CORPS FINIS

par

Mathieu Vienney

La plupart des résultats de base sur les corps finis, y compris l'existence et l'unicité se trouvent dans de nombreux livres d'algèbre, on pourra citer par exemple [Per82] ou [Lan02].
Le livre de Lidl et Niederreiter [LN97] est également une excellent référence, incluant des sujets plus approfondis.

1. Notations et rappels

Tous les anneaux considérés seront considérés commutatifs unitaires, et un morphisme d'anneaux $A \to B$ enverra 1_A sur 1_B.
De même, les corps seront toujours commutatifs [1]. Un ensemble muni de deux lois de composition qui vérifie tous les axiomes d'un corps sauf la commutativité de la multiplication sera appelé une algèbre à division [2].

Proposition 1.1. — *Si A est un anneau, on appelle caractéristique de A, et on note $\mathbf{car}A$ l'unique entier positif n tel que le noyau de l'unique morphisme $\mathbf{Z} \to A$ soit égal à $n\mathbf{Z}$.*
Si A est intègre, alors $\mathbf{car}A$ est égal à 0 où à un nombre premier p.
On appelle alors sous-corps premier de A l'image du morphisme $\mathbf{Z} \to A$: il est isomorphe à $\mathbf{Q}$ si $\mathbf{car}A = 0$ et à $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ si $\mathbf{car}A = p$.
Si A est de caractéristique p, alors l'application $x \mapsto x^p$ est un endomorphisme d'anneau de A, appelé morphisme de Frobenius.

La proposition suivante donne quelques exemples de corps :

1. Contrairement à la terminologie de Bourbaki qui autorise la multiplication des corps à être non-commutative.
2. On rencontre parfois la terminologie *corps non commutatif*, ou encore *corps gauche*, en anglais *skew field*.

Proposition 1.2. — *Un anneau intègre fini est un corps.*

Démonstration. — Soit A un tel anneau, et $x \in A - \{0\}$. Alors $x \mapsto a.x$ est injective, donc surjective par cardinalité. En particulier, il existe un inverse à a, qui est l'image réciproque de 1 par cette application. □

En particulier, on en déduit que si p est un nombre premier, alors $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ est un corps de cardinal p.
En fait, l'hypothèse de commutativité de l'anneau est superflue par le théorème suivant :

Théorème 1.3 **(Wedderburn)**. — *Une algèbre à division finie est un corps.*

La proposition suivante résulte en fait d'un résultat de théorie des groupes :

Proposition 1.4. — *Si G est un sous-groupe du groupe multiplicatif d'un corps, alors G est cyclique.*

Corollaire 1.5. — *Si K est un corps fini de cardinal q, alors $(K^\times, \times)$ est isomorphe à $\mathbf{Z}/(q-1)\mathbf{Z}$.*

Corollaire 1.6. — *Un corps fini n'est jamais algébriquement clos.*

Démonstration. — Soit K un corps de cardinal q. Alors tous les éléments non nuls de K vérifient $x^{q-1} = 1$, et donc tous les éléments de K vérifient $x^q - x = 0$. Par conséquent, le polynôme $X^q - X + 1$ ne possède pas de racine dans K. □

1.1. Quelques rappels de théorie des corps. — Dans toute cette partie, K est un corps, et si besoin, on notera $\overline{K}$ une clôture algébrique de K. On rappelle qu'une telle clôture existe et est unique à K-isomorphisme près. Tous les faits suivants sont rappelés sans démonstration. On pourra par exemple consulter [Per82] ou [Lan02].

Définition 1.7. — Si $P \in K[X]$ est un polynôme irréductible, on appelle corps de rupture de P une extension L/K telle qu'il existe $\alpha \in L$ tel que
- $P(\alpha) = 0$,
- $L = K(\alpha)$.

Théorème 1.8. — *Si $P \in K[X]$ est un polynôme irréductible, alors il existe un corps de rupture de P.*
De plus, si L est un corps de rupture de P, alors L est K-isomorphe à $K[X]/(P)$. En particulier, si L et L' sont deux corps de rupture de P, alors ils sont K-isomorphes.

