Université Pierre et Marie Curie
Cours de cryptographie MM029 - 2009/10
Alain Kraus

Chapitre III - Corps finis

Nous admettrons que tout corps fini est commutatif. Ce résultat a été établi en 1905 par Wedderburn. Les premiers exemples de corps finis sont les quotients de l'anneau $\mathbb{Z}$

$$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z},$$

où p est un nombre premier. D'autres exemples sont fournis par les quotients

$$\mathbb{F}_p[X]/(F),$$

où F est un polynôme irréductible de $\mathbb{F}_p[X]$. Un tel corps est de cardinal p^d, où d est le degré de F. Nous reviendrons sur ce point, et démontrerons que l'on obtient de la sorte tous les corps finis. On établira que pour tout nombre premier p et tout entier $n \geq 1$, il existe un corps à p^n éléments et qu'il est unique à isomorphisme près. On abordera par ailleurs le problème du logarithme discret, qui est très important en cryptographie.

Table des matières

1. Rappels sur l'anneau $K[X]$ et ses quotients

Soient K un corps commutatif et $K[X]$ l'anneau des polynômes à coefficients dans K. Pour tout $F \in K[X]$, notons $\deg(F)$ son degré. Rappelons que le degré du polynôme nul est « moins l'infini », qui est par définition un élément plus petit que tout entier naturel,

satisfaisant aux règles usuelles d'addition. Le groupe des éléments inversible de $K[X]$ est K^* (l'ensemble des polynômes de degré 0). L'anneau $K[X]$ est euclidien, avec l'application degré comme stathme euclidien. Autrement dit, $K[X]$ est un anneau intègre et pour tous A et B dans $K[X]$ avec $B \neq 0$, il existe un unique couple de polynômes (Q, R), tels que

$$A = BQ + R \quad \text{avec} \quad \deg(R) < \deg(B).$$

On dit que Q est le quotient et que R est le reste de la division euclidienne de A par B. Un polynôme est dit unitaire si son coefficient de plus haut degré vaut 1. On déduit du lemme 0.9 que $K[X]$ est un anneau principal. En particulier :

Proposition 3.1. *Soit I un idéal non nul de $K[X]$. Il existe un unique polynôme unitaire P de $K[X]$ tel que l'on ait $I = (P)$.*

Le pgcd de deux polynômes A et B, non tous les deux nuls, est l'unique polynôme unitaire $D \in K[X]$ tel que

$$(D) = (A) + (B).$$

Il existe donc U et V dans $K[X]$ tels que $D = AU + BV$ (relation de Bézout). La détermination de D et de relations de Bézout entre A et B s'effectue, comme dans $\mathbb{Z}$, avec l'algorithme d'Euclide étendu, qui vaut dans ce cadre sans modifications. On dit que A et B sont premiers entre eux si leur pgcd est 1. Tel est le cas si et seulement si il existe U et V dans $K[X]$ tels que $AU + BV = 1$. Il en résulte que si F, G, H sont des polynômes non nuls de $K[X]$ tels que F divise GH et que F soit premier avec G, alors F divise H (théorème de Gauss).

Définition 3.1. *Un polynôme de $K[X]$ est dit irréductible (dans $K[X]$, ou sur K), si son degré est supérieur ou égal à 1 et si l'ensemble de ses diviseurs est formé des éléments non nuls de K et des polynômes qui lui sont associés* [(1)].

Un polynôme $P \in K[X]$ de degré ≥ 1 est irréductible s'il ne possède pas de diviseur $Q \in K[X]$ tel que $1 \leq \deg(Q) \leq \deg(P) - 1$. Deux polynômes irréductibles de $K[X]$ sont premiers entre eux ou associés. Un polynôme qui n'est pas irréductible est dit réductible.

Soit $\mathbb{P}$ l'ensemble des polynômes irréductibles unitaires de $K[X]$. Comme dans le cas de l'anneau $\mathbb{Z}$, on dispose du théorème fondamental de l'arithmétique de $K[X]$.

Théorème 3.1. *Soit P un polynôme non nul de $K[X]$. Alors P s'écrit de manière unique sous la forme*

$$P = \lambda \prod_{F \in \mathbb{P}} F^{n_F}, \tag{1}$$

[(1)] Rappelons que deux polynômes F et G de $K[X]$ sont dits associés s'il existe $\lambda \in K^*$ tel que $F = \lambda G$. La définition 3.1 est un cas particulier de la notion générale d'élément irréductible dans un anneau commutatif.

où $\lambda \in K$, et où les n_F sont des entiers naturels nuls sauf un nombre fini d'entre eux.

Démonstration : Prouvons l'assertion d'existence. L'énoncé est vrai si le degré de P est nul, auquel cas on prend $\lambda = P$ et tous les n_F nuls. Considérons un entier $n \geq 1$. Supposons que l'on ait une décomposition de la forme (1) pour les polynômes non nuls de degré $\leq n-1$ et que $\deg(P) = n$. Soit E l'ensemble des diviseurs de P de degré ≥ 1. Il n'est pas vide car P est dans E. Il existe donc un élément $Q \in E$ de degré minimum. Ce polynôme est irréductible. Il existe $R \in K[X]$ tel que $P = QR$ et $\deg(R) \leq n-1$. D'après l'hypothèse de récurrence, R possède une décomposition de la forme (1). Il en est donc de même de P, d'où l'assertion d'existence. On admettra ici l'unicité.

Rappelons que si P est un polynôme et a un élément de K, on dit que a est racine de P si l'on a $P(a) = 0$, autrement dit, si la fonction polynôme associée à P s'annule en a. Tel est le cas si et seulement si $X - a$ divise P. De plus, si P est de degré n, alors P possède au plus n racines dans K. En effet, on vérifie en utilisant le théorème de Gauss, que si P possédait au moins $n+1$ racines, il serait divisible par un polynôme de degré $n+1$.

Passons maintenant aux quotients de $K[X]$. Considérons un idéal I de $K[X]$. Pour tout $P \in K[X]$, posons $\overline{P} = P + I$ la classe de P modulo I. C'est le sous-ensemble de $K[X]$ formé des polynômes Q tels que $P - Q$ appartienne à I. On sait déjà que $K[X]/I$ est muni de la structure d'anneau définie par les égalités

$$\overline{P} + \overline{Q} = \overline{P+Q} \quad \text{et} \quad \overline{P}\,\overline{Q} = \overline{PQ}.$$

On munit de plus $K[X]/I$ d'une structure de K-espace vectoriel, via la loi externe

$$K \times K[X]/I \to K[X]/I$$

qui au couple $(\lambda, \overline{P}) \in K \times K[X]/I$ associe $\overline{\lambda P}$. Par définition, on a donc l'égalité

$$\lambda \overline{P} = \overline{\lambda P}.$$

On vérifie que cette définition a bien un sens, autrement dit, qu'elle ne dépend que de la classe de P et pas d'un de ses représentants. Pour tous $\lambda \in K$ et $P \in K[X]$, on a

$$(\lambda + I)(P + I) = \lambda P + I = \lambda(P + I).$$

De plus, si I est distinct de $K[X]$, le corps K est isomorphe à un sous-anneau de $K[X]/I$, via l'application qui à $\lambda \in K$ associe $\lambda + I$.

Proposition 3.2. *Soit P un polynôme non nul de $K[X]$ degré n. Posons $\alpha = X + (P)$ dans $K[X]/(P)$.*

1) Le K-espace vectoriel $K[X]/(P)$ est de dimension finie n, dont une base est le système $\left(1, \alpha, \cdots, \alpha^{n-1}\right)$.

