8 Corps finis et leur clôture algébrique

Version du 5 janvier 2006

30 Corps finis

30.1 Cardinal et groupe multiplicatif d'un corps fini

Soit k un corps fini. Son sous-corps premier est fini donc, d'après le paragraphe 23.1, k est de caractéristique $p > 0$. On identifiera son sous-corps premier à $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Tout corps contenant k a même sous-corps premier, donc est aussi de caractéristique p.

Lemme 30.1.1 *Soient $k \subseteq k'$ deux corps finis, de cardinal q et q' respectivement.*

1) *On a $q' = q^n$, où $n = [k' : k]$.*

2) *Par conséquent, si $p = \mathrm{car}(k)$ et $m = [k : \mathbb{F}_p]$, alors $q = p^m$ et $q' = p^{mn}$.*

Démonstration. 1) Comme k' est fini, c'est un k-espace vectoriel de dimension finie n. Alors $k' \cong k^n$ comme k-espace vectoriel, et donc $|k'| = |k|^n$. Ceci prouve 1).

Le même argument appliqué à $\mathbb{F}_p \subseteq k$ montre que $q = p^m$, d'où le lemme. □

Corollaire 30.1.2 *Si k est un corps fini de caractéristique p, alors le cardinal de k est une puissance de p.*

Théorème 30.1.3 (Groupe multiplicatif d'un corps fini)
Soit k un corps fini de cardinal $q = p^n$. Le groupe multiplicatif $k^\times = k \setminus \{0\}$ est un groupe cyclique d'ordre $q - 1$.

Démonstration. $k^\times$ est un groupe abélien fini ; c'est donc un $\mathbb{Z}$-module de type fini et de torsion. D'après le théorème de structure des modules de type fini sur un anneau principal, il existe des entiers $d_1 \geq \cdots \geq d_r > 1$ tels que d_i divise d_{i-1}, pour $i = r, r-1, \ldots, 2$ et

$$k^\times \cong \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_r\mathbb{Z}.$$

Alors, d'une part, $|k^\times| = d_1 d_2 \cdots d_r$ et, d'autre part, tout élément $x \in k^\times$ vérifie $x^d = 1$, où $d = d_1$. Or, comme $k[X]$ est intègre, le polynôme $X^d - 1$ a au plus d racines dans k. Il en résulte que $r = 1$ et $k^\times \cong \mathbb{Z}/d\mathbb{Z}$ est cyclique, d'ordre $d = |k^\times| = q - 1$. Ceci prouve le théorème. □

30.2 La formule du binôme

Soient k, n deux entiers tels que $0 \leq k \leq n$. On rappelle la définition du coefficient binomial :

$$\binom{n}{k} := \frac{n!}{k!(n-k)!}.$$

(On le note aussi C_n^k.) C'est le nombre de façons de choisir k éléments dans un ensemble à n éléments. Pour $k = 0$ ou n, ceci vaut 1. On rappelle aussi la formule de Pascal (pour $k \geq 1$) :

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1},$$

qu'on obtient en remarquant que, quand on prend k éléments dans $\{1, \ldots, n\}$, on peut ou bien prendre, ou ne pas prendre, n. On rappelle aussi la formule du binôme, valable dans tout anneau commutatif.

Lemme 30.2.1 (Formule du binôme)
Soit A un anneau commutatif et $a, b \in A$. Pour tout $n \geq 1$, on a :

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}.$$

Démonstration. Par récurrence sur n, en utilisant la formule de Pascal. □

Lemme 30.2.2 *Soit $p \in \mathbb{N}$ un nombre premier. Alors p divise $\binom{p}{k}$ pour tout $k = 1, \ldots, p-1$.*

Démonstration. p divise $p! = k!(p-k)!\binom{p}{k}$ et est premier avec $k!(p-k)!$, donc divise $\binom{p}{k}$. □

30.3 Endomorphismes de Frobenius

Proposition 30.3.1 (L'endomorphisme de Frobenius Fr_p)
Soit K un corps de caractéristique $p > 0$. Alors l'application $x \mapsto x^p$ est un endomorphisme du corps K, noté Fr_p. De plus, si K est fini, alors Fr_p est un automorphisme de K.

Démonstration. Il est clair que $1^p = 1$ et $(ab)^p = a^p b^p$ pour tout $a, b \in K$. L'égalité $(a+b)^p = a^p + b^p$ résulte de la formule du binôme et du lemme précédent. Donc, Fr_p est un morphisme de corps de K vers K, c.-à-d., un endomorphisme de corps de K. Il est bien sûr injectif, comme tout morphisme de corps. Par conséquent, si K est fini, Fr_p est bijectif donc un automorphisme de K. □

Corollaire 30.3.2 (Les endomorphismes de Frobenius $\mathrm{Fr}_q = \mathrm{Fr}_{p^n}$)
Soient K un corps de caractéristique $p > 0$ et $n \geq 1$. L'application $\mathrm{Fr}_p^n := \mathrm{Fr}_p \circ \cdots \circ \mathrm{Fr}_p$ (n fois), qui à tout x associe x^{p^n}, est un endomorphisme du corps K. On le note aussi Fr_{p^n} ou Fr_q si $q = p^n$. Si K est fini, c'est un automorphisme de K.

