# Notes sur les corps finis pour les candidats d'agrégation

Maher Boudabra

8 juin 2023

Pour ceux qui aiment exécuter des codes des calculs formels et numériques, je vous conseille énormément de jeter un coup d'œil sur **Pari Gp** disponible sur https://pari.math.u-bordeaux.fr/ ; c'est rapide, gratuit et surtout intelligent :).

## 1 Rappels

### 1.1 L'essentiel.

Dans cette partie je veux rappeler quelques notions concernant les corps en général.

**Définition 1.** On dit qu'un corps $L$ est une extension d'un corps $K$ si tout simplement $K \subset L$. On note $L/K$ mais c'est rien à voir avec le quotient !!!

**Définition 2.** On dit que $\theta \in L/K$ est algébrique sur $K$ si $\theta$est une racine d'un polynôme non nul à coefficients sur $K$, i.e s'il existe $f \in K[x] \setminus \{0\}$ tel que $f(\theta) = 0$. Un élément non algébrique est dit transcendant.

Lorsqu'on parle d'un élément algébrique / transcendant, if ne faut jamais oublier par rapport au quel corps il est algébrique. Par exemple $\pi$ est algébrique sur $\mathbb{R}$ mais pas sur $\mathbb{Q}$ !!!

Un autre formulation du fait que $\theta$ est algébrique ( resp. transcendant ) est de dire que l'idéal $I_\theta := \{f \in K[x] | \, f(\theta) = 0\}$ est non trivial (resp. trivial), ou encore que le morphisme

$$\vartheta_\theta : \begin{array}{c} K[x] \longrightarrow K[\theta] \subset L \\ f \longmapsto f(\theta) \end{array}$$

est non injective ( resp. injective). Dans le cas où $\theta$ est algébrique, alors on peut trouver un polynôme $\varpi_\theta$ de dégrée minimale tel que

$$I_\theta = \varpi_\theta K[x]$$

En particulier $\varpi_\theta$ est nécessairement irréductible sur $K$. Par exemple $\varpi_{\sqrt{2}} = x^2 - 2$ sur $\mathbb{Q}$.

**Théorème 3.** (Anneau et corps engendrés par un élément). Si $\theta \in L/K$ alors

- *le plus petit anneau contenant $K$ et $\theta$ est*

$$K[\theta] := \{f(\theta) | \, f \in K[x]\}$$

- *le plus petit corps contenant $K$ et $\theta$ est*

$$K(\theta) := \left\{ \frac{f(\theta)}{g(\theta)} | \, f, g \in K[x], \; g(\theta) \neq 0 \right\}$$

*Démonstration.* Immédiat avec la définition des tels structures algébriques. □

Si $\theta \in K$ alors

$$K[\theta] = K(\theta) = K.$$

Il est évident que $K[\theta] \subset K(\theta)$, mais quoi dire quant à la réciproque ? Le résultat suivant caractérise même l'égalité entre les deux.

**Théorème 4.** *Soit $\theta \in L/K$. Alors : $K[\theta] = K(\theta)$ si et seulement si $\theta$ est algébrique sur $K$.*

*Démonstration.* Sans perdre de généralité on suppose que $\theta \notin K$.

- Si $K[\theta] = K(\theta)$ alors $\frac{1}{\theta} = h(\theta)$ pour un certain $h \in K[x]$, et donc $f(\theta) = 0$ où $f(x) = xh(x) - 1 \in K[x]$. Ainsi $\theta$ est algébrique.
- Supposons que $\theta$ est algébrique sur $K$ et soit $\xi := \frac{f(\theta)}{g(\theta)} \in K(\theta)$. Le polynôme $g$ est premier avec $\varpi_\theta$ (Pourquoi ?) et donc d'après le théorème de Bézout on peut trouver $\ell, v \in K[x]$ tels que

$$\ell g + v\varpi_\theta = 1. \tag{1.1}$$

En évaluant (1.1) en $\theta$, on obtient

$$\ell(\theta)g(\theta) + v(\theta)\underbrace{\varpi_\theta(\theta)}_{=0} = 1$$

et par suite $\ell(\theta)g(\theta) = 1$ ou $\ell(\theta) = \frac{1}{g(\theta)}$. Finalement

$$\xi = \frac{f(\theta)}{g(\theta)} = f(\theta)\ell(\theta) = (f \times \ell)(\theta) \in K[\theta]$$

d'où le résultat puisque $K[\theta] \subset K(\theta)$ est toujours vraie.

□

**Exemple 5.** On a $\mathbb{Q}[\sqrt{2}] = \mathbb{Q}(\sqrt{2})$ et $\mathbb{Q}[\pi] \subsetneq \mathbb{Q}(\pi)$.

Pour $\theta$ algébrique, la preuve du théorème précédent donne un manière pratique pour écrire $\xi = \frac{f(\theta)}{g(\theta)}$ sous une forme polynomiale, il suffit de trouver l'inverse (représentant) $\ell$ de $g$ dans le quotient $\frac{K[x]}{<\varpi_\theta>}$ et ainsi $\xi = f(\theta)\ell(\theta)$.