2) Posons $P = a_0 + a_1X + \cdots + a_nX^n$ ($a_i \in K$). On a l'égalité

$$\sum_{i=0}^{n} a_i\alpha^i = 0. \tag{2}$$

Démonstration : Vérifions que $\left(1, \alpha, \cdots, \alpha^{n-1}\right)$ est un système libre. Soient λ_i des éléments de K tels que

$$\sum_{i=0}^{n-1} \lambda_i\alpha^i = 0.$$

Cette égalité signifie que l'on a

$$\sum_{i=0}^{n-1} \lambda_i X^i \in (P).$$

Puisque P est de degré n, cela entraîne que tous les λ_i sont nuls. Démontrons que le système considéré est générateur. Soit ξ un élément de $K[X]/(P)$. Il existe $F \in K[X]$ tel que $\xi = F+(P)$. On a $P \neq 0$. Il existe donc Q et R dans $K[X]$ tels que l'on ait $F = PQ+R$ avec $\deg(R) < n$, d'où $\xi = \overline{R}$ et notre assertion.
Par ailleurs, on a $\overline{P} = 0$, autrement dit, on a

$$\sum_{i=0}^{n} \overline{a_iX^i} = \sum_{i=0}^{n} a_i\overline{X}^i = 0,$$

d'où l'égalité (2).

Le résultat qui suit concerne la structure d'anneau de $K[X]/(P)$, qui n'est autre que l'analogue du lemme 1.8 sur la description des éléments inversibles des quotients de $\mathbb{Z}$.

Proposition 3.3. *Soit P un polynôme de $K[X]$. Le groupe des éléments inversibles de l'anneau $K[X]/(P)$ est formé des classes de polynômes qui sont premiers avec P.*

Démonstration : Soit F un polynôme de $K[X]$ premier avec P. Il existe U et V dans $K[X]$ tels que $UP+VF = 1$. On a $\overline{V}\ \overline{F} = 1$, donc $\overline{F}$ est inversible. Inversement, soit $\overline{F}$ un élément inversible de $K[X]/(P)$. Il existe $Q \in K[X]$ tel que $\overline{F}\ \overline{Q} = 1$. Cette égalité signifie que $FQ - 1$ appartient à (P), autrement dit qu'il existe $U \in K[X]$ tel que $FQ + UP = 1$, donc F et P sont premiers entre eux.

Corollaire 3.1. *Soit P un polynôme non nul de $K[X]$. Les conditions suivantes sont équivalentes :*

1) l'anneau $K[X]/(P)$ est intègre.

2) Le polynôme P est irréductible dans $K[X]$.

3) L'anneau $K[X]/(P)$ est un corps.

Démonstration : Supposons que $K[X]/(P)$ soit intègre. Tout d'abord, P n'est pas inversible, sinon on a $(P) = K[X]$ et $K[X]/(P)$ est l'anneau nul, ce qui est exclu par définition. On a donc $\deg(P) \geq 1$. Soit F un diviseur de P. Il s'agit de montrer que F est inversible ou bien que F et P sont associés. Il existe $Q \in K[X]$ tel que $P = FQ$, d'où $\overline{F}\,\overline{Q} = 0$. Par hypothèse, cela entraîne que $\overline{F} = 0$ ou $\overline{Q} = 0$. Si $\overline{F} = 0$, alors F est dans (P) i.e. P divise F. Par suite, P et F sont associés. Si $\overline{Q} = 0$, alors Q et P sont associés, d'où $\deg(F) = 0$ i.e. F est inversible. Cela prouve que P est irréductible dans $K[X]$. Supposons alors P irréductible dans $K[X]$ et prouvons que tout élément non nul $\overline{F}$ de $K[X]/(P)$ est inversible. Puisque P est irréductible et que P ne divise pas F, les polynômes F et P sont premiers entre eux. D'après la proposition 3.3, $\overline{F}$ est donc inversible, donc $K[X]/(P)$ est un corps. La dernière implication est immédiate.

2. Caractéristique d'un anneau

Soit A un anneau. Notons 1_A l'élément neutre multiplicatif de A. Soit $f : \mathbb{Z} \to A$ l'application de $\mathbb{Z}$ dans A définie par

$$f(m) = m1_A \quad \text{pour tout } m \in \mathbb{Z}. \tag{3}$$

C'est un morphisme d'anneaux (et d'ailleurs le seul). Son noyau est un idéal de $\mathbb{Z}$. Il existe donc un unique entier naturel n tel que l'on ait

$$\mathrm{Ker}(f) = n\mathbb{Z}.$$

Définition 3.2. *L'entier n est la caractéristique de A.*

Lemme 3.1. *Si A est intègre, sa caractéristique est nulle ou est un nombre premier. Tel est en particulier le cas si A est un corps commutatif.*

Démonstration : L'anneau $\mathbb{Z}/n\mathbb{Z}$ est isomorphe à un sous-anneau de A, à savoir l'image de f. Puisque A est intègre, il en est de même de $\mathbb{Z}/n\mathbb{Z}$. Si n n'est pas nul, $\mathbb{Z}/n\mathbb{Z}$ est un corps, et n est premier.

Théorème 3.2. *Soit K un corps commutatif d'élément neutre multiplicatif 1_K. Soit m un entier relatif.*

1) Supposons K de caractéristique zéro. On a $m1_K = 0$ si et seulement si $m = 0$. Dans ce cas, K contient un unique sous-corps isomorphe à $\mathbb{Q}$.

2) Supposons K de caractéristique un nombre premier p. On a $m1_K = 0$ si et seulement si p divise m. Dans ce cas, K contient un unique sous-corps isomorphe à $\mathbb{F}_p$.

Démonstration : Supposons K de caractéristique 0. Le morphisme $f : \mathbb{Z} \to K$ défini par (3) est alors injectif, d'où la première équivalence. L'application de $\mathbb{Q}$ dans K qui à

$a/b \in \mathbb{Q}$ associe $a1_K(b1_K)^{-1}$, prolonge f de $\mathbb{Z}$ à $\mathbb{Q}$, et est un morphisme de corps (notons que b étant non nul, on a $b1_K \neq 0$, et l'on vérifie que cette application est bien définie). Son image est donc un sous-corps de K isomorphe à $\mathbb{Q}$. Par ailleurs, soient Q_1 et Q_2 deux sous-corps de K isomorphes à $\mathbb{Q}$. L'intersection $Q_1 \cap Q_2$ est un sous-corps de Q_1 et de Q_2. Puisque $\mathbb{Q}$ ne contient pas de sous-corps autres que lui-même, tel est aussi le cas de Q_1 et Q_2, d'où $Q_1 \cap Q_2 = Q_1 = Q_2$, et l'unicité annoncée. Si K est de caractéristique p, le noyau de f est l'idéal $p\mathbb{Z}$. Par suite, on a $m1_K = 0$ i.e. m appartient au noyau de f si et seulement si p divise m. L'image de f est un sous-corps de K isomorphe à $\mathbb{F}_p$. L'unicité d'un tel sous-corps résulte du fait que $\mathbb{F}_p$ n'a pas d'autres sous-corps que lui-même.

Les corps $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sont de caractéristique 0. Pour tout p premier, $\mathbb{F}_p$ est de caractéristique p.

Corollaire 3.2. *Soit K un corps fini. La caractéristique de K est un nombre premier p et K contient un unique sous-corps isomorphe à $\mathbb{F}_p$. De plus, il existe un entier $n \geq 1$ tel que le cardinal de K soit p^n.*

Démonstration : Puisque K est fini, K ne contient pas de sous-corps isomorphe à $\mathbb{Q}$. La caractéristique de K est donc un nombre premier p et K contient un unique sous-corps isomorphe à $\mathbb{F}_p$. Par suite, K est naturellement muni d'une structure d'espace vectoriel sur $\mathbb{F}_p$. Le corps K étant fini, la dimension de K sur $\mathbb{F}_p$ est finie. Si n est cette dimension, K est isomorphe (comme espace vectoriel) à $\mathbb{F}_p^n$, et K est de cardinal p^n.

Corollaire 3.3. *Soit K un corps fini de cardinal p. Alors K est isomorphe à $\mathbb{F}_p$.*

Démonstration : C'est immédiat vu que K contient un sous-corps isomorphe à $\mathbb{F}_p$.

Corollaire 3.4. *Soient K un corps fini et F un polynôme irréductible de degré n dans $K[X]$. L'anneau $K[X]/(F)$ est un corps fini, de même caractéristique que K, et son cardinal est $|K|^n$.*

Démonstration : L'anneau $K[X]/(F)$ est un corps (cor. 3.1). Il contient un sous-corps isomorphe à K, donc sa caractéristique est la même que celle de K. Le K-espace vectoriel $K[X]/(F)$ étant de dimension n (prop. 3.2), il est isomorphe à K^n, d'où l'assertion.

3. Groupe multiplicatif d'un corps fini

Théorème 3.3. *Soient K un corps commutatif et H un sous-groupe fini de K^*. Alors, H est un groupe cyclique.*

Démonstration : C'est une conséquence directe du lemme 1.12, car pour tout entier $d \geq 1$, le polynôme $X^d - 1 \in K[X]$ possède au plus d racines dans K.

Parce que tout corps fini est commutatif, on obtient :

Corollaire 3.5. *Si K est un corps fini, le groupe multiplicatif K^* est cyclique.*

Compte tenu du théorème 1.10, on obtient l'énoncé suivant :

Corollaire 3.6. *Soit K un corps fini de cardinal q. Le groupe K^* possède exactement $\varphi(q-1)$ générateurs, où φ est la fonction indicatrice d'Euler. De plus, si α est un générateur de K^*, alors l'ensemble des générateurs de K^* est*

$$\Big\{\alpha^k \;\Big|\; 1 \leq k \leq q-1 \text{ et } \operatorname{pgcd}(k, q-1) = 1\Big\}.$$

Exemple 3.1. Considérons le polynôme $F = X^3 + X + 1 \in \mathbb{F}_5[X]$. Posons

$$K = \mathbb{F}_5[X]/(F).$$

Le polynôme F est irréductible sur $\mathbb{F}_5$, car il est de degré 3 et n'a pas de racines dans $\mathbb{F}_5$, donc K est un corps. Sa caractéristique est 5 et son cardinal est $5^3 = 125$. Le groupe K^* est cyclique d'ordre 124. Les ordres possibles de ses éléments sont $1, 2, 4, 31, 62$ et 124. Il possède soixante générateurs. Soit α la classe de X modulo (F). Le système $(1, \alpha, \alpha^2)$ est une base de K sur $\mathbb{F}_5$.
Vérifions que 2α est un générateur de K^*. On a

$$\alpha^3 = -1 - \alpha \quad \text{et} \quad \alpha^5 = 1 + \alpha - \alpha^2.$$

Puisque K est de caractéristique 5, il en résulte que l'on a

$$\alpha^{15} = -(1+\alpha)^5 = -1 - \alpha^5 = \alpha^2 - \alpha - 2,$$

d'où les égalités

$$\alpha^{30} = \alpha^2 + 1 \quad \text{et} \quad \alpha^{31} = -1.$$

Ainsi, α est d'ordre 62. Par ailleurs, on a $2^4 \equiv 1$ mod. 5 et $2^{31} \equiv 3$ mod. 5, d'où $(2\alpha)^{31} = 2$ et $(2\alpha)^{62} = -1$, ce qui entraîne notre assertion.

4. Corps finis comme quotients de $\mathbb{F}_p[X]$

Théorème 3.4. *Soit K un corps fini de cardinal p^n. Il existe un polynôme $F \in \mathbb{F}_p[X]$ de degré n irréductible sur $\mathbb{F}_p$, tel que les corps K et $\mathbb{F}_p[X]/(F)$ soient isomorphes.*

Démonstration : Soit α un générateur de K^*. Considérons l'application

$$\psi : \mathbb{F}_p[X] \to K$$

définie pour tout $P = \sum a_i X^i \in \mathbb{F}_p[X]$ par l'égalité

$$\psi(P) = \sum a_i \alpha^i,$$

où l'on identifie ici $a_i \in \mathbb{F}_p$ avec n'importe quel entier relatif dont la classe modulo p est a_i. Cela est licite car K est de caractéristique p. C'est un morphisme d'anneaux. Il est surjectif car α est un générateur de K^*. Le noyau de ψ est un idéal non nul I de $\mathbb{F}_p[X]$ et $\mathbb{F}_p[X]/I$ est un anneau isomorphe à K. Il existe $F \in \mathbb{F}_p[X]$ non nul tel que $I = (F)$ (prop. 3.1). Puisque $\mathbb{F}_p[X]/(F)$ est un corps, F est irréductible sur $\mathbb{F}_p$. Si m est le degré de F, le cardinal de $\mathbb{F}_p[X]/(F)$ est p^m. C'est le cardinal de K, d'où $m = n$ et le résultat.

Les corps finis de cardinal p^n s'obtiennent donc exclusivement à partir des polynômes irréductibles de degré n dans $\mathbb{F}_p[X]$. Autrement dit :

Proposition 3.4. *Soient p un nombre premier et n un entier ≥ 1. Les deux assertions suivantes sont équivalentes :*

1) il existe un corps à p^n éléments.

2) Il existe un polynôme irréductible de degré n dans $\mathbb{F}_p[X]$.

Il s'agit maintenant de démontrer l'existence de polynômes irréductibles de tout degré $n \geq 1$ dans $\mathbb{F}_p[X]$, et ensuite de prouver que si U et V sont des polynômes irréductibles de degré n dans $\mathbb{F}_p[X]$, alors les corps $\mathbb{F}_p[X]/(U)$ et $\mathbb{F}_p[X]/(V)$ sont isomorphes (unicité à isomorphisme près des corps à p^n éléments).

5. Polynômes irréductibles sur un corps fini

On va établir le résultat suivant :

Théorème 3.5. *Soient K un corps fini de cardinal q et n un entier naturel non nul. L'ensemble des diviseurs irréductibles du polynôme $X^{q^n} - X \in K[X]$ est formé des polynômes irréductibles de $K[X]$ de degré divisant n. Plus précisément, on a l'égalité*

$$X^{q^n} - X = \prod F, \tag{4}$$

où F parcourt l'ensemble des polynômes irréductibles unitaires de $K[X]$ de degré divisant n.

La démonstration repose sur plusieurs lemmes intermédiaires, qui sont par eux mêmes intéressants d'un point de vue pratique. On suppose dans ce qui suit que K est un corps fini de caractéristique p et de cardinal q (qui est donc une puissance de p).

Lemme 3.2. *Soit k un entier naturel. Pour tous x et y dans K on a*

$$(x+y)^{p^k} = x^{p^k} + y^{p^k}.$$

Démonstration : L'énoncé est vrai si $k = 0$. Soit k un entier ≥ 0 tel que l'égalité annoncée soit vérifiée. Pour tous $x, y \in K$, on a

$$(x+y)^{p^{k+1}} = \left((x+y)^{p^k}\right)^p = \left(x^{p^k} + y^{p^k}\right)^p.$$

Pour tout entier $j = 1, \cdots, p-1$, le coefficient binômial C_p^j est divisible par p. La formule du binôme de Newton entraîne alors l'égalité $(x+y)^{p^{k+1}} = x^{p^{k+1}} + y^{p^{k+1}}$.

Lemme 3.3. *Soit L un corps fini contenant K.*

1) Pour tout $x \in L$, x appartient à K si et seulement si on a $x^q = x$.

2) Pour tout $F \in L[X]$, F appartient à $K[X]$ si et seulement si on a $F(X^q) = F(X)^q$.

Démonstration : 1) Soit x un élément de L. Si x est dans K^*, vu que K^* est un groupe d'ordre $q-1$, on a $x^{q-1} = 1$, d'où $x^q = x$. Par ailleurs, le polynôme $X^q - X \in L[X]$ possède au plus q racines, donc K est l'ensemble de ses racines, d'où l'assertion 1.

