \{x^n\}_{n\in\mathbf{N}}$, et ainsi φ est surjectif. Soit $P \in \mathbf{F}_p[X]$ un générateur de son noyau. Par le théorème de factorisation φ induit un isomorphisme $\mathbf{F}_p[X]/\langle P\rangle \cong \mathbf{K}$. Comme $\mathbf{K}$ est un corps, P est nécessairement irréductible. □

4.6 Interlude cryptographique : Diffie-Hellman, El Gamal

Le fait que le groupe multiplicatif d'un corps fini soit cyclique a des applications à certains protocoles cryptographiques basés sur les groupes cycliques.

4.6.1 Complexité de certains calculs modulaires

Cette section peut être réservée à une seconde lecture.

Qui dit étude de protocoles cryptographiques dit nécessairement étude de la complexité des algorithmes mis en jeu. Un algorithme de chiffrement et/ou de déchiffrement qui fonctionne « sur le papier » mais qui dans la pratique prendrait des années de calculs sur les machines actuellement disponibles [10] n'a évidemment aucun intérêt pour les applications cryptographiques. A contrario, il est crucial de s'assurer que les algorithmes susceptibles de « casser » les protocoles cryptographiques mis en jeu sont eux inutilisables à cause du temps de calcul rédhibitoire que nécessiteraient leur application effective (il est en fait souvent très difficile de s'en assurer *stricto sensu*).

Ce n'est absolument pas le lieu ici de faire un cours général sur la complexité algorithmique. On va juste expliciter quelques ordres de grandeur permettant de mieux appréhender l'intérêt des protocoles présentés ci-dessous. Ces protocoles mettent en jeu des calculs modulo p, où p est un nombre premier assez grand, et la connaissance d'un générateur explicite de $\mathbf{F}_p^\times$. Assez grand signifiera dans la pratique que le nombre N de chiffre de p est de l'ordre d'une centaine de chiffres. Il est à noter que p est alors largement supérieur au nombre estimé d'atomes de l'univers... *Nous passons ici sous silence les méthodes permettant de construire de manière efficace de tels nombres premiers p et un générateur explicite de $\mathbf{F}_p^\times$.* Il est à noter que la démonstration donnée ci-dessus du fait que le groupe multiplicatif d'un corps fini est cyclique ne donne aucun moyen effectif d'exhiber un générateur. Les autres démonstrations connues ne font pas mieux de ce point de vue.

Étant alors donné un élément de $(\mathbf{Z}/p\mathbf{Z})^\times$, représenté sous la forme $[n]_p$, où n est un entier compris entre 1 et $p-1$, et un exposant a qui est un entier compris entre 1 et $p-2$, notre but est d'estimer le coût du calcul de $[n]_p^a$ (sous la forme $[m]_p$ où m est un entier compris entre 1 et $p-1$). On va voir que même si p (et donc possiblement n et a) représente un entier inimaginablement gigantesque, ce coût est lui-même extrêmement raisonnable. De manière formelle, il est logarithmique en la taille de p, ce qui traduit une grande efficacité même quand p devient très grand ; la fonction logarithme tend vers l'infini mais à une vitesse *phénoménalement* lente.

Le coût va être estimé en termes du nombre d'opérations élémentaires nécessaires mis en jeu, où les « opérations élémentaires » sont ici l'addition ou la multiplication de deux chiffres (compris entre 0 et 9 si on représente les entiers en décimal, mais évidemment les machines elles calculent en binaire).

Commençons par estimer le coût de la multiplication de deux entiers modulo p. On suppose donnés des entiers $0 \leqslant n \leqslant p-1$ et $0 \leqslant m \leqslant p-1$ et on veut calculer $[nm]_p$. On calcule donc le produit de m par n et on réduit le résultat modulo p, c'est à dire on calcule le reste de la division euclidienne de ab par p.

Sachant que le nombre de chiffres de m et n est majoré par N, et en se rappelant

10. On ne parlera pas ici, en particulier par manque de compétence, des aspects prometteurs du développement récent du calcul quantique.

l'algorithme basique de multiplication appris à l'école primaire, on constate que le coût de la multiplication de m par n est majoré par quelque chose de l'ordre de N^2 opérations. Si N de l'ordre de 100, c'est plus que raisonnable.

Il s'agit maintenant d'estimer le coût de la division euclidienne du produit nm par p. On se rappelle là encore la méthode enseignée à l'école primaire. On va abaisser au pire N fois une unité. À la première étape et après chaque abaissement, il faudra effectuer la division euclidienne par p d'un nombre au plus égal à $10p-1$: au pire 9 soustractions d'un entier de l'ordre de N chiffres par un entier de N chiffres, chaque soustraction coûtant de l'odre de N opérations élémentaires. Chaque étape coûte donc de l'ordre de N opérations élementaire. Au final le coût de la division euclidienne est de l'ordre de N^2 opérations.

La multiplication modulaire de deux entiers modulo p a donc un coût de l'ordre de N^2 opérations élémentaires. Encore une fois, c'est ridiculement bas au vu de l'ordre de grandeur de p lui-même.

Nous allons enfin pouvoir estimer la complexité de l'exponentiation modulaire. Étant donnés un entier n et un entier positif a, on veut calculer $[n]_p^a$. Naïvement, cela se décompose en a multiplications modulo p, et comme a peut être de l'ordre de grandeur de N, cela représente un coût de l'ordre de $N^2 10^N$ opérations, ce qui pour le coup représente un changement d'ordre de grandeur radical par rapport aux complexités précédentes (pour mémoire : 10^N est bien supérieur au nombre d'atomes de l'univers).

Mais on peut faire heureusement beaucoup mieux avec l'exponentiation binaire. Décomposons a en binaire :

$$a = \sum_{i=0}^{M} \varepsilon_i 2^i, \quad \varepsilon_i \in \{0,1\}$$

Si g est un élément de n'importe quel groupe multiplicatif, on peut alors écrire

$$g^a = \prod_{i=0,\ \varepsilon_i=1}^{M} g^{2^i}$$

On intialise r à 1 ou g selon que ε_0 vaut 0 ou 1. On calcule successivement tous les g^{2^i} par élévations au carré. Parallèlement, si $\varepsilon_i = 1$, on remplace r par $r.g^{2^i}$. On a donc effectué M élevations au carrés et au pire $M+1$ multiplications dans le groupe G. Ainsi le calcul de g^a nécessite de l'ordre de M^2 multiplications dans le groupe G. Par ailleurs M est le nombre de chiffres de a en écriture binaire, qui est de l'ordre de grandeur du nombre de chiffres de a en décimal (en fait dans la pratique les machines effectuent tous les calculs en binaire ; ça ne change rien aux ordres de grandeur discutés ici). Ainsi en revenant à notre situation initiale, l'exponentiation modulo p nécessitera de l'ordre de $N^2 \times N^2 = N^4$ opérations élémentaires. Toujours aussi raisonnable et ridiculement bas par rapport à l'ordre de grandeur de p lui-même.

Si l'on souhaite par contre calculer successivement *toutes* les puissances $[n]_p^3$, $[n]_p^4$ jusqu'à $[n]_p^a$ (et l'on verra ci-dessous pourquoi on pourrait être amené à vouloir le faire) on revient

a priori à une décomposition en a multiplications modulo p et à un coût prohibitif d'un ordre de grandeur de $N^2 10^N$ opérations.

Il est utile de noter qu'un autre type de calcul modulaire rapide est le calcul d'un inverse modulo p. Ceci revient, étant donné un entier n compris entre 1 et $p-1$, à calculer une relation de Bezout pour n et p. En utilisant l'algorithme d'Euclide, on peut montrer que le coût maximal est de l'ordre de grandeur de N^2.

4.6.2 L'échange de clés de Diffie-Hellman

Alice et Bob veulent s'échanger un secret commun via un canal de communication à distance mais craignent qu'Ève ne puisse écouter la communication. Pour comprendre l'intérêt de ce qui va suivre, il faut insister sur le fait qu'on est en outre dans une situation où la nature exacte du secret n'importe pas. Ce qui fera la valeur du secret est uniquement le fait qu'Alice et Bob seront les seuls à le connaître. Dans la pratique, le secret peut par exemple être une clef pour des échanges ultérieurs basés sur un protocole de cryptographie à clef secrète.