Remarque 1.9. — À l'intérieur de $\overline{K}$, il n'y a pas unicité d'un corps de rupture : il peut y avoir deux corps de rupture distincts d'un même polynôme P. Par exemple dans $\mathbf{Q}[X]$, le polynôme $P = X^3 - 2$ est irréductible, et $\mathbf{Q}(\sqrt[3]{2}) \subset \overline{\mathbf{Q}}$ et $\mathbf{Q}(j\sqrt[3]{2}) \subset \overline{\mathbf{Q}}$ sont deux sous-corps distincts de $\overline{\mathbf{Q}}$, qui sont deux corps de rupture de P. Par contre, le théorème nous affirme qu'ils sont isomorphes.

On prendra donc toujours soin à parler d'*un* corps de rupture, et non pas *du* corps de rupture.

Définition 1.10. — Si $P \in K[X]$, on appelle corps de décomposition de P une extension L/K telle qu'il existe $\alpha_1, \ldots, \alpha_n \in L$ tels que :
- $L = K(\alpha_1, \ldots, \alpha_n)$,
- $P = \prod_{i=1}^{n}(X - \alpha_i) \in L[X]$.

En particulier, on demande à P d'être scindé (avec éventuellement des racines multiples) dans L.

Théorème 1.11. — *Si $P \in K[X]$, il existe un corps de décomposition de P.*
De plus, si L et L' sont deux corps de décomposition de P, alors il existe un isomorphisme de K-extensions $L \simeq L'$.

Remarque 1.12. — Une fois l'existence d'un corps de rupture pour un polynôme irréductible établie, la preuve de l'existence d'un corps de décomposition se fait par récurrence en utilisant des corps de rupture des facteurs irréductibles de P.
La définition prouve notamment qu'un corps de décomposition est une extension algébrique de K.
Cette fois on a l'unicité du corps de décomposition au sein d'une clotûre algébrique. En effet, si $P = \prod_{i=1}^{n}(X - \alpha_i) \in \overline{K}[X]$, alors un sous-corps de $\overline{K}$ qui est un corps de décomposition de P est nécessairement le corps engendré sur K par les α_i. Une fois une clôture algébrique fixée, on pourra donc parler *du* corps de décomposition de P.

Définition 1.13. — Un polynôme est dit séparable si P est à racines simples dans une clotûre algébrique (ou dans un corps de décomposition). Un élément d'une extension L de K est dit séparable si son polynôme minimal sur K est séparable. Une extension algébrique L/K est dite séparable si tous les éléments de L sont séparables sur K.
Un corps est dit parfait si toutes ses extensions algébriques sont séparables. Tout corps de caractéristique nulle est parfait, et un corps de caractéristique $p > 0$ est parfait si et seulement si l'application $x \mapsto x^p$ est surjective de K dans lui-même.

Théorème 1.14 **(Théorème de l'élément primitif)**. — *Si L/K est une extension séparable finie, alors elle est monogène : il existe $x \in L$ tel que $L = K(x)$.*

Remarque 1.15. — Le théorème n'est bien sûr plus valable pour une extension qui n'est plus finie.

2. Existence et unicité des corps finis

Nous avons déjà donné un exemple de corps fini : il s'agit de $\mathbf{F}_p$, qui est de cardinal p. En fait, nous avons une restriction sur le cardinal d'un corps fini.

Proposition 2.1. — *Soit K un corps fini, de caractéristique p. Alors il existe $n \geq 1$ tel que K soit de cardinal p^n.*

Démonstration. — K est un espace vectoriel sur son sous-corps premier, isomorphe à $\mathbf{F}_p$. Il est de dimension finie par cardinalité, et alors le cardinal de K est $p^{\dim_{\mathbf{F}_p} K}$. □

Lemme 2.2. — *Si k est un corps de cardinal $q = p^n$, alors le polynôme $X^q - X$ est scindé sur K.*

Démonstration. — Puisque $K^\times$ est cyclique, de cardinal $q-1$, tout élément non nul x de K vérifie $x^{q-1} = 1$, et donc tout élément de K est racine de $X^q - X$. Par cardinalité, on en déduit que $X^q - X = \prod_{x \in K}(X - x) \in K[X]$. □

Corollaire 2.3. — *Si K est de cardinal q, alors K est un corps de décomposition de $X^q - X \in \mathbf{F}_p[X]$.*

Le théorème suivant est fondamental dans l'étude des corps finis, puisqu'il prouve qu'il existe une réciproque à la proposition 2.1.

