

Chapitre 8

Corps finis et leur clôture algébrique

Version du 1^{er} décembre 2004

Erratum. Dans la version du 22 novembre du Chap. 7, au début de la démonstration du théorème d'Artin, il n'est pas évident a priori que $\dim_L K$ soit finie. Par conséquent, il faut remplacer les deux premières lignes de la p. 123 par : "Posons $n = |G|$. D'après la proposition 7.5.3, on a $\dim_L K \geq n$. Supposons que $\dim_L K > n$. Alors, posant $r = n + 1$, il existe des éléments $\varepsilon_1, \dots, \varepsilon_r \in L$ linéairement indépendants sur K ", et les trois dernières lignes de la p. 123 par : "Cette contradiction montre que l'hypothèse $\dim_K L > n$ est impossible. On a donc $\dim_K L = n$, ce qui prouve le point 1)." De plus, toujours p. 123, deux lignes en dessous du système (*), supprimer les mots : "Supposons $r > n$."

8.1 Cardinal et groupe multiplicatif d'un corps fini

Soit k un corps fini. Son sous-corps premier est fini donc, d'après le paragraphe 7.1.2, 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 8.1.1 *Soient $k \subseteq k'$ deux corps finis, de cardinal q et q' respectivement.*

- 1) *Soit $n = [k' : k]$. Alors $q' = q^n$.*
- 2) *Par conséquent, si $p = \text{car}(k)$ 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. \square

Corollaire 8.1.2 *Si k est un corps fini de caractéristique p , alors le cardinal de k est une puissance de p .*

Théorème 8.1.3 (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 $d = d_1 \geq \dots \geq d_r > 1$ tels que d_i divise d_{i-1} , pour $i = r, r - 1, \dots, 2$ et

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

Alors, d'une part, $|k^\times| = dd_2 \dots d_r$ et, d'autre part, tout élément $x \in k^\times$ vérifie $x^d = 1$. 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. \square

8.2 Endomorphismes de Frobenius

8.2.1 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 $k \geq 1$) :

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

(Quand on prend k éléments dans $\{1, \dots, n\}$, on peut ou bien prendre, ou ne pas prendre, n .) On rappelle aussi la formule du binôme, valable dans tout anneau commutatif.

Lemme 8.2.1 (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 8.2.2 Soit $p \in \mathbb{N}$ un nombre premier. Alors p divise $\binom{p}{k}$ pour tout $k = 1, \dots, p-1$.

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

8.2.2 Les morphismes Fr_p et Fr_{p^n} **Proposition 8.2.3 (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 8.2.4 (Les endomorphismes de Frobenius $\text{Fr}_q = \text{Fr}_{p^n}$)

Soient K un corps de caractéristique $p > 0$ et $n \geq 1$. L'application $\text{Fr}_p^n := \text{Fr}_p \circ \dots \circ \text{Fr}_p$ (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 8.2.5 Soient p un nombre premier, $n \geq 1$ et $q = p^n$. Alors p divise $\binom{q}{i}$ pour tout $i = 1, \dots, q-1$.

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

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

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

$$(2) \quad (1 + X)^q = 1 + X^q.$$

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

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

Lemme 8.3.1 *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. \square

Théorème 8.3.2 (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 7.6.2, 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 8.1.3, 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 7.3.3, L est isomorphe à K . Le théorème est démontré. \square

Théorème 8.3.3 (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 8.1.1) 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,

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

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 8.1.3, 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. \square

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

Lemme 8.4.1 *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 $\{1, g, \dots, g^{d-1}\}$; 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 8.4.2 (L'isomorphisme $\text{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \cong \mathbb{Z}/n\mathbb{Z}$)

Soit q une puissance d'un nombre premier p et soit $n \geq 1$. L'extension $\mathbb{F}_q \subseteq \mathbb{F}_{q^n}$ est galoisienne. Son groupe de Galois $\text{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) = \text{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q^n})$ est un groupe 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, a fortiori, séparable sur \mathbb{F}_q . Donc, d'après le 2ème théorème fondamental (7.4.4), l'extension $\mathbb{F}_q \subseteq \mathbb{F}_{q^n}$ est galoisienne. De plus, d'après le théorème d'Artin (7.5.4), on a

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

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

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

Comme le polynôme $X^{q^d} - X$ a au plus q^n racines, ceci entraîne que $d \geq n$. Par conséquent, $d = n$ et le sous-groupe cyclique de G engendré par Fr_q égale G . Ceci achève la preuve du théorème. \square

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

On rappelle (cf. 7.7.2) qu'une extension $k \subset K$ est dite simple 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 8.5.1 *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 $\text{Irr}_{\mathbb{F}_q}(\xi)$ est de degré n .

