EXTENSIONS DE CORPS

Ce polycopié présente les notions de base sur les extensions de corps et leurs applications (incluant les corps finis), allant jusqu'à la préparation de la théorie de Galois.

Tous les corps considérés seront commutatifs, et on désigne toujours par K un corps de base fixé.

1 Extensions de corps

Définition.

Une *extension L de K*, notée L/K, est la donnée d'un corps L et, de manière équivalente, de

(i) Un morphisme de corps $\iota : K \to L$ (forcément injectif).

(ii) Une structure de K-espace vectoriel sur L.

Pour faciliter les notations, on supposera souvent que $K \subset L$ en tant qu'ensembles. Le morphisme de corps est alors l'inclusion, et la structure de K-espace vectoriel est celle donnée par multiplication par les éléments de K dans L.

— Une *sous-extension de L/K* est un sous-corps de L contenant K.

— L'extension L/K est *finie* si L est de dimension finie en tant que K-espace vectoriel, *infinie* sinon. On appelle *degré de l'extension*, noté $[L : K]$, cette dimension.

— Si L et L' sont deux extensions de K, un *K-morphisme* $\sigma : L \to L'$ est un morphisme de corps qui est de plus K-linéaire (ce qui revient à dire qu'il est l'identité sur K si $K \subset L, L'$). Si σ est un isomorphisme, son inverse est également K-linéaire et on parle alors d'*isomorphisme de K-extensions*.

— En particulier, les automorphismes de L/K sont les automorphismes K-linéaires de L, on note leur ensemble $\mathrm{Aut}_K(L)$.

Exercice 1. Vérifier l'équivalence, et pourquoi on peut toujours se ramener à $K \subset L$.

Exemple. Le corps $\mathbb{C}$ est une extension de $\mathbb{R}$ finie de degré 2, et $\mathbb{R}$ est une extension infinie de $\mathbb{Q}$ car il est indénombrable.

Proposition 1 (Théorème de la base téléscopique)**.**

Soient M/L et L/K deux extensions finies.

On pose $(e_i)_{i\in I}$ une K-base de L et $(f_j)_{j\in J}$ une L-base de M. Alors, $(e_i f_j)_{(i,j)\in I\times J}$ est une K-base de M.

En particulier, M/K est une extension finie et

$$[M : K] = [M : L][L : K].$$

Démonstration. Soit $m \in M$. Par hypothèse, on peut écrire

$$m = \sum_{j\in J} \mu_j f_j, \quad m_j \in L.$$

Ensuite, par hypothèse sur L, pour tout $j \in J$, on peut écrire

$$\mu_j = \sum_{i\in I} \lambda_{i,j} e_i.$$

Alors, on a

$$m = \sum_{\substack{i\in I\\ j\in J}} \lambda_{i,j} e_i f_j,$$

ce qui prouve que la famille $(e_i f_j)_{i,j}$ est K-génératrice de M. Réciproquement, supposons qu'on a une telle écriture pour $m = 0$, montrons que les $\lambda_{i,j}$ sont tous nuls. On écrit

$$0 = \sum_{j \in J} (\sum_{i \in I} \lambda_{i,j} e_i) f_j$$

donc par liberté de $(f_j)_j$, pour tout $j \in J$,

$$\sum_{i \in I} \lambda_{i,j} e_i = 0,$$

et donc les $\lambda_{i,j}$ sont tous nuls par liberté de $(e_i)_i$. On a donc bien prouvé que notre famille est une K-base, et le reste en découle directement. □

Voici une construction naturelle d'extension de corps. Avant de la poser, on donne le lemme suivant, car il sera utilisé à répétition (et sans mention explicite) dans la suite.

Lemme. *Soient A et A' deux K-algèbres (unitaires, commutatives). Alors, pour tout morphisme de K-algèbres $\sigma : A \to A'$, tout polynôme $Q \in K[X]$ et tout $a \in A$,*

$$Q(\sigma(a)) = \sigma(Q(a)).$$

En particulier, si $A = K[a]$ pour un certain a, un tel morphisme σ est entièrement déterminé par $\sigma(a)$.