Théorème 2.4 **(Existence et unicité des corps finis)**. — *Soit p un nombre premier, et $n \geq 1$. Alors il existe un corps de cardinal p^n.*
De plus, si K et K' sont deux corps de cardinal p^n, alors $K \simeq K'$.

Démonstration. — Commençons par l'existence. Si on savait qu'il existe toujours un polynôme irréductible de degré n sur $\mathbf{F}_p[X]$, alors il serait possible de conclure directement en prenant un corps de décomposition d'un tel polynôme. Malheureusement nous n'en savons pas autant, nous reviendrons sur l'existence, et même le dénombrement de tels polynômes plus loin.
Si $q = p^n$, soit $P = X^q - X \in \mathbf{F}_p[X]$, et soit K un corps de décomposition de P. Puisque le polynôme $P' = -1$ ne possède pas de racines, P est un polynôme séparable, et donc possède q racines distinctes dans K.
Soit S l'ensemble de ces racines. Alors S est un sous-corps de K puisque

- $0, 1 \in S$,
- $(a-b)^q = a^q - b^q$,
- $(ab^{-1})^q = a^q b^{-q}$.

Mais nous avons dit que l'ensemble de ces racines était de cardinal q, donc $S = K$ est un corps de cardinal q.

Passons à l'unicité. Si K est un corps de cardinal q, alors par le corollaire 2.3, K est un corps de rupture de $X^q - X \in \mathbf{F}_p[X]$. Le résultat est alors une conséquence de l'unicité (à isomorphisme près) du corps de décomposition. □

On notera $\mathbf{F}_q$ un corps de cardinal q, unique à isomorphisme près (on verra plus tard que si $n \geq 2$, alors $\mathbf{F}_q$ admet des isomoprhismes non triviaux, donc il n'y a en général pas unicité de l'isomorphisme entre deux corps de même cardinal).


Si $n > 1$, alors $\mathbf{F}_{p^n}$ n'est pas l'anneau $\mathbf{Z}/p^n\mathbf{Z}$ (d'ailleurs ce dernier n'est alors plus intègre). Toutefois, les structures additives et mutliplicatives de $\mathbf{F}_{p^n}$ ne sont pas mystérieuses : on a

- $(\mathbf{F}_{p^n}, +) = (\mathbf{Z}/p\mathbf{Z})^n$,
- $\mathbf{F}_{p^n}^\times, \times) = \mathbf{Z}/(p^n - 1)\mathbf{Z}$.

Ce qui est plus mystérieux (encore que...) est le lien entre ces deux structures.

Nous verrons au chapitre suivant comment construire les corps finis et calculer dedans.

Nous savons que si K est un corps de cardinal $q = p^n$, alors tous ses sous-corps sont de cardinal une puissance de p. Le théorème suivant nous renseigne sur le lien entre ces différents sous-corps.

Théorème 2.5. — *Soit K un corps de cardinal $q = p^n$. Alors tout sous-corps de $\mathbf{F}_q$ est de cardinal p^m (et donc isomorphe à $\mathbf{F}_{p^m}$) où m divise n.*
Inversement, si $m \mid n$, alors il existe un unique sous-corps de K de cardinal p^m.

Démonstration. — Si L est un sous-corps de K, alors $\mathbf{F}_p \subset L \subset K$, et donc

$$n = [K : \mathbf{F}_p] = [K : L][L : \mathbf{F}_p],$$

donc $[L : \mathbf{F}_p]$ est un diviseur de n, et le cardinal de L est $p^{[L:\mathbf{F}_p]}$.