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

Corollaire 8.5.2 *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 8.5.1 *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 8.5.3 *Pour tout $n \geq 1$, on a*

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

Par conséquent,

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

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 8.4.2, l'extension $\mathbb{F}_q \subseteq \mathbb{F}_{q^d}$ est galoisienne, alors $P = \text{Irr}_{\mathbb{F}_q}(\alpha)$ est scindé sur \mathbb{F}_{q^d} . Par conséquent, P divise le polynôme

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

De plus, on a vu dans la preuve du théorème 8.3.3 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 8.3.3), et de l'égalité

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

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 $R = \text{Irr}_{\mathbb{F}_q}(\alpha)$ 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 8.3.3, 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. \square

Théorème 8.5.4 (Description des 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,

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

En particulier, l'orbite de α sous $\text{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q)$ a exactement d éléments.

Démonstration. D'après le théorème 8.4.2, l'extension $\mathbb{F}_q \subseteq \mathbb{F}_{q^d}$ est galoisienne, de groupe

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

D'autre part, d'après la proposition 7.4.1, l'on a :

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

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

8.6 La clôture algébrique de \mathbb{F}_q

8.6.1 Corps algébriquement clos

Définition 8.6.1 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 8.6.2 Un corps K est dit algébriquement clos si tout $P \in K[X]$ non constant a au moins une racine dans K .

Lemme 8.6.1 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 une 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 . \square

Définition 8.6.3 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 .

8.6.2 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

$$K_0 \subseteq K_1 \subseteq K_2 \subseteq \dots$$

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

Proposition 8.6.2 (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 éléments 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

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

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. \square

Théorème 8.6.3 (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 $P = a_0 + a_1X + \dots + a_dX^d \in \overline{\mathbb{F}_p}[X]$, non-constant. Il existe $i \geq 1$ tel que $a_0, \dots, a_d \in K_i = \mathbb{F}_{p^i}$. Soit K'_i un corps de décomposition de P sur K_i et soit $r = [K'_i : K_i]$. Alors K'_i est isomorphe au sous-corps $\mathbb{F}_{p^{n_i r}}$ 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,

$$(1) \quad K = \bigcup_{n \geq 1} K_n.$$

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

$$(2) \quad L = \bigcup_{n \geq 1} L_n.$$

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 1er théorème fondamental 7.3.5, 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 (τ_1, τ_2, \dots) d'isomorphismes $\tau_n : L_n \xrightarrow{\sim} K_n$, tels que $\tau_1 = \text{id}_{\mathbb{F}_q}$ et

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

On définit alors $\tau : L \rightarrow K$ 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. \square

8.6.3 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. On renvoie à [Ja2, §8.1] ou [Dou], tome 2, §5.2 pour une démonstration, et à [La, §VII.2] pour une autre.

Théorème 8.6.4 (Théorème de Steinitz)

Tout corps k admet une clôture algébrique, unique à k -isomorphisme près.

Remarque 8.6.1 On verra plus loin que le corps \mathbb{C} des nombres complexes est algébriquement clos. Ceci peut se démontrer, par exemple, par des méthodes d'analyse élémentaire, ou bien en utilisant la théorie de Galois. D'autre part, on a les résultats ci-dessous.

Proposition 8.6.5 (Fermeture algébrique de k dans K)

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

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

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

Démonstration. Posons $K' = K_{\text{alg}/k}$. 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 . \square

Théorème 8.6.6 *Soit $k \subseteq L$ une extension de corps. On suppose L algébriquement clos. Posons*

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

Alors \bar{k} est une clôture algébrique de k .

Démonstration. D'après la proposition précédente, \bar{k} est un corps, algébrique sur k . Montrons que \bar{k} est algébriquement clos. Soit $P = a_0 + a_1X + \dots + a_dX^d \in \bar{k}[X]$. Comme les a_i sont algébriques sur k , le sous-corps $K = k[a_0, \dots, a_d]$ est de degré fini n sur k , d'après la proposition 7.2.5.

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 \bar{k} . Ceci montre que \bar{k} est algébriquement clos. Le théorème est démontré. \square

En admettant pour le moment le fait que \mathbb{C} soit algébriquement clos, on obtient ainsi le corollaire suivant.

Corollaire 8.6.7 *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

1	Anneaux, idéaux, localisation	1
1.1	Anneaux et corps	1
1.2	Idéaux, idéaux premiers et maximaux	3
1.3	Anneaux quotients	5
1.3.1	Anneaux non-commutatifs et idéaux bilatères	8
1.4	Anneaux de fractions, localisation	9
1.4.1	Le cas intègre	9
1.4.2	Le cas général	12
2	Modules et produit tensoriel	15
2.1	Modules : définitions	15
2.2	Modules quotients	18
2.3	Modules de type fini	19
2.4	Modules quotients associés à un idéal bilatère	21
2.5	Groupes ou modules d'homomorphismes	23
2.5.1	Applications à valeurs dans un A -module	24
2.5.2	Morphismes de A -modules	24
2.6	Produits et sommes directes	25
2.7	A -modules libres et A -modules sans torsion	30
2.8	A -modules libres de type fini, invariance du rang	34
2.9	Lemme de Zorn et existence de sous-modules maximaux	36
2.9.1	Le lemme de Zorn	36
2.9.2	Sous-modules maximaux des modules de type fini	37
2.10	Produit tensoriel	38
2.10.0	Remarque préliminaire	39
2.10.1	Applications bilinéaires	39
2.10.2	Définition du produit tensoriel	41
2.10.3	Propriétés du produit tensoriel	43