Définition (Corps de rupture)**.**
Soit $P \in K[X]$ irréductible. Le *corps de rupture de P* (sur K) est le corps $K[X]/(P)$. C'est une extension de corps de K de degré $\deg P$.

Pour toute extension L/K, les K-morphismes $\sigma : K[X]/(P) \to L$ sont en bijection avec les racines de P dans L via l'application $\sigma \mapsto \sigma(\overline{X})$. Le corps de rupture est ainsi « la plus petite extension contenant une racine de P ».

Démonstration. Tout d'abord, $K[X]/(P)$ est bien un corps car P étant irréductible, (P) est un idéal maximal de $K[X]$ (cet anneau étant principal, mais on peut le vérifier à la main avec une relation de Bézout). La structure d'extension de K peut se voir alternativement comme la structure K-linéaire naturelle, ou bien l'image de K via la projection canonique $K[X] \to K[X]/(P)$.

Soit maintenant une extension L/K. Si σ est un K-morphisme de $K[X]/(P)$ dans L, par construction, pour tout polynôme Q de $K[X]$ et tout $x \in K[X]/(P)$ on a

$$\sigma(Q(x)) = Q(\sigma(x)).$$

En particulier, pour $x = \overline{X}$ et $Q = P$, on a $P(\sigma(\overline{X})) = \sigma(P(\overline{X})) = \sigma(\overline{P}) = 0$. Donc $\sigma(\overline{X})$ est bien une racine de P dans L.

Réciproquement, si x est une racine de P dans L, le morphisme d'évaluation $K[X] \to L$ qui à Q associe $Q(x)$ est un morphisme d'anneaux, et son noyau contient (P) par hypothèse, d'où la factorisation $K[X]/(P) \to L$. □

Lorsqu'on s'intéresse à une extension de corps, on essaie, comme souvent, de la décrire la plus simplement possible, donc par générateurs.

Définition (Générateurs)**.**
Soit L une extension de K et S une partie de L. On note $K(S)$ la plus petite sous-extension de L contenant S (par exemple l'intersection de toutes ces sous-extensions). C'est également l'ensemble des fractions rationnelles en les éléments de S.

En particulier, pour tout $x \in L$, on note $K(x)$ l'extension engendré par x. On dit que L/K est engendrée par x si $L = K(x)$.

Remarque. Attention, le fait d'être engendré par une certaine famille dépend du corps de base ! Penser à $L = L(1)$ par exemple, ou un peu plus subtilement à $\mathbb{C}/\mathbb{Q}$ comparée à $\mathbb{C}/\mathbb{R}$.

Exercice 2. Trouver des générateurs de $\mathbb{C}/\mathbb{R}$ et $K(X)/K$.

Maintenant qu'on a affaire à des générateurs, il s'agit de comprendre la structure d'un $K(x)$.

Définition (Eléments algébriques ou transcendants)**.**
Soit L/K une extension de corps.

— Un élément $x \in L$ est *algébrique (sur K)* s'il existe un polynôme non nul $P \in K[X]$ tel que $P(x) = 0$, *transcendant* sinon. Le *polynôme minimal de x sur K*, noté $P_{\min,x}$ est alors le polynôme unitaire de $K[X]$ de plus petit degré annulant x. Il est irréductible, et le *degré de x sur K* est $\deg P_{\min,x}$. Alors, $K(x)$ est égal à $K[x]$, l'ensemble des polynômes en x, lui-même K-isomorphe à $K[X]/(P)$.

— Si $x \in L$ est transcendant sur K, $K(x)$ est K-isomorphe à $K(X)$, en particulier de dimension infinie. Un élément $x \in L$ est donc algébrique si et seulement si $K(x)/K$ est finie.

— L'extension L/K est *algébrique* si tous ses éléments sont algébriques, *transcendante* sinon. Elle est *purement transcendante* si tous les éléments de $L \backslash K$ sont transcendants.