Démonstration. Ceci résulte immédiatement de la proposition précédente. □

Corollaire 30.3.3 *Soient p un nombre premier, $n \geq 1$ et $q = p^n$. Alors p divise $\binom{q}{i}$ pour tout $i = 1, \ldots, q-1$.*

Démonstration. Plaçons-nous dans le corps $K = \mathbb{F}_p(X)$ des fractions rationnelles sur $\mathbb{F}_p$ et notons π la projection $\mathbb{Z} \to \mathbb{F}_p$. D'une part, on a

$$(1+X)^q = \sum_{i=0}^{q} \pi\left(\binom{q}{i}\right) X^i. \tag{1}$$

D'autre part, comme $\mathrm{Fr}_q = \mathrm{Fr}_p^n$ est un endomorphisme de K, l'on a

$$(1+X)^q = 1 + X^q. \tag{2}$$

En comparant (1) et (2), on obtient que $\binom{q}{i} \equiv 0 \bmod p$, pour $i = 1, \ldots, q-1$. Ceci prouve le corollaire. □

30.4 Existence et unicité des corps $\mathbb{F}_{p^n}$

Lemme 30.4.1 *Soient K un corps et τ un endomorphisme de K. Alors l'ensemble des éléments invariants*

$$K^\tau := \{x \in K \mid \tau(x) = x\}$$

est un sous-corps de K.

Démonstration. C'est clair. □

Théorème 30.4.2 (Existence et unicité de $\mathbb{F}_q$)
Soient p un nombre premier, $n \geq 1$ et $q = p^n$. Soit K un corps de décomposition sur $\mathbb{F}_p$ du polynôme $X^q - X$. Alors, $|K| = q$. Réciproquement, tout corps fini à q éléments est isomorphe à K. Par conséquent, il existe à isomorphisme près, un unique corps fini à q éléments. On le note $\mathbb{F}_q$ ou $\mathbb{F}_{p^n}$.

Démonstration. Soit K un corps de décomposition du polynôme $Q := X^q - X$ sur $\mathbb{F}_p$. Le polynôme dérivé Q' égale -1 donc n'a pas de racines en commun avec Q. Par conséquent, d'après la proposition 25.2.3, Q a q racines distinctes dans K.

Or, le point-clé est que ces racines sont exactement les solutions de l'équation $x^q = x$, c.-à-d., les éléments de K fixés par l'endomorphisme Fr_q. Par conséquent, ces racines forment un sous-corps K_1 de K, de cardinal q. Comme, par hypothèse, K est engendré par ces racines, on obtient $K = K_1$, et donc K est de cardinal q. Ceci prouve le point 1).

Réciproquement, supposons que L soit un autre corps fini de cardinal q. D'après le théorème 30.1.3, le groupe multiplicatif $L^\times$ est cyclique, d'ordre $q - 1$. Donc, tout élément $x \in L^\times$ vérifie

$$x^{q-1} = 1 \quad \text{et donc} \quad x^q = x.$$

Donc, tout élément de $L = L^\times \cup \{0\}$ est une racine du polynôme $Q = X^q - X$. Comme $|L| = q$, alors Q a toutes ses racines dans L, et puisque leur ensemble égale L tout entier, L est un corps de décomposition de Q sur $\mathbb{F}_p$. Par conséquent, d'après le théorème 24.2.3, L est isomorphe à K. Le théorème est démontré. □

Théorème 30.4.3 (Existence et unicité des extensions $\mathbb{F}_q \subseteq \mathbb{F}_{q^n}$)
Soient p un nombre premier, $q = p^d$ et $q' = p^n$ deux puissances de p.

1) *S'il existe une extension $\mathbb{F}_q \subseteq \mathbb{F}_{q'}$ alors q' est une puissance de q, c.-à-d., n est un multiple de d.*

2) *Réciproquement, si $n = rd$, c.-à-d., si $q' = q^r$, alors le corps $\mathbb{F}_{q'}$ contient un* **unique** *sous-corps de cardinal q ; c'est le sous-corps des invariants de* Fr_q.

Démonstration. 1) On a déjà vu (lemme 30.1.1) que si $\mathbb{F}_q \subseteq \mathbb{F}_{q'}$ alors $\mathbb{F}_{q'}$ est un $\mathbb{F}_q$-espace vectoriel de dimension finie r, d'où $q' = q^r$, c.-à-d., $n = dr$.

