

Corps finis

Lionel Fourquaux

8 juin 2016

1 Caractéristique et sous-corps premier

Proposition 1.1. Soit k un corps. Notons 1_k l'élément neutre de la multiplication de k . L'application

$$\iota: \begin{cases} \mathbb{Z} & \longrightarrow & k \\ n & \longmapsto & n1_k \end{cases}$$

est un morphisme de $\mathbb{Z}$ -algèbres, dont le noyau est un idéal premier de $\mathbb{Z}$, et dont l'image est le plus petit sous-anneau unitaire non nul de k .

Démonstration. L'application ι est clairement un morphisme de $\mathbb{Z}$ -algèbres, en particulier d'anneaux, donc son noyau est un idéal de $\mathbb{Z}$ et son image est un sous-anneau unitaire non nul de k .

Tout sous-anneau unitaire non nul de k contient 1_k et est un sous-groupe pour l'addition, donc contient l'image de ι .

Comme l'image de ι est un sous-anneau de k , c'est un anneau intègre, donc le noyau de ι est un idéal premier de $\mathbb{Z}$. $\square$

Corollaire 1.2. Le noyau de l'application ι de la proposition 1.1 est de la forme $p\mathbb{Z}$ avec $p = 0$ ou p un nombre premier. Cet entier p est appelé la caractéristique du corps k .

Démonstration. En effet, les idéaux premiers de $\mathbb{Z}$ sont $\{0\}$ et les $p\mathbb{Z}$ pour p un nombre premier. $\square$

Proposition 1.3. Si k est un corps, le plus petit sous-corps de k , appelé le sous-corps premier de k , est isomorphe à :

- $\mathbb{Q}$ si k est de caractéristique nulle ;
- $\mathbb{Z}/p\mathbb{Z}$ si k est de caractéristique $p > 0$.

Démonstration. Si k est de caractéristique $p > 0$, alors le plus petit sous-anneau unitaire non nul de k est l'image de l'application ι de la proposition 1.1, qui est isomorphe à $\mathbb{Z}/p\mathbb{Z}$ puisque le noyau de ι est $p\mathbb{Z}$. L'image de ι est donc un sous-corps de k (puisque $\mathbb{Z}/p\mathbb{Z}$ est un corps), donc c'est aussi le plus petit sous-corps de k .

Si k est de caractéristique nulle, alors son plus petit sous-anneau unitaire non nul est isomorphe (via ι) à $\mathbb{Z}$. Alors, le corps $\mathbb{Q}$ des fractions de $\mathbb{Z}$ s'injecte dans k (par propriété universelle du corps des fractions), et même dans tout sous-corps de k . L'image de $\mathbb{Q}$ par cette injection est clairement le plus petit sous-corps de k . $\square$

Corollaire 1.4. Tout corps fini est une extension de $\mathbb{Z}/p\mathbb{Z}$, où $p > 0$ est la caractéristique du corps.

Démonstration. En effet, si k est un corps fini, il ne peut pas contenir de sous-corps isomorphe à $\mathbb{Q}$ (qui est infini), donc, par la proposition 1.3, la caractéristique de k ne peut pas être nulle. Le second cas de la proposition 1.3 permet alors de conclure. $\square$

Corollaire 1.5. *Le cardinal d'un corps fini est une puissance d'un nombre premier, et ce nombre premier est sa caractéristique.*

Démonstration. Soit k un corps fini. C'est une extension de $\mathbb{Z}/p\mathbb{Z}$, où p est la caractéristique de k , donc, en particulier, k est muni d'une structure de $\mathbb{Z}/p\mathbb{Z}$ -espace vectoriel. De plus, k contient une famille génératrice finie (l'ensemble de ses éléments) donc k est un espace vectoriel de dimension finie sur $\mathbb{Z}/p\mathbb{Z}$. Notons d sa dimension.