Démonstration. Le polynôme minimal est irréductible ici car si $(QR)(x) = 0$, par intégrité $Q(x) = 0$ ou $R(x) = 0$. Ensuite, si x est algébrique de polynôme minimal P, le morphisme naturel du corps de rupture de P vers L qui à $\overline{X}$ associe x a pour image exactement $K[x]$, d'où l'isomorphisme. □

On peut maintenant formuler et démontrer une forme d'unicité du corps de rupture

Définition. Une extension L/K est un corps de rupture de $P \in K[X]$ irréductible si elle est de la forme $L = K[x]$ avec x une racine de P dans L. Tous les corps de rupture de P sont K-isomorphes.

Démonstration. Soit L un corps de rupture de P et x une racine de P dans L telle que $L = K[x]$. Alors, par la construction originale du corps de rupture, on a un K-morphisme $K[X]/(P) \to L$ envoyant $\overline{X}$ sur x, mais il est surjectif par hypothèse, donc c'est un isomorphisme, ce qui prouve par transitivité le résultat. □

Proposition 2. *Toute extension finie L/K est algébrique. Réciproquement, une extension L/K est algébrique si et seulement si elle est réunion de ses sous-extensions finies.*

De plus, si $x, y \in L$ sont algébriques sur K, $x + y$ et xy le sont également. Ainsi, l'ensemble des éléments de L sur K est une sous-extension de L.

Démonstration. Soit L/K une extension finie de degré n et $x \in L$. Par hypothèse, la famille $(1, x, \cdots, x^n)$, de cardinal $n+1$, est nécessairement K-liée, d'où un polynôme annulateur de x (de degré au plus n), celui-ci est donc algébrique.

Réciproquement, si L/K est algébrique, chaque $x \in L$ est contenu dans l'extension finie $K[x]/K$.

Prenons maintenant $x, y \in L$ algébriques sur K. Alors, y est algébrique sur le corps $K[x]$, car il l'est déjà sur K. On a donc $K[x][y]/K$ finie, mais cette extension contient entre autres $x + y$ et xy, donc ceux-ci sont algébriques par le raisonnement précédent. Enfin, x^{-1} est algébiique car $K(x^{-1}) = K(x)$ qui est une extension finie de K. □

Exercice 3.

(*a*) Soit L une extension de K et x, y algébriques sur K de degrés respectifs m et n premiers entre eux. Montrer que

$$[K(x, y) : K] = mn.$$

(*b*) Soient M/L et L/K deux extensions de corps. Montrer que si L/K est algébrique, tout $x \in M$ algébrique sur L est également algébrique sur K.

Exercice 4.

(*a*) Calculer les polynômes minimaux de $\sqrt{d}$ pour tout entier $d \in \mathbb{Z}$ (on choisit une racine carrée de d dans $\mathbb{C}$), et en déduire les degrés des $\mathbb{Q}(\sqrt{d})$ sur $\mathbb{Q}$. Faire de même pour d'autres racines n-ièmes d'entiers de votre choix.

(*b*) Montrer que pour tout corps K, l'extension $K(X)/K$ est purement transcendante. Montrer que toute extension purement transcendante de K engendrée par un seul élément est en fait celle-ci.

(*c*) Montrer que l'extension $\mathbb{R}/\mathbb{Q}$ est transcendante.

(*d*) Soit $\sigma : L \to L$ K-linéaire avec une extension L/K algébrique. En raisonnant sur toutes les racines des polynômes minimaux d'éléments de x, montrer que σ est automatiquement un automorphisme.

Théorème 1 (Liouville)**.**

Soit $\alpha \in \mathbb{C}$ algébrique irrationnel de degré d sur $\mathbb{Q}$.

Montrer qu'alors, il existe une constante $C > 0$ telle que pour tout rationnel p/q, on a l'inégalité

$$|\alpha - p/q| \geq \frac{C}{q^d}.$$

Démonstration. Soit $P_{\min,\alpha} \in \mathbb{Q}[X]$ le polynôme minimal de α sur $\mathbb{Q}$. On fixe $m \geq 1$ tel que $P = mP_{\min,\alpha} \in \mathbb{Z}[X]$.