2) Soit $F = \sum a_k X^k$ un polynôme de $L[X]$. On a

$$F(X)^q = \Big(\sum a_k X^k\Big)^q = \sum a_k^q X^{kq}.$$

Cette dernière égalité se démontre comme le lemme 3.2 en procédant par récurrence sur le nombre de monômes de F. D'après la première assertion, F appartient à $K[X]$ si et seulement si $a_k^q = a_k$ pour tout k, d'où le résultat.

Lemme 3.4. *Soient F un polynôme unitaire irréductible de $K[X]$ et L un corps fini contenant K dans lequel F a une racine α. Il existe un plus petit entier $r \geq 1$ tel que l'on ait $\alpha^{q^r} = \alpha$. On a $r = \deg(F)$ et l'égalité*

$$F = \prod_{i=0}^{r-1} \Big(X - \alpha^{q^i}\Big).$$

Démonstration : Il existe un entier $m \geq 1$ tel que le cardinal de L soit q^m. On a $\alpha^{q^m} = \alpha$, donc il existe un plus petit entier $r \geq 1$ tel que l'on ait $\alpha^{q^r} = \alpha$. Par ailleurs, α étant racine de F, on déduit du lemme 3.3 que les éléments α^{q^i} pour $i = 1, \cdots, r-1$ sont aussi des racines de F. Posons

$$G = \prod_{i=0}^{r-1} \Big(X - \alpha^{q^i}\Big).$$

Puisque les α^{q^i} pour $i = 0, \cdots, r-1$ sont distincts deux à deux[(2)], il en résulte que G divise F dans $L[X]$. De plus, on a les égalités

---

[(2)] On peut justifier cette assertion comme suit. Supposons qu'il existe deux entiers i et j compris entre 0 et $r-1$ tels que $i < j$ et $\alpha^{q^i} = \alpha^{q^j}$. On a alors l'égalité

$$\left(\frac{\alpha^{q^{j-i}}}{\alpha}\right)^{q^i} = 1.$$

Il s'agit d'en déduire que $\alpha^{q^{j-i}} = \alpha$, ce qui conduira à une contradiction vu le caractère

$$G(X)^q = \prod_{i=0}^{r-1}\left(X - \alpha^{q^i}\right)^q = \prod_{i=0}^{r-1}\left(X^q - \alpha^{q^{i+1}}\right) = G(X^q).$$

Par suite, G appartient à $K[X]$ (lemme 3.3). Le quotient et le reste de la division euclidienne de F par G étant indépendants du corps de base, vu leur caractère d'unicité, on en déduit que G divise F dans $K[X]$. Le polynôme F étant irréductible, G étant de degré au moins 1, et F et G étant unitaires, on a donc $F = G$, d'où le résultat.

Remarque 3.1. Le lemme 3.4 montre qu'un polynôme irréductible F de $K[X]$ qui a une racine dans un surcorps fini L de K, a toutes ses racines dans L. De plus, si r est le degré de F, et si $\alpha \in L$ est une racine de F, alors les racines de F sont les α^{q^i} pour $i = 0, \cdots, r-1$.

Fin de la démonstration du théorème 3.5.

Soit $F \in K[X]$ un polynôme irréductible unitaire de degré r. Il s'agit de démontrer l'équivalence suivante :

$$F \text{ divise } X^{q^n} - X \iff r \text{ divise } n. \tag{5}$$

Considérons un corps fini L contenant K dans lequel F a une racine α : un tel corps L existe[(3)]. D'après le lemme 3.4, r est le plus petit entier ≥ 1 tel que $\alpha^{q^r} = \alpha$ et on a

$$F = \prod_{i=0}^{r-1}\left(X - \alpha^{q^i}\right). \tag{6}$$

Par ailleurs, on a

$$\alpha^{q^{ir}} = \alpha \quad \text{pour tout } i \in \mathbb{N}. \tag{7}$$

En effet, cette égalité est vraie si $i = 0$, et si elle est vérifiée pour un entier $i \geq 0$, on a

$$\alpha^{q^{(i+1)r}} = \left(\alpha^{q^{ir}}\right)^{q^r} = \alpha^{q^r} = \alpha.$$

---

minimal de r. Tout revient ainsi à démontrer que pour tout $y \in L$, l'égalité $y^q = 1$ entraîne $y = 1$. Les entiers q et $q^m - 1$ étant premiers entre eux, il existe u et v dans $\mathbb{Z}$ tels que l'on ait $uq + v(q^m - 1) = 1$. Pour tout $y \in L$, on a $y^{q^m - 1} = 1$. Par suite, si $y^q = 1$, on obtient $y = y^{uq + v(q^m - 1)} = 1$, et notre assertion.

(3) L'anneau $K[X]/(F)$ est un corps fini qui contient un sous-corps isomorphe à K. En identifiant K et ce sous-corps, on peut alors prendre $L = K[X]/(F)$. Si α est la classe de X modulo (F), on a $F(\alpha) = 0$ (prop. 3.2). Cette identification n'a pas d'importance pour obtenir le théorème 3.5. Cela étant, si l'on souhaite un corps L contenant K au sens strict du terme, on peut prendre pour L la réunion de K et du complémentaire de l'image de K dans $K[X]/(F)$. Cet ensemble est canoniquement en bijection avec $K[X]/(F)$. Par transport de structure on munit alors L d'une structure de corps, contenant K comme sous-corps, et F a une racine dans L.

Supposons alors que F divise $X^{q^n} - X$. Puisque $F(\alpha) = 0$, on a $\alpha^{q^n} = \alpha$. Il existe deux entiers naturels t et s tels que l'on ait $n = rt + s$ avec $0 \leq s < r$. On a donc

$$\alpha^{q^n} = \left(\alpha^{q^{tr}}\right)^{q^s}.$$

D'après (7), on a $\alpha^{q^{tr}} = \alpha$. Par suite, on a $\alpha = \alpha^{q^s}$, ce qui d'après le caractère minimal de r, entraîne $s = 0$, ainsi r divise n.
Inversement, supposons que r divise n. On déduit de (7) que l'on a $\alpha^{q^n} = \alpha$, autrement dit, que α est racine du polynôme $X^{q^n} - X$. Les éléments

$$\alpha, \alpha^q, \cdots, \alpha^{q^{r-1}},$$

sont donc des racines deux à deux distinctes de $X^{q^n} - X$. Il résulte de (6) que F divise $X^{q^n} - X$ dans $L[X]$, donc aussi dans $K[X]$ car F est à coefficients dans K. Cela prouve l'équivalence (5).

On déduit de (5) que l'on a une égalité de la forme

$$X^{q^n} - X = \prod_F F^{n_F},$$

où F parcourt l'ensemble des polynômes irréductibles unitaires de $K[X]$ de degré divisant n, et où les n_F sont des entiers naturels non nuls. Tout revient alors à démontrer que les n_F sont égaux à 1. Étant donné un tel polynôme F, on a $X^{q^n} - X = F^{n_F} Q$ où $Q \in K[X]$, d'où l'on déduit, en considérant les polynômes dérivés des deux membres de cette égalité (on a $q1_K = 0$ car K est de caractéristique p),

$$-1 = n_F F^{n_F - 1} F' Q + F^{n_F} Q'.$$

Par suite, $F^{n_F - 1}$ divise -1 dans $K[X]$, d'où $n_F = 1$ et le résultat.

Exemples 3.2.