Le secret est modélisé par un élément d'un groupe cyclique G (noté ici multiplicativement), dont on connaît par ailleurs un générateur g. Dans la pratique G a un grand cardinal, et peut se représenter concrètement.

L'échange du secret se déroule ainsi.

1. Alice choisit G et g, ainsi qu'un entier a choisi au hasard, et calcule g^a (dans la pratique un tel calcul est très rapide même si G et a sont « grand ») Elle transmet à Bob « en clair » G, g et g^a. Par contre, elle tient secrète la valeur de l'entier a.
2. Bob, ayant reçu ces informations, choisit à son tour un entier b au hasard qu'il tient secret, Il calcule et envoie « en clair » la valeur de g^b à Alice.

Les communications en clair sont susceptibles d'être interceptées par Ève. Au terme de l'échange ci-dessus, les informations connues par les différents protagonistes sont les suivantes :

1. Alice connaît G, g, a, g^b ;
2. Bob connaît G, g, b, g^a ;
3. Ève connaît G, g, g^a, g^b.

Le secret partagé par Alice et Bob sera l'élément g^{ab}. Chacun possède les informations pour le calculer facilement : Alice calcule g^b à la puissance a et Bob g^a à la puissance b.

Pourquoi ça marche ? Rappelons que même si G et l'exposant a sont « grands », il est très rapide d'élever un élément de G à la puissance a (*cf.* la section précédente).

Par contre, même en connaissant g et g^a, comme Ève, il est très difficile, **en tout cas on le croit**, de déterminer a : c'est ce qu'on appelle le *problème du logarithem discret*. Plus généralement, **on croit** qu'il est difficile, connaissant g, g^a et g^b, de calculer g^{ab} (*problème de Diffie-Hellman*).

Insistons sur le fait que « difficile » doit se comprendre en termes de la complexité algorithmique. Bien sûr, on peut toujours, connaissant g et g^a, imaginer déterminer a en calculant les puissances successives g^2, g^3,... jusqu'à trouver un puissance adéquate. Mais c'est beaucoup trop long dans la pratique (*cf.* la section précédente). Et on ne connaît aucun algorithme général de complexité raisonnable permettant de résoudre le logarithme discret, et on croit qu'il n'en existe pas (mais on ne sait pas le démontrer).

Un autre aspect très important : dans la pratique la difficulté à résoudre le problème du log discret n'a de sens que vis-à-vis d'une certaine représentation du groupe cyclique G.

Ainsi si on représente G comme le groupe *additif* $\mathbf{Z}/n\mathbf{Z}$, même avec n très grand le problème du log discret est facile : il s'agit, connaissant un générateur $[m]_n$ (en d'autres termes un entier m premier à n) et $[am]_n$ de retrouver a : on calcule un inverse r de m modulo n et on calcule $[r]_n[am]_n = [a]_n$ (tout cela est très rapide même si n est très grand, *cf.* la section précédente).

Par contre si G est le groupe cyclique $(\mathbf{Z}/p\mathbf{Z})^\times$, avec p assez grand (voire le groupe multiplicatif d'un corps fini plus général), on pense (plus précisément « on croit », « on a foi en le fait » ...) que les problèmes du log discret et de Diffie Hellman sont difficiles, et donc que le protocole d'échange de secret présenté ci-dessus est sûr.

Noter que connaissant un générateur $[n]_p$ de $(\mathbf{Z}/p\mathbf{Z})^\times$ on peut construire de manière effective un morphisme de groupes

$$\psi\colon (\mathbf{Z}/(p-1)\mathbf{Z}, +) \xrightarrow{\sim} ((\mathbf{Z}/p\mathbf{Z})^\times, \times)$$

qui soit un isomorphisme : à $[m]_{p-1}$ on associe $[n^m]_p$. De manière effective signifie ici : étant donné un élément explicite de $\mathbf{Z}/(p-1)\mathbf{Z}$, on peut calculer son image par φ en un temps raisonnable. Mais ça ne veut pas dire que *l'application inverse* de ψ puisse être construite de manière effective (c'est justement le problème du logarithme discret). On retrouve ici un cas particulier d'un concept fréquent en cryptographie : l'utilisation d'une applications φ bijective et facile à calculer dont l'inverse n'est pas facile à calculer

Moralement : les représentations des groupes cycliques d'ordre n pour lesquels les problèmes du log discret et apparentés sont difficiles sont celles pour lesquels $\mathbf{Z}/n\mathbf{Z}$ a été suffisamment « mélangé ».

4.6.3 Le système de cryptographie à clef publique El Gamal

La situation ressemble à la précédente mais avec une différence de taille : cette fois, Bob veut transmettre à Alice un secret bien déterminé, un message par exemple. Ève est toujours susceptible d'écouter la communication.

Les choses se déroulent alors ainsi :

1. Alice choisit un groupe cyclique G noté multiplicativement, et un générateur g de G. Elle choisit un entier a (dans la pratique, au hasard et assez grand) qu'elle tient

soigneusement secret : il constitue sa clef privée. Elle calcule g^a et rend public (G, g, g^a) (sa clef publique).

2. Bob veut transmettre un secret à Alice, modélisé par un élément h du groupe G. Il choisit un entier b (dans la pratique, au hasard et assez grand), calcule $h.(g^a)^b$ et g^b et envoie le résultat à Alice.
3. Alice, connaissant a et g^b, calcule facilement g^{ab} en élevant g^b à la puissance a, puis l'inverse de g^{ab} en l'élevant à la puissance card$G - 1$, et en déduit aussitôt h à partir de $h.g^{ab}$.

Ève, même en connaissant G, g, $h.g^{ab}$, g^a et g^b, ne peut pas trouver facilement g^{ab} et donc h si le problème de Diffie Hellman est difficile.

4.7 Deux corps finis de même cardinal sont isomorphes

Le lemme qui suit aurait pu figurer plus tôt dans le chapitre.

Lemme 8. *Soit* $\mathbf{K}$ *un corps fini de cardinal* N *et* x *un élément de* $\mathbf{K}$*. Alors on a* $x^N = x$*.*

Démonstration. C'est immédiat si $x = 0_{\mathbf{K}}$. Sinon, x est un élément du groupe $\mathbf{K}^\times$ qui est de cardinal $\text{card}(\mathbf{K}) - 1 = N - 1$. D'après le théorème de Lagrange, on a $x^{N-1} = 1_K$. En multipliant cette égalité par x, on obtient le résultat voulu. □

Lemme 9. *Soit* p *un nombre premier et* $P \in \mathbf{F}_p[X]$ *un polynôme irréductible de degré* n*. Alors* P *divise* $X^{p^n} - X$*.*

Démonstration. Soit $\mathbf{K}$ le corps $\mathbf{F}_p[X]/\langle P\rangle$ et x l'image de X dans $\mathbf{K}$. D'après la proposition 11 du chapitre 3, le polynôme minimal de x sur $\mathbf{F}_p$ est P. D'après la proposition 1, $\mathbf{K}$ est de cardinal p^n. D'après le lemme 8, on a $x^{p^n} = x$, en d'autres termes x est racine du polynôme $X^{p^n} - X$. Comme le polynôme minimal de x sur $\mathbf{F}_p$ est P, on obtient bien que P divise $X^{p^n} - X$. □

Théorème 10. *Soit* p *un nombre premier et* n *un entier strictement positif. Soit* $\mathbf{K}$ *et* $\mathbf{L}$ *deux corps finis de cardinal* p^n*. Alors les corps* $\mathbf{K}$ *et* $\mathbf{L}$ *sont isomorphes.*

Démonstration. D'après le théorème 7, il existe $P \in \mathbf{F}_p[X]$ irréductibles de degré n tel que le corps $\mathbf{K}$ est isomorphe à $\mathbf{F}_p[X]/\langle P\rangle$. Il s'agit de montrer que ce dernier corps est isomorphe à $\mathbf{L}$.

Notons que tout élément de $\mathrm{Hom}_{\mathbf{F}_p-\mathrm{Alg}}(\mathbf{F}_p[X]/\langle P\rangle, \mathbf{L})$ est automatiquement un isomorphisme. En effet un élément de ce dernier ensemble est automatiquement injectif car $\mathbf{K}$ est un corps et $\mathbf{L}$ n'est pas l'anneau nul, donc il est bijectif pour des raisons de cardinalité.

