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

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

Commençons par quelques notations et rappels.

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

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

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

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

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

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

On démontre d'abord un critère général de cyclicité.

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

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

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

(3)⇒(1) : L'hypothèse permet d'écrire

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

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

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

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

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

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

Remarque 19. L'exercice 3.16 propose une autre démonstration du théorème précédent, basée sur le théorème de structure des groupes abéliens finis. Le corollaire 43 du chapitre 2 reste un argument clef.

Voici une conséquence importante du théorème 6.

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

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

4.6 Interlude cryptographique : Diffie-Hellman, El Gamal

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

4.6.1 Complexité de certains calculs modulaires

Cette section peut être réservée à une seconde lecture.

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

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

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

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

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

Sachant que le nombre de chiffres de m et n est majoré par N, et en se rappelant l'algorithme basique de multiplication appris à l'école primaire, on constate que le coût de la multiplication de m par n est majoré par quelque chose de l'ordre de N^2 opérations. Si

N de l'ordre de 100, c'est plus que raisonnable.

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

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

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

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

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

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

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

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

Si l'on souhaite par contre calculer successivement *toutes* les puissances $[n]_p^3$, $[n]_p^4$ jusqu'à $[n]_p^a$ (et l'on verra ci-dessous pourquoi on pourrait être amené à vouloir le faire) on revient a priori à une décomposition en a multiplications modulo p et à un coût prohibitif d'un ordre de grandeur de $N^2 10^N$ opérations.

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

4.6.2 L'échange de clés de Diffie-Hellman

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

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

L'échange du secret se déroule ainsi.

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

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

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

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

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

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

Insistons sur le fait que « difficile » doit se comprendre en termes de la complexité algorithmique. Bien sûr, on peut toujours, connaissant g et g^a, imaginer déterminer a en

calculant les puissances successives g^2, g^3,... jusqu'à trouver un puissance adéquate. Mais c'est beaucoup trop long dans la pratique (*cf.* la section précédente). Et on ne connaît aucun algorithme général de complexité raisonnable permettant de résoudre le logarithme discret, et on croit qu'il n'en existe pas (mais on ne sait pas le démontrer).

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

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

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

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

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

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

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

4.6.3 Le système de cryptographie à clef publique El Gamal

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

Les choses se déroulent alors ainsi :

1. Alice choisit un groupe cyclique G noté multiplicativement, et un générateur g de G. Elle choisit un entier a (dans la pratique, au hasard et assez grand) qu'elle tient soigneusement secret : il constitue sa clef privée. Elle calcule g^a et rend public (G, g, g^a) (sa clef publique).

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

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

4.7 Deux corps finis de même cardinal sont isomorphes

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

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

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

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

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

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

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

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

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

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

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

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

□

Remarque 20. Il peut être utile de rappeler comment à partir de l'élément y considéré dans la démonstration on construit un morphisme de $\mathbf{F}_p$-algèbres de $\mathbf{F}_p[X]/\langle P\rangle$ vers $\mathbf{L}$: on considère l'unique morphisme de $\mathbf{F}_p$-algèbre de $\mathbf{F}_p[X]$ vers $\mathbf{L}$ qui envoie X sur y. Ce morphisme a pour noyau $\langle P\rangle$ et induit donc le morphisme cherché.

Remarque 21. Considérons deux corps finis de même cardinal. Le théorème précédent montre qu'il existe alors un isomorphisme de l'un sur l'autre. Il est important de noter qu'un tel isomorphisme n'est pas unique en général.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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