Inversement, supposons que m soit un diviseur de n. Il est classique que $p^m - 1$ divise $p^n - 1$. Alors $X^{p^n} - X = X \prod_{d|p^n-1} \overline{\Phi_d}(X)$, et donc $X^{p^m} - X = X \prod_{d'|p^m-1} \overline{\Phi_{d'}}(X)$ divise $X^{p^n} - X$, où $\overline{\Phi_d} \in \mathbf{F}_p[X]$ désigne la réduction modulo p du d-ième polynôme cyclotomique. En particulier, puisque $X^{p^n} - X$ est scindé à racines simples dans K, c'est également le cas de $X^{p^m} - X$. On peut montrer comme précédemment en utilisant le morphisme de Frobenius que l'ensemble de ses racines forme un sous-corps de K, de cardinal p^m.
Un tel sous-corps est alors unique, puisqu'il s'agit d'un corps de décomposition de $X^{p^n} - X$, et donc est nécessairement le sous-corps-corps de K engendré par les racines de $X^{p^n} - X$. □

Remarque 2.6. — Ce théorème nous permet vraiment de connaitre les différentes extensions de $\mathbf{F}_p$: les liens entre elles sont juste donnés par les relations de divisibilité entre leurs degrés.

Proposition 2.7. — *Un corps fini est parfait.*

Démonstration. — Un corps de caractéristique p est parfait si et seulement le morphisme de Frobenius y est surjectif. Or, dans un corps fini, il est bijectif. □

Corollaire 2.8. — *Il existe des polynômes irréductibles sur* $\mathbf{F}_q$ *de tout degré.*

Démonstration. — $\mathbf{F}_{q^n}$ est une extension séparable de degré n de $\mathbf{F}_q$, donc il existe $\alpha \in \mathbf{F}_{q^n}$ tel que $\mathbf{F}_{q^n} = \mathbf{F}_q(\alpha)$. Soit alors P_α le polynôme minimal de α sur $\mathbf{F}_q$: il est irréductible par définition, et nécessairement de degré n, puisque $\mathbf{F}_{q^n}$ en est un corps de rupture sur $\mathbf{F}_q$. □

Remarque 2.9. — En fait, nous verrons plus tard une formule permettant de donner exactement le nombre de tels polynômes.

3. Polynômes et racines dans les corps finis

Dans un corps fini, il n'y a plus de bijection entre polynômes et fonctions polynomiales. Par exemple, dans $\mathbf{F}_q$, $x \mapsto x$ et $x \mapsto x^q$ définissent la même fonction.

3.1. Quelques mots sur la clôture algébrique d'un corps fini. — Soit $\overline{\mathbf{F}_p}$ une clôture algébrique de $\mathbf{F}_p$.
Alors $X^{p^n} - X$ est scindé (à racines simples) dans $\overline{\mathbf{F}_p}$. On montre aisément que l'ensemble de ses racines forme un corps, qui est donc de cardinal p^n : il est isomorphe à $\mathbf{F}_{p^n}$. Inversement, un sous-corps de $\overline{\mathbf{F}_p}$ de cardinal p^n devra être égal à l'ensemble de ces racines.

Proposition 3.1. — $\overline{\mathbf{F}_p}$ *contient un unique sous-corps de cardinal* p^n*, pour tout* $n \geq 1$*. On le note* $\mathbf{F}_{p^n} \subset \overline{\mathbf{F}_p}$*.*

Théorème 3.2. — *On a*

$$\overline{\mathbf{F}_p} = \bigcup_{n \geq 1} \mathbf{F}_{p^n}.$$

Démonstration. — Si $\alpha \in \overline{\mathbf{F}_p}$, alors α est algébrique sur $\mathbf{F}_p$, et donc si P_α est son polynôme minimal, $n = \deg P_\alpha$, alors $\mathbf{F}_p(\alpha) = \mathbf{F}_{p^n}$, et donc $\alpha \in \mathbf{F}_{p^n}$. □

Remarque 3.3. — Cette construction n'est valable qu'à l'intérieur d'une clôture algébrique de $\mathbf{F}_p$, ou au moins d'une extension algébriquement close de $\mathbf{F}_p$. Sans ça, l'union n'a plus de sens ensemblistement (tout ce qu'on sait faire est prendre une union de sous-ensembles d'un même ensemble). On peut toutefois s'en tirer au prix d'un procédé de limite inductive (à déconseiller fortement le jour de l'oral sauf si vous êtes vraiment familier avec cette construction).