**Définition 6.** $L$ est dit algébriquement clos si tout polynôme $f \in L[x]$ admet au moins une racine dans $L$.

**Exemple 7.** $\mathbb{C}$ est algébriquement clos.

**Définition 8.** La dimension de $L/K$ vue comme un $K$ - e.v s'appelle la dimension de $L$ sur $K$ et on la note $[L : K]$.

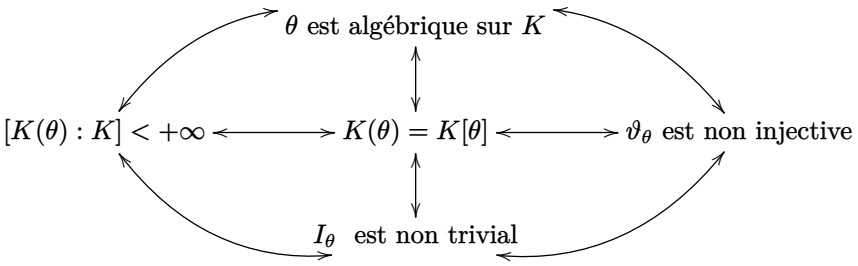
**Exemple 9.** On a

- $[\mathbb{C} : \mathbb{R}] = 2$.
- $[\mathbb{C} : \mathbb{Q}] = +\infty$.

Plus généralement on a le résultat suivant.

**Proposition 10.** *Si $\theta \in L/K$ alors : $[K(\theta) : K]$ est fini si et seulement si $\theta$ est algébrique sur $K$.*

**Moralité**




**Théorème 11.** *A isomorphisme près, tout corps commutatif $K$ admet un unique clôture algébrique, et notée $\overline{L}/K$.*

*Démonstration.* Voir [1]. □

### 1.2 Généralisations

On définit d'une manière plus générale

$$K[\theta_1,...,\theta_r] := \{f(\theta_1,...,\theta_r)|\ f \in K[x_1,...,x_r]\}$$

et

$$K(\theta_1,...,\theta_r) := \left\{ \frac{f(\theta_1,...,\theta_r)}{g(\theta_1,...,\theta_r)}|\ f \in K[x_1,...,x_r],\ g(\theta_1,...,\theta_r) \neq 0 \right\} \text{ (corps)}$$

où $\theta_1,...,\theta_r \in L/K$.

Soit $f$ un polynôme irréductible de $K[x]$ et $\theta_1,...,\theta_r$ ses racines distinctes dans $\overline{K}$. Chaque corps $K(\theta_i)$ s'appelle corps de rupture de $f$. Le corps de rupture est un corps minimal dans lequel $f$ admet au moins une racine. Il est unique à isomorphisme près, plus précisément, isomorphe à $\frac{K[x]}{<f>}$.

Le corps $K(\theta_1,...,\theta_r)$ s'appelle corps des racines de $f$, même pour $f$ quelconque. C'est unique à isomorphisme près aussi.

# 2 Introduction

### 2.1 Un exemple sans effort !

Un corps fini est tout simplement un corps ayant un nombre fini des éléments. Ce type des corps possède également des propriétés intéressantes et surtout surprenantes, notamment la commutativité. Les corps finis sont largement utilisés dans la vie courante, à savoir en informatique, codage, cryptographie etc ....

Les premiers exemples des corps finis qu'on peut rencontrer sont les anneaux $\mathbb{Z}/p\mathbb{Z}$ où $p$ est un nombre premier. On peut même vérifier que

$$\frac{\mathbb{Z}}{n\mathbb{Z}} \text{ est un corps ssi } n \text{ est premier}$$

Sauf mention contraire, on va utiliser les notations suivantes :

- $p$ désigne un nombre premier.
- $\mathbb{F}_q$ désigne un corps fini à $q$ éléments.
- $\mathcal{I}_{d,q}$ est l'ensemble des polynômes irréductibles normalisés à coefficients dans $\mathbb{F}_q$.
- Dans $\mathbb{Z}/n\mathbb{Z}$, les élément serons notés $x, y...$, c-à-d sans bar au dessus ( $\overline{x}$ ).

J'ai essayé de faire une étude élémentaire pour un corps à 4 éléments, et je pense que ça peut être donné comme une introduction pour cette leçon.

Voici l'approche que j'ai suivi : Soit $F = \{0, 1, \alpha, \beta\}$ un tel corps à 4 éléments (distincts).

1. Tout d'abords, on a $\alpha^{-1}, \beta^{-1} \in \{1, \alpha, \beta\}$. 1 est à éliminer car sinon $\alpha = \beta = 1$, ce qui contredit le fait que $\#F = 4$.
2. Supposons que $\alpha^{-1} = \alpha$ : ceci impliquera que $\alpha^2 = 1 \Longrightarrow \alpha = \pm 1 \Longrightarrow \alpha = -1$. Dans ce cas, on a nécessairement $\beta^{-1} = \beta$ (car $\beta^{-1} = \alpha$ ssi $\alpha^{-1} = \beta$). Ceci va entrainer la diminution de cardinal de $F$ par 1 au moins. On conclut ainsi que $\alpha^{-1} = \beta$ et $\beta^{-1} = \alpha$.
3. De même, on peut voir par élimination que

   $$\alpha^3 = \beta^3 = 1^3 = 1.$$

   En particulier

   $$\alpha^3 - 1 = \underbrace{(\alpha - 1)}_{\neq 0}(\alpha^2 + \alpha + 1) = 0 \tag{2.1}$$

   et

   $$\beta^3 - 1 = \underbrace{(\beta - 1)}_{\neq 0}(\beta^2 + \beta + 1) = 0 \tag{2.2}$$

   Par conséquence, le polynôme minimal de $\alpha$ et $\beta$ est $x^2 + x + 1$.
4. Il nous reste la caractéristique. On $-1 \in \{1, \alpha, \beta\}$. Si $-1 = \alpha$ alors $\alpha^{-1} = \alpha$ ce qui n'est pas le cas, de même pour le cas où $-1 = \beta$. Ainsi $-1 = 1$ et ensuite la caractéristique est 2.