Par ailleurs, d'après le théorème 8 du chapitre 3, l'ensemble $\mathrm{Hom}_{\mathbf{F}_p-\mathrm{Alg}}(\mathbf{F}_p[X]/\langle P\rangle, \mathbf{L})$ est en bijection avec l'ensemble des racines du polynôme P dans $\mathbf{L}$. Il suffit donc de montrer que ce dernier ensemble est non vide.

D'après le lemme 9, il existe $R \in \mathbf{F}_p[X]$ tel que

$$X^{p^n} - X = PR$$

On a en particulier $\deg(R) < p^n$. Comme $\mathrm{card}(\mathbf{L}) = p^n$, ceci montre qu'il existe $y \in \mathbf{L}$ tel que $R(y) \neq 0$. Comme $y^{p^n} = y$ (d'après le lemme 8) et $\mathbf{L}$ est intègre, on a donc $P(y) = 0$. Ceci conclut la démonstration.

□

Remarque. Il peut être utile de rappeler comment à partir de l'élément y considéré dans la démonstration on construit un morphisme de $\mathbf{F}_p$-algèbres de $\mathbf{F}_p[X]/\langle P\rangle$ vers $\mathbf{L}$: on considère l'unique morphisme de $\mathbf{F}_p$-algèbre de $\mathbf{F}_p[X]$ vers $\mathbf{L}$ qui envoie X sur y. Ce morphisme a pour noyau $\langle P\rangle$ et induit donc le morphisme cherché.

Remarque. Considérons deux corps finis de même cardinal. Le théorème précédent montre qu'il existe alors un isomorphisme de l'un sur l'autre. Il est important de noter qu'un tel isomorphisme n'est pas unique en général.

On peut même être plus précis. Reprenons les notations utilisées précédemment. Tout d'abord, rappelons que d'après le théorème 2 du chapitre 3, tout anneau possède au plus une structure de $\mathbf{F}_p$-algèbre. En particulier un morphisme d'anneaux d'une $\mathbf{F}_p$-algèbre vers une autre est automatiquement un morphisme de $\mathbf{F}_p$-algèbres.

Ainsi d'après la démonstration ci-dessus, l'ensemble des isomorphismes de $\mathbf{K}$ sur $\mathbf{L}$ s'identifie à l'ensemble des racines du polynôme P dans $\mathbf{L}$. On va montrer que cet ensemble est exactement de cardinal $\deg(P) = n$. Ainsi il y a exactement n isomorphismes d'un corps de cardinal p^n sur un autre. Du point de vue de la terminologie de la théorie de Galois, ceci montre qu'un corps de cardinal p^n est une extension galoisienne de $\mathbf{F}_p$.

D'après le lemme 8, tout élément de $\mathbf{L}$ est racine du polynôme $X^{p^n} - X$. Comme ce dernier polynôme est de degré p^n égal au cardinal de $\mathbf{L}$, cela signifie que sa décomposition en facteurs irréductibles dans $\mathbf{L}[X]$ s'écrit

$$X^{p^n} - X = \prod_{y \in \mathbf{L}} X - y$$

Comme P est un diviseur de $X^{p^n} - X$, la décomposition en facteurs irréductibles de P dans $\mathbf{L}[X]$ est un produit de polynômes de degré 1 deux à deux distincts. Donc P a exactement $\deg(P)$ racines dans $\mathbf{L}$.

4.8 Toute puissance d'un nombre premier est le cardinal d'un corps fini

Nous avons vu que d'une part, tout corps fini avait pour cardinal une puissance d'un nombre premier, et que d'autre part, deux corps finis de même cardinal étaient nécessairement isomorphes. Nous allons compléter ce résultat de la façon suivante :

Théorème 11. *Soit p un nombre premier et n un entier strictement positif. À isomorphisme près, il existe un unique corps fini de cardinal p^n.*

Vu le théorème 10, il suffit de montrer qu'il existe un corps fini de cardinal p^n. Nous allons d'abord en donner une démonstration simple mais conditionnée à un résultat que nous admettrons.

Théorème 12. *Soit p un nombre premier. Alors il existe un corps algébriquement clos $\mathbf{L}$ qui contient $\mathbf{F}_p$.*

Démonstration. Admettant le théorème 12, démontrons le théorème 11. Soit p un nombre premier et n un entier strictement positif. Soit $\mathbf{L}$ un corps algébriquement clos contenant $\mathbf{F}_p$. Soit

$$\mathbf{K} = \{x \in \mathbf{L}, x^{p^n} - x = 0\}.$$

En d'autres termes, $\mathbf{K}$ est l'ensemble des racines dans $\mathbf{L}$ du polynôme $P := X^{p^n} - X$. Par ailleurs comme $\mathbf{L}$ est de caractéristique p, le polynôme dérivé P' de P s'écrit $P' = p^n \cdot X^{p^n} - 1 = 0 - 1 = -1$. En particulier, on a $\text{pgcd}(P, P') = 1$. D'après la proposition 70 du chapitre 2, P n'a pas de facteur multiple. Comme $\mathbf{L}$ est algébriquement clos, P se décompose donc dans $\mathbf{L}[X]$ en un produit de facteurs unitaires de degré un qui sont deux à deux distincts. Ainsi $\text{card}(\mathbf{K}) = \deg(P) = p^n$.

Par ailleurs on peut montrer que $\mathbf{K}$ est un sous-anneau de $\mathbf{L}$ (faites-le). C'est donc un anneau intègre fini, donc c'est un corps fini d'après la proposition 2. □

Une autre démonstration un peu plus « terre à terre » du théorème 11 sera vue en TD. Elle consiste à évaluer pour tout n le nombre de polynômes irréductibles de degré n sur $\mathbf{F}_p$, afin de montrer qu'il est non nul. On y démontrera au passage le résultat important suivant

Théorème 13. *Soit p un nombre premier. On note $\mathrm{Irr}(p,n)$ l'ensemble des polynômes irréductibles unitaires de degré n dans $\mathbf{F}_p$. On a alors*

$$X^{p^n} - X = \prod_{r|n} \prod_{P \in \mathrm{Irr}(p,r)} P$$

Les deux derniers théorèmes de cette section répondent essentiellement à la question : quelles sont les extension $\mathbf{K} \to \mathbf{L}$, avec $\mathbf{K}$ et $\mathbf{L}$ des corps finis ?

Théorème 14. *Soit p un nombre premier, n un entier strictement positif. et $\mathbf{K}$ un corps fini de cardinal p^n. Soit d un diviseur positif de n et*

$$\mathbf{L} := \{x \in \mathbf{K}, x^{p^d} = x\}.$$

Alors $\mathbf{L}$ est un sous-corps de $\mathbf{K}$ de cardinal p^d, et c'est l'unique sous-corps de cardinal p^d de $\mathbf{K}$.

Démonstration. (esquisse) En utilisant le morphisme de Frobenius, on montre que $\mathbf{L}$ est un sous-corps de $\mathbf{K}$ (faites-le). Par ailleurs $\mathbf{L}^\times$ est le sous-groupe du groupe cyclique $\mathbf{K}^\times$ des élément dont l'ordre divise $p^d - 1$. En particulier $\mathbf{L}^\times$ est de cardinal $p^d - 1$ et donc $\mathbf{L}$ est de cardinal p^d. D'après lemme 8, tout sous-corps de $\mathbf{K}$ de cardinal p^d est inclus dans $\mathbf{L}$, donc lui est égal pour des raisons de cardinalité. □

Le théorème 11 montre que pour tout entier strictement positif n, il existe une extension de $\mathbf{F}_p$ de cardinal p^n. Plus généralement, on a le résultat suivant.

Théorème 15. *Soit p un nombre premier et n un entier strictement positif. Soit $\mathbf{K}$ un corps fini de cardinal p^n et N un entier strictement positif. Alors il existe un sous-corps de $\mathbf{K}$ de cardinal N si et seulement s'il existe un diviseur positif d de n tel que $N = p^d$, et dans ce cas ce sous-corps est unique.*

En particulier, si $\mathbf{K}$ est un corps fini de cardinal q, il existe une extension de $\mathbf{K}$ de cardinal N si et seulement si N est une puissance de q

Ainsi le seul sous-corps d'un corps à $8 = 2^3$ élément est $\mathbf{F}_2$. Un corps à 16 éléments possède deux sous-corps : $\mathbf{F}_2$ et un corps à 4 éléments.

Démonstration. D'après le théorème 14, il suffit de montrer : soit $\mathbf{L}$ un sous-corps de $\mathbf{K}$. Alors il existe un diviseur positif d de n tel que $\text{card}(\mathbf{L}) = p^d$. Mais $\mathbf{K}$ est un $\mathbf{L}$-espace vectoriel de dimension finie. Donc $\text{card}(\mathbf{K}) = \text{card}(\mathbf{L})^r = p^n$. Ceci impose $\text{card}(\mathbf{L}) = p^d$ avec d entier positif vérifiant $rd = n$. □

4.9 Application des corps finis aux codes correcteurs d'erreur

Cette section se veut une introduction succincte et très partielle à la vaste théorie des codes correcteurs, l'une des applications pratiques les plus célèbres de la théorie des corps finis [11]. Les exigences du programme officiel du module ANAR en la matière ne sont pas claires : le contenu exact est « codes cycliques », sans aucune autre précision. On se concentre ici sur les aspects directement liés aux outils mathématiques qu'on a vus dans les sections précédentes, sans vraiment insister sur l'aspect pratique de la mise en oeuvre effective des codes correcteurs et l'efficacité des algorithmes de décodage ; il faudrait déjà pour cela introduire la notion de complexité d'un algorithme ; ceux qui connaissent cette notion pourront essayer d'estimer la complexité des algorithmes présentés et/ou se reporter aux références ci-dessous. La démonstration de certains résultats fait l'objet d'exercices de TD.

Si vous souhaitez approfondir le sujet, l'ouvrage destiné aux étudiants de licence le plus complet en ce qui concerne la théorie des codes est sans doute le *Cours d'algèbre*, de Michel Demazure, aux éditions Cassini. Il contient entre autre un chapitre décrivant précisément le codage réellement employé sur les disques compacts.

Nous signalons aussi comme références utiles :

- le complément 1 du chapitre 4 de *Mathématiques L2*, ouvrage collectif aux éditions Pearson ;
- le chapitre 21 de *Toute l'algèbre de la licence*, de Jean-Pierre Escofier, aux éditions Dunod.

Ces deux références couvrent peu ou prou le même matériel que ce qui suit, avec sans doute plus d'exemples.

4.9.1 Introduction en agitant les mains

L'idée de départ qui sous-tend la théorie des codes correcteurs d'erreurs est la suivante.

Soit, dans une situation donnée, $\mathcal{A}$ un ensemble (fini) d'informations susceptible d'être transmises par un certain canal. Le canal de transmission n'étant pas parfait, ces informations sont également susceptibles d'être altérées au cours de la transmission.

11. À une époque encore récente, il était rare d'entendre parler de corps finis sans être informé qu'ils étaient indispensables à la technologie des disques compacts ; cet exemple précis est un peu désuet aujourd'hui, mais on peut en fait citer essentiellement tout ce qui touche au stockage de données numériques et à leur tranmission.

Pour pallier ce problème, on construit une bijection (le codage) de $\mathcal{A}$ sur une partie $\mathcal{C}$ d'un plus gros ensemble d'informations $\mathcal{B}$. Cet ensemble $\mathcal{B}$ est munie d'une certaine distance qui mesure à quel point deux éléments de $\mathcal{B}$ sont semblables.

Le codage doit vérifier, vis-à-vis de cette distance, les propriétés suivantes :

- si la transmission d'un élément de $\mathcal{C}$ n'est pas trop perturbée, le résultat sera un élément de $\mathcal{B}$ à distance pas trop grande de c ;
- les éléments de $\mathcal{C}$ sont assez éloignés les uns des autres.

Ainsi, connaissant le résultat $b \in \mathcal{B}$ de la transmission pas trop perturbée d'un élément c de $\mathcal{C}$, on peut retrouver l'élément c initialement transmis : c'est l'élément $c \in \mathcal{C}$ qui se trouve à distance minimale de b.

Les alphabets radio (« Alpha, Bravo, Charlie… ») constituent une illustration basique mais assez parlante de ce type de construction.

Ici l'ensemble $\mathcal{A}$ est l'ensemble des lettres de l'alphabet, destinées à être transmises oralement par ondes radios (typiquement un indicatif de navigation aérienne du genre « ATC ») et l'ensemble $\mathcal{B}$ est (disons) l'ensemble des mots de la langue utilisée pour la communication radio. La distance entre deux éléments de $\mathcal{B}$ mesure à quel point les prononciations de ces deux éléments sont phonétiquement différentes. Le codage associe à chacune des lettres de l'alphabet un mot qui commence par la lettre en question (Alpha pour A, Bravo pour B, Charlie pour C, etc). Ce codage est choisi de sorte que l'ensemble des mots associés aux lettres de l'alphabet soient mutuellement assez éloignés phonétiquement les uns des autres. Ainsi même si la communication est un peu parasitée, il sera facile de retrouver que l'émetteur a voulu transmettre par exemple Bravo (donc la lettre B) et pas un autre mot du code. En particulier il y a peu de risque de confondre après une communication pas trop parasitée les mots Bravo et Charlie, alors que phonétiquement la prononciation des lettres B et C peut facilement être confondue dès qu'il y a un peu de « friture » sur la ligne.

4.9.2 Un cadre théorique (un peu trop) général

Les messages (ou « mots ») susceptibles d'être transmis sont écrits dans un certain *alphabet*, en d'autres termes un certain ensemble fini A. L'ensemble des messages susceptibles d'être transmis est alors A^k, où k est un certain entier. Si le message à transmettre a une longueur strictement supérieure à k, on le découpe en « blocs » de taille fixe égale à k.

Un *codage* est une application injective $c\colon A^k \to A^n$, où n est un entier supérieur à k (on code en « ajoutant de la redondance »). Le *code* proprement dit est alors l'image $\mathscr{C} := c(A^k) \subset A^n$, et n est appelé la *longueur* du code : c'est la longueur des mots qui vont être réellement transmis, afin de permettre la correction de certaines erreurs éventuelles de transmission.

On définit la *distance* entre deux éléments $(a_i)_{1\leqslant i\leqslant n}$ et $(b_i)_{1\leqslant i\leqslant n}$ de A^n comme étant

$$d((a_i),(b_i)) = \mathrm{card}(\{i \in \{1,\dots,n\}, a_i \neq b_i\}).$$

On vérifie que $d\colon A^n \times A^n \to \mathbf{N}$ est bien une distance sur A^n, appelée *distance de Hamming*.

Le processus de codage/transmission/correction/décodage peut alors se décrire ainsi ;

1. Soit $\boldsymbol{m} \in A^k$ un mot à transmettre ; **(A)** on code $\boldsymbol{m}$ en $\boldsymbol{n} := c(\boldsymbol{m}) \in A^n$
2. On transmet $\boldsymbol{n}$; à la réception on obtient un élément $\boldsymbol{n'}$ de A^n éventuellement distinct de $\boldsymbol{n}$ à cause des erreurs de transmission
3. **(B)** On calcule $\boldsymbol{n''} \in \mathscr{C}$ un élément qui minimise la distance de $\boldsymbol{n'}$ à $\mathscr{C}$ et **(C)** on calcule $\boldsymbol{m''} \in A^k$ tel que $c(\boldsymbol{m''}) = \boldsymbol{n''}$.

Le *nombre d'erreurs de transmission* dans le processus décrit ci-dessus est $d(\boldsymbol{n}, \boldsymbol{n'})$. S'il n'y a pas d'erreur, on aura $\boldsymbol{n''} = \boldsymbol{n'}$ et $\boldsymbol{m''} = \boldsymbol{m}$.

La *distance minimale* du code $\mathscr{C}$ est la distance minimale entre deux éléments distincts [12] de $\mathscr{C}$. On la note δ.

Soit τ le plus grand entier strictement inférieur à $\delta/2$. On constate alors : *le processus décrit ci-dessus corrige de manière certaine τ erreurs de transmission (ou moins)*. On dit que le code est τ-correcteur. Plus précisément, dès que $d(\boldsymbol{n'}, \boldsymbol{n}) \leqslant \tau$, on a nécessairement $\boldsymbol{n''} = \boldsymbol{n}$ d'après la définition de δ et l'inégalité triangulaire. En revanche, on peut trouver au moins un couple $(\boldsymbol{n}, \boldsymbol{n'}) \in \mathscr{C} \times A^n$ tel que $d(\boldsymbol{n}, \boldsymbol{n'}) \geqslant \tau + 1$ et $\boldsymbol{n}$ ne minimise pas la distance de $\boldsymbol{n'}$ à $\mathscr{C}$ ou, dans le meilleur des cas, n'est pas l'unique élément de $\mathscr{C}$ vérifiant cette propriété.

Il est intuitivement clair que k étant fixé, on peut, en augmentant la longueur n, rendre δ (et donc τ) aussi grand que l'on veut pour un bon choix du code. Bien entendu augmenter n est coûteux dans la pratique, puisque cela revient à augmenter la taille de l'information effectivement transmise. Il est moins évident a priori de construire des codes efficaces *et* peu coûteux, c'est-à-dire qui permettent de corriger de manière certaine un nombre raisonnable d'erreurs tout en gardant une longueur raisonnable. Noter que dans la pratique il est important aussi de disposer d'algorithmes efficaces pour effectuer les opérations **(A)**, **(B)** et **(C)** de la procédure ci-dessus. L'opération **(A)** s'appelle *codage*, l'opération **(B)** *correction* et **(B)**+**(C)** *correction + décodage* ; parfois **(B)** est appelée décodage.

Il s'avère que pour construire des codes ayant de bonnes propriétés au sens ci-dessus, il est plus ou moins nécessaire de mettre plus de structure sur les objets considérés.

4.9.3 Codes linéaires

On s'intéresse désormais exclusivement à la famille particulière des codes *linéaires*.

Plus précisément, en conservant les notations précédentes, on suppose désormais que $A = \mathbf{K}$ est un corps fini et que $\varphi\colon \mathbf{K}^k \to \mathbf{K}^n$ est $\mathbf{K}$-linéaire. En particulier le code $\mathcal{C}$ est alors un sous-espace vectoriel de dimension k de $\mathbf{K}^n$. Dans la pratique, il est fréquent (mais pas systématique) de prendre pour $\mathbf{K}$ le corps à deux éléments, ce qui est très adapté à la représentation par bits utilisée par les ordinateurs.

On définit le *poids* $\omega(\boldsymbol{n})$ d'un élément $\boldsymbol{n}$ de $\mathbf{K}^n$ comme étant son nombre de composantes non nulles, c'est-à-dire $d(\boldsymbol{n}, (0, \ldots, 0))$. La distance minimale δ de $\mathcal{C}$ coïncide alors avec le

12. On écarte systématiquement dans la suite le cas où le code $\mathscr{C}$ est réduit à un élément, de peu d'intérêt dans la pratique.

poids minimal des élément non nuls de $\mathcal{C}$. Ceci vient du fait que $\mathcal{C}$ est un sous-groupe de $\mathbf{K}^n$ et que la distance de Hamming est invariante par translation.

Les paramètres essentiels d'un code linéaire sont sa longueur n, sa dimension k et sa distance minimale δ. On dit que le code est de paramètres $[n, k, \delta]$. Parfois on précise aussi dans les paramètres le cardinal q du corps fini $\mathbf{K}$.

Rappelons que l'on cherche à obtenir des codes de longueur n assez petite tout en étant de distance minimale δ assez grande. De ce point de vue, on a la contrainte suivante, appelée *borne de Singleton*[13].

Proposition 16. *Avec les hypothèse précédentes (code linéaire de dimension k, de longueur n et de distance minimale δ) on a*

$$\delta \leqslant n - k + 1.$$

Cette borne quantifie le fait intuitif qu'on ne peut pas avoir à la foit n petit (peu de redondance) et δ grand (beaucoup d'erreurs corrigées de manière certaine). Les codes linéaires dont les paramètres vérifient l'égalité $\delta = n - k + 1$ sont dits de type MDS (pour l'anglais *maximal distance separable*). Nous en verrons quelques exemples.

Dans la pratique, l'application linéaire φ est donnée par une matrice $G \in \mathcal{M}_{k,n}(\mathbf{K})$ à k lignes et n colonnes à coefficients dans $\mathbf{K}$ et de rang k, appelée *matrice génératrice du code*. Les lignes de G forment donc une base de $\mathscr{C}$. *Bien noter qu'ici et dans la suite, conformément à la tradition en théorie des codes, les éléments de $\mathbf{K}^n$ sont identifiés à des vecteurs lignes.* Cette matrice génératrice permet l'opération de codage **(A)** de la manière très simple suivante : à un élément x de $\mathbf{K}^k$, on associe $x \cdot G \in \mathbf{K}^n$.

L'opération **(C)** de décodage après correction (étant donné $y \in \mathcal{C}$, trouver $x \in \mathbf{K}^n$ telle que $x \cdot G = y$) sera également très simple si la matrice génératrice G est sous forme dite *systématique*. Ceci signifie que la matrice G s'écrit par blocs $G = (I_k|\tilde{G})$ où $\tilde{G} \in \mathcal{M}_{k,n-k}(\mathbf{K})$. Noter qu'on peut toujours se ramener à ce cas quitte à bien choisir la base de $\mathcal{C}$ et *à effectuer une permutation adéquate des coordonnées*. Dans ce cas le décodage après correction est simplissime : étant donné $y \in \mathcal{C}$, l'unique $x \in \mathbf{K}^k$ tel que $y = x \cdot G$ est obtenu en ne gardant que les k premières coordonnées de y.

Identifiant le $\mathbf{K}$-espace vectoriel $\mathbf{K}^n$ à son espace dual, une *matrice de contrôle* pour le code $\mathscr{C}$ est une matrice $H \in \mathcal{M}_{n-k,n}(\mathbf{K})$ dont les lignes forment une base de l'orthogonal $\mathscr{C}^\perp$ de $\mathscr{C}$, où pour mémoire

$$\mathscr{C}^\perp = \{y \in \mathbf{K}^n, \quad \forall x \in \mathscr{C}, \quad \langle y\,,\, x\rangle = 0\}.$$

13. du nom de R.C. Singleton, auteur d'un article de 1964 où ce résultat est démontré

Dans la pratique, déterminer une matrice de contrôle revient donc à déterminer un système de $n-k$ équations linéaires homogènes en n variables décrivant $\mathscr{C}$. On a donc

$$\mathscr{C} = \{x \in \mathbf{K}^n, \quad x \cdot {}^tH = 0\}.$$

Si la matrice génératrice G est sous forme systématique $G = (I_k|\tilde{G})$, on constate aisément que $H = (-{}^t\tilde{G}|I_{n-k})$ est une matrice de contrôle. La connaissance de la matrice de contrôle permet, au moins théoriquement, de déterminer la distance minimale du code.

Proposition 17. *Avec les hypothèse et notations précédentes, soit H une matrice de contrôle de $\mathscr{C}$. Soit d l'unique entier strictement positif vérifiant la propriété suivante :*

1. *il existe d colonnes de H qui forment un système lié ;*
2. *tout sous-ensemble de colonnes de H de cardinal $d-1$ est un système libre.*

Alors d est la distance minimale de $\mathscr{C}$.

Le *syndrome* d'un élément $y \in \mathbf{K}^n$ est $s(y) := y \cdot {}^tH$. En particulier le syndrome définit une application linéaire surjective $s\colon \mathbf{K}^n \to \mathbf{K}^{n-k}$, de noyau $\mathscr{C}$.

Soit $x \in \mathscr{C}$ un mot à transmettre, et $y \in \mathbf{K}^n$ le mot finalement transmis. On appelle $e = y-x$ le *vecteur d'erreurs* ; on a en particulier $s(y) = s(e)$. Déterminer $x' \in \mathscr{C}$ tel que $d(y,x') = d(y,\mathscr{C})$ revient alors à déterminer un élément y' de poids minimal de l'ensemble

$$\{z \in \mathbf{K}^n, \quad s(z) = s(y)\}.$$

En effet, posant alors $x' = y - y'$, on aura $s(x') = s(y) - s(y') = 0$ donc $x' \in \mathscr{C}$, et par ailleurs si x'' est un élément quelconque de $\mathscr{C}$ on a $s(y-x'') = s(y)$ donc, par définition de y',

$$\omega(y-x'') \geqslant \omega(y') = \omega(y-x').$$

On a donc bien $d(y,x'') \geqslant d(y,x')$.