2) Réciproquement, supposons $n = dr$, c.-à-d., $q' = q^r$. D'après le théorème précédent, le polynôme

$$X^{q'} - X = X^{q^r} - X$$

est scindé dans $\mathbb{F}_{q'}$ et ses racines, deux à deux distinctes, sont exactement les éléments de $\mathbb{F}_{q'}$. D'autre part,

$$\begin{aligned} X^{q^r} - X &= X^q - X + X^{q^2} - X^q + \cdots + X^{q^r} - X^{q^{r-1}} \\ &= X^q - X + (X^q - X)^q + \cdots + (X^q - X)^{q^{r-1}}. \end{aligned}$$

Donc $X^q - X$ divise $X^{q^r} - X$ et a aussi toutes ses racines dans $\mathbb{F}_{q'}$. Ces racines sont exactement les points fixes dans $\mathbb{F}_{q'}$ de l'endomorphisme de Frobenius Fr_q, donc forment un sous-corps K de cardinal q, isomorphe à $\mathbb{F}_q$.

Enfin, supposons que L soit un autre sous-corps de $\mathbb{F}_{q'}$ de cardinal q. D'après le théorème 30.1.3, le groupe multiplicatif $L^\times$ est cyclique, d'ordre $q - 1$. Donc, tout élément $x \in L^\times$ vérifie

$$x^{q-1} = 1 \quad \text{et donc} \quad x^q = x.$$

Par conséquent, les éléments de $L = L^\times \cup \{0\}$ sont exactement les racines dans $\mathbb{F}_{q'}$ du polynôme $X^q - X$. Il en résulte $L = K$. Le théorème est démontré. □

30.5 Groupe de Galois de $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$

Lemme 30.5.1 *Soit G un groupe fini.*

1) *Pour tout sous-groupe H, on a $|G| = |H| \cdot |G/H|$. En particulier, $|H|$ divise $|G|$.*

2) *Soit $g \in G$. L'ensemble $\{n \in \mathbb{Z} \mid g^n = 1\}$ est un sous-groupe non-nul de $\mathbb{Z}$, donc de la forme $d\mathbb{Z}$, pour un certain $d \geq 1$, appelé l'***ordre** *de g. On a $d = 1 \Leftrightarrow g = 1$. Le sous-groupe de G engendré par g est égal à $\{1, g, \ldots, g^{d-1}\}$; il est de cardinal d et isomorphe à $\mathbb{Z}/d\mathbb{Z}$. En particulier, d divise n.*

Démonstration. On rappelle que G/H désigne l'ensemble des classes à gauche gH. C'est un ensemble fini, puisque G est fini. De plus, deux classes distinctes $gH \neq g'H$ sont disjointes. En effet, sinon il existerait $h, h' \in H$ tels que $gh = g'h'$, et l'on aurait $gH = g'H$. De plus, chaque classe gH est de cardinal $|H|$, puisque l'application $H \mapsto gH$, $h \mapsto gh$ est une bijection. Donc G est la réunion disjointe de $|G/H|$ classes, chacune de cardinal $|H|$. Le point 1) en résulte.

Soit $g \in G$. On pose $g^0 = 1$. Comme G est fini, les éléments g^k, $k \geq 1$, ne peuvent être tous distincts. Donc il existe $r < s$ tels que $g^r = g^s$, d'où $g^{s-r} = 1$. Ceci montre que l'ensemble

$$\{n \in \mathbb{Z} \mid g^n = 1\}$$

n'est pas réduit à $\{0\}$. Comme $g^m g^n = g^{m+n}$, on voit que cet ensemble est un sous-groupe non nul de $\mathbb{Z}$, donc est de la forme $d\mathbb{Z}$, pour un unique $d \geq 1$, et le reste du point 2) s'obtient facilement. □

Théorème 30.5.2 (L'isomorphisme $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \cong \mathbb{Z}/n\mathbb{Z}$**)** *Soient $n \geq 1$ et q une puissance d'un nombre premier p.*

L'extension $\mathbb{F}_q \subseteq \mathbb{F}_{q^n}$ est galoisienne. Son groupe de Galois $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ *est cyclique d'ordre n, engendré par l'automorphisme de Frobenius* Fr_q.

Démonstration. $\mathbb{F}_{q^n}$ est un corps de décomposition du polynôme $Q = X^{q^n} - X$ sur $\mathbb{F}_p$, donc a fortiori sur $\mathbb{F}_q$. De plus, Q a des racines distinctes dans $\mathbb{F}_{q^n}$ (puisque $Q' = -1$) donc est séparable sur $\mathbb{F}_q$. Donc, d'après le deuxième théorème fondamental (26.1.5), l'extension $\mathbb{F}_q \subseteq \mathbb{F}_{q^n}$ est galoisienne. De plus, d'après le théorème d'Artin (26.3.1), on a

$$|\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)| = [\mathbb{F}_{q^n} : \mathbb{F}_q] = n.$$