En tant qu'espace vectoriel, k est isomorphe à $(\mathbb{Z}/p\mathbb{Z})^d$ (par choix d'une base), donc $|k| = p^d$. $\square$

2 Groupe multiplicatif d'un corps fini

Proposition 2.1. *Soit k un corps, et soit*

$$\mu(k) = \{ x \in k / \exists e \in \mathbb{N}^* x^e = 1 \}$$

le sous-groupe de $k^\times$ formé des racines de l'unité. Alors tout sous-groupe fini de $\mu(k)$ est cyclique.

Démonstration. Soit G un sous-groupe fini de $\mu(k)$, d'ordre n .

Si $d > 0$ est un entier divisant n , alors on a deux cas.

- Ou bien il n'existe pas d'élément $x \in G$ d'ordre d .
- Ou bien il existe un $x \in G$ d'ordre d . Il engendre alors un sous-groupe cyclique de G , isomorphe à $\mathbb{Z}/d\mathbb{Z}$. Celui-ci contient $\phi(d)$ éléments d'ordre d , où ϕ désigne la fonction indicatrice d'Euler. D'autre part, les éléments de $\mu(k)$ dont l'ordre divise d sont les racines de $X^d - 1$ dans k . Il y en a donc au plus d , or le sous-groupe engendré par x contient d tels éléments, donc ce sous-groupe contient tous les éléments de G dont l'ordre divise d . En particulier, G contient exactement $\phi(d)$ éléments d'ordre d .

En comptant les éléments de G selon leur ordre, on trouve donc

$$n = |G| = \sum_{d|n} \underbrace{|\{ x \in G / x \text{ est d'ordre } d \}|}_{=0 \text{ ou } \phi(d)} \leq \sum_{d|n} \phi(d).$$

Or, pour tout entier $d > 0$ divisant n , le groupe $\mathbb{Z}/n\mathbb{Z}$ contient $\phi(d)$ éléments d'ordre d (car les éléments dont l'ordre divise d sont ceux du sous-groupe $\frac{n}{d}\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/d\mathbb{Z}$), donc

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

On en déduit donc que pour tout entier $d > 0$ divisant n , on a

$$|\{ x \in G / x \text{ est d'ordre } d \}| = \phi(d) > 0.$$

En particulier (avec $d = n$), le groupe G contient un élément d'ordre n , donc il est cyclique. $\square$

Corollaire 2.2. *Si k est un corps fini, alors le groupe $k^\times$ est cyclique.*

Démonstration. Si le corps k a q éléments, alors $k^\times$ est un groupe d'ordre $q - 1$, donc tous les éléments de $k^\times$ sont des racines $(q - 1)$ -ièmes de l'unité, donc $k^\times$ est un sous-groupe fini de $\mu(k)^1$, donc il est cyclique. $\square$

Corollaire 2.3. *Les extensions finies de corps finis sont monogènes.*

Démonstration. Soit k'/k une extension finie de corps finis. Notons α un générateur du groupe cyclique $k'^\times$, alors on a $k' = k[\alpha] = k(\alpha)$. $\square$

3 Théorie de Galois des corps finis

Proposition 3.1. *Si k est un corps de caractéristique p , alors l'application*

$$\varphi: \begin{cases} k & \longrightarrow k \\ x & \longmapsto x^p \end{cases}$$

est un morphisme de corps, appelé le morphisme de Frobenius. Si k est un corps fini, alors c'est un automorphisme.

Démonstration. On a $\varphi(xy) = x^p y^p = \varphi(x)\varphi(y)$ et $\varphi(1) = 1^p = 1$. De plus,

$$\begin{aligned} \varphi(x + y) &= (x + y)^p \\ &= \sum_{i=0}^p \binom{p}{i} x^i y^{p-i} && \text{par formule du binôme} \\ &= x^p + y^p && \text{car } \binom{p}{i} \equiv 0 \pmod{p} \text{ si } 1 \leq i \leq p-1, \text{ et} \\ & && k \text{ est de caractéristique } p \\ &= \varphi(x) + \varphi(y). \end{aligned}$$

L'application φ est donc un morphisme de corps. En particulier, elle est injective. Si k est fini, elle est donc bijective. $\square$

Si k'/k est une extension de corps finis, notons $\text{Gal}(k'/k)$ le groupe des automorphismes k -linéaires² de k' .

Si k est un corps de caractéristique p , alors son sous-corps premier est $\mathbb{Z}/p\mathbb{Z}$. Comme le sous-corps premier est engendré (comme groupe) par 1, qui est fixe par tous les automorphismes, les éléments du sous-corps premiers sont fixes par les automorphismes de k , donc $\text{Gal}(k/(\mathbb{Z}/p\mathbb{Z}))$ est le groupe des automorphismes de k , et $\varphi \in \text{Gal}(k/(\mathbb{Z}/p\mathbb{Z}))$.

Lemme 3.2. *Si k est un corps fini de caractéristique p , de cardinal $q = p^d$, alors son automorphisme de Frobenius φ est d'ordre d .*

1. Bien sûr, on a en fait $\mu(k) = k^\times$.

2. Autrement dit, ce sont les automorphismes de k' qui fixent les éléments du sous-corps k .

Démonstration. Soit g un générateur du groupe cyclique $k^\times$, et soit $e \in \mathbb{Z}$. Alors :

$$\begin{aligned}
 \varphi^e = \text{id} &\iff \varphi^e(g) = g \\
 &\iff g^{p^e} = g \\
 &\iff q-1 \mid p^e - 1 && \text{car } g \text{ est d'ordre } |k^\times| = q-1 \\
 &\iff d \mid e && \text{car } p \text{ est d'ordre } d \text{ dans } \mathbb{Z}/(q-1)\mathbb{Z}, \text{ puisque } 1, \\
 & && p, p^2, \dots, p^{d-1} \text{ sont deux à deux distinct modulo } q-1 = p^d - 1 > p^{d-1}, \text{ et } p^d \equiv 1 \pmod{q-1}.
 \end{aligned}$$

□

On en déduit la structure du groupe $\text{Gal}(k'/k)$.

Proposition 3.3. Soit k'/k une extension de corps finis. Soient p leur caractéristique, $q = |k|$, $q' = |k'|$, $d = [k : \mathbb{Z}/p\mathbb{Z}]$ et $d' = [k' : \mathbb{Z}/p\mathbb{Z}]$, de sorte que $q = p^d$, $q' = p^{d'}$ et $\frac{d'}{d} = [k' : k]$. Soit $\varphi : k' \rightarrow k'$ l'automorphisme de Frobenius. Alors $\text{Gal}(k'/k)$ est un groupe cyclique, d'ordre $[k' : k]$, engendré par $\varphi_q = \varphi^d$ (que l'on appelle parfois le morphisme de Frobenius relatif).

Démonstration. D'après le lemme 3.2, $\varphi_q|_k = \text{id}_k$, donc $\varphi_q \in \text{Gal}(k'/k)$. De plus, φ est d'ordre d' (dans le groupe des automorphismes de k') et $d \mid d'$, donc φ_q est d'ordre $\frac{d'}{d}$.

Soit $\alpha \in k'$ tel que $k' = k(\alpha)$. L'application

$$\begin{cases} \text{Gal}(k'/k) & \longrightarrow & k' \\ \sigma & \longmapsto & \sigma(\alpha) \end{cases}$$

est injective. En effet, si $\sigma_0(\alpha) = \sigma_1(\alpha)$, alors $(\sigma_1^{-1}\sigma_0)(\alpha) = \alpha$, donc $\sigma_1^{-1}\sigma_0 = \text{id}_{k'}$ (puisque $k' = k(\alpha)$), donc $\sigma_0 = \sigma_1$. Soit $Q \in k[X]$ le polynôme minimal de α , alors l'image de l'application $\sigma \mapsto \sigma(\alpha)$ est contenue dans l'ensemble des racines de Q (puisque $Q(\sigma(\alpha)) = \sigma(Q(\alpha)) = \sigma(0) = 0$), donc $|\text{Gal}(k'/k)| \leq \deg Q \leq [k' : k] = \frac{d'}{d}$.

Comme $\text{Gal}(k'/k)$ contient un élément d'ordre $\frac{d'}{d}$, on en déduit qu'il est cyclique, d'ordre $\frac{d'}{d}$, engendré par φ_q . □

Lemme 3.4. Soit k'/k une extension de corps finis. Si H est un sous-groupe de $\text{Gal}(k'/k)$, et si k'^H est le sous-corps de k' formé des éléments de k' fixes sous l'action de H , alors on a $[k' : k'^H] = |H|$.

Démonstration. Notons que $H \subseteq \text{Gal}(k' : k'^H)$. D'après la proposition 3.3, on a donc $|H| \leq [k' : k'^H]$.

Soit $\alpha \in k'$ tel que $k' = k(\alpha)$. On a alors $k' = k'^H(\alpha)$. Le polynôme

$$\prod_{\sigma \in H} (X - \sigma(\alpha))$$

est à coefficients dans k'^H car les polynômes symétriques en les $\sigma(\alpha)$ sont fixes sous l'action de H . C'est un polynôme annulateur de α , de degré $|H|$, donc $[k' : k'^H] \leq |H|$, d'où l'égalité. □

Le théorème suivant est la correspondance de Galois dans le cadre des corps finis.

Proposition 3.5. Soit k'/k une extension de corps finis. Alors l'ensemble $\mathfrak{K}$ des extensions intermédiaires entre k et k' est en bijection avec l'ensemble $\mathfrak{G}$ des sous-groupes de $\text{Gal}(k'/k)$, par les deux applications inverses l'une de l'autre :

$$\begin{cases} \mathfrak{K} & \longrightarrow & \mathfrak{G} \\ \kappa & \longmapsto & \text{Gal}(k'/\kappa) \end{cases} \quad \text{et} \quad \begin{cases} \mathfrak{G} & \longrightarrow & \mathfrak{K} \\ H & \longmapsto & k'^H \end{cases}.$$

Démonstration. Si $\kappa \in \mathfrak{K}$, on a $\kappa \subseteq k'^{\text{Gal}(k'/\kappa)}$, or le lemme 3.4 et la proposition 3.3 donnent

$$[k' : k'^{\text{Gal}(k'/\kappa)}] = |\text{Gal}(k'/\kappa)| = [k' : \kappa],$$

donc $\kappa = k'^{\text{Gal}(k'/\kappa)}$.

Si $H \in \mathfrak{G}$, on a $H \subseteq \text{Gal}(k'/k'^H)$, et la proposition 3.3 et le lemme 3.4 donnent

$$|\text{Gal}(k'/k'^H)| = [k' : k'^H] = |H|,$$

donc $H = \text{Gal}(k'/k'^H)$. □

Corollaire 3.6. Si k'/k est une extension de corps finis, alors pour tout diviseur d de $[k' : k]$ il existe un unique sous-corps κ de k' contenant k tel que $[\kappa : k] = d$

Démonstration. D'après la proposition 3.5, cela revient à montrer que le groupe cyclique $\text{Gal}(k'/k)$, qui est d'ordre $[k' : k]$, a un unique sous-groupe d'indice d , ce qui est vrai (c'est le sous-groupe des multiples de d). □

4 Existence et unicité

Proposition 4.1. Si p est un nombre premier et si $m > 0$ est un entier, il existe un corps fini de cardinal p^m , et celui-ci est unique à isomorphisme près.

Démonstration. Notons $q = p^m$. Soit k un corps de décomposition du polynôme $X^q - X \in (\mathbb{Z}/p\mathbb{Z})[X]$ sur $\mathbb{Z}/p\mathbb{Z}$, et soit $\varphi : x \mapsto x^p$ le morphisme de Frobenius (absolu) de k .

Notons κ le sous-corps de k formé des éléments fixes par φ^m . Alors φ^m est trivial dans $\text{Gal}(\kappa/(\mathbb{Z}/p\mathbb{Z}))$, qui est cyclique, engendré par φ , d'ordre $[\kappa : \mathbb{Z}/p\mathbb{Z}]$, d'après la proposition 3.3. On trouve donc que $[\kappa : \mathbb{Z}/p\mathbb{Z}] \mid m$, et donc $|\kappa| \leq q$.

D'autre part, les racines dans k' du polynôme $X^q - X$ sont par définition fixes par φ^m , donc elles sont dans κ . Or ce polynôme est scindé sur k (par définition de k), et à racines simples car il est premier à sa dérivée (qui est -1). On a donc $q \leq |\kappa|$, donc $|\kappa| = q$. Il existe donc un corps à q éléments.

Comme le polynôme $X^q - X$ est scindé sur κ , par minimalité du corps de décomposition, on a $k = \kappa$.

Si k' est un corps à q éléments, ses éléments sont tous fixes par $x \mapsto x^q$ (par le lemme 3.2), i.e. ils sont tous racines du polynôme $X^q - X \in (\mathbb{Z}/p\mathbb{Z})[X]$. Donc ce polynôme est scindé sur k' , et comme l'ensemble de ses racines engendre (et est même égal à) k' , le corps k' est un corps de décomposition de $X^q - X$. Par unicité à isomorphisme près du corps de décomposition, on en déduit que k et k' sont isomorphes. □

On note usuellement $\mathbb{F}_q$ « le » corps à q éléments, pour q une puissance d'un nombre premier.

En général³, il n'y a pas unicité de l'isomorphisme entre deux corps finis de même cardinal.

3. Il y a unicité si et seulement si ce cardinal est premier.

Corollaire 4.2. Pour tout corps fini k et tout entier $d > 0$, il existe un polynôme $Q \in k[X]$ irréductible sur k de degré d .

Démonstration. D'après la proposition 4.1, il existe un corps k' à $|k|^d$ éléments. D'après le corollaire 3.6, k' contient un sous-corps à $|k|$ éléments, et d'après la proposition 4.1, celui-ci est isomorphe à k . Quitte à les identifier, on peut voir k' comme une extension de k .

Soit $\alpha \in k'$ tel que $k' = k[\alpha]$ (cf. corollaire 2.3), et soit $Q \in k[X]$ le polynôme minimal de α sur k . Alors Q est irréductible sur k , et $\deg Q = [k' : k] = d$. $\square$

5 Factorisation de $X^{q^m} - X$

Le polynôme $X^{q^m} - X \in \mathbb{F}_q[X]$ est premier à sa dérivée -1 . Il est donc sans facteur carré, et il suffit de connaître ses diviseurs irréductibles pour en déduire sa factorisation.

Soit $Q \in \mathbb{F}_q[X]$ un polynôme irréductible, et soit $k = \mathbb{F}_q[X]/(Q(X))$. On note α la classe de X dans k .

$$\begin{aligned}
 Q \mid (X^{q^m} - X) &\iff \alpha^{q^m} - \alpha = 0 \\
 &\iff \varphi_q^m(\alpha) = \alpha \\
 &\iff \varphi_q^m \text{ est l'identité sur } \mathbb{F}_q[\alpha] && \text{car } \varphi_q \text{ est un morphisme de } \mathbb{F}_q\text{-algèbres} \\
 &\iff \varphi_q^m = \text{id}_k && \text{car } k = \mathbb{F}_q[\alpha] \\
 &\iff \varphi_q^m = 1 \text{ dans le groupe } \text{Gal}(k/\mathbb{F}_q) \\
 &\iff \deg(Q) \mid m && \text{car } \varphi_q \text{ est d'ordre } [k : \mathbb{F}_q] = \deg(Q).
 \end{aligned}$$

On a donc :

$$X^{q^m} - X = \prod_{\substack{Q \in \mathbb{F}_q[X] \\ Q \text{ unitaire irréductible} \\ \deg(Q) \mid m}} Q.$$

6 Carrés dans les corps finis