1) La décomposition de $X^8 - X \in \mathbb{F}_2[X]$ en produit de polynômes irréductibles sur $\mathbb{F}_2$ est donnée par l'égalité

$$X^8 - X = X(X+1)(X^3 + X + 1)(X^3 + X^2 + 1).$$

2) De même, on vérifie que la décomposition de $X^9 - X \in \mathbb{F}_3[X]$ en produit de polynômes irréductibles unitaires sur $\mathbb{F}_3$ est

$$X^9 - X = X(X+1)(X+2)(X^2+1)(X^2+X+2)(X^2+2X+2).$$

6. Théorème d'existence et dénombrement

On considère dans ce paragraphe un corps fini K de cardinal q.

Notation. Pour tout $n \geq 1$, notons $I_n(q)$ le nombre de polynômes irréductibles unitaires de degré n dans $K[X]$.

La formule (4) permet de calculer $I_n(q)$. En effet, dans le produit intervenant dans (4), pour chaque diviseur d de n il y a $I_d(q)$ facteurs de degré d. En considérant les degrés des polynômes de chaque membre, on obtient

$$q^n = \sum_{d|n} I_d(q) d. \tag{8}$$

Le théorème d'existence des corps finis est une conséquence de l'énoncé suivant :

Théorème 3.6. *Pour tout $n \geq 1$, on a $I_n(q) > 0$.*

Démonstration : Considérons un entier $n \geq 1$. Pour tout entier d tel que $1 \leq d \leq n$, on a (cf. (8))

$$q^d = dI_d(q) + \sum_{d'|d,\ d'<d} d' I_{d'}(q),$$

par suite on a

$$dI_d(q) \leq q^d.$$

D'après la formule

$$q^n = nI_n(q) + \sum_{d|n,\ d<n} dI_d(q),$$

on obtient ainsi

$$q^n \leq nI_n(q) + \sum_{d|n,\ d<n} q^d \leq nI_n(q) + \sum_{k=0}^{n-1} q^k = nI_n(q) + \frac{q^n - 1}{q - 1} < nI_n(q) + q^n,$$

d'où $I_n(q) > 0$ et le résultat.

Corollaire 3.7. *Pour tout entier $n \geq 1$ et tout nombre premier p, il existe un corps de cardinal p^n.*

Démonstration : C'est une conséquence directe du théorème 3.6, appliqué avec $q = p$, et de la proposition 3.4.

On va maintenant établir une formule permettant de calculer directement $I_n(q)$. Il nous faut pour cela démontrer une formule d'inversion, que l'on appelle la formule d'inversion de Möbius. Définissons d'abord ce que l'on appelle la fonction de Möbius.

Définition 3.3. *La fonction de Möbius* $\mu : \mathbb{N} \to \{0, \pm 1\}$ *est définie pour tout* $n \in \mathbb{N}$ *par les égalités*

$$\mu(n) = \begin{cases} (-1)^r & \text{si } n \text{ est le produit de } r \text{ nombres premiers distincts} \\ 0 & \text{sinon.} \end{cases}$$

Notons que l'on a $\mu(1) = 1$. Vérifions que pour tout $n \geq 1$, on a la formule

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{sinon.} \end{cases} \tag{9}$$

Supposons $n \geq 2$. Considérons la décomposition en facteurs premiers de n,

$$n = p_1^{n_1} \cdots p_r^{n_r}$$

avec des entiers $n_i \geq 1$, les p_i étant des nombres premiers distincts deux à deux. Parmi les diviseurs de n, seuls ceux qui sont sans facteurs carrés ont une contribution non nulle dans la somme des $\mu(d)$. Par suite, on a

$$\sum_{d|n} \mu(d) = C_r^0 - C_r^1 + \cdots + (-1)^r C_r^r = (1-1)^r = 0,$$

d'où la relation (9).

On va établir l'énoncé suivant :

Théorème 3.7. *Pour tout* $n \geq 1$*, on a l'égalité*

$$nI_n(q) = \sum_{d|n} \mu(d)\ q^{\frac{n}{d}}. \tag{10}$$

C'est une conséquence directe de la formule (8) et du résultat qui suit, connu sous le nom de formule d'inversion de Möbius.

Théorème 3.8. *Soient* G *un groupe abélien additif et* f *une fonction de* $\mathbb{N}^*$ *à valeurs dans* G*. Soit* $g : \mathbb{N}^* \to G$ *la fonction définie pour tout* $n \in \mathbb{N}^*$ *par l'égalité*

$$g(n) = \sum_{d|n} f(d).$$

Alors, pour tout $n \in \mathbb{N}^*$*, on a*

$$f(n) = \sum_{d|n} \mu(d) g\Big(\frac{n}{d}\Big). \tag{11}$$

Remarque 3.2. L'application $d \mapsto \frac{n}{d}$ permute entre eux les diviseurs de n. Ainsi, la formule (11) s'écrit aussi

$$f(n) = \sum_{d|n} \mu\Big(\frac{n}{d}\Big) g(d).$$

Démonstration : Soit n un entier naturel non nul. Pour tout $r \geq 1$, posons

$$\delta(r) = \sum_{k|r} \mu(k).$$

D'après la formule (9), on a l'égalité

$$f(n) = \sum_{d|n} \delta(d) f\Big(\frac{n}{d}\Big),$$

autrement dit,

$$f(n) = \sum_{d|n} \sum_{k|d} \mu(k) f\Big(\frac{n}{d}\Big).$$

Pour chaque diviseur k de n, posons

$$S_k = \Big\{ d \geq 1 \;\Big|\; k|d \text{ et } d|n \Big\}.$$

L'ensemble $\big\{(k,d) \mid d|n \text{ et } k|d\big\}$ est la réunion disjointe des ensembles $\big\{(k,d) \mid d \in S_k\big\}$, où k parcourt les diviseurs de n. On a donc l'égalité

$$f(n) = \sum_{k|n} \mu(k) \sum_{d \in S_k} f\Big(\frac{n}{d}\Big).$$

Par ailleurs, pour tout k divisant n, l'application $\big\{j \geq 1 \mid j|\frac{n}{k}\big\} \to S_k$ qui à j associe kj est une bijection. Par suite, on a

$$\sum_{d \in S_k} f\Big(\frac{n}{d}\Big) = \sum_{j|\frac{n}{k}} f\Big(\frac{n}{kj}\Big).$$

La formule (11) en résulte, vu que pour tout k divisant n, on a

$$g\Big(\frac{n}{k}\Big) = \sum_{j|\frac{n}{k}} f\Big(\frac{n}{kj}\Big).$$

Remarque 3.3. Le membre de droite de la formule (10) est divisible par n, ce qui n'est pas évident a priori. Il est instructif de le prouver directement. Plus précisément, démontrons que l'on a

$$\sum_{d|n} \mu(d) x^{\frac{n}{d}} \equiv 0 \text{ mod. } n \quad \text{pour tout } x \in \mathbb{Z}. \tag{12}$$

Pour tout $k \in \mathbb{Z}$, tout nombre premier p et tout $r \geq 1$, vérifions d'abord que l'on a

$$k^{p^r} \equiv k^{p^{r-1}} \text{ mod. } p^r. \tag{13}$$

Supposons que p ne divise pas k. L'entier k est alors inversible modulo p^r, et le groupe $\left(\mathbb{Z}/p^r\mathbb{Z}\right)^*$ étant d'ordre $\varphi(p^r) = p^r - p^{r-1}$, on a

$$k^{p^r - p^{r-1}} \equiv 1 \text{ mod. } p^r,$$

d'où la congruence (13) dans ce cas. Si p divise k, alors $k^{p^r} - k^{p^{r-1}}$ est divisible par $p^{p^{r-1}}$. Par ailleurs, on vérifie (par récurrence sur r) que l'on a $p^{r-1} \geq r$, d'où la condition (13). Soit alors x un entier relatif. Afin d'établir (12), il suffit de démontrer que pour tout nombre premier p divisant n, on a

$$\sum_{d|n} \mu(d) x^{\frac{n}{d}} \equiv 0 \text{ mod. } p^{v_p(n)},$$

où $v_p(n)$ est l'exposant de p dans la décomposition de n en produit de facteurs premiers. Considérons un diviseur premier p de n. Posons

$$r = v_p(n) \quad \text{et} \quad n = p^r m.$$

Dans la somme $\sum \mu(d) x^{\frac{n}{d}}$, les termes donnant une contribution éventuellement non nulle sont ceux pour lesquels d est premier à p, ou bien ceux pour lesquels d est de la forme pj avec j premier avec p. Compte tenu de l'égalité $\mu(pj) = -\mu(j)$, on obtient

$$\sum_{d|n} \mu(d) x^{\frac{n}{d}} = \sum_{j|n,(p,j)=1} \mu(j) \left(x^{\frac{n}{j}} - x^{\frac{n}{pj}} \right).$$

Chaque entier j divisant n et premier avec p est un diviseur de m. Pour un tel entier j, on a donc

$$x^{\frac{n}{j}} - x^{\frac{n}{pj}} = y^{p^r} - y^{p^{r-1}} \quad \text{avec} \quad y = x^{\frac{m}{j}}.$$

La condition (13) entraîne alors le résultat.