5. En faisant (2.1) − (2.2), on tire

$$\begin{aligned}\alpha^2+\alpha-\beta^2-\beta &= (\alpha-\beta)(\alpha+\beta)+(\alpha-\beta)\\ &= (\alpha-\beta)(\alpha+\beta+1)\\ &= 0\end{aligned}$$

et donc $\alpha+\beta+1=0$ car $\alpha\neq\beta$.

On obtient ainsi le table arithmétique de $F$ :

| $+$ | $0$ | $1$ | $\alpha$ | $\beta$ |
|---|---|---|---|---|
| $0$ | $0$ | $1$ | $\alpha$ | $\beta$ |
| $1$ | $1$ | $0$ | $\beta$ | $\alpha$ |
| $\alpha$ | $\alpha$ | $\beta$ | $0$ | $1$ |
| $\beta$ | $\beta$ | $\alpha$ | $1$ | $0$ |

| $\times$ | $0$ | $1$ | $\alpha$ | $\beta$ |
|---|---|---|---|---|
| $0$ | $0$ | $0$ | $0$ | $0$ |
| $1$ | $0$ | $1$ | $\alpha$ | $\beta$ |
| $\alpha$ | $0$ | $\alpha$ | $\beta$ | $1$ |
| $\beta$ | $0$ | $\beta$ | $1$ | $\alpha$ |

Comme vous pouvez remarquer, l'approche est entièrement élémentaire. En particulier on a vérifié que $F$ contient $\mathbb{Z}/2\mathbb{Z}$.

## 2.2 Premiers pas.

Pour déterminer l'inverse d'un élément non nul $x\in\mathbb{Z}/p\mathbb{Z}$, on utilise l'identité de Bézout. Puisque $\text{pgcd}(x,p)=1$, il existe $a,b\in\mathbb{Z}$ tels que

$$ax+bp=1.$$

Ainsi par passage modulo $p$, on obtient $x^{-1}=a$. Grosso-modo, $\mathbb{Z}/p\mathbb{Z}$ est l'ensemble des restes possibles de la division euclidienne par $p$, i.e

$$\frac{\mathbb{Z}}{p\mathbb{Z}}=\{1,2,...,p-1\}$$

Faites attention, un élément de $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ n'est pas un entier, c'est plutôt une classe entière.

**Lemme 12.** *$\mathbb{F}_q$ contient une copie d'un certain $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$ [1]. Le nombre $p$ est premier et s'appelle la caractéristique de $\mathbb{F}_q$.*

*Démonstration.* L'homomorphisme

$$\varphi:\begin{aligned}\mathbb{Z}&\longrightarrow\mathbb{F}_q\\ n&\longmapsto n\cdot 1\end{aligned}$$

a un noyau non trivial vu que $\#\mathbb{F}_q=q<\#\mathbb{Z}$. Donc $\ker\varphi=p\mathbb{Z}$ pour un certain $p$, ce dernier est premier puisqu'un corps est intègre.

$$\mathbb{Z}/\ker\varphi=\frac{\mathbb{Z}}{p\mathbb{Z}}\simeq\text{Im}\varphi\hookrightarrow\mathbb{F}_q$$

et par suite $\text{Im}\varphi$ est isomorphe à $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$, c à d une copie conforme de $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$. On note $p=\text{car}(\mathbb{F}_q)$. □

**Proposition 13.** *Le nombre des éléments de $\mathbb{F}_q$ est une puissance de sa caractéristique $p$.*

*Démonstration.* Le corps $\mathbb{F}_q$ peut être vu comme un $\mathbb{F}_p$ - e.v ( à isomorphisme près ), et donc d'après un certain théorème d'algèbre linéaire, on a

$$\mathbb{F}_q\underset{\text{comme e.v}}{\simeq}\mathbb{F}_p^d$$

où $d$ est la dimension de $\mathbb{F}_q$. Finalement $\#\mathbb{F}_q=p^d$. □

**Corollaire 14.** *Tout corps $\mathbb{F}_{p^d}$ est une extension algébrique de $\mathbb{F}_p$.*

**Moralité** Il est un tabou de parler d'un corps fini de cardinal $12,14,....$

Une autre chose à mentionner, un corps finis $\mathbb{F}_q$ n'est jamais clos puisque

$$\prod_{\xi\in\mathbb{F}_q}(x-\xi)+1$$

ne s'annule jamais sur $F$.

1. $\mathbb{F}_p\simeq\mathbb{Z}/p\mathbb{Z}$

# 3 Étude algébriques des corps finis.

Le plus fameux propriété concernant les corps finis est la commutativité, ce résultat est dû à Wedderburn.