D'autre part, Fr_q est un $\mathbb{F}_q$-automorphisme de $\mathbb{F}_{q^n}$, c.-à-d., un élément de $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$; soit d son ordre. L'égalité $\mathrm{Fr}_q^d = \mathrm{id}_{\mathbb{F}_{q^n}}$ équivaut à

$$\forall x \in \mathbb{F}_{q^n}, \quad x = \mathrm{Fr}_q^d(x) = x^{q^d}.$$

Comme le polynôme $X^{q^d} - X$ a au plus q^d racines, ceci entraîne que $d \geq n$. Par conséquent, $d = n$ et donc Fr_q est un générateur de $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$, qui est donc isomorphe à $\mathbb{Z}/n\mathbb{Z}$. Le théorème est démontré. □

30.6 Théorème de l'élément primitif, et polynômes irréductibles sur $\mathbb{F}_q$

On rappelle qu'une extension $k \subset K$ est dite monogène s'il existe $\xi \in K$ tel que $K = k(\xi)$; dans ce cas, on dit que ξ est un élément **primitif** de K sur k.

Théorème 30.6.1 *On considère une extension $\mathbb{F}_q \subset \mathbb{F}_{q^n}$. Soit ξ un générateur du groupe multiplicatif $\mathbb{F}_{q^n}^\times$.*

1) *$\mathbb{F}_{q^n} = \mathbb{F}_q[\xi]$, c.-à-d., ξ est un élément primitif.*

2) *Le polynôme minimal $\mathrm{Irr}_{\mathbb{F}_q}(\xi)$ est de degré n.*

Démonstration. 1) est clair car $\mathbb{F}_q[\xi]$ contient $\{1, \xi, \xi^2, \ldots, \xi^{q^n-1}\} = \mathbb{F}_{q^n}^\times$, ainsi que 0, donc égale $\mathbb{F}_{q^n}$. Le point 2) en découle car le degré de $\mathrm{Irr}_{\mathbb{F}_q}(\xi)$ est le degré sur $\mathbb{F}_q$ de $\mathbb{F}_q[\xi] = \mathbb{F}_q$, qui égale n. □

Corollaire 30.6.2 *Pour tout corps fini $\mathbb{F}_q$, et tout $n \geq 1$, il existe dans $\mathbb{F}_q[X]$ au moins un polynôme irréductible unitaire de degré n.*

Définition 30.6.3 *Pour tout $d \geq 1$, notons $I(d,q)$ l'ensemble des polynômes irréductibles unitaires de degré d dans $\mathbb{F}_q[X]$ et posons $i(d,q) = |I(d,q)|$.*

Théorème 30.6.4 *Pour tout $n \geq 1$, on a*

$$X^{q^n} - X = \prod_{d|n} \prod_{P \in I(d,q)} P. \tag{1}$$

Par conséquent,

$$q^n = \sum_{d|n} d\, i(d,q). \tag{2}$$

Démonstration. Fixons $n \geq 1$. On va démontrer le théorème en trois étapes.

1. Soient d divisant n et $P \in I(d,q)$. Le corps de rupture $\mathbb{F}_q[X]/(P)$ est de degré d sur $\mathbb{F}_q$, donc est isomorphe à $\mathbb{F}_{q^d}$. Par conséquent, P a au moins une racine α dans $\mathbb{F}_{q^d}$. Comme, d'après le théorème 30.5.2, l'extension $\mathbb{F}_q \subseteq \mathbb{F}_{q^d}$ est galoisienne, alors $P = \mathrm{Irr}_{\mathbb{F}_q}(\alpha)$ est scindé sur $\mathbb{F}_{q^d}$. Par conséquent, P divise le polynôme

$$X^{q^d} - X = \prod_{x \in \mathbb{F}_{q^d}} (X - x). \tag{$*_d$}$$

De plus, on a vu dans la preuve du théorème 30.4.3 que $X^{q^d} - X$ divise $X^{q^n} - X$. Ceci découle aussi de l'inclusion $\mathbb{F}_{q^d} \subseteq \mathbb{F}_{q^n}$ (établie en 30.4.3), et de l'égalité

$$(*_n) \qquad X^{q^n} - X = \prod_{x \in \mathbb{F}_{q^n}} (X - x).$$

Donc, P divise $Q_n := X^{q^n} - X$. Ceci montre que Q_n est divisible par le terme de droite de (1).

2. Réciproquement, soit R un facteur irréductible, unitaire, de degré d, de Q_n dans $\mathbb{F}_q[X]$ et soit α une racine de R dans $\mathbb{F}_{q^n}$. Alors $R = \mathrm{Irr}_{\mathbb{F}_q}(\alpha)$ et donc $\deg_{\mathbb{F}_q}(\alpha) = d$. Par conséquent, on a

$$\mathbb{F}_{q^d} \cong \mathbb{F}_q[\alpha] \subseteq \mathbb{F}_{q^n},$$

et, d'après le théorème 30.4.3, ceci entraîne que $d \mid n$. Ceci montre que Q_n n'a pas d'autres facteurs irréductibles que les $P \in I(d, q)$, pour $d \mid n$.