3	Algèbres, polynômes, algèbres de type fini	49
3.1	Algèbres et extension des scalaires	49
3.1.1	Algèbres	49
3.1.2	Extension et restriction des scalaires	49
3.1.3	Localisation de modules	51
3.1.4	Produit tensoriel de A -algèbres	52
3.2	Algèbres de polynômes et algèbres de type fini	53
3.2.1	Monoïdes et algèbres associées	53
3.2.2	Algèbres de polynômes	54
3.2.3	Algèbres de type fini	56
4	Anneaux et modules noethériens	57
4.1	Modules noethériens	57
4.2	Anneaux noethériens	59
4.3	Le théorème de transfert de Hilbert	60
4.4	Un résultat d'Artin et Tate	61
4.5	Divisibilité, éléments irréductibles	62
5	Anneaux euclidiens, principaux, factoriels	65
5.1	Anneaux principaux et anneaux euclidiens	65
5.2	Propriétés de l'anneau $A[X]$	66
5.3	Anneaux factoriels	67
5.3.1	Anneaux factoriels, lemmes d'Euclide et Gauss	67
5.3.2	Les anneaux principaux sont factoriels	70
5.4	Valuations, PGCD et PPCM	71
5.4.1	Valuations	71
5.4.2	PPCM et PGCD	73
5.4.3	Le théorème de Bezout	74
5.5	Le théorème de transfert de Gauss	75
5.5.1	Énoncé du théorème	75
5.5.2	Contenu d'un polynôme	76
5.5.3	Preuve du théorème de transfert de Gauss	78
6	Modules sur les anneaux principaux	79
6.1	Idéaux étrangers et théorème chinois	79
6.2	Annulateurs et décomposition de modules	83
6.2.1	Annulateurs et modules de torsion	83
6.2.2	Décomposition des modules de \mathcal{I} -torsion	84
6.2.3	Décomposition primaire des modules de torsion sur un anneau principal	86

6.3	Modules de type fini sur un anneau principal	89
6.3.1	Les résultats fondamentaux	90
6.3.2	Réduction des matrices sur un anneau principal	92
6.3.3	Démonstration du point 1) du théorème fondamental	98
6.3.4	Décomposition en somme de modules monogènes	98
6.3.5	Unicité des facteurs invariants	100
7	Extensions de corps et théorie de Galois	103
7.1	Sous-corps premier et caractéristique	103
7.1.1	Les corps fondamentaux \mathbb{Q} et \mathbb{F}_p	103
7.1.2	Sous-corps premier et caractéristique	104
7.2	Extensions, éléments algébriques ou transcendants, degré	106
7.2.1	Généralités sur les extensions	106
7.2.2	Éléments algébriques ou bien transcendants	107
7.2.3	Degré d'une extension	108
7.3	Corps de rupture et corps de décomposition	110
7.3.1	Corps de rupture d'un polynôme	110
7.3.2	Corps de décomposition d'un polynôme	111
7.4	L'arrivée des groupes	114
7.4.1	Le groupe des k -automorphismes d'une extension	114
7.4.2	Polynômes et extensions séparables	116
7.4.3	Extensions galoisiennes	117
7.5	Sous-corps invariants et correspondance de Galois	120
7.5.1	Indépendance des caractères	120
7.5.2	Invariants d'un groupe fini : théorème d'Artin	122
7.5.3	Un rappel sur les groupes	124
7.5.4	Le couronnement : correspondance de Galois	125
7.6	Séparabilité	127
7.6.1	L'opérateur de dérivation	127
7.6.2	Racines multiples et séparabilité	128
7.7	Clôture normale, théorème de l'élément primitif	129
7.7.1	Clôture normale ou galoisienne	129
7.7.2	Extensions simples, éléments primitifs	130
8	Corps finis et leur clôture algébrique	133
8.1	Cardinal et groupe multiplicatif d'un corps fini	133
8.2	Endomorphismes de Frobenius	134
8.2.1	La formule du binôme	134

8.2.2	Les morphismes Fr_p et Fr_{p^n}	135
8.3	Existence et unicité des corps \mathbb{F}_{p^n}	136
8.4	Groupe de Galois de \mathbb{F}_{q^n} sur \mathbb{F}_q	138
8.5	Théorème de l'élément primitif, et polynômes irréductibles sur \mathbb{F}_q	139
8.6	La clôture algébrique de \mathbb{F}_q	141
8.6.1	Corps algébriquement clos	141
8.6.2	Le corps $\overline{\mathbb{F}_p}$	142
8.6.3	Clôtures algébriques en général	144

Bibliographie

[] Voici une bibliographie provisoire (elle aussi en évolution au fil du texte).

- [AM] M. Atiyah, I. G. Macdonald, Commutative algebra, Addison-Wesley, 1969.
- [Art] E. Artin, Galois Theory, nouvelle édition, Dover, 1998.
- [Bla] A. Blanchard, Les corps non commutatifs, P.U.F., 1972.
- [BAlg] N. Bourbaki, Algèