PREMIÈRE PARTIE

CULTURE DU CODAGE

0. Quelques rappels essentiels

Ce mini-paragraphe veut seulement rassembler les quelques prérequis les plus significatifs, pour les «faire remonter à la surface». Pour des raisons de volume disponible, et parce que ces résultats font partie des prérequis, ils sont donnés sans démonstration ; le lecteur trouvera facilement dans la littérature ces résultats classiques.

0.1. Corps et anneaux — Les structures algébriques au centre de cet ouvrage sont les corps finis, essentiellement en caractéristique 2. Nous en rappelons le b-a-ba. On suppose que le lecteur sait qu'un anneau quotient $\mathbb{Z}[X]/\langle f\rangle$, où f est un polynôme irréductible de degré d, est un corps à p^d éléments, et que ce corps contient canoniquement un zéro de f ; c'est *un corps de rupture de* f ; le plus petit corps dans lequel f se factorise en produits linéaires est *le corps de décomposition de* f.

PROPOSITION 0.1. — *Soit* $\mathbb{K}$ *un corps fini de caractéristique* p. *L'application* $\mathbb{K} \to \mathbb{K}$, $t \mapsto t^p$, *est un automorphisme de* $\mathbb{K}$ *qui fixe* $\mathbb{Z}/p\mathbb{Z}$ (l'automorphisme de FROBENIUS).

PROPOSITION 0.2. — [Théorème de Wedderburn] — *Tout corps fini est commutatif et son groupe multiplicatif est cyclique*.

Un générateur du groupe multiplicatif d'un corps fini est appelé *un élément primitif*. Cette notion est centrale en nombre d'endroits de l'ouvrage. Nous utiliserons les lettres grecques α, β, γ, et δ pour désigner un élément primitif d'un corps fini.

PROPOSITION 0.3. — *Soit* $\mathbb{K}$ *un corps fini à* $q = p^d$ *éléments. Alors il est un corps de décomposition de* $X^q - X$ *sur* $\mathbb{Z}/p\mathbb{Z}$. *Inversement, si* $q = p^d$, *un corps de décomposition de* $X^q - X$ *sur* $\mathbb{Z}/p\mathbb{Z}$ *est un corps à* q *éléments*.

PROPOSITION 0.4. — *Un corps $\mathbb{K}$ de cardinal p^d possède un sous corps de cardinal p^c si et seulement si c divise d, et chacun de ces sous-corps est unique. Pour chaque entier $d > 0$ et chaque nombre premier p, il existe exactement un seul corps (à isomorphie près) de cardinal p^d* (on le note $\mathbb{F}_{p^d}$).

Il résulte de ces énoncés que $\mathbb{F}_{q=2^m}$, outre 0 et 1, est formé exactement des éléments de la forme α^k, $1 \leq k \leq q-2$, pour au moins un élément α, que α^m est combinaison linéaire de 1, α, α^2, …, α^{m-1}, que les corps finis de caractéristique 2 peuvent essentiellement être vus comme formant un treillis[0.1] dont le plus grand élément, identifiable à la réunion des $\mathbb{F}_{q=2^k}$, est la clôture algébrique de $\mathbb{F}_2$.

Dans notre vocabulaire, *anneau* signifiera anneau unitaire ; nous demandons donc aux morphismes de préserver l'unité, et aux sous-anneaux de contenir l'unité de l'anneau. Les anneaux qui nous concernent sont souvent des anneaux de polynômes. Rappelons qu'on appelle *valuation d'un polynôme* le degré de son terme de plus petit degré ; on note $\mathrm{val}(f)$ la valuation d'un polynôme f. C'est une notion qui reviendra en de nombreux endroits de cet opuscule.

valuation d'un polynôme

PROPOSITION 0.5. — *Si A est intègre, $A[X_1, \ldots, X_n]$, $n > 0$, est factoriel.*

Un anneau est dit intègre quand le produit de deux éléments non nuls est non nul. De même que l'on construit $\mathbb{Q}$ comme corps de fractions de l'anneau intègre $\mathbb{Z}$, on construit formellement le corps de fractions de tout anneau intègre A. C'est le quotient de $A \times A \setminus \{0\}$ par la relation d'équivalence définie par $(P, Q) \equiv (R, S) \iff PS = QR$. On écrit $\dfrac{P}{Q}$ ou encore P/Q pour désigner la classe de (P, Q), et on parle de fractions. L'addition en «passant au même dénominateur», $\dfrac{P}{Q} + \dfrac{R}{S} = \dfrac{PS + QR}{QS}$, est bien définie, de même que le produit, $\dfrac{P}{Q} \times \dfrac{R}{S} = \dfrac{PR}{QS}$. L'élément $0/1$, qui est la classe de $(0, Q)$, est le neutre pour l'addition, et $1/1$ le neutre pour la multiplication ; chaque élément non nul est inversible, l'inverse de P/Q ($P \neq 0$) étant Q/P. On écrit $\mathbb{F}_A$ pour désigner le corps de fractions de A.