3.2. Polynômes irréductibles. — Dans tout ce paragraphe, on pourra se placer dans une clôture algébrique de $\mathbf{F}_p$, et les corps de rupture et corps de décomposition considérés seront alors vus comme sous-corps de cette clôture algébrique.

Lemme 3.4. — *Soit $P \in \mathbf{F}_q[X]$, irréductible de degré m. Alors P divise $X^{q^n} - X$ si et seulement si m divise n.*

Démonstration. — Si P divise $X^{p^n} - X$, soit α une racine de P dans un corps de décomposition de P sur $\mathbf{F}_q$. Alors $\alpha^{q^n} = \alpha$, donc $\mathbf{F}_q(\alpha)$ est un sous-corps de $\mathbf{F}_{q^n}$, donc de degré (égal à m) sur $\mathbf{F}_p$ divisant n.

Inversement, si m divise n, alors $\mathbf{F}_{q^m} \subset \mathbf{F}_{q^n}$. Si α est une racine de P dans un corps de décomposition de P sur $\mathbf{F}_q$, alors $[\mathbf{F}_q(\alpha) : \mathbf{F}_q] = m$, et donc $\mathbf{F}_q(\alpha) = \mathbf{F}_{q^m}$.
On en déduit que $\alpha \in \mathbf{F}_{q^n}$, et donc que α est racine de $X^{q^n} - X$. Mais P étant irréductible, c'est le polynôme minimal de α, et donc il divise $X^{p^n} - X$. □

Théorème 3.5. — *Pour tout entier $n \in \mathbf{N}$, le produit des polynômes irréductibles unitaires de $\mathbf{F}_q[X]$ dont le degré divise n est égal à $X^{p^n} - X$.*

Démonstration. — Par la proposition précédente, les facteurs irréductibles de $X^{p^n} - X$ sont exactement les polynômes irréductibles unitaires de degré divisant n.
Il suffit donc de voir qu'il n'y a pas de facteurs multiples, mais puisque $(X^{p^n} - X)' = -1$, $X^{p^n} - X$ ne possède pas de facteurs multiples, d'où le résultat. □

Ce résultat permet de dénombrer précisément le nombre de polynômes irréductibles de degré donné dans $\mathbf{F}_q[X]$, ce qui nécessite l'utilisation de la formule d'inversion de Möbius.

Si on note a_d le nombre de polynômes irréductibles unitaires de degré d sur $\mathbf{F}_q$, alors le théorème précédent nous permet d'obtenir immédiatement la formule suivante :

$$q^n = \sum_{d|n} d a_d.$$

Une application de la formule d'inversion de Möbius nous permet alors d'obtenir immédiatement le résultat suivant :

Proposition 3.6. — *Pour tout entier $n \geq 1$,*

$$a_n = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d.$$

Remarque 3.7. — Si on ne souhaite pas parler d'extension séparable et d'élément primitif, l'un des moyens d'obtenir l'existence de polynômes irréductibles de tout degré est de prouver cette formule, puis de montrer que a_n est toujours strictement positif (ce que nous savons déjà).

Proposition 3.8. — *Soit $P \in \mathbf{F}_q[X]$ irréductible de degré m. Alors P possède une racine α dans $\mathbf{F}_{q^m}$.*
De plus, toutes les racines de P sont simples, données par $\alpha, \alpha^q, \dots, \alpha^{q^m-1}$.

Démonstration. — Un corps de rupture de P est $\mathbf{F}_{q^m}$. Si $\beta \in \mathbf{F}_{q^m}$ est une racine de P, alors β^q est aussi une racine de P. En effet, notons $P = \sum a_i X^i$. Alors $P(\beta^q) = \sum a_i \beta^{qi} = \sum a_i^q \beta^{iq} = P(\beta)^q$.
Donc $\alpha, \alpha^q, \dots, \alpha^{q^m-1}$ sont des racines de P. Supposons qu'elles ne soient pas distinctes, et que $\alpha^{q^i} = \alpha^{q^j}$, avec $0 \leq i < j \leq q^m - 1$. En multipliant par α^{q^m-j}, on obtient $\alpha^{q^{m-j+i}} = \alpha^{q^m} = \alpha$. Or ceci n'est posible que si m divise $m - j + i$, d'où une contradiction. □

Nous en déduisons le résultat suivant, qui est vraiment typique des corps finis et n'est plus valide dans un corps quelconque.