Exemples 3.3.

1) La formule (10), avec $n = 1$, entraîne $I_1(q) = q$ comme attendu. Pour $n = 2$, on obtient

$$I_2(q) = \frac{q(q-1)}{2}.$$

De même, avec $n = 3$, on constate que l'on a

$$I_3(q) = \frac{q(q^2-1)}{3}.$$

Avec $q = 2$, on obtient ainsi $I_3(2) = 2$, les deux polynômes irréductibles (unitaires) de degré 3 dans $\mathbb{F}_2[X]$ étant $X^3 + X^2 + 1$ et $X^3 + X + 1$.

2) En utilisant (10), on vérifie que

$$I_{50}(2) = 22.517.997.465.744.$$

Cela fournit de nombreuses façons de construire un corps de cardinal 2^{50}, qui est par ailleurs unique à isomorphisme près, comme on le constatera dans le paragraphe suivant.

3) Calculons $I_{70}(q)$. On a le tableau suivant :

d	1	2	5	7	10	14	35	70
$\mu(d)$	1	-1	-1	-1	1	1	1	-1
$\frac{n}{d}$	70	35	14	10	7	5	2	1

On en déduit que l'on a

$$I_{70}(q) = \frac{1}{70}\Big(q^{70} - q^{35} - q^{14} - q^{10} + q^7 + q^5 + q^2 - q\Big).$$

Compte tenu de (12), on obtient au passage l'identité

$$x^{70} - x^{35} - x^{14} - x^{10} + x^7 + x^5 + x^2 - x = 0 \quad \text{pour tout } x \in \mathbb{Z}/70\mathbb{Z}.$$

4) Vérifions que la «probabilité» pour qu'un polynôme unitaire de $K[X]$ de grand degré n choisi au hasard, soit irréductible sur K, est $\frac{1}{n}$.

On a l'égalité (formule (8))

$$nI_n(q) + \sum_{d|n, d<n} I_d(q)d = q^n.$$

Par ailleurs, on a vu que pour tout $d \leq n$, on a $dI_d(q) \leq q^d$. On a ainsi

$$q^n - nI_n(q) \leq \sum_{d|n, d<n} q^d \leq \sum_{k=0}^{[\frac{n}{2}]} q^k = \frac{q^{[\frac{n}{2}]+1} - 1}{q-1} < q^{[\frac{n}{2}]+1}.$$

On obtient les inégalités

$$\frac{q^n - q^{[\frac{n}{2}]+1}}{n} \leq I_n(q) \leq \frac{q^n}{n}.$$

Il en résulte que la suite $\left(\frac{nI_n(q)}{q^n}\right)$ est convergente de limite 1. Quand n tend vers l'infini, on a donc

$$\frac{I_n(q)}{q^n} \sim \frac{1}{n}.$$

Il y a q^n polynômes unitaires de degré n dans $K[X]$, d'où l'estimation annoncée.

5) La fonction φ étant la fonction indicatrice d'Euler, on a vu que tout entier $n \geq 1$ est la somme des $\varphi(d)$, où d parcourt l'ensemble des diviseurs de n. La formule d'inversion de Möbius entraîne alors l'égalité

$$\frac{\varphi(n)}{n} = \sum_{d|n} \frac{\mu(d)}{d} \quad \text{pour tout } n \geq 1.$$

6) Pour tout $n \geq 1$, notons R_n l'ensemble des racines primitives n-ièmes de l'unité de $\mathbb{C}^*$. Rappelons que le n-ième polynôme cyclotomique de $\mathbb{C}[X]$ est défini par l'égalité

$$\Phi_n(X) = \prod_{\zeta \in R_n} (X - \zeta).$$

Son degré est $\varphi(n)$. Vérifions que

$$X^n - 1 = \prod_{d|n} \Phi_d(X). \tag{14}$$

L'ensemble des racines du polynôme $X^n - 1$ est la réunion disjointe des R_d où d divise n. Il en résulte que les polynômes

$$X^n - 1 \quad \text{et} \quad \prod_{d|n} \prod_{\xi \in R_d} (X - \xi)$$

ont les mêmes racines. Leurs racines sont simples. Puisqu'ils sont unitaires, ils sont donc égaux, ce qui entraîne (14). On peut en déduire que $\Phi_n(X)$ est dans $\mathbb{Z}[X]$. Par ailleurs, la formule (11), utilisée (multiplicativement) avec le groupe abélien multiplicatif formé des fractions rationnelles non nulles à coefficients dans $\mathbb{C}$, implique alors l'égalité

$$\Phi_n(X) = \prod_{d|n} \left(X^d - 1\right)^{\mu(\frac{n}{d})}.$$

7. Théorème d'unicité

Il s'agit de démontrer l'énoncé suivant :

Théorème 3.9. *Deux corps finis ayant le même nombre d'éléments sont isomorphes.*

Démonstration : Soient K et L des corps à q éléments et p leur caractéristique. On a $q = p^n$ pour un entier $n \geq 1$. Il existe un polynôme irréductible $F \in \mathbb{F}_p[X]$, de degré n, tel que K soit isomorphe à $\mathbb{F}_p[X]/(F)$ (th. 3.4). Le polynôme F divise $X^q - X \in \mathbb{F}_p[X]$ (th. 3.5). Par ailleurs, pour tout $x \in L$, on a $x^q = x$. On a donc l'égalité

$$X^q - X = \prod_{a \in L} (X - a).$$

Le polynôme F possède ainsi une racine $a \in L$. Considérons l'application

$$\psi : \mathbb{F}_p[X] \to L$$

définie pour tout $P \in \mathbb{F}_p[X]$ par $\psi(P) = P(a)$. C'est un morphisme d'anneaux. Vu que F est irréductible dans $\mathbb{F}_p[X]$ et que $F(a) = 0$, le noyau de ψ est l'idéal (F). Il en résulte que $\mathbb{F}_p[X]/(F)$ est isomorphe à l'image de ψ, qui n'est autre que L, car L et $\mathbb{F}_p[X]/(F)$ ont le même cardinal. Cela entraîne que les corps K et L sont isomorphes.

Ce résultat justifie l'abus courant consistant à parler « du » corps à q éléments. On le note souvent $\mathbb{F}_q$, y compris si q n'est pas premier, mais une puissance d'un nombre premier. On a par exemple

$$\mathbb{F}_8 = \mathbb{F}_2[X]/(X^3 + X + 1), \quad \mathbb{F}_{81} = \mathbb{F}_3[X]/(X^4 + X^3 + 2), \quad \mathbb{F}_{125} = \mathbb{F}_5[X]/(X^3 + X + 1),$$

$$\mathbb{F}_{p^2} = \mathbb{F}_p[X]/(X^2 + 1) \quad \text{si } p \text{ est premier congru à 3 modulo 4.}$$

8. Problème du logarithme discret

Soit K un corps à q éléments. Le groupe multiplicatif K^* est cyclique (cor. 3.5). Soit g l'un de ses générateurs (il en possède $\varphi(q-1)$). On a

$$K^* = \left\{ g^i \;\middle|\; 0 \leq i \leq q-2 \right\}.$$

Le problème du logarithme discret de base g dans K^* est le suivant :

Problème. Étant donné un élément $x \in K^*$, trouver l'entier i tel que l'on ait

$$x = g^i \quad \text{et} \quad 0 \leq i \leq q-2.$$

On note parfois cet entier i, $\log_g(x)$ ou bien $\mathrm{ind}_g(x)$. C'est le logarithme discret de base g de x.