[0.1] Un treillis est un ensemble partiellement ordonné dans lequel chaque paire admet une borne supérieure et une borne inférieure.

Un anneau intègre A se plonge canoniquement dans son corps de fractions par $t \mapsto \dfrac{t}{1}$; nous notons i_A ce plongement.

PROPOSITION 0.6. — *Tout corps $\mathbb{K}$ contenant un anneau intègre A contient canoniquement son corps de fraction : si $j : A \to \mathbb{K}$ injecte un anneau dans un corps $\mathbb{K}$, alors il existe un unique homomorphisme $u : \mathbb{F}_A \to \mathbb{K}$ tel que $j = u \circ i_A$.*

PROPOSITION 0.7. — *Si A est factoriel et si $f(x) \in A[x]$ est irréductible, alors f est aussi irréductible dans $\mathbb{F}_A[x]$.*

Si $\mathfrak{p}$ est un idéal premier de A, l'ensemble des fractions dont le dénominateur n'appartient pas à $\mathfrak{p}$ forment un anneau, le *localisé de A en $\mathfrak{p}$*, $A_{\mathfrak{p}}$. Les localisés $A_{\mathfrak{p}}$ sont des exemples d'anneaux qui n'ont qu'un seul idéal maximal. Ces anneaux sont dits *locaux*. Un anneau intègre A est dit *valué* son corps de fraction ou son inverse est dans A ; un anneau valué est local.

localisé de A en p

anneau local

anneau valué

Une autre notion d'algèbre commutative que le lecteur rencontrera est celle de radical ; le *radical* d'un idéal $\mathfrak{I}$ d'un anneau commutatif A est l'ensemble des éléments de A dont une puissance appartient à $\mathfrak{I}$. C'est un idéal (vérification laissée au lecteur) ; un idéal est dit radical s'il contient tous les éléments dont il contient une puissance ; les idéaux radicaux jouent un rôle très important en géométrie algébrique ; le lecteur pourra consulter [17] par exemple sur le *Nullstellensatz* de HILBERT, et de manière plus générale, [18] sur ces notions qu'il rencontrera dans la partie *Boîte à outils* de l'ouvrage.

radical

idéal radical

Une fonction $f : \mathbb{K}^n \to \mathbb{K}$ est dite symétrique si elle ne change pas de valeur quand on permute ses arguments. En développant le polynôme :

$$(X + x_1) \dots (X + x_n) = X^n + a_1 X^{n-1} + a_2 X^{n-2} + \dots + a_n, \qquad \text{(P)}$$

on vérifie que a_1 est la somme des x_i, que a_2 est la somme des $x_i x_j$ pour tous les couples (i, j) tels que $i \neq j$, que a_k est la somme de tous les produits de $x_{i_1} \dots x_{i_k}$, les indices i_h étant deux à deux distincts, et que a_n est le produit de tous les x_i. On peut montrer que toute relation symétrique est une expression algébrique en les a_i, à coefficients entiers. Par exemple, $x_1^3 + x_2^3 + x_3^3 = a_1^3 + a_1\, a_2 + a_3$, ou encore $\dfrac{1}{x_1} + \dfrac{1}{x_2} + \dfrac{1}{x_3} = \dfrac{a_2}{a_3}$. Cela est en particulier vrai des *sommes de* NEWTON $s_k = x_1^k + x_2^k + \dots + x_n^k$.

somme de Newton

PROPOSITION 0.8. — *Les sommes de* NEWTON *et les coefficients* a_i *du produit* (P) *sont liés par les relations de Newton* —se rappeler que nous sommes en caractéristique 2— *:* $0 = s_1 + a_1$, $0 = s_2 + a_1 s_1$, $\ldots$, $0 = s_n + a_1\, s_{n-1} + \cdots + a_{n-1} s_1 + n a_n$.