Corollaire 3.9. — *Si $P \in \mathbf{F}_p[X]$ est un polynôme irréductible, alors un corps de rupture de P en est un corps de décomposition.*

Corollaire 3.10. — *Deux polynômes irréductibles de même degré ont même corps de décomposition.*

3.2.0.1. Application : construction des corps de petit cardinal.— Nous savons que $\mathbf{F}_{p^n} = \mathbf{F}_p[X]/(P)$, où $P \in \mathbf{F}_p[X]$ est irréductible de degré n.
Il est possible d'énumérer récusrivement les polynômes irréductibles de degré donné de $\mathbf{F}_p[X]$. Par exemple, pour $p = 2$, X^2+X+1 est le seul polynpôme de degré 2 ne possèdant pas de racine, et donc le seul irréductible. En degré 3, seuls $X^3 + X^2 + 1$ et $X^3 + X + 1$ ne possèdent pas de racine. Enfin, un polynôme irréductible de degré 4 ne doit pas avoir de racine, et ne doit pas être produit de deux facteurs irréductibles de degré 2. On en déduit qu'ici $X^4 + X^3 + 1$, $X^4 + X + 1$ et $X^4 + X^3 + X^2 + X + 1$ conviennent. Et ainsi de suite...
Notons que si on souhaite effectuer des calculs, nous avons tout intérêt à choisir un polynôme irréductible qui possède le moins de coefficients non nuls possible.

Remarque 3.11. — Profitons-en pour rappeler qu'un polynôme de $\mathbf{F}_2[X]$ possède 0 comme racine si et seulement si son terme constant est nul, et 1 comme racine si et seulement si il possède un nombre impair de coefficients non nuls.

3.3. Racines de l'unité dans les corps finis. — Nous savons déjà que $\mathbf{F}_q$ contient $q - 1$ racines $(q - 1)$-ièmes de l'unité distinctes.
De même, remarquons que $\mathbf{F}_q$ ne contient pas de racine q-ième de l'unité non triviale, puisque $X^q - 1 = (X - 1)^q$.

Définition 3.12. — On notera $\mu_n(\overline{\mathbf{F}_p}) = \{x \in \overline{\mathbf{F}_p} : x^n = 1\}$ l'ensemble des racines n-ièmes de l'unité dans une clôture algébrique de $\mathbf{F}_p$.

Proposition 3.13. — *Soit $n \geq 1$ et p un entier premier. Alors :*

(1) Si p ne divise pas n, alors $\mu_n(\overline{\mathbf{F}_p})$ est cyclique d'ordre n.

(2) Si $n = p^k m$, avec p ne divisant pas m, alors $\mu_n(\overline{\mathbf{F}_p}) = \mu_m(\overline{\mathbf{F}_p})$, chaque racine m-ième de l'unité étant racine de multiplicité p^k de $X^n - 1$.

Démonstration. — Dans le cas où p et n sont premiers entre eux, alors $(X^n-1)' = nX^{n-1}$ est non nul et premier avec $X^n - 1$, donc $X^n - 1$ ne possède que des racines simples dans $\overline{\mathbf{F}_p}$. La structure de groupe de $\mu_n(\overline{\mathbf{F}_p})$ découle alors de la proposition 1.4.

Dans le cas où p divise n, alors le résultat est immédiat car $(X^n - 1) = (X^m - 1)^{p^k}$. □

3.4. Groupe de Galois des corps finis. — La théorie de Galois n'est pas au programme de l'agrégation, mais un candidat à l'aise avec le sujet pourra sans problème en parler un peu. Il semble toutefois utile de connaitre au moins le groupe de Galois d'une extension de corps finis, et si l'on ne souhaite pas parler de groupe de Galois, il suffit de voir cela comme le groupe des automorphismes $\mathbf{F}_p$-linéaires de $\mathbf{F}_q$.