3. Enfin, les facteurs irréductibles de Q_n sont tous de multiplicité 1, puisque Q_n a des racines simples, d'après $(*_n)$. Ceci prouve l'égalité (1) du théorème, et l'égalité (2) en découle en prenant les degrés. □

Théorème 30.6.5 (Polynômes irréductibles sur $\mathbb{F}_q$) *Soit $P \in I(d, q)$ et soit $\alpha \in \mathbb{F}_{q^d}$ une racine de P. Alors,*

$$(3) \qquad P = (X - \alpha)(X - \alpha^q) \cdots (X - \alpha^{q^{d-1}}).$$

Démonstration. D'après le théorème 30.5.2, l'extension $\mathbb{F}_q \subseteq \mathbb{F}_{q^d}$ est galoisienne, de groupe

$$G := \mathrm{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q) = \{1, \mathrm{Fr}_q, \ldots, \mathrm{Fr}_q^{d-1}\} \cong \mathbb{Z}/d\mathbb{Z}.$$

D'autre part, d'après la proposition 24.3.2, l'on a :

$$P = \mathrm{Irr}_{\mathbb{F}_q}(\alpha) = \prod_{\beta \in G\alpha} (X - \beta).$$

Comme $\deg P = d$, l'orbite $G\alpha$ a d éléments ; elle est donc formée des éléments $\alpha, \alpha^q, \ldots, \alpha^{q^{d-1}}$, qui sont deux à deux distincts. Ceci prouve le théorème. □

31 Clôtures algébriques

31.1 Corps algébriquement clos

Définition 31.1.1 *Soit $k \subseteq K$ une extension de corps et soit $P \in k[X]$ non constant. On dit que P est* **scindé** *dans $K[X]$, ou sur K, si P se décompose dans $K[X]$ comme produit de facteurs du premier degré, c.-à-d.,*

$$P = c(X - \alpha_1) \cdots (X - \alpha_d),$$

où $d = \deg P$, c est le coefficient dominant de P, et les α_i sont dans K (pas nécessairement distincts).

Définition 31.1.2 *Un corps K est dit* **algébriquement clos** *si tout $P \in K[X]$ non constant a au moins une racine dans K.*

Lemme 31.1.3 *Si K est algébriquement clos, tout $P \in K[X]$ non constant est scindé.*

Démonstration. Par récurrence sur $d = \deg P$. C'est clair si $d = 1$. Supposons $d \geq 2$ et l'assertion établie en degré $< d$. Soit $P \in K[X]$ de degré d. Comme K est algébriquement clos, P possède dans K au moins un racine α, donc se factorise en $P = (X - \alpha)Q$, avec $Q \in K[X]$ de degré $d - 1$. Par hypothèse de récurrence, Q est scindé dans $K[X]$, et donc il en est de même de P. □

Définition 31.1.4 *Soit $k \subseteq K$ une extension de corps. On dit que K est une* **clôture algébrique de** *k si K est algébriquement clos et si tout élément de K est algébrique sur k.*

31.2 Le corps $\overline{\mathbb{F}}_p$

Soit $(m_i)_{i \geq 1}$ une suite d'entiers ≥ 1 tendant vers $+\infty$ et « suffisamment divisible » au sens suivant : pour tout $i \geq 1$, m_i divise m_{i+1}, et i divise m_i. On peut prendre, par exemple, $m_i = i!$.

Posons $K_0 = \mathbb{F}_p$ et pour tout $i \geq 1$, soit K_i un corps de décomposition sur K_{i-1} du polynôme

$$X^{p^{m_i}} - X.$$

Alors, $K_i \cong \mathbb{F}_{p^{m_i}}$ et on a une suite croissante

$$K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots$$

On note $\overline{\mathbb{F}}_p$ la réunion des K_i.

Proposition 31.2.1 (Premières propriétés de $\overline{\mathbb{F}}_p$)

1) *Pour tout $d \geq 1$, $\overline{\mathbb{F}}_p$ contient un unique sous-corps de cardinal p^d ; on le notera $\mathbb{F}_{p^d}(\overline{\mathbb{F}}_p)$.*

2) *Fixons $r \geq 1$ et $q = p^r$. On a $\overline{\mathbb{F}}_p = \bigcup_{n\geq 1} \mathbb{F}_{q^{n!}}(\overline{\mathbb{F}}_p)$.*

Démonstration. 1) Soient $d \geq 1$ et $q = p^d$. Par hypothèse, d divise m_d donc

$$\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^{m_d}} \subseteq \overline{\mathbb{F}}_p.$$

De plus, le polynôme $X^q - X$ a toutes ses racines, deux à deux distinctes, dans $\mathbb{F}_q$, et ces racines sont exactement les éléments de $\mathbb{F}_q$.

Par conséquent, $\mathbb{F}_q$ est l'unique sous-corps de $\overline{\mathbb{F}}_p$ de cardinal q. En effet, si L en est un autre alors, comme le groupe multiplicatif $L^\times$ est cyclique d'ordre $q-1$, les éléments de L sont exactement les racines dans $\overline{\mathbb{F}}_p$ du polynôme $X^q - X$, c.-à-d., les élément de $\mathbb{F}_q$. Ceci prouve le point 1).

2) Pour tout $d \geq 1$, notons simplement $\mathbb{F}_{p^d}$ l'unique sous-corps de $\overline{\mathbb{F}}_p$ de cardinal p^d. Par définition, l'on a

$$\overline{\mathbb{F}}_p = \bigcup_{i\geq 1} \mathbb{F}_{p^{m_i}}.$$

Fixons $q = p^r$ et montrons que

$$(*) \qquad \bigcup_{i\geq 1} \mathbb{F}_{p^{m_i}} = \bigcup_{n\geq 1} \mathbb{F}_{q^{n!}}.$$

Pour tout $i \geq 1$, on a $\mathbb{F}_{p^{m_i}} \subseteq \mathbb{F}_{q^{m_i!}}$, puisque m_i divise $m_i!$. Ceci prouve l'inclusion $\subseteq$. Réciproquement, soit $n \geq 1$. Par hypothèse, $i = rn!$ divise $m_i = m_{rn!}$ et donc $\mathbb{F}_{q^{n!}} \subseteq \mathbb{F}_{p^{m_{rn!}}}$. Ceci prouve l'inclusion $\supseteq$, et donc l'égalité dans $(*)$. La proposition est démontrée. □

Théorème 31.2.2 (Existence et unicité d'une clôture algébrique de $\mathbb{F}_q$)

1) *$\overline{\mathbb{F}}_p$ est une clôture algébrique de $\mathbb{F}_q$, pour tout $q = p^d$.*

2) *Toute clôture algébrique de $\mathbb{F}_q$ est $\mathbb{F}_q$-isomorphe à $\overline{\mathbb{F}}_p$.*

Démonstration. Fixons $q = p^d$ et désignons par $\mathbb{F}_q$ l'unique sous-corps de $\overline{\mathbb{F}}_p$ à q éléments.

1) Soit $x \in \overline{\mathbb{F}}_p$. Il existe $i \geq 1$ tel que $x \in \mathbb{F}_{p^{m_i}}$, et donc x est algébrique sur $\mathbb{F}_p$, et a fortiori sur $\mathbb{F}_q$. Donc, pour prouver 1), il suffit de montrer que $\overline{\mathbb{F}}_p$ est algébriquement clos. Soit $P = X^d + a_1 X^{d-1} + \cdots + a_d \in \overline{\mathbb{F}}_p[X]$,

non constant. Il existe $i \geq 1$ tel que $a_0, \ldots, a_d \in \mathbb{F}_{p^i}$. Soit K un corps de décomposition de P sur $\mathbb{F}_{p^i}$ et soit $r = [K : \mathbb{F}_{p^i}]$. Alors K est isomorphe au sous-corps $\mathbb{F}_{p^{ir}}$ de $\overline{\mathbb{F}}_p$ et donc P est scindé sur ce sous-corps, a fortiori sur $\overline{\mathbb{F}}_p$. Ceci prouve que $\overline{\mathbb{F}}_p$ est une clôture algébrique de $\mathbb{F}_q$.

Posons $K = \overline{\mathbb{F}}_p$ et, pour tout $n \geq 1$, désignons par K_n l'unique sous-corps de K de cardinal $q^{n!}$. Ainsi, K_1 est le corps $\mathbb{F}_q$ considéré dans le théorème, et l'on a, d'après la proposition précédente,

$$K = \bigcup_{n \geq 1} K_n. \tag{1}$$

Considérons une extension $\mathbb{F}_q \subset L$ et supposons que L soit une clôture algébrique de $\mathbb{F}_q$. Comme L est algébriquement clos, le polynôme $Q_n := X^{q^{n!}} - X \in L[X]$ est scindé ; et comme ses racines sont simples, L contient un sous-corps de cardinal $q^{n!}$. En raisonnant comme dans la preuve de la proposition précédente, on obtient que L contient un unique sous-corps de cardinal $q^{n!}$, dont les éléments sont les racines dans L de Q_n. Notons-le L_n. En particulier, L_1 égale $\mathbb{F}_q$, identifié à K_1.

D'autre part, soit $x \in L$. Par hypothèse, x est algébrique sur $\mathbb{F}_q$; soit $d = \deg_{\mathbb{F}_q}(x)$ son degré. Alors le sous-corps $\mathbb{F}_q[x]$ de L est de cardinal q^d, donc est contenu dans L_d (puisque d divise $d!$). Par conséquent, on a

$$L = \bigcup_{n \geq 1} L_n. \tag{2}$$

Montrons maintenant, par récurrence sur n, qu'on peut prolonger l'identification $L_1 = K_1 = \mathbb{F}_q$ en un $\mathbb{F}_q$-isomorphisme $\tau_n : L_n \xrightarrow{\sim} K_n$.

Supposons l'assertion établie au cran n. Commençons par remarquer que $\tau_n(Q_{n+1}) = Q_{n+1}$, puisque les coefficients de Q_{n+1} sont dans $\mathbb{F}_p$. Observons ensuite que, comme L_{n+1}, resp. K_{n+1}, contient L_n, resp. K_n, et est formé des racines de Q_{n+1} dans L, resp. K, alors L_{n+1}, resp. K_{n+1}, est un corps de décomposition de Q_{n+1} sur L_n, resp. K_n. Par conséquent, d'après le premier théorème fondamental 24.2.5, τ_n se prolonge en un $\mathbb{F}_q$-isomorphisme $\tau_{n+1} : L_{n+1} \xrightarrow{\sim} K_{n+1}$.

On obtient ainsi une suite infinie $(\tau_1, \tau_2, \cdots)$ d'isomorphismes $\tau_n : L_n \xrightarrow{\sim} K_n$, tels que $\tau_1 = \mathrm{id}_{\mathbb{F}_q}$ et

$$\forall r \geq n, \quad \tau_r|_{L_n} = \tau_n. \tag{3}$$

On définit alors $\tau : L \to K$ par la formule : $\tau(x) = \tau_n(x)$ si $x \in L_n$. Ceci est bien défini d'après (3). Il est alors clair que τ est un morphisme de corps,

donc est injectif. De plus, son image contient K_n, pour tout $n \geq 1$, donc égale K. Par conséquent, τ est un $\mathbb{F}_q$-isomorphisme de L sur K. Le théorème est démontré. □

31.3 Clôtures algébriques en général

Dans le cas des corps finis, on a pu démontrer explicitement, de façon constructive, l'existence et l'unicité d'une clôture algébrique. En fait, on peut démontrer ce résultat pour un corps arbitraire, en utilisant des arguments de théorie des ensembles et le lemme de Zorn. C.-à-d., on a le théorème ci-dessous.

Théorème 31.3.1 (Steinitz) *Tout corps k admet une clôture algébrique, unique à k-isomorphisme (non-unique) près.*

Démonstration. Pour l'existence, l'idée est très simple. La réunion d'une famille filtrante d'extensions algébriques de k est une extension algébrique de k. L'ensemble des extensions algébriques de k vérifie donc les hypothèses du Lemme de Zorn (11.2.6) donc possède un élément maximal K.

Soit $P \in K[X]$ un polynôme irréductible, et $L = K[X]/(P)$ son corps de rupture. Les extensions K/k et L/K sont algébriques, donc par transitivité L/k l'est aussi (23.5.5 ou 23.3.9). Donc, par maximalité, $K = L$, donc P a une racine dans K. Ceci prouve que K est algébriquement clos, donc une clôture algébrique de k.

Le problème de la « démonstration » ci-dessus est qu'on sait, depuis Cantor, qu'il n'existe pas d'« ensemble » de tous les ensembles. Il n'est pas clair que les extensions algébriques de k forment un ensemble, et donc qu'on puisse appliquer le lemme de Zorn. En fait, par un argument de cardinalité, on peut effectuer qu'on peut effectivement parler de l'**ensemble** des extensions algébriques de k, de façon à rendre rigouresue l'idée de démonstration ci-dessus. Pour cela, voir [Ja2, §8.1] ou [Dou], tome 2, §5.2 (complétés par [La], Appendice 2, pour les questions de cardinalité).

Une autre démonstration se trouve dans [La, §VII.2], et ces références démontrent aussi l'unicité à k-isomorphisme près. □

Remarque 31.3.2 Par ailleurs, on a déjà vu que le corps $\mathbb{C}$ des nombres complexes est algébriquement clos (3.1, 28.1). De plus, on a les résultats ci-dessous.

Proposition 31.3.3 (Fermeture algébrique de k dans K)

Soit $k \subset K$ une extension de corps. L'ensemble

$$K_{\mathrm{alg}/k} = \{x \in K \mid x \text{ est algébrique sur } k\}$$

est un sous-corps de K, appelé la fermeture algébrique de k dans K.