0.2. Matrices de Vandermonde. Résultantes —

Le lecteur est supposé connaître l'algèbre linéaire enseignée au premier cycle universitaire. En particulier, tout ce qui concerne les déterminants et la dualité doit lui être assez familier. Les points particuliers suivants nous seront utiles.

On appelle *matrice de* VANDERMONDE une matrice de la forme

$$\begin{pmatrix} x_1 & x_2 & \ldots & x_n \\ x_1^2 & x_2^2 & \ldots & x_n^2 \\ \vdots & & & \vdots \\ x_1^n & x_2^n & \ldots & x_n^n \end{pmatrix}$$

Son déterminant est $\prod_{1\leq j\leq n} x_j \prod_{1\leq i<j\leq n}(x_j - x_i)$; elle est donc inversible si et seulement si les x_i sont non nuls et distincts. Nous nous intéresserons à un cas particulier. Soit α un élément primitif de $\mathbb{F}_{2^m}$ (et posons $n = 2^m - 1$) ; la matrice de VANDERMONDE $V(x)$, pour $x = \alpha^k$, $1 \leq k \leq n-1$, est la matrice de $M_n(\mathbb{F}_q)$ de terme général $v_{ij} = x^{(i-1)(j-1)}$:

$$V(x) = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ 1 & x & \ldots & x^{n-1} \\ \vdots & & & \vdots \\ 1 & x^{n-1} & \ldots & x^{(n-1)^2} \end{pmatrix}.$$

Il est laissé en exercice au lecteur de montrer que l'inverse de $V(x)$ est $V(x^{-1})$.

Une autre application essentielle de l'algèbre linéaire pour nous est la résultante de deux polynômes. Nous nous restreignons à la situation suivante. Considérons deux polynômes homogènes distincts et irréductibles :

$$P = \sum_{0\leq k\leq m} a_k\, X^k \qquad Q = \sum_{0\leq k\leq n} b_k\, X^k$$

de $\overline{\mathbb{F}}_2[Y,Z][X] \simeq \overline{\mathbb{F}}_2[X,Y,Z]$, n'appartenant pas à $\overline{\mathbb{F}}_2[X,Y]$; les a_k et b_k sont des polynômes homogènes en (X,Y), de degrés respectifs $m-k$ et

$n-k$. À quelle condition P et Q ont-ils une racine commune $(x_0, y_0, z_0) \in P^2(\overline{\mathbb{F}}_2)$? Considérons, E_k étant l'espace vectoriel sur le corps commutatif $\mathbb{K} = \overline{\mathbb{F}}_2(Y, Z)$ engendré par les X^i pour $0 \leq i \leq k-1$ et l'application linéaire : $\phi : E_n \times E_m \to E_{m+n}$, $(U, V) \mapsto PU + QV$.

Formons la matrice de ϕ dans les bases canoniques (les monômes X^k) : sa première colonne est formée des coefficients de P (des polynômes homogènes en (X, Y), sa deuxième de ceux de XP, sa n-ième de ceux de $X^{n-1}P$, sa $n+1$-ième de ceux de Q enfin sa dernière de ceux de $X^{m-1}Q$. On commence par écrire la diagonale principale, dont les n premiers termes sont égaux à a_0, les m suivants à b_n ; puis au-dessous de chaque a_0 il y a un a_1, au-dessous de chaque a_i il y a un a_{i+1},.., jusqu'à a_m ; au-dessus de chaque b_n il y a un b_{n-1}, jusqu'à b_0, ensuite des 0. C'est la *matrice de* SYLVESTER des deux polynômes.

matrice de Sylvester

$$S = (s_{i,j}) = \begin{pmatrix} p_m & 0 & \cdots & 0 & q_n & 0 & \cdots & \cdots & 0 \\ \vdots & p_m & \ddots & \vdots & \vdots & q_n & \ddots & & \vdots \\ \vdots & \vdots & \ddots & 0 & \vdots & \vdots & \ddots & \ddots & \vdots \\ \vdots & \vdots & & p_m & \vdots & \vdots & & \ddots & 0 \\ \vdots & \vdots & & \vdots & q_0 & \vdots & & & q_n \\ p_0 & \vdots & & \vdots & 0 & q_0 & & & \vdots \\ 0 & p_0 & & \vdots & \vdots & 0 & \ddots & & \vdots \\ \vdots & 0 & \ddots & \vdots & \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & p_0 & 0 & \cdots & \cdots & 0 & q_0 \end{pmatrix}$$

Elle a $m+n$ lignes et autant de colonnes. Le déterminant de cette matrice est la *résultante* des deux polynômes, noté $R(P, Q)$.

résultante

Si P et Q avaient un diviseur commun D de degré $d \geq 1$ en X, ce qui est exclu par hypothèse, on aurait $P = P^*D$ et $Q = Q^*D$, P^* et Q^* étant de degré en X respectivement, inférieur ou égal à $m-1$ et $n-1$, donc appartenant à E_m, pour P^*, et E_n, pour Q^*. Alors $\phi(Q^*, P^*)$ serait nul, ϕ ne serait pas injective et $\det(S)$ serait nul.

PROPOSITION 0.9. — *Si P et Q sont des polynômes de $\overline{\mathbb{F}}_2[Y, Z][X]$ sans diviseurs communs, leur résultante $R(P, Q) \in \overline{\mathbb{F}}_2[Y, Z]$ n'est pas le polynôme nul.*

PROPOSITION 0.10. — *Soient $P(X, Y, Z)$ et $Q(X, Y, Z)$ de polynômes homogènes de degré m et n respectivement. Leur résultante $R(P, Q)$ est*

un polynôme homogène en (Y, Z) *de degré* mn*, et les assertions suivantes sont équivalentes :*

(a) il existe au moins un $a \in \overline{\mathbb{F}}_2$ *tel que* P *et* Q *s'annulent simultanément en le point* (a, b, c) *de* $P^2(\overline{\mathbb{F}}_2)$*,*

(b) $R(P, Q)$ *s'annule en* (b, c)*.*

Les points de $P^2(\overline{\mathbb{F}}_2)$ *en lesquels* P *et* Q *s'annulent simultanément sont en nombre fini.*

1. Survol historique

1.1. Préhistoire — L'idée de transmettre et de conserver l'information sous forme de suites de symboles est fort ancienne. Langages, de plus en plus élaborés, et gravures préhistoriques en témoignent. Plus récemment, les feux de colline en colline, les tam-tams africains, les sifflements stridents des Guanches (peuple autochtone des îles Canaries), les sémaphores, etc., ont assuré la transmission, l'écriture et la conservation.

Le fameux métier à tisser de l'ingénieur JACQUARD (1752-1834) utilise, ce qui est une première historique, un système de cartes perforées. Le télégraphe de l'ingénieur (et peintre) américain Samuel MORSE date de la même époque. La nature elle-même a mis au point, au cours de millions d'années, le code génétique, très longue suite dont les éléments (l'alphabet) sont les molécules d'adénine, de cytosine, de guanine et de thymine. Il assure à la fois la conservation et la transmission. La notion de message secret n'est pas non plus nouvelle. La cryptographie consiste à rendre un message indécodable, sauf pour son destinataire, et l'authentification, à vérifier une «signature» (numérique ou non), ce qui est fondamental pour la finance et le développement du commerce électronique.

1.2. Les débuts — L'arrivée de l'électronique a donné au traitement de l'information un prodigieux essor, en utilisant un alphabet binaire (formé des lettres 0 et de 1, appelés bits, contraction de «*binary unit*», unité binaire). Malheureusement, le canal de transmission peut introduire des erreurs, ou des paquets d'erreurs, dans les suites, et il est primordial de les détecter et de les corriger. Si la transmission s'effectue par un canal sûr, comme une ligne téléphonique (si l'on excepte les risques de foudre), il peut n'y avoir que de rares erreurs isolées, sans grande importance pour la parole, mais qui peuvent fausser des données numériques et des calculs. Pour les disques compacts, les erreurs proviennent des défauts et dépots de

surface, de l'usure, et apparaissent par paquets («*bursts*» en anglais). Pour les transmissions à très longue distance, les conditions atmosphériques, le vent solaire, les éruptions solaires, la faiblesse du signal reçu par rapport au bruit de fond local, amènent des paquets d'erreurs.

La première idée de correction, la longueur des suites étant fixée, consiste à les répéter un certain nombre de fois. Pour corriger une erreur, il faut envoyer trois fois le message : les suites 000, 100, 010 et 001 donneront 0, le 0 étant majoritaire, et les suites 111, 110, 101 et 110 se liront 1. Pour corriger n erreurs, il faut $2n + 1$ répétitions : la réflexion mathématique permet heureusement de faire beaucoup mieux.

Ayant besoin de corriger une erreur éventuelle sur chaque suite de longueur $7 = 2^3 - 1$, Richard HAMMING a inventé vers 1947, et publié en 1950, le code qui porte son nom [1.1,1.2], de décodage très rapide, et qui marque la naissance des codes correcteurs d'erreurs. Ce code est dit de *longueur sept*, ce qui est la longueur de ses mots, c'est-à-dire des suites appartenant au code. Il a $2^4 = 16$ mots, ce qui correspond à quatre bits d'information, le trois autres, de contrôle, permettant de détecter et de corriger une erreur. Un tel code est dit «*en blocs*».

longueur

code en blocs

Remarquons que l'adjonction d'un bit de parité à sept bits d'information, rendant pair le nombre de 1 dans le mot, permet de détecter la présence d'une erreur (la somme des coefficients étant alors égale à 1) sur un octet (huit bits formant un octet), mais non de la localiser et de la corriger.

La *distance de* HAMMING de deux mots quelconques est le nombre de coordonnées par lesquelles ils diffèrent. Elle est pour ce code au moins égale à trois, ce qui explique qu'il ne puisse corriger qu'une erreur : deux erreurs font passer du voisinage d'un mot à celui d'un autre mot.

distance de Hamming

Le décodage mathématique est très simple, et ici le petit nombre de réceptions possibles ($2^7 = 128$) autorise une méthode directe, consistant à regrouper les huit réceptions donnant le même mot du code à une erreur près. Ainsi, les réceptions :

$$1101000,\quad 0101000,\quad 1001000,\quad 1111000,$$
$$1100000,\quad 1101100,\quad 1101010,\quad 1101001,$$

donnent toutes le mot 1101000, en tête de liste, dont elles ne diffèrent, à partir de la deuxième, que par une coordonnée. Les 128 réceptions possibles

---

[1.1] R.W. Hamming : *Error detecting and error correcting codes*, Bell Syst. Tech. J., vol. 29, pp. 147-160 (1950).

[1.2] M. J. E. Golay : *Notes on digital coding*, Proc. IEEE, vol. 37, p. 657 (1949).

sont ainsi rassemblées en 16 classes disjointes, contenant chacune un et un seul mot du code. S'il y a deux erreurs sur le mot précédent, par exemple 1011000, la réception passe dans la classe du mot 1011100, et le décodage donne un résultat faux. Remarquons ici que toutes les réceptions possibles sont associées à un mot : le code est dit parfait.

code parfait

Les *codes de* HAMMING , généralisant le précédent, ont été construits par J. E. GOLAY. Ils sont, en binaire, de longueur $2^k - 1$, et corrigent une erreur. Certains sont encore utilisés de nos jours dans des domaines où les erreurs sont statistiquement rares et isolées, par exemple par France-Télécom (téléphone numérique, Minitel).

code de Hamming

Pendant que Hamming mettait au point son code et la technologie associée, d'une part, Claude Elwood SHANNON, qui travaillait dans le même bureau des Bell Labs, élaborait la théorie de l'information [1.3] ,[1.4], et d'autre part, l'équipe de William SHOCKLEY, également aux Bell Labs, inventait le transistor.

La théorie de SHANNON annonce la possibilité de corriger une réception entachée d'erreur, pourvu que l'erreur soit inférieure à la partie utile. Ceci fournit une borne à l'efficacité.

Quant au transistor, selon qu'il laisse ou non passer le courant, il permet la transmission physique des bits.

Ces trois inventions simultanées ont assuré, avec la miniaturisation des circuits, le prodigieux développement de l'informatique et de la communication.

Considérons un code de longueur n, ayant 2^k mots, et de distance d (deux quelconques de ses mots ont au moins d de leurs coordonnées qui diffèrent). Ce code peut corriger au plus $(d-1)/2$ erreurs, car plus d'erreurs donnent une réception plus proche, ou aussi proche, d'un autre mot, comme nous l'avons remarqué pour le code de HAMMING. Le rendement de ce code est égal à k/n, et son taux de correction à d/n.

1.3. Les années cinquante — Dans un domaine de communication donné, le choix du code se fait d'après les besoins et les contraintes : fréquence des erreurs, vitesse de transmission, nécessité d'avoir le résultat

---

[1.3] C. E. Shannon : *A mathematical theory of communication*, Bell Syst. Tech. J., vol. 27, pp. 379-423, 623-656 (1948).

[1.4] C. E. Shannon : *Communication in presence of noise* IEEE, vol. 37 : pp. 10-21 (1949).