Nous connaissons déjà un automorphisme non trivial (dès que $q \neq p$) de $\mathbf{F}_q$: il s'agit du morphisme d'élévation à la puissance p, qui est d'ordre n si $q = p^n$. Ainsi, $\mathrm{Gal}(\mathbf{F}_q/\mathbf{F}_p)$ contient un sous-groupe isomorphe à $\mathbf{Z}/n\mathbf{Z}$.

En fait, il s'agit là de tous les automorphismes de $\mathbf{F}_q$, ce qui s'obtient aisément si l'on sait qu'une extension de degré n possède au plus n automorphismes. Toutefois, dans ce cas il est possible de le reprouver directement :

Théorème 3.14. — *Les automorphismes de corps de $\mathbf{F}_{p^n}$ sont exactement les puissances de l'automorphisme de Frobenius $\varphi : x \mapsto x^p$. En particulier,* $\mathrm{Gal}(\mathbf{F}_{p^n}/\mathbf{F}_p) = \mathbf{Z}/n\mathbf{Z}$.

Démonstration. — Soit $\psi \in \mathrm{Gal}(\mathbf{F}_{p^n}/\mathbf{F}_p)$, et soit $\alpha \in \mathbf{F}_{p^n}$ tel que $\mathbf{F}_{p^n} = \mathbf{F}_p(\alpha)$. Soit $P = \sum_{i=0}^{n} a_i X^i$ le polynôme minimal de α sur $\mathbf{F}_p$.
Alors $\psi(\alpha)$ doit être une racine de P, et par la proposition 3.8, doit être de la forme α^{p^j}, pour $0 \leq j \leq n-1$. Mais puisque ψ est $\mathbf{F}_p$-linéaire, $\psi = \varphi^j$. □

Remarque 3.15. — La même preuve nous montrerait que l'ensemble des automorphismes $\mathbf{F}_q$-linéaires de $\mathbf{F}_{q^n}$ est le groupe cyclique engendré par $x \mapsto x^q$, et donc isomorphe à $\mathbf{Z}/n\mathbf{Z}$.
Mais le lecteur familier avec la théorie de Galois peut en déduire ce résultat directement en voyant qu'il s'agit d'un sous-groupe d'ordre n de $\mathrm{Gal}(\mathbf{F}_{q^n}/\mathbf{F}_p)$.

4. Quelques remarques complémentaires

Il existe de nombreuses analogies entre les anneaux de polynômes sur les corps finis et l'anneau des nombres entiers (ou plus généralement les anneaux d'entiers de corps de nombre). On pourra lire avec profit les deux premiers chapitres de [Ros02] pour comprendre cette analogie. On y trouvera notamment une preuve de la formule donnant le nombre de polynômes irréductibles de degré donné qui utilise un analogue de la fonction ζ de Riemann et un développement en produit eulérien.

Il peut être utile, notamment pour les candidats en option C de connaitre l'algorithme de Berlekamp, qui est un algorithme de factorisation des polynômes à coefficients dans un corps fini.

Enfin, des exemples d'application, comme les codes correcteurs d'erreur seront toujours fort appréciés par un jury d'agreg.

Références

[Lan02] Serge Lang, *Algebra*, 3rd ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002.

[LN97] Rudolf Lidl and Harald Niederreiter, *Finite fields*, 2nd ed., Encyclopedia of Mathematics and its Applications, vol. 20, Cambridge University Press, Cambridge, 1997. With a foreword by P. M. Cohn.

[Per82] Daniel Perrin, *Cours d'algèbre*, Collection de l'École Normale Supérieure de Jeunes Filles [Collection of the École Normale Supérieure de Jeunes Filles], vol. 18, École Normale Supérieure de Jeunes Filles, Paris, 1982 (French). Edited with the collaboration of Marc Cabanes and Martine Duchene.

[Ros02] Michael Rosen, *Number theory in function fields*, Graduate Texts in Mathematics, vol. 210, Springer-Verlag, New York, 2002.

Mathieu Vienney