**Théorème 15** (**Wedderburn**). *Un corps fini est commutatif.*

*Démonstration.* Vous pouvez consulter [1], [2]. □

**Proposition 16.** *Le groupe multiplicatif de $\mathbb{F}_q$ est cyclique. En particulier, les éléments de $\mathbb{F}_q$ obéissent l'équation*

$$x^q - x = 0.$$

Il convient de signaler que la première partie de la proposition a une version plus générale : tout sous groupe fini du groupe multiplicatif d'un corps est cyclique. Pour la preuve, vous pouvez consulter [1].

**Théorème 17.** *L'ensemble des racines de $x^{p^d} - x$ dans la clôture algébrique $\overline{\mathbb{F}}_p$ est un corps à $p^d$ éléments.*

*Démonstration.* La preuve est basé sur deux choses :

(*i*) $C_p^k = 0$ dans $\mathbb{F}_p$ for $k \in \{1, ..., p-1\}$, et par suite $(x+y)^p = x^p + y^p$ et par itération $(x+y)^{p^d} = x^{p^d} + y^{p^d}$

(*ii*) $x^{p^d} - x$ n'a pas des racinés multiples puisque $\left(x^{p^d} - x\right)' = -1$. □

**Théorème 18.** *Les corps finis ayant le même cardinal sont isomorphe.*

*Démonstration.* La preuve est basée sur (17). Vous pouvez consulter [2] par exemple. □

Le théorème (17) montre l'existence des corps finis, mais il est assez abstrait et non pratique. Le théorème suivant est beaucoup plus simple.

**Théorème 19.** *Si $f$ est un polynôme irréductible de dégrée $d$ sur $\mathbb{F}_p$ , alors $\frac{\mathbb{F}_p[x]}{<f>}$ est un corps fini à $p^d$ éléments.*

*Démonstration.* L'idéal $< f >$ est maximal puisque $f$ est irréductible, et donc $\frac{\mathbb{F}_p[x]}{<f>}$ est un corps de $p^d$ éléments. □

**Exemple 20.** On retrouve par exemple que $\mathbb{F}_4 = \frac{\mathbb{F}_2[x]}{<x^2+x+1>}$ .

On a $\mathbb{F}_{p^2} = \frac{\mathbb{F}_p[x]}{<x^2-a>}$ pour tout $a$ non carré dans $\mathbb{F}_p$.

**Moralité** Si on arrive à capter un polynôme irréductible de dégrée $d$ sur $\mathbb{F}_p$, alors on peut facilement construire notre corps fini, tout simplement en considérant le quotient $\frac{\mathbb{F}_p[x]}{<f>}$ qui n'est autre que les restes possibles de la division euclidienne polynomiale par $f$. En particulier, pour trouver l'inverse d'un élément non nul $h \in \frac{\mathbb{F}_p[x]}{<f>}$, il suffit de trouver deux polynômes $h, g$ tels que

$$hg + \ell f = 1$$

et passer modulo $f$. On obtient $h^{-1} = g$. (Ici je confonds la classe et son représentant).

**Exemple 21.** C'est quoi l'inverse de $x+1$ dans $\frac{\mathbb{F}_2[x]}{<x^2+x+1>}$ ? On a

$$-x \times (x+1) + (x^2 + x + 1) = 1$$

et donc $(x+1)^{-1} = -x = x$ ( $1 = -1$ dans $\mathbb{F}_2$).

La question qui se pose ici est la suivante : Est ce qu'il y a des polynômes irréductibles de toutes les dégrées ? La réponse est affirmative.

**Théorème 22.** *Le nombre des polynômes irréductibles de dégrée $d$ sur $\mathbb{F}_p$ est donné par*

$$\#\mathcal{I}_{d,p} = \frac{1}{n} \sum_{\ell | d} \mu(\tfrac{d}{\ell}) p^{\ell} \tag{3.1}$$

*où $\mu(\cdot)$ est la fonction de Möbius. En particulier $\mathcal{I}_{d,p} \neq \emptyset$.*

*Démonstration.* Voir [3, Algèbre]. Une preuve élémentaire et élégante qui fait appel juste au principe d'*inclusion-exclusion* est disponible sur https://arxiv.org/pdf/1001.0409.pdf. Par exemple on a

$$\frac{1}{30}(2^{30} - 2^{15} - 2^{10} - 2^6 + 2^5 + 2^3 + 2^2 - 2) = 35790267$$

polynômes irréductibles de dégrée 30 sur $\mathbb{F}_2$. □

La formule (3.1) reste valable même si on remplace $p$ par une certaine puissance $q$ de $p$, et on trouve

$$\#\mathcal{I}_{d,q} = \frac{1}{n}\sum_{\ell|d} \mu(\tfrac{d}{\ell})q^{\ell}$$

**Lemme 23.** *Pour tout polynôme $f \in \mathbb{F}_p$, on a*

$$f\left(x^{p^n}\right) = f(x)^{p^n}$$

*Démonstration.* Utilisez le point $(i)$ dans le théorème 4. □

Un important corolaire de ce lemme est le suivant :

**Corollaire 24.** *Soit $f$ un irréductible sur $\mathbb{F}_p$. Alors le corps de rupture de $f$ ainsi que son corps de décomposition sont les mêmes.*

*Démonstration.* Soit $\theta$ une racine de $f$. En vertu de (23), $\left\{\theta^{p^t}\right\}_{0\leq t\leq d-1}$ sont aussi des racines, où $d = \deg f$. L'irréductibilité de $f$ entraine que

$$\{h \in \mathbb{F}_p[x] \mid h(\theta) = 0\} =< f >$$

De plus, $\left\{\theta^{p^t}\right\}_{0\leq t\leq d-1}$ sont 2 à 2 distincts ( Pourquoi ?) . Et donc

$$\underbrace{\mathbb{F}_p[\theta]}_{\text{corps de rupture}} \subset \underbrace{\mathbb{F}_p\left[\theta, \theta^p, ..., \theta^{p^{d-1}}\right]}_{\text{corps des racines}} \subset \mathbb{F}_p[\theta]$$

Ce qui achève la preuve. □

**Proposition 25.** $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n} \iff m \mid n$.

*Démonstration.* Si $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$, alors $\mathbb{F}^*_{p^m} \subset \mathbb{F}^*_{p^n}$,et donc par le théorème de Lagrange

$$\#\mathbb{F}^*_{p^m} = p^m - 1 \mid \#\mathbb{F}^*_{p^n} = p^n - 1$$

et par suite $m \mid n$ ( Un résultat classique dit que $\text{pgcd}(p^m - 1, p^n - 1) = p^{\text{pgcd}(m,n)} - 1$, trouvez le dans les maths en tête par exemple )

Réciproquement, si $m \mid n$ alors

$$\left\{x \in \overline{\mathbb{F}}_p \mid x^{p^m} = x\right\} \subset \left\{x \in \overline{\mathbb{F}}_p \mid x^{p^n} = x\right\}$$

puisque pour tout $x$ dans l'ensemble gauche on a :

$$\underbrace{\left(\left(\left(x^{p^m}\right)^{p^m}\right)^{\cdots}\right)^{p^m}}_{\frac{n}{m} \text{ fois}} = x = x^{p^{m\times\frac{n}{m}}} = x^{p^n}$$

Mais $\left\{x \in \overline{\mathbb{F}}_p \mid x^{p^m} = x\right\}$ et $\left\{x \in \overline{\mathbb{F}}_p \mid x^{p^n} = x\right\}$ ne sont autres que deux copies de de $\mathbb{F}_{p^m}$ et $\mathbb{F}_{p^n}$. D'où le résultat. □

Une interprétation est la suivante : Dans $\mathbb{F}_{p^n}$ on a autant des sous corps que des diviseur de $n$.

**Corollaire 26.** *La clôture algébrique $\overline{\mathbb{F}_p}$ de $\mathbb{F}_p$ est donnée par*

$$\bigcup_{n\geq 0} \mathbb{F}_{p^{n!}}.$$

**Définition 27.** On dit qu'un élément $\xi$ est primitif de $\mathbb{F}_q$ si $\mathbb{F}_q = \mathbb{F}_p(\xi)$.

**Théorème 28.** *Dans un corps fini il y a au moins un élément primitif.*

Noter que le théorème de l'élément primitif est vraie dans le cadre des extension algébriques finies.

*Démonstration.* Tout élément générateur du groupe multiplicatif $\mathbb{F}_q^\times$ est aussi primitif. Le nombre des élément primitifs est donc minoré par $\varphi(q-1) > 0$. □

La preuve précédente utilise dedans le fait que le groupe multiplicatif $\mathbb{F}_q^\times$ est cyclique. On donne maintenant une autre preuve plus élémentaire et qui vas de plus nous servir à minorer la probabilité de choisir au hasard un élément primitif.

Un élément $\xi$ est primitif ssi $\xi$ n'est pas racine de tout polynôme $x^{p^t} - x$ pour tout $t < n$ ( plus précisément $t$ diviseur propre de $n$). L'ensemble des racines des tels polynômes est borné par

$$\sum_{t=0}^{n-1} p^t = \frac{1-p^n}{1-p}.$$

Ainsi le nombre des éléments primitifs est au moins $p^n - \frac{1-p^n}{1-p} > 0$.

La borne $\sum_{t=0}^{n-1} p^t$ peut être remplacée par $\sum_{t=1}^{\lfloor n/2 \rfloor} p^t$ qui est plus optimale. Un gout probabiliste de la proposition précédente est le suivant : La probabilité de choisir par hasard un élément primitif de $\mathbb{F}_{p^n}$ est au moins

$$1 - \frac{1}{p^n} \cdot \frac{p - p^{1+\lfloor n/2 \rfloor}}{1-p} = 1 - \frac{1}{p-1}\left(\frac{1}{p^{n-1-\lfloor n/2 \rfloor}} - \frac{1}{p^{n-1}}\right) \geq 1 - \frac{1}{(p-1)(p^{n-1-\lfloor n/2 \rfloor})} \geq 1 - \frac{1}{(p-1)(p^{n/2-1})}$$

A titre indicatif, si on note $f(p,n) := 1 - \frac{1}{(p-1)(p^{n/2-1})}$ alors on la chance d'attraper un élément primitif dans $\mathbb{F}_{23^2}$ est au moins $f(23,2) \approx 0.95$. La croissance rapide de $f(p,n)$ implique que c'est quasi certain d'avoir un élément primitif lors d'un choix au hasard.