Cette remarque justifie la méthode suivante de décodage de codes linéaires, dite *par syndrome* : on détermine au préalable, pour chaque valeur possible σ du syndrome, l'élément $y(\sigma)$ de $\mathbf{K}^n$ de poids minimal parmi les éléments de $\mathbf{K}^n$ de syndrome σ et on stocke ces valeurs dans une table.

Ensuite, pour chaque mot $y \in \mathbf{K}^n$ reçu après transmission, on calcule $\sigma = s(y)$ et on décode y en $y - y(\sigma)$.

Noter qu'il y a $\mathrm{card}(\mathbf{K})^{n-k}$ valeurs possibles du syndrome. Dans la pratique la méthode précédente n'est réellement efficace que lorsque $n-k$ est petit. D'autres méthodes plus efficaces [14] ont été mises au point pour des familles particulières de codes linéaires. Nous

14. Pour préciser ce que l'on entend par « efficace », il faudrait introduire la notion de complexité d'un algorithme, ce que nous ne ferons pas dans le cadre de ce cours.

décrivons ci-dessous une telle méthode pour les codes dits BCH, qui font partie de la famille plus générale des codes cycliques qui font l'objet de la partie suivante.

4.9.4 Codes cycliques

Rappelons les hypothèses et notation : $\mathbf{K}$ est un corps fini, n et k sont des entiers strictement positifs, $\varphi\colon \mathbf{K}^k \to \mathbf{K}^n$ est une application $\mathbf{K}$-linéaire injective et $\mathscr{C} = \varphi(\mathbf{K}^k)$ est le code linéaire associé.

Définition 18. Le code $\mathscr{C}$ est dit *cyclique* s'il est invariant par l'application de décalage

$$T\colon \begin{array}{ccc} \mathbf{K}^n & \longrightarrow & \mathbf{K}^n \\ (a_0, a_1, \ldots, a_{n-2}, a_{n-1}) & \longmapsto & (a_{n-1}, a_0, \ldots, a_{n-3}, a_{n-2}) \end{array}.$$

On obtient une reformulation importante de cette propriété en identifiant $\mathbf{K}^n$ à l'espace vectoriel sous-jacent à la $\mathbf{K}$-algèbre quotient $\mathbf{K}[X]/\langle X^n - 1\rangle$. Notant abusivement X l'image de X dans cette algèbre quotient, on sait (proposition 6 de la section 3) que $\{1, X, \ldots, X^{n-1}\}$ est une base du $\mathbf{K}$-espace vectoriel sous-jacent, au moyen de laquelle on identifie cet espace vectoriel sous-jacent à $\mathbf{K}^n$. On vérifie alors que via cette identification, l'application de décalage T ci-dessus correspond exactement à la multiplication par X. Ainsi les codes cycliques sont exactement les sous $\mathbf{K}$-espaces vectoriels de $\mathbf{K}[X]/\langle X^n - 1\rangle$ invariants par multiplication par X, ou, ce qui revient au même, par multiplication par n'importe quel élément de $\mathbf{K}[X]/\langle X^n - 1\rangle$. En d'autres termes

Proposition 19. *Modulo l'identification $\mathbf{K}^n \cong \mathbf{K}[X]/\langle X^n - 1\rangle$ décrite ci-dessous, les codes cycliques de $\mathbf{K}^n$ sont exactement les idéaux de $\mathbf{K}[X]/\langle X^n - 1\rangle$.*

Par la proposition 20 de la section 2, les idéaux de $\mathbf{K}[X]/\langle X^n - 1\rangle$ sont en bijection naturelle avec les idéaux de $\mathbf{K}[X]$ contenant l'idéal $\langle X^n - 1\rangle$. Au vu de la proposition 30 de la section 2, ce dernier ensemble d'idéaux est en bijection naturelle avec l'ensemble des diviseurs unitaires de $X^n - 1$. Si g est un tel diviseur unitaire, le code cyclique correspondant sera dit engendré par g.

Nous avons décrit les codes cycliques mais pas les applications de codage correspondantes. Si $\mathscr{C}$ est un code cyclique correspondant à l'idéal engendré par un diviseur unitaire g de $X^n - 1$, sa dimension est $k := n - \deg(g)$. Un codage systématique est alors donné par l'application qui à $(a_1, \ldots, a_k) \in \mathbf{K}^k$ associe

$$\sum_{i=1}^{k} a_i X^{n-i} - r_{\boldsymbol{a}}(X) \in \mathbf{K}[X]/\langle X^n - 1\rangle$$

où $r_{\boldsymbol{a}}(X)$ est (l'image dans $\mathbf{K}[X]/\langle X^n-1\rangle$ du) le reste de la division euclidienne de $\sum_{i=1}^{k} a_i X^{n-i}$ par g.

Noter que dans le cas d'un code cyclique engendré par un polynôme g, la borne de Singleton peut se réécrire

$$\deg(g) \geqslant \delta - 1.$$

Nous allons à présent donner une minoration de la distance minimale d'un code cyclique de $\mathbf{K}[X]/\langle X^n - 1\rangle$, sous l'hypothèse supplémentaire que n et $q := \mathrm{card}(\mathbf{K})$ sont premiers entre eux.

Cette hypothèse garantit que $[q]_n$ est un élément du groupe $(\mathbf{Z}/n\mathbf{Z})^\times$. Soit $r \geqslant 1$ son ordre. Ainsi r est le plus petit entier strictement positif vérifiant $q^r = 1 \pmod n$. Soit maintenant $\mathbf{L}$ un corps à q^r éléments contenant $\mathbf{K}$ (*cf.* le théorème 15). Comme n divise $q^r - 1 = \mathrm{card}(\mathbf{L}^\times)$ et que $\mathbf{L}^\times$ est un groupe cyclique, il existe dans $\mathbf{L}^\times$ un élément α d'ordre n. Noter que comme $\alpha^n = 1$, l'expression α^i a un sens pour $i \in \mathbf{Z}/n\mathbf{Z}$. Comme α est d'ordre n, l'ensemble $\{\alpha^i\}_{i\in\mathbf{Z}/n\mathbf{Z}} \subset \mathbf{L}$ est de cardinal n. C'est donc l'ensemble des racines du polynôme $X^n - 1$ dans $\mathbf{L}$, et ce polynôme est entièrement décomposé dans $\mathbf{L}$:

$$X^n - 1 = \prod_{i\in\mathbf{Z}/n\mathbf{Z}} (X - \alpha^i).$$

En particulier tout diviseur unitaire $g \in \mathbf{L}[X]$ de $X^n - 1$ s'écrit

$$g = \prod_{i\in\Sigma} (X - \alpha^i)$$

où Σ est une partie de $\mathbf{Z}/n\mathbf{Z}$. En fait l'application

$$\Sigma \mapsto g_\Sigma := \prod_{i\in\Sigma} (X - \alpha^i)$$

est une bijection de l'ensemble des parties de $\mathbf{Z}/n\mathbf{Z}$ sur l'ensemble des diviseurs unitaires *dans* $\mathbf{L}[X]$ de $X^n - 1$; attention, ce dernier ensemble contient l'ensemble des diviseurs unitaires dans $\mathbf{K}[X]$ de $X^n - 1$, c'est-à-dire l'ensemble des codes cycliques de $\mathbf{K}[X]/\langle X^n - 1\rangle$, mais il est strictement plus gros dès que $r \geqslant 2$; en effet, dans ce dernier cas, on a $\alpha \notin \mathbf{K}$, et donc $X - \alpha \notin \mathbf{K}[X]$. On démontrera en TD :

Proposition 20. *Avec les hypothèses et notations ci-dessus, $g_\Sigma \in \mathbf{K}[X]$ si et seulement si Σ est stable par multiplication par q.*

L'application réciproque de l'application ci-dessus sera notée $g \mapsto \Sigma_g$.