Pour toute fraction p/q, par l'égalité des accroissements finis, il existe $y \in [\alpha, p/q]$ (ou l'intervalle inverse) tel que

$$|P(p/q)| = |P(\alpha) - P(p/q)| = |\alpha - p/q||P'(y)|.$$

Mais comme P est à coefficients entiers et n'annule pas p/q (sinon, comme il est irréductible, il serait de degré 1, or α est irrationnel), on a $|P(p/q)| \geq 1/q^d$. On a donc

$$|\alpha - p/q| \geq \frac{1}{q^d |P'(y)|}.$$

Il suffit alors de poser $C = \min(1, \min_{|y-1|\leq 1} \frac{1}{|P'(y)|})$ pour conclure. □

Exercice 5.

On appelle *nombre de Liouville* tout nombre réel α tel que pour tout $d \geq 2$ et tout $C > 0$, il existe un rationnel p/q tel que $|\alpha - p/q| < Cq^{-d}$.

(a) Montrer que tout nombre de Liouville est transcendant.

(b) Donner un exemple direct de nombre de Liouville.

(c) Montrer que l'ensemble des nombres de Liouville est de mesure de Lebesgue nulle, mais que celui des réels transcendants est de mesure pleine.

Définition (Clôture algébrique)**.**

Un corps L est *algébriquement clos* si tous les polynômes irréductibles de $L[X]$ sont de degré 1 (ce qui revient à dire qu'il n'admet aucune extension algébrique/finie non triviale).

Une *clôture algébrique* du corps K est une extension L/K qui est à la fois algébrique et algébriquement close. Il existe toujours une telle extension, souvent notée $\overline{K}$, et deux clôtures algébriques de K sont toujours K-isomorphes deux à deux.

Exemple. Le corps $\mathbb{C}$ est algébriquement clos, et l'ensemble des nombres complexes algébriques sur $\mathbb{Q}$ est une clôture algébrique de $\mathbb{Q}$.

Exercice 6. [Construction de la clôture algébrique]

On fixe un corps K quelconque.

(a) Soit S l'ensemble des polynômes irréductibles de $K[X]$. On pose $A = K[(X_P)_{P\in S}]$ et I l'idéal de A engendré par les $P(X_P), P \in S$. Montrer que $I \neq A$.

(b) En prenant $\mathfrak{m}$ un idéal maximal de A contenant I, montrer que dans l'extension $K_1 = A/\mathfrak{m}$ de K, tout polynôme irréductible de $K[X]$ a une racine.

(c) Itérer le procédé pour construire une suite d'extensions de corps

$$K \subset K_1 \subset K_2 \subset \cdots$$

et montrer que $K_\infty = \bigcup_{n\in\mathbb{N}} K_n$ est un corps algébriquement clos.

(d) En posant $\overline{K}$ l'ensemble des éléments de K_∞ algébriques sur K, montrer que $\overline{K}$ est bien une clôture algébrique de K.

(e) Pour toute extension algébrique L de K, montrer qu'il existe un plongement de L dans $\overline{K}$ prolongeant l'inclusion $K \subset \overline{K}$. En déduire que la clôture algébrique de K est unique à isomorphisme près.

(f) Montrer que pour toute extension finie L de $\overline{K}$, il existe au plus $[L : K]$ plongements K-linéaires distincts de L dans $\overline{K}$. On note $[L : K]_s$ le nombre de ces plongements. Montrer que pour une extension finie M de L, $[M : K]_s = [M : L]_s[L : K]_s$ (utile pour l'exercice sur les extensions séparables).

Plutôt que de manipuler impunément la clôture algébrique (qui relève en général de l'axiome du choix), on peut se concentrer sur une autre manière d'avoir les racines d'un polynôme : le corps de décomposition.

Définition (Corps de décomposition)**.**
Soit $P \in K[X]$.
Un *corps de décomposition de P sur K* est une extension (finie) L de K telle que P est scindé de racines $\alpha_1, \cdots, \alpha_r$ sur K et que

$$L = K(\alpha_1, \cdots, \alpha_r).$$

Exercice 7. Donner des corps de décomposition de $X^4 - 1$ et $X^3 - 2$ sur $\mathbb{Q}$.

Proposition 3.
Soit $P \in K[X]$. Il existe toujours un corps de décomposition de P sur K, et si L et L' sont deux tels corps, il existe un K-isomorphisme entre L et L'. On s'autorise donc souvent à dire « le » corps de décomposition de P.

Démonstration. La preuve de l'existence, est relativement directe. Si P n'est pas scindé sur K (auquel cas K convient), soit Q un facteur irréductible de P sur $K[X]$. Alors, dans K_1 le corps de rupture de Q sur K, le polynôme P admet une racine, notée α, et $K_1 = K[\alpha]$. On a donc

$$P = (X - \alpha)P_1, \quad P_1 \in K_1[X].$$

On recommence avec un facteur irréductible de P_1 si celui-ci n'est pas scindé sur K_1, ce qui donne une tour d'extensions

$$K \subset K_1 \subset \cdots K_d$$

où d est majoré par le degré de P (vu que le degré du polynôme considéré décroît de 1 à chaque étape). Par construction, K_d est une extension dans laquelle P devient scindé, et on n'a utilisé que des racines de P pour l'engendrer, donc c'est bien un corps de décomposition.

La preuve de l'unicité est un peu plus subtile et requiert une définition supplémentaire. Supposons qu'on a un isomorphisme de corps $i : K \to K'$ et des extensions respectives L et L' de K et K'. Alors, un i-isomorphisme $\sigma : L \to L'$ est un isomorphisme de corps entre L et L' tel que pour tous $\lambda \in K, x \in L$,

$$\sigma(\lambda x) = i(\lambda)\sigma(x).$$

Pour tout polynôme $P \in K[X]$, on note $i(P) \in K'[X]$ le polynôme obtenu en appliquant i à chacun de ses coefficients. On va alors montrer le lemme suivant.

Lemme. *Pour tous corps K, K' et $i : K \to K'$ un isomorphisme, et tout polynôme $P \in K[X]$, si L et L' sont des corps de décomposition respectivement de P sur K et $i(P)$ sur K', alors il existe un i-isomorphisme $\sigma : L \to L'$.*

Ce lemme, appliqué à $K' = K$ et i l'identité, implique bien l'unicité des corps de décomposition, et on va le démontrer par récurrence sur le degré de P.

Si P est constant ou de degré 1, il n'y a rien à faire car forcément ses racines appartiennent au corps de base donc $L = K$, $L' = K'$.

Supposons maintenant que le lemme est vrai pour tout polynôme (et tous corps notés comme ci-dessus) de degré n. Soit $P \in K[X]$ de degré $n+1$, L un corps de décomposition de P sur K et L' un corps de décomposition de P sur K', avec $i : K \to K'$ un isomorphisme de corps.

Alors, en prenant une racine α_1 de P dans L, considérons son polynôme minimal P_1 sur K. Il est irréductible sur K donc $i(P_1)$ est irréductible sur K', mais par ailleurs il divise $i(P)$ qui est scindé sur L' par hypothèse. Il existe donc α_1' une racine de $i(P_1)$ dans L.

On peut alors construire un i-isomorphisme j entre $K[\alpha_1]$ et $K'[\alpha_1']$, en envoyant α_1 sur α_1' (en passant par les corps de rupture respectifs de P_1 et $i(P_1)$). Mais par hypothèse, L est alors un corps de décomposition de $P/(X-\alpha_1)$ sur $K[\alpha_1]$, et de même pour L' et $i(P)/(X-\alpha_1') = j(P/(X-\alpha_1))$. On peut donc appliquer l'hypothèse de récurrence à ce polynôme, aux extensions et à j, ce qui conclut la preuve. □

Exercice 8. Montrer que le corps de décomposition d'un polynôme de degré au plus n sur K est de degré au plus $n!$ sur K.

Exercice 9. Donner les corps de décomposition de $X^4 - 2$, $X^5 - 3$ et $X^n - 1$ sur $\mathbb{Q}$.

L'unicité du corps de décomposition a une application très importante : les corps finis.

2 Le cas des corps finis

Dans cette section (pour être sûr), tout les corps considérés sont commutatifs, de sorte qu'on a pas besoin d'utiliser le théorème de Wedderburn.