Un cas particulier où on peut déterminer exactement le nombre des éléments primitifs est le suivant.

**Proposition 29.** *Si $n = v^d$ avec $v$ premier alors on a $p^n - p^{v^{d-1}}$ éléments primitifs dans $\mathbb{F}_q$. Plus précisément, l'ensemble des tels éléments est $\mathbb{F}_{p^n} - \mathbb{F}_{p^{q^{d-1}}}$.*

*Démonstration.* Les diviseurs non triviaux de $n$ sont $q^t$, $t = 1, ..., d-1$. □

**Exemple 30.** Le corps $\mathbb{F}_{16}$ possède $2^{2^2} - 2^{2^{2-1}} = 16 - 4 = 12$. On remarque que c'est plus grand strictement que le nombre $\varphi(15) = 8$ représentant celui des générateurs de $\mathbb{F}_{16}^\times$.

**Lemme 31.** *Soit $f \in \mathcal{I}_{d,p}$. Alors*

$$f \mid x^{p^n} - x \iff d \mid n$$

*Démonstration.* Il résulte des équivalences suivantes

$$f \mid x^{p^n} - x \iff \mathbb{F}_{p^d} \subset \mathbb{F}_{p^n} \overset{(25)}{\iff} d \mid n$$

□

**Théorème 32.** *Dans $\mathbb{F}_p[x]$, on a*

$$x^{p^n} - x = \prod_{\substack{f \in \mathcal{I}_{d,p} \\ d \mid n}} f(x)$$

*In particulier, on retrouve le petit théorème de Fermat*

$$x^p - x = \prod_{\xi \in \mathbb{F}_p} (x - \xi)$$

*Démonstration.* On a

$$x^{p^n} - x = \prod_{\substack{f \in \mathcal{I}_{d,p} \\ d \mid n}} f(x)^{\nu_f} \tag{3.2}$$

où $\nu_f \in \mathbb{N}$. Or $x^{p^n} - x$ n'a que des racines simples car $\left(x^{p^n} - x\right)' = -1 \neq 0$. Donc $\nu_f = 1$ pour tout $f \in \mathcal{I}_{d,p}$. □

*Remarque* 33. Notez qu'on peut exprimer (3.2) avec une forme plus sophistiquée, à savoir

$$x^{p^n} - x = \prod_{d=1}^{+\infty} \left( \prod_{f \in \mathcal{I}_{d,p}} f(x) \right)$$

en remarquant que $\mathcal{I}_{d,p} = \emptyset$ si $d \nmid n$.

# 4 Factorisation des polynômes sur les corps finis.

## 4.1 Factorisation grossière.

**Définition 34.** Un polynôme $f$ de $\mathbb{F}_p[x]$ est dit *square free* s'il ne contient aucun facteur carré, i.e

$$h^2 \nmid f$$

pour tout $h \in \mathbb{F}_p[x]$.

**Lemme 35.** *Soit $f$ un polynôme square free de dégrée $d$ sur $\mathbb{F}_p$. Pour tout $r > 0$ on pose*

$$A_r = \prod_{\substack{h \in \mathcal{I}_{r,p} \\ h \mid f}} h.$$

*Alors*

$$A_r = \begin{cases} \text{pgcd}\,(f, x^p - x) & r = 1 \\ \text{pgcd}\left( \frac{f}{A_1 A_2 \cdots A_{r-1}}, x^{p^r} - x \right) & r > 1 \end{cases}$$

1. Si on utilise un polynôme arbitraire $f$ , l'algorithme précédent vas donner les facteurs sans préciser leurs multiplicités. Autrement dit, le produit des facteurs obtenus est exactement $\frac{f}{\text{gcd}(f,f')}$ qui est square free. Donc, pour gagner du temps, il vaut mieux utiliser dès le début le polynôme $\frac{f}{\text{gcd}(f,f')}$.
2. Lorsque l'algorithme retourne la valeur 1 pour un certain $A_r$, cela veut dire que $f$ n'a pas des racines dans $\mathbb{F}_{p^r} \setminus \mathbb{F}_{p^{r-1}}$.
3. Lorsque $f$ est de la forme
$$f = \prod_{\substack{h \in \mathcal{I}_{d,p} \\ h \mid f}} h$$
pour un certain $d$, l'algorithme va retourner $f$ comme facteur, autrement dit, il donne que des facteurs en bloc. Ceci représente un inconvénient malheureusement. Par d'exemple, si $f = x^3 + x^2 + x + 8$ sur $\mathbb{F}_{11}$ , l'algorithme ne va pas donner une factorisation. A titre d'information, la factorisation d'un tel polynôme est
$$f = (x-1)(x-2)(x-7)$$

**Exemple 36.** Soit à factoriser, sur $\mathbb{F}_7$, le polynôme

$$f = x^7 + 3x^6 + 3x^5 + x^4 + 3x^3 + 4x^2 + 3x + 3$$

On a :

1. $A_1 = \text{pgcd}\left(f, x^7 - x\right) = x^2 + 3x + 3.$
2. $A_2 = \text{pgcd}\left( \frac{f}{x^2+3x+3}, x^{7^2} - x \right) = x^2 + 4x + 6$
3. $A_2 = \text{pgcd}\left( \frac{f}{(x^2+3x+3)(x^2+4x+6)}, x^{7^3} - x \right) = x^3 + 3x^2 + 3x + 6$
4. C'est tout puisque la somme des dégrées est 7.