Ceci étant posé, on a l'estimation suivante pour la distance minimale d'un code cylique de $\mathbf{K}[X]$.

Proposition 21. *On conserve les hypothèse et notations précédentes. Soit $g \in \mathbf{K}[X]$ un diviseur unitaire de $X^n - 1$. On suppose qu'il existe $\nu \in \mathbf{Z}/n\mathbf{Z}$ et $2 \leqslant d \leqslant n$ un entier positif tels que*

$$\{\nu + [i]_n\}_{0 \leqslant i \leqslant d-2} \subset \Sigma_g.$$

Alors le code cyclique engendré par g est de distance minimale au moins d.

Cette propriété est à la base de la définition des codes cycliques dits BCH [15]. L'intérêt de ces codes est qu'ils bénéficient d'algorithmes de décodage efficaces. Noter que nous n'avons rien dit pour l'instant du problème du décodage pour les codes cycliques ; bien entendu, comme pour tout code linéaire, la méthode de décodage par syndrome est disponible, mais nous avons déjà signalé qu'elle était en général inefficace dans la pratique.

4.9.5 Codes BCH

On rappelle le contexte et les notations : $\mathbf{K}$ est un corps fini de cardinal q, n est un entier positif premier à la caractéristique de $\mathbf{K}$, r est l'ordre [16] de q dans $(\mathbf{Z}/n\mathbf{Z})^\times$, $\mathbf{L}$ est un corps de cardinal q^r contenant $\mathbf{K}$ et $\alpha \in \mathbf{L}^\times$ est un élément d'ordre n. Soit $2 \leqslant d \leqslant n$ un entier. Soit $\mathcal{I} \in \mathbf{K}[X]$ l'idéal des polynômes $P \in \mathbf{K}[X]$ vérifiant

$$\forall i \in \{1, \dots, d-1\}, \quad P(\alpha^i) = 0.$$

C'est un idéal de $\mathbf{K}[X]$ qui contient $\langle X^n - 1 \rangle$. Son image $\mathscr{C}$ dans $\mathbf{K}[X]/\langle X^n - 1 \rangle$ définit donc un code cyclique de $\mathbf{K}[X]/\langle X^n - 1 \rangle$ de distance minimale δ *au moins* égale à d d'après la proposition 21 : on appelle un tel code un *code BCH de longueur n et de distance assignée d*. Soit t le plus grand entier strictement inférieur à $\frac{d}{2}$. L'algorithme de correction décrit ci-dessous permettra de corriger de manière certaine t erreurs. Signalons que la distance minimale réelle du code est en général strictement supérieur à d (mais difficile à calculer dans la pratique) ; le code pourrait donc, en théorie, corriger de manière certaine plus d'erreurs, mais on ne dispose pas a priori d'algorithme efficace pour ce faire. Cependant nous verrons en TD le cas particulier où $\mathbf{L} = \mathbf{K}$, c'est-à-dire $n = q - 1$ et α est un générateur de $\mathbf{K}^\times$. On obtient alors par la construction ci-dessus un code de distance minimale exactement d, qui est en outre de type MDS. De tels codes sont appelés codes de Reed-Solomon [17].

La dimension du code obtenu est $n - \deg(g)$ où $g \in \mathbf{K}[X]$ est le générateur unitaire de l'idéal $\mathcal{I}$ défini ci-dessus. D'après la proposition 20, on a $g = g_\Sigma$ où Σ est la plus petite partie de $\mathbf{Z}/n\mathbf{Z}$ contenant $\{[i]_n\}_{1 \leqslant i \leqslant d-1}$ et stable par multiplication par q. Comme $q^r = 1$

15. du nom de leurs inventeurs : R. Bose, D. K. Ray-Chaudhuri et A. Hocquenghem
16. En particulier, n divise $q^r - 1$; si $n = q^r - 1$, on parle de code BCH *primitif*.
17. du nom de leurs inventeurs I.S. Reed et G. Solomon

(mod n), l'ensemble

$$\{[q^s i]_n\}_{\substack{1 \leqslant i \leqslant d-1 \\ 0 \leqslant s \leqslant r-1}}$$

contient $\{[i]_n\}_{1 \leqslant i \leqslant d-1}$ et est stable par multiplication par q. Il contient donc Σ. Rappelant que $\deg(g) = \mathrm{card}(\Sigma)$, on en déduit la majoration

$$\deg(g) \leqslant r(d-1).$$

Décrivons à présent l'algorithme de correction. Rappelons qu'on désigne par t le plus grand entier strictement inférieur à $\frac{d}{2}$. Soit $\boldsymbol{m}$ un mot de $\mathscr{C}$ et $\boldsymbol{m}'$ le mot transmis. On suppose comme annoncé que $f := d(\boldsymbol{m}, \boldsymbol{m}') \leqslant t$. Soit $\boldsymbol{e} = \boldsymbol{m} - \boldsymbol{m}'$. Il s'agit donc de retrouver $\boldsymbol{m}$ (ou, ce qui revient au même, $\boldsymbol{e}$) à partir de $\boldsymbol{m}'$.

Notons qu'en particulier, $\boldsymbol{m}$, $\boldsymbol{m}'$ et $\boldsymbol{e}$ sont des éléments de $\mathbf{K}[X]/\langle X^n - 1\rangle$. Comme $\alpha^n = 1$, pour n'importe quel élément $\boldsymbol{p}$ de $\mathbf{K}[X]/\langle X^n - 1\rangle$ et n'importe quel $j \in \mathbf{N}$, la valeur de $P(\alpha^j)$ ne dépend pas du choix du relevé P de $\boldsymbol{p}$ dans $\mathbf{K}[X]$, et est notée $\boldsymbol{p}(\alpha^j)$.

Soit j tel que $1 \leqslant j \leqslant 2t$. Comme on a $2t \leqslant d-1$ et $\boldsymbol{m} \in \mathscr{C}$, par définition de $\mathscr{C}$, on a l'égalité $\boldsymbol{m}(\alpha^j) = 0$. Posons alors

$$s_j := \boldsymbol{m}'(\alpha^j) = \boldsymbol{e}(\alpha^j) \in \mathbf{L}.$$

Posons également

$$\boldsymbol{s}(Z) := \sum_{j=1}^{2t} s_j Z^{j-1} \in \mathbf{L}[Z].$$

Notons que $\deg(\boldsymbol{s}) \leqslant 2t-1$ et qu'on peut déterminer $\boldsymbol{s}$ à partir de $\boldsymbol{m}'$.

Identifions à présent $\boldsymbol{e}$ à l'unique relevé de $\boldsymbol{e}$ dans $\mathbf{K}[X]$ de degré strictement inférieur à n, et écrivons

$$\boldsymbol{e}(X) = \sum_{i=1}^{f} a_i X^{r_i}$$

avec $1 \leqslant r_1 < r_2 < \cdots < r_f < n$ et les a_i sont tous non nuls. Pour déterminer $\boldsymbol{e}$ (et donc $\boldsymbol{m}$) il s'agit de déterminer les r_i et les a_i. Pour cela, il suffit de connaître le polynôme

$$\boldsymbol{\sigma}(Z) = \prod_{i=1}^{f} (1 - \alpha^{r_i} Z) \in \mathbf{L}[Z].$$

En effet, si on connaît $\boldsymbol{\sigma}(Z)$, on connaît $f = \deg(\boldsymbol{\sigma}(Z))$ et on peut déterminer les entiers j tels que $0 \leqslant j \leqslant n-1$ et $\boldsymbol{\sigma}(\alpha^j) = 0$ (en les testant tous), ce qui permet d'obtenir les r_i. La détermination des a_i se fait alors en résolvant le système linéaire

$$s_j = \sum_{i=1}^{f} a_i \alpha^{j r_i}, \quad 1 \leqslant j \leqslant f$$

dont la matrice est un Vandermonde.