Si $\mathbb{F}$ est un corps fini, il est forcément de caractéristique finie p (un nombre premier), et ceci en fait un $\mathbb{F}_p$-espace vectoriel. Il est donc de cardinal $q = p^n$. Il reste à étudier l'existence et l'unicité de tels corps. Dans la suite, on notera toujours q une puissance de p.

Proposition 4. *Soit $\mathbb{F}$ un corps fini de cardinal q. Alors, pour tout $x \in \mathbb{F}$, $x^q = x$.*
De plus, le morphisme $x \mapsto x^p$, appelé le Frobenius, est un automorphisme de corps.

Démonstration. Le groupe $\mathbb{F}^*$ est de cardinal $q-1$, donc par le théorème de Lagrange, pour tout élément de $\mathbb{F}^*$, $x^{q-1} = x$. En multipliant cette égalité par x, on obtient l'égalité voulue, valide aussi pour $x = 0$.

Ensuite, le morphisme $\varphi : x \mapsto x^p$ est bien multiplicatif, et additif car $\mathbb{F}$ est de caractéristique p (utiliser le binôme de Newton, pour rappel). C'est donc un morphisme de corps, injectif donc surjectif par argument de cardinal. □

Pour l'instant, on ne connaît comme corps finis que les $\mathbb{F}_p$. Il s'agit donc d'en trouver des extensions.

Si $P \in \mathbb{F}_p[X]$ est irréductible de degré n, son corps de rupture sur $\mathbb{F}_p$ est donc de cardinal $q = p^n$. Si on sait qu'il existe des irréductibles de tout degré (ce qui est vrai), on peut donc construire des corps finis de tous les cardinaux possibles, mais on n'en sait pas beaucoup plus. La bonne construction est en fait par corps de décomposition.

Exemple. Le corps $\mathbb{F}_2[X]/(X^2 + X + 1)$ est fini de cardinal 4.

Proposition 5. *Pour tout nombre premier p et tout $n \in \mathbb{N}$, soit $\mathbb{F}$ le corps de décomposition de $X^{p^n} - X$ sur $\mathbb{F}_p$. Alors, c'est un corps de cardinal $q = p^n$, et réciproquement tout corps fini de cardinal $q = p^n$ est un corps de décomposition pour ce polynôme.*

Démonstration. Par définition, $\mathbb{F}$ est un corps sur lequel $P = X^q - X$ est scindé. Ce polynôme est à racines simples, car $P' = -1$ est inversible, en particulier premier à p. Dans $\mathbb{F}$, l'ensemble des racines de P est donc de cardinal exactement q, et c'est un sous-corps de $\mathbb{F}$ car le Frobenius est un morphisme de corps. Comme $\mathbb{F}$ est par définition engendré par ces racines, il est donc bien de cardinal q. Réciproquement, pour tout corps $\mathbb{F}$ de cardinal q, on sait que les éléments de $\mathbb{F}$ sont les racines de P par la proposition précédente, et donc $\mathbb{F}$ est en particulier un corps de décomposition de P sur $\mathbb{F}_p$. □

Corollaire 6. *Deux corps finis de même cardinal sont isomorphes.*

Démonstration. On utilise la proposition précédente et l'unicité du corps de décomposition. □

Voici quelques propriétés importantes supplémentaires.

Proposition 7.
Soit $\mathbb{F}_{p^n}$ un corps de cardinal p^n.

(a) Les sous-corps de $\mathbb{F}_{p^n}$ sont exactement les $\mathbb{F}_{p^d} = \{x \in \mathbb{F}_{p^n} \mid x^{p^d} = x\}$ avec d divisant n, et alors

$$[\mathbb{F}_{p^n} : \mathbb{F}_{p^d}] = n/d.$$

(*b*) *Pour tout* $n \in \mathbb{N}^*$,

$$X^{p^n} - X = \prod_P P$$

où P *parcourt les polynômes irréductibles de* $\mathbb{F}_p[X]$ *de degré divisant* n.