Ainsi

$$f = (x^2 + 3x + 3)(x^2 + 4x + 6)(x^3 + 3x^2 + 3x + 6)$$

## 4.2 Algorithme de Berlekamp

Un bon livre que je conseille ici est [4, Tome I]. C'est le livre avec lequel j'ai arrivé à comprendre l'algorithme de Berlekamp.

On considère un polynôme $f$ square free sur $\mathbb{F}_q$. On note

$$f = \prod_{i=1}^{r} f_i \tag{4.1}$$

la factorisation de $f$ en produit des facteurs irréductibles $f_1, ..., f_r$. Notre but est de trouver ces $f_1, ..., f_r$. L'idée essentielle de Berlekamp était de trouver un polynôme $v$ tel que $f$ divise $v^q - v$. Comme dans l'arithmétique usuel, on peut écrire

$$v(x)^q \equiv v(x) \bmod f$$

au lieu de $f$ divise $v^q - v$.

**Lemme 37.** *On a*

$$\frac{\mathbb{F}_q[x]}{< f >} \simeq \frac{\mathbb{F}_q[x]}{< f_1 >} \times \frac{\mathbb{F}_q[x]}{< f_2 >} \times \cdots \times \frac{\mathbb{F}_q[x]}{< f_r >}$$

*Démonstration.* C'est le lemme chinois tout simplement. □

**Théorème 38.** *S'il existe $v \in \mathbb{F}_q[x]$ tel que $f$ divise $v^q - v$, alors*

$$f(x) = \prod_{\xi \in \mathbb{F}_q} \operatorname{pgcd}(f(x), v(x) - \xi)$$

*Démonstration.* Les $\{v(x) - \xi\}_{\xi \in \mathbb{F}_q}$ sont 2 à 2 premiers entre eux, donc

$$\prod_{\xi \in \mathbb{F}_q} \operatorname{pgcd}(f(x), v(x) - \xi) = \operatorname{pgcd}\left(f(x), \prod_{\xi \in \mathbb{F}_q} (v(x) - \xi)\right).$$

Maintenant, en se basant sur l'identité

$$x^q - x = \prod_{\xi \in \mathbb{F}_q} (x - \xi)$$

on obtient

$$\prod_{\xi \in \mathbb{F}_q} \operatorname{pgcd}(f(x), v(x) - \xi) = \operatorname{pgcd}\left(f(x), \underbrace{v(x)^q - v(x)}_{\text{divisible par } f}\right) = f(x)$$

□

La question qui se pose ici est comment trouver un tel polynôme $v$ ? C'est la partie qui m'a trop énervé hhh.

Notons $d_k$ la dégrée de chaque $f_i$ apparaissant dans (4.1). Chaque quotient $\mathbb{F}_q[X] / < f_k >$ n'est autre que le corps fini $\mathbb{F}_{q^{d_k}}$ puisque $f_k$ est irréductible et c'est ici où on a besoin d'une telle hypothèse. Maintenant, soit $\xi_1, ..., \xi_r$ dans $\mathbb{F}_q$. Le lemme chinois garantie (c'est même son but) l'existence d'un élément $v \in \mathbb{F}_q[x]$ tel que

$$v(x) \equiv \xi_k \bmod f_k$$

pour tout $k$ entre 1 et $r$. Dans l'autre coté on a

$$v(x)^q \equiv v(x) \bmod f$$

puisque

$$\xi^q = \xi$$

sur $\mathbb{F}_q$.

Réciproquement, si $v(x)^q \equiv v(x) \bmod f$ alors, par l'identité

$$v(x)^q - v(x) = \prod_{\xi \in \mathbb{F}_q} (v(x) - \xi),$$

chaque $f_k$ divise au moins un certain $v(x) - \xi_k$ où $\xi_k \in \mathbb{F}_q$, i.e

$$v(x) \equiv \xi_k \bmod f_k$$

Par conséquence, on peut conclure qu'au total, on a autant des choix pour $v$ que pour les $\xi_k$, qui n'est autre que

$$q^r \tag{4.2}$$

choix.

Les candidats $v$ qu'on cherche sont finalement les points fixes de l'application $\mathbb{F}_q$- linéaire

$$\begin{array}{rccc} \omega : & \dfrac{\mathbb{F}_q[x]}{< f >} & \longrightarrow & \dfrac{\mathbb{F}_q[x]}{< f >}. \\ & v & \longmapsto & v(x)^q \end{array}$$

Dire point fixe d'un application linéaire, c'est dire le noyau de $\omega - Id_R$ où $R := \mathbb{F}_q[X] / < f >$(Anneau de Berlekamp). La question se réduit donc à trouver

$$\mathbf{W} := \ker(\omega - Id_R)$$

Voici comment procéder :

1. Pour tout $\ell$ entre 0 et $\deg f - 1$, calculer $\omega(x^\ell) = x^{\ell q} \bmod f$. Autrement dit pour chaque $\ell$, effectuer la division euclidienne de $x^{\ell q}$ par $f$ et garder le reste, disons

$$\rho_\ell := a_{0,\ell} + a_{1,\ell} x + \cdots + a_{\deg f - 1, \ell} x^{\deg f - 1}$$

2. La matrice de $\omega$ est tout simplement

$$\Omega = [a_{i,\ell}]_{0 \le i, \ell \le \deg f - 1} \in M(\deg f, \mathbb{F}_q)$$

3. Trouver un base de $W$. En particulier le nombre $r$ des facteurs irréductibles $f_i$ (figurant aussi dans (4.2)) est en fait la dimension de $W$. A titre d'information, $\mathbf{1}$ est dedans, ce qui n'est pas une surprise puisque $\xi^q - \xi = 0$ pour tout $\xi \in \mathbb{F}_q$, n'est ce pas ?.
   Deux cas se représentent également :
   (a) $r = \dim W = 1$ : $f$ est irréductible.
   (b) $r = \dim W > 1$ : $f$ est réductible et si on calcule les $\{\text{pgcd}(f(x), v(x) - \xi)\}_{\xi \in \mathbb{F}_q}$ pour quelques $v \in W$ jusqu'à recouvrir les facteurs $f_k$.

Je peut deviner une question que vous devez poser : Est ce qu'un seul choix $v \in W$ ne suffit pas ? Voici pourquoi la réponse est négative : Si c'était le cas, chaque $\{\text{pgcd}(f(x), v(x) - \xi)\}_{\xi \in \mathbb{F}_q}$ serait exactement l'un des $f_k$, mais ceci ne peut pas avoir lieu que si $q = r$, qui n'est pas toujours le cas. Pour balayer plusieurs choix possibles de $v$, on peut créer un code qui utilise un choix aléatoire pour $v$ à chaque fois. Autrement dit, si $\mathbf{1}, \sigma_\mathbf{2}, ..., \sigma_\mathbf{r}$ est la base (fixée) de $W$, on utilise $v$ de la forme

$$v = \lambda_1 \mathbf{1} + \lambda_2 \sigma_\mathbf{2} + ... + \lambda_r \sigma_\mathbf{r}$$

où les $\lambda_i$ sont choisis suivant un générateur aléatoire (uniforme) sur $\mathbb{F}_q$.

Je vous donne un code que j'ai écrit avec **Pari-GP.**

**Algorithme 1** Algorithme de Berlekamp sur $\mathbb{F}_p$

```
Ber_alg(p)={
  1. print(" Input non constant polynomial") ;
  2. f=input() ;
  3. g=f*Mod(1,p) ;
  4. f=f*Mod(1,p) ;
  5. f=(f/gcd(deriv(f),f)) ; % le square free dérivé de f
  6. d=poldegree(f) ;
  7. Id=matid(d) ; % la matrice identité
  8. Q=matrix(d,d,i,j,polcoeff(x^(p*(j-1))*Mod(1,p)%f,i-1))-Id ; % la matrice Ω − I_d
  9. W=matker(Q) ; % base de W
 10. s=(matsize(W))[2] ; % la dimension de W
 11. printf("Your normalised polynomial is " f "\n") ;
 12. if( s==1, printf("Your normalised polynomial is irreducible")) ;
 13. if( s>1, R=vector(s,i,random(p)) ; % vecteur aléatoire de F_p
     v=Mod(1,p)*sum(j=1,s,R[j]*sum(k=1,d,W[k,s]*x^(k-1))) ; % polynôme v aléatoire de W
     printf( "Some factors are :\n") ;
     fact=[;] ; % tableau unidimensionnel qui va contenir les facteurs
     for ( i=1,p,a=1/pollead(gcd(f,v-i)) ;
     if(poldegree(gcd(f,v-i))>0,fact=matconcat([fact ;[a*gcd(f,v-i),valuation(g,a*gcd(f,v-i))]]))
         ) ; % la valuation donne les multiplicités
     fact ;
     W ;
      ) ;
}
```

**Exemple 39.** Soit à factoriser

$$f = x^{11} + x^5 + x + 1$$

sur $\mathbb{F}_{11}$. Le code donne cette matrice

$$\begin{bmatrix} x^3 + 4x^2 + 10x + 3 & 1 \\ x^5 + 11x^4 + 7x^3 + 12x^2 + 8x + 7 & 1 \\ x^3 + 11x^2 + 8x + 5 & 1 \end{bmatrix}$$

où la deuxième colonne encode les multiplicités éventuelles. Donc la factorisation n'est autre que

$$f = (x^3 + 4x^2 + 10x + 3)(x^5 + 11x^4 + 7x^3 + 12x^2 + 8x + 7)(x^3 + 11x^2 + 8x + 5).$$

# References


[1] G. Gras and M.-N. Gras, *Algèbre fondamentale: arithmétique: niveau L3 et M1.* Elllipses, 2004. 1.1, 3, 3

[2] I. Gozard, *Théorie de galois.* Ellipses, 1997. 3, 3

[3] X. Gourdon, *Les Maths en tête: Mathématiques pour M*: algebre.* Ellipses-Marketing, 1994. 3

[4] J. M. Arnaudiès and J. Bertin, *Groupes, algèbres et géométrie.* Ellipses, 1993. 4.2