Il reste donc à expliquer comment calculer $\boldsymbol{\sigma}(Z)$ à partir des données déjà connues. Posons

$$\boldsymbol{\omega}(Z) = \sum_{i=1}^{f} a_i \alpha^{r_i} \prod_{1 \leqslant k \neq i \leqslant f} (1 - \alpha^{r_k} Z) \in \mathbf{L}[Z].$$

On vérifie aussitôt que $\deg(\boldsymbol{\omega}) < t$ et qu'aucune des racines de $\boldsymbol{\sigma}(Z)$ n'est racine de $\boldsymbol{\omega}(Z)$. En particulier $\boldsymbol{\sigma}(Z)$ et $\boldsymbol{\omega}(Z)$ sont premiers entre eux. En outre on vérifie facilement la relation

$$\boldsymbol{s}(Z)\boldsymbol{\sigma}(Z) = \boldsymbol{\omega}(Z) \pmod{Z^{2t}}.$$

Lemme 22. *Soit $\boldsymbol{\sigma}_0, \boldsymbol{\omega}_0 \in \mathbf{L}[Z]$ tels que $\deg(\boldsymbol{\sigma}_0) \leqslant t$, $\deg(\boldsymbol{\omega}_0) < t$ et*

$$\boldsymbol{s}(Z)\boldsymbol{\sigma}_0(Z) = \boldsymbol{\omega}_0(Z) \pmod{Z^{2t}}.$$

Alors il existe $\mathbf{C}(Z) \in \mathbf{L}[Z]$ tel que $\boldsymbol{\sigma}_0(Z) = \mathbf{C}(Z)\boldsymbol{\sigma}(Z)$ et $\boldsymbol{\omega}_0(Z) = \mathbf{C}(Z)\boldsymbol{\omega}(Z)$.

Démonstration. On a

$$\boldsymbol{\sigma}_0(Z)\boldsymbol{\omega}(Z) = \boldsymbol{s}(Z)\boldsymbol{\sigma}(Z)\boldsymbol{\sigma}_0(Z) = \boldsymbol{\omega}_0(Z)\boldsymbol{\sigma}(Z) \pmod{Z^{2t}}$$

Ainsi

$$\boldsymbol{\sigma}_0(Z)\boldsymbol{\omega}(Z) - \boldsymbol{\omega}_0(Z)\boldsymbol{\sigma}(Z) = 0 \pmod{Z^{2t}}$$

Mais $\deg(\boldsymbol{\sigma}_0(Z)\boldsymbol{\omega}(Z) - \boldsymbol{\omega}_0(Z)\boldsymbol{\sigma}(Z)) < 2t$ donc

$$\boldsymbol{\sigma}_0(Z)\boldsymbol{\omega}(Z) - \boldsymbol{\omega}_0(Z)\boldsymbol{\sigma}(Z) = 0$$

Or $\boldsymbol{\omega}(Z)$ et $\boldsymbol{\sigma}(Z)$ sont premiers entre eux. Par le lemme de Gauss, $\boldsymbol{\omega}(Z)$ divise $\boldsymbol{\omega}_0(Z)$ et on conclut facilement. □

Si, connaissant $\boldsymbol{s}(Z)$, on sait construire $\boldsymbol{\omega}_0$ et $\boldsymbol{\sigma}_0$ ayant la propriété de l'énoncé de lemme, on en déduit facilement $\boldsymbol{\sigma}$ et $\boldsymbol{\omega}$: comme $\boldsymbol{\omega}$ et $\boldsymbol{\sigma}$ sont premiers entre eux, le polynôme $\mathbf{C}$ de la conclusion de l'énoncé est le pgcd de $\boldsymbol{\omega}_0$ et $\boldsymbol{\sigma}_0$. La construction de $\boldsymbol{\omega}_0$ et $\boldsymbol{\sigma}_0$ à partir de $\boldsymbol{s}(Z)$ est basée sur l'algorithme d'Euclide étendu pour les polynômes, plus précisément sur la proposition suivante. Les notations sont celles de la partie 6.6.3 (partie 3 des notes de cours sur le chapitre 6). Pour obtenir $\boldsymbol{\omega}_0$ et $\boldsymbol{\sigma}_0$, on applique la proposition qui suit avec $a = Z^{2t}$ et $b = \boldsymbol{s}(Z)$ (*cf.* ci-dessous pour les détails).

Proposition 23. *On reprend les notations de la partie 6.6.3 du cours en supposant en outre que $A = \mathbf{K}[X]$, où $\mathbf{K}$ est un corps. Alors :*

1. *pour tout entier n vérifiant $1 \leqslant n \leqslant N+1$, on a*
$$\deg(r_n) < \deg(r_{n-1}) \ ;$$
2. *pour tout entier n vérifiant $1 \leqslant n \leqslant N$, on a*
$$\deg(r_{n-1}) = \deg(q_n) + \deg(r_n) \ ;$$
3. *On suppose en outre que $\deg(a) \geqslant \deg(b)$; alors pour tout entier n vérifiant $1 \leqslant n \leqslant N$, on a*
$$\deg(v_n) = \deg(r_{-1}) - \deg(r_{n-1}).$$

Démonstration. Pour tout entier n vérifiant $1 \leqslant n \leqslant N+1$, r_n est par définition le reste d'une division euclidienne par r_{n-1}, ce qui montre que $\deg(r_n) < \deg(r_{n-1})$.

Soit n un entier vérifiant $1 \leqslant n \leqslant N$. On a

$$r_{n-1} = r_n\, q_n + r_{n+1}$$

or $\deg(r_{n+1}) < \deg(r_n) < \deg(r_{n-1})$. En particulier, on a $q_n \neq 0$ et $\deg(r_{n-1}) = \deg(q_n) + \deg(r_n)$.

Pour la dernière propriété, on raisonne par récurrence sur n. On a $v_1 = -q_0 v_0 = -q_0$. Par ailleurs on a

$$a = bq_0 + r_1$$

avec $\deg(r_1) < \deg(b)$. Comme $\deg(a) \geqslant \deg(b)$, on a nécessairement $q_0 \neq 0$ et

$$\deg(a) = \deg(bq_0) = \deg(b) + \deg(q_0).$$

Ainsi

$$\deg(v_1) = \deg(q_0) = \deg(a) - \deg(b) = \deg(r_{-1}) - \deg(r_0).$$

Donc la propriété est vérifiée pour $n = 1$.

Supposons la propriété vérifiée pour tout entier n vérifiant $1 \leqslant n \leqslant N-1$. On a par définition de l'algorithme d'Euclide étendu

$$v_{n+1} = v_{n-1} - q_n\, v_n.$$

Or, en utilisant l'hypothèse de récurrence, on a

$$\deg(q_n v_n) = \deg(q_n) + \deg(v_n) = \deg(q_n) + \deg(r_{-1}) - \deg(r_{n-1})$$

$$= \deg(q_n) + \deg(r_{-1}) - (\deg(q_n) + \deg(r_n)) = \deg(r_{-1}) - \deg(r_n).$$

Par ailleurs si $n \geqslant 2$, on a d'après l'hypothèse de récurrence

$$\deg(v_{n-1}) = \deg(r_{-1}) - \deg(r_{n-2}).$$

Comme $\deg(r_{n-2}) > \deg(r_n)$, on a

$$\deg(v_{n-1}) < \deg(r_{-1}) - \deg(r_n) = \deg(q_n v_n),$$

d'où

$$\deg(v_{n+1}) = \deg(q_n v_n) = \deg(r_{-1}) - \deg(r_n)$$

ce qui conclut.

Si $n = 1$, on a

$$\deg(q_n v_n) = \deg(q_1 v_1) = \deg(r_{-1}) - \deg(r_1) = \deg(a) - \deg(b) + \deg(r_0) - \deg(r_1) > 0$$

et $\deg(v_{n-1}) = \deg(v_0) = 0$. Là encore, on a donc $\deg(v_{n-1}) < \deg(q_n v_n)$ et on conclut comme dans le cas $n \geqslant 2$. □

Soit t un entier strictement positif. Appliquons ce qui précède dans le cas où a est de degré $2t$ et b de degré $2t-1$, en conservant les même notations. Soit m le plus petit entier n compris entre 1 et $N+1$ tel que $\deg(r_n) < t$. En particulier $\deg(r_{m-1}) > t$ et

$$\deg(v_m) = \deg(r_{-1}) - \deg(r_{m-1}) \leqslant 2t - t = t$$

Ainsi, on a

$$v_m b = r_m \pmod{a}$$

avec $\deg(v_m) \leqslant t$ et $\deg(r_m) < t$.