Certains algorithmes de cryptographie sont basés sur le fait que, pour certains corps finis de grand cardinal q, ce problème soit difficile à résoudre. Tel est par exemple le cas si l'on ne sait pas factoriser $q-1$, notamment si $q-1$ possède un grand diviseur premier. L'algorithme de Silver, Pohlig et Hellman, que l'on décrit après, permet de résoudre ce problème si l'on connaît la décomposition de $q-1$ en facteurs premiers.

Abordons ce problème dans un cas simple. Prenons le corps de cardinal 27,

$$K = \mathbb{F}_3[X]/(X^3 + 2X + 1).$$

Notons que $X^3 + 2X + 1$ est irréductible dans $\mathbb{F}_3[X]$, car il est de degré 3 et n'a pas de racines dans $\mathbb{F}_3$. Le groupe K^* est d'ordre 26. Les ordres de ses éléments autres que l'élément neutre, sont donc 2, 13 ou 26. Le seul élément d'ordre 2 est -1. Posons

$$\alpha = X + (X^3 + 2X + 1).$$

Vérifions que α est un générateur de K^*. On a $\alpha^3 = \alpha - 1$, d'où $\alpha^9 = \alpha^3 - 1$ (car K est de caractéristique 3) i.e. $\alpha^9 = \alpha + 1$, d'où $\alpha^{12} = \alpha^2 - 1$, puis $\alpha^{13} = -1$ et notre assertion.

Résolvons alors le problème du logarithme discret de base α dans K^*. Tout élément de K^* s'écrit de manière unique sous la forme $a + b\alpha + c\alpha^2$ avec $a, b, c \in \mathbb{F}_3$. Il s'agit donc pour chacun de ces éléments de déterminer l'entier i tel que l'on ait

$$a + b\alpha + c\alpha^2 = \alpha^i \quad \text{avec} \quad 0 \leq i \leq 25.$$

On vérifie les calculs suivants :

x	1	2	α	$\alpha+1$	$\alpha+2$	2α	$2\alpha+1$	$2\alpha+2$	α^2	α^2+1	α^2+2	$2\alpha^2$	$2\alpha^2+1$
$\log_\alpha(x)$	0	13	1	9	3	14	16	22	2	21	12	15	25

x	$2\alpha^2+2$	$\alpha^2+\alpha+1$	$\alpha^2+2\alpha+1$	$\alpha^2+2\alpha+2$	$\alpha^2+\alpha+2$	$2\alpha^2+2\alpha+1$
$\log_\alpha(x)$	8	6	18	7	11	24

x	$2\alpha^2+2\alpha+2$	$2\alpha^2+\alpha+2$	$2\alpha^2+\alpha+1$	$\alpha^2+\alpha$	$\alpha^2+2\alpha$	$2\alpha^2+2\alpha$	$2\alpha^2+\alpha$
$\log_\alpha(x)$	19	5	20	10	4	23	17

Les générateurs de K^* sont les éléments α^k avec $1 \leq k \leq 26$ et k premier avec 26. Il y en a douze. Compte tenu de ce qui précède, ce sont les éléments

$$\alpha, \quad 1+\alpha, \quad 2+\alpha, \quad 1+\alpha^2, \quad 2\alpha^2, \quad 1+2\alpha^2, \quad 2+2\alpha+\alpha^2, \quad 2+\alpha+\alpha^2,$$

$$2+2\alpha+2\alpha^2, \quad 2+\alpha+2\alpha^2, \quad 2\alpha+2\alpha^2, \quad \alpha+2\alpha^2.$$

9. Algorithme de Silver, Pohlig et Hellman

Soit K un corps fini à q éléments. Soit g un générateur de K^*. On va décrire ici un algorithme permettant de résoudre le problème du logarithme discret de base g dans K^*, dans le cas où l'on connaît la décomposition de $q-1$ en facteurs premiers. Cet algorithme est d'autant plus efficace que les diviseurs premiers de $q-1$ sont petits.

Partons d'un élément $x \in K^*$. Il s'agit de déterminer l'entier n tel que l'on ait

$$x = g^n \quad \text{et} \quad 0 \leq n \leq q-2.$$

Notons

$$q-1 = \prod_{p|q-1} p^{r_p}$$

la décomposition de $q-1$ en facteurs premiers. Afin de calculer n, l'idée est qu'il suffit de connaître n modulo p^{r_p} pour chaque diviseur premier p de $q-1$, le théorème chinois permettant ensuite de retrouver n.

L'algorithme est le suivant. Soit p un diviseur premier de $q-1$. Puisque K^* est cyclique d'ordre $q-1$, il existe un unique sous-groupe μ_p de K^* d'ordre p, qui n'est autre que l'ensemble des racines p-ièmes de l'unité de K^* (th. 1.9). Un générateur ζ de μ_p est

$$\zeta = g^{\frac{q-1}{p}}, \tag{15}$$

car c'est un élément d'ordre p de K^*. On a donc

$$\mu_p = \left\{1, \zeta, \zeta^2, \cdots, \zeta^{p-1}\right\}.$$

Par ailleurs, il existe des entiers n_i tels que l'on ait

$$n \equiv n_0 + n_1 p + \cdots + n_{r_p-1} p^{r_p-1} \text{ mod. } p^{r_p} \quad \text{avec} \quad 0 \leq n_i < p. \tag{16}$$

Conformément à la stratégie annoncée, on est confontré au problème de la détermination des n_i. On calcule n_0 à partir de l'élément $x^{\frac{q-1}{p}}$. En effet, on a

$$\left(x^{\frac{q-1}{p}}\right)^p = 1,$$

de sorte $x^{\frac{q-1}{p}}$ appartient à μ_p. En écrivant que l'on a $x = g^n$, et en utilisant le fait que $g^{q-1} = 1$, on obtient alors les égalités

$$x^{\frac{q-1}{p}} = (g^n)^{\frac{q-1}{p}} = (g^{n_0})^{\frac{q-1}{p}} = \zeta^{n_0}, \tag{17}$$

ce qui permet d'obtenir n_0. On procède de même pour les autres coefficients n_i. Posons

$$x_i = \frac{x}{g^{n_0+\cdots+n_{i-1}p^{i-1}}} \quad \text{pour tout} \quad i \geq 1 \quad \text{et} \quad i \leq r_p - 1. \tag{18}$$

En écrivant de nouveau que $x = g^n$, on a alors

$$x_i^{\frac{q-1}{p^{i+1}}} = (g^{n_i})^{\frac{q-1}{p}} = \zeta^{n_i}, \tag{19}$$

et l'on détermine ainsi n_i, d'où la connaissance de n modulo p^{r_p}. En effectuant ces calculs pour chaque diviseur premier de $q-1$, et en utilisant le théorème chinois, on peut ainsi obtenir n modulo $q-1$, puis l'entier n.