(*c*) *Pour tout polynôme irréductible* P *de degré* d *de* $\mathbb{F}_p[X]$, *le corps de rupture de* P *sur* $\mathbb{F}_p$ *est de cardinal* p^d, *et c'est également son corps de décomposition.*

Démonstration. (*a*) Si $\mathbb{F}$ est un sous-corps de $\mathbb{F}_{p^n}$, alors $\mathbb{F}_{p^n}$ est un $\mathbb{F}$-espace vectoriel donc p^n est une puissance du cardinal de $\mathbb{F}$. Ceci implique que $N = p^d$ avec d divisant n, et alors le degré de l'extension est bien d. Ensuite, si $\mathbb{F}$ est de cardinal p^d, il vérifie que $x^{p^d} = x$ pour chacun de ces éléments, donc c'est exactement $\mathbb{F}_{p^d}$ avec notre notation.

(*b*) On a déjà montré que $X^{p^n} - X$ est scindé à racines simples (dans un corps $\mathbb{F}_{p^n}$ de cardinal p^n fixé), donc il suffit de montrer que les facteurs irréductibles de $X^{p^n} - X$ dans $\mathbb{F}_p[X]$ sont exactement les polynômes irréductibles P de degré d divisant n. Soit P un tel polynôme. Le corps de rupture de P sur $\mathbb{F}_p$ est de cardinal p^d, donc inclus naturellement dans $\mathbb{F}_{p^n}$. En particulier, sa racine sur $\mathbb{F}_p$ est également racine de $X^{p^n} - X$. Comme P est le polynôme minimal de cette racine, on en déduit que P divise $X^{p^n} - X$. Réciproquement, soit α une racine de $X^{p^n} - X$ dans $\mathbb{F}_{p^n}$ (où il est scindé à racines simples). Son polynôme minimal sur $\mathbb{F}_p$ est de degré d, et on a (par propriété des corps de rupture) sun morphisme de corps de $\mathbb{F}_{p^d}$ vers $\mathbb{F}_{p^n}$ d'où d divise n. □

Exercice 10. Utiliser la décomposition des $X^{p^n} - X$ et la formule d'inversion de Möbius pour dénombrer les polynômes irréductibles sur $\mathbb{F}_p$.

Il reste maintenant à comprendre les automorphismes des corps finis.

Proposition 8.

Soit q *une puissance de* p.

Pour tout polynôme P *irréductible de degré* n *sur* $\mathbb{F}_q$, *pour toute racine* α *de* P *dans une extension* $\mathbb{F}_{q^k}$ *de* $\mathbb{F}_q$, *les racines de* P *dans* $\mathbb{F}_{q^k}$ *sont exactement* $\alpha, \alpha^q, \cdots, \alpha^{q^{k-1}}$ *(toutes distinctes).*

En conséquence, tout automorphisme de corps de $\mathbb{F}_{q^k}$ *fixant* $\mathbb{F}_q$ *est une puissance de* $x \mapsto x^q$. *Le groupe de ces automorphismes est donc isomorphe à* $\mathbb{Z}/k\mathbb{Z}$.

Démonstration. Soit P un tel polynôme. Le morphisme de corps $x \mapsto x^q$ fixe point par point $\mathbb{F}_q$ comme on l'a vu, donc pour tout $x \in \mathbb{F}_{q^k}$,

$$P(x^q) = P(x)^q.$$

En conséquence, $\alpha, \alpha^q, \cdots, \alpha^{q^{n-1}}$ sont bien des racines de P si α l'est. Il suffit de montrer qu'elles sont toutes distinctes. Si jamais $\alpha^{q^i} = \alpha^{q^j}$ pour $0 \leq i < j \leq n-1$, en appliquant l'inverse de l'automorphise $x \mapsto x^q$ à répétition, on a $\alpha = \alpha^{q^{j-i}}$. Cela implique que α appartient au corps $\mathbb{F}_{q^{j-i}}$, mais alors son polynôme minimal est de degré au plus $j-i$, or celui-ci est de degré n, contradiction. Les n racines exhibées sont donc bien distinctes deux à deux, et scindent explicitement P. □