Démonstration. Posons $K' = K_{\mathrm{alg}/k}$. Il est clair que $1 \in K'$. Soient $x, y \in K'$. Alors la sous-algèbre $k[x]$ est un corps, de degré $d = \deg_k(x)$ sur k. Comme y est algébrique sur k, il l'est aussi sur $k[x]$ et donc la sous-algèbre $k[x, y] = k[x][y]$ est un corps, égal à $k(x, y)$, et de degré $f = \deg_{k[x]}(y)$ sur $k[x]$. Donc,

$$[k(x, y) : k] = [k(x, y) : k(x)][k(x) : k] = fd < \infty.$$

Comme $k(x, y)$ contient $x + y$ et xy, ces deux éléments sont algébriques sur k, c.-à-d., appartiennent à K'. Ceci montre que K' est un sous-corps de K. □

Théorème 31.3.4 *Soit $k \subseteq L$ une extension de corps. On suppose L algébriquement clos. Posons*

$$\overline{k} = L_{\mathrm{alg}/k} = \{x \in L \mid x \text{ est algébrique sur } k\}.$$

Alors $\overline{k}$ est une clôture algébrique de k.

Démonstration. D'après la proposition précédente, $\overline{k}$ est un corps, algébrique sur k. Montrons que $\overline{k}$ est algébriquement clos. Soit $P = a_0 + a_1X + \cdots + a_dX^d \in \overline{k}[X]$. Comme les a_i sont algébriques sur k, le sous-corps $K = k[a_0, \ldots, a_d]$ est de degré fini n sur k, d'après la proposition 23.5.6.

D'autre part, comme L est algébriquement clos, il existe $\alpha \in L$ tel que $P(\alpha) = 0$. Alors α est algébrique sur K et donc $K(\alpha)$ est de degré fini, disons r, sur K. Alors

$$rn = [K(\alpha) : k] = [K(\alpha) : k(\alpha)][k(\alpha) : k],$$

d'où $[k(\alpha) : k] < +\infty$. Donc α est algébrique sur k, c.-à-d., appartient à $\overline{k}$. Ceci montre que $\overline{k}$ est algébriquement clos. Le théorème est démontré. □

Comme $\mathbb{C}$ est algébriquement clos, on obtient ainsi le corollaire suivant. (*cf.* 2.4.5 ; à ce propos, deux lignes au-dessus de la proposition 2.4.5, corriger $\mathbb{Q}$ en $\overline{\mathbb{Q}}$.)

Corollaire 31.3.5 *Le corps $\overline{\mathbb{Q}} := \{z \in \mathbb{C} \mid z \text{ est algébrique sur } \mathbb{Q}\}$ est une clôture algébrique de $\mathbb{Q}$.*

Table des matières

Bibliographie

[Art] E. Artin, Galois Theory, nouvelle édition, Dover, 1998.

[AM] M. Atiyah, I. G. Macdonald, Commutative algebra, Addison-Wesley, 1969.

[BAlg] N. Bourbaki, Algèbre, Chapitres 4 à 7, Masson, 1981.

[BM] J. Briançon, Ph. Maisonobe, Éléments d'algèbre commutative (niveau M1), Ellipses, 2004.

[De] R. Dedekind, Sur la théorie des nombres entiers algébriques, Gauthier-Villars, 1877 ; traduit en anglais avec une introduction de J. Stillwell dans : Theory of algebraic integers, Cambridge Univ. Press 1996.

[ChL] A. Chambert-Loir, A field guide to algebra, Springer, 2005 ; version française : Algèbre corporelle (sic !), Presses de l'École polytechnique, 2005.

[Die] J. Dieudonné, Cours de géométrie algébrique, tome 2, P.U.F., 1974.

[Dou] A. Douady, R. Douady, Algèbre et théories galoisiennes (2 tomes), Cedic Fernand Nathan, 1977, 2ème éd., Cassini, 2005.

[Elk] R. Elkik, Cours d'algèbre, Ellipses, 2002.

[Esc] J.-P. Escofier, Théorie de Galois, Dunod, 2000.

[Ja1] N. Jacobson, Basic algebra I, W. H. Freeman & Co., 1974.

[Ja2] N. Jacobson, Basic algebra II, W. H. Freeman & Co., 1980.

[Kru] W. Krull, Idealtheorie, Springer Verlag, 1937 (2e édition 1968).

[La] S. Lang, Algebra, Addison-Wesley, 1965. Traduction française de la 3ème édition : Algèbre, Dunod, 2004.

[Ne04] J. Nekovàř, Théorie de Galois, cours UPMC 2003/4, disponible à l'adresse : www.math.jussieu.fr/~nekovar/co/ln

[Pe1] D. Perrin, Cours d'algèbre, E.N.S.J.F. 1981, et 3ème édition, Ellipses, 1996.

[Pe2] D. Perrin, Géométrie algébrique - Une introduction, Inter Éditions/-CNRS Éditions, 1995.

[Sa] P. Samuel, Théorie algébrique des nombres, Hermann, 1967.

[Se] J.-P. Serre, Représentations linéaires des groupes finis, (3ème édition corrigée), Hermann, 1978.

[St] J. Stillwell, Chapitre d'introduction dans [De].

[Ti] J.-P. Tignol, Galois' Theory of algebraic equations, World Scientific, 2001.

[vdW] B. L. van der Waerden, History of algebra from al-Khwarizmi to Emmy Noether, Springer Verlag, 1985.