Exemple 3.4. Prenons le corps $K = \mathbb{F}_{53}$, de cardinal $q = 53$. On a $q - 1 = 4 \times 13$. Un générateur de K^* est $g = 2$ (la classe de 2 modulo 53). En effet, on a $53 \equiv 5$ mod. 8, d'où $\left(\frac{2}{53}\right) = -1$, ce qui entraîne (critère d'Euler)

$$2^{26} \equiv -1 \text{ mod. } 53,$$

et notre assertion. Déterminons le logarithme discret de base 2 de 23 dans K^*, autrement dit, l'entier n tel que

$$23 \equiv 2^n \text{ mod. } 53 \quad \text{et} \quad 0 \leq n \leq 51.$$

Reprenons les notations utilisées ci-dessus. On détermine d'abord n modulo 4. On a

$$\mu_2 = \Big\{1, -1\Big\}.$$

Par ailleurs, il existe des entiers n_0 et n_1 égaux à 0 ou 1, tels que l'on ait

$$n \equiv n_0 + 2n_1 \text{ mod. } 4.$$

D'après la formule (17), on a la congruence

$$23^{26} \equiv (-1)^{n_0} \text{ mod. } 53.$$

On a (critère d'Euler)

$$\left(\frac{23}{53}\right) \equiv 23^{26} \text{ mod. } 53.$$

D'après la loi de réciprocité quadratique, on a

$$\Big(\frac{23}{53}\Big) = \Big(\frac{53}{23}\Big) = \Big(\frac{7}{23}\Big) = -\Big(\frac{23}{7}\Big) = -\Big(\frac{2}{7}\Big) = -1,$$

d'où $23^{26} \equiv -1$ mod. 53, puis $n_0 = 1$. L'élément $x_1 \in K^*$, défini par la formule (18), est ici

$$x_1 = \frac{23}{2} = 38.$$

D'après la formule (19), on obtient

$$38^{13} \equiv (-1)^{n_1} \text{ mod. } 53.$$

On vérifie que l'on a dans K^* les égalités $38^4 = 10$, $38^{12} = 46$ puis $38^{13} = -1$, d'où $n_1 = 1$. Il en résulte que l'on a

$$n \equiv 3 \text{ mod. } 4. \tag{20}$$

Déterminons maintenant la congruence de n modulo 13. D'après la formule (15), on a

$$\mu_{13} =< 2^4 >,$$

d'où l'on déduit que

$$\mu_{13} = \Big\{1, 16, 44, 15, 28, 24, 13, 49, 42, 36, 46, 47, 10\Big\},$$

où les éléments sont rangés par ordre croissant des puissances du générateur 16. On cherche l'entier n_0 compris entre 0 et 12 tel que l'on ait $n \equiv n_0$ mod. 13. On a (formule (17)),

$$23^4 \equiv 16^{n_0} \text{ mod. } 53.$$

Puisque l'on a $23^4 \equiv 1$ mod. 53, on en déduit que $n_0 = 0$, i.e. que l'on a

$$n \equiv 0 \text{ mod. } 13. \tag{21}$$

L'entier n cherché est donc l'unique entier compris entre 0 et 51 tel que les congruences (20) et (21) soient satisfaites, ce qui conduit à $n = 39$ (théorème chinois). On obtient ainsi dans K^* l'égalité $23 = 2^{39}$, d'où

$$\log_2(23) = 39.$$

Exemple 3.5. Prenons le corps $K = \mathbb{F}_3[X]/(X^3 + 2X + 1)$ étudié précédemment et $x = \alpha^2 + 1$, où α est la classe de X modulo $(X^3 + 2X + 1)$. L'élément $g = \alpha$ est un générateur de K^*. (Re)déterminons l'entier

$$n = \log_\alpha(\alpha^2 + 1).$$

On vérifie que l'on a $x^{13} = 2 = -1$, d'où il résulte que n est impair. Par ailleurs, on a $\mu_{13} =< \alpha^2 >$ et l'on vérifie les égalités $x^2 = 2\alpha + 1 = (\alpha^2)^8$. On a donc $n \equiv 8$ mod. 13, d'où $n = 21$ comme attendu.

Remarque 3.4. Soit K un corps de cardinal q tel que q ne soit pas une puissance de 2. Dans ce cas, 2 divise $q - 1$. Étant donné un élément $x \in K^*$, dans la formule (17) utilisée avec $p = 2$, l'entier n_0 vaut 1 si et seulement si x n'est pas un carré dans K.

10. Algorithme Baby step - Giant step

Soient K un corps fini de cardinal q et g un générateur de K^*. On décrit ici un algorithme permettant de résoudre le problème du logarithme discret de base g dans K^* en $O\big(\sqrt{q}\big)$ opérations. Posons

$$m = \big[\sqrt{q-1}\big].$$

Soit x un élément de K^*. Il existe un unique entier n tel que l'on ait

$$x = g^n \quad \text{avec} \quad 0 \leq n < q - 1.$$

Afin de déterminer n, considérons l'ensemble

$$A = \Big\{ g^k \mid 0 \leq k < m \Big\}.$$

Il existe un plus petit entier naturel h tel que

$$xg^{-hm} \in A. \tag{22}$$

En effet, il existe des entiers naturels u et v tels que

$$n = um + v \quad \text{et} \quad 0 \leq v < m.$$

On a $g^{um+v} = x$, d'où $g^v = xg^{-um} \in A$ et l'assertion. Il existe un unique entier r tel que

$$g^r = xg^{-hm} \quad \text{et} \quad 0 \leq r < m. \tag{23}$$

Vérifions alors que l'on a

$$n = hm + r. \tag{24}$$

L'élément xg^{-um} appartient à A. Par suite, on a $u \geq h$. Supposons $u > h$. On a alors

$$mh + r < m(h + 1) \leq mu \leq mu + v = n.$$

Compte tenu de (23), cela contredit le fait que n soit le petit entier naturel k tel que $x = g^k$. On a donc $u = h$, puis $r = v$ et l'égalité (24).
Les inégalités $mh \leq n < q - 1$ impliquent

$$h < \frac{q-1}{m},$$

ce qui garantit de trouver n en $O(\sqrt{q})$ opérations.

L'algorithme Baby step Giant step consiste à expliciter l'ensemble A, en calculant g, $g^2, \cdots$, en multipliant successivement chaque résultat par g (Baby step), et ensuite à calculer xg^{-m}, $xg^{-2m}, \cdots$, en multipliant successivement chaque résultat par g^{-m} (Giant step), jusqu'à déterminer l'entier h défini par la condition (22).

Exemple 3.6. Posons $K = \mathbb{F}_{127}$. Montrons que 3 est un générateur de K^*. L'ordre de K^* est $126 = 2.3^2.7$. D'après le critère d'Euler, on a

$$\Big(\frac{3}{127}\Big) \equiv 3^{63} \text{ mod. } 127.$$

On a

$$\Big(\frac{3}{127}\Big) = -\Big(\frac{127}{3}\Big) = -\Big(\frac{1}{3}\Big) = -1,$$

d'où $3^{63} \equiv -1$ mod. 127. Par ailleurs, on a $3^6 \equiv 94$ mod. 127, $3^{14} \equiv 22$ mod. 127, d'où $3^{18} \equiv 4$ mod. 127, $3^{42} \equiv 107$ mod. 127 et l'assertion.

Déterminons le logarithme discret de base 3 de 91 dans K^*, autrement dit l'entier n vérifiant la condition

$$3^n \equiv 91 \text{ mod. } 127 \quad \text{avec} \quad 0 \leq n < 126.$$

On a ici $m = 11$ et l'ensemble A est formé des classes modulo 127 des entiers 3^r pour $0 \leq r < 11$. On vérifie que l'on a

$$A = \Big\{1, 3, 9, 27, 81, 116, 94, 28, 84, 125, 121\Big\},$$

où les éléments sont rangés suivant les valeurs croissantes de r. Il s'agit alors d'expliciter le plus petit entier naturel h tel que 91.3^{-hm} modulo 127 appartienne à A. On trouve $h = 7$ et l'on a

$$91.3^{-77} \equiv 94 \text{ mod. } 127.$$

On obtient $n = hm + r$ avec $r = 6$, d'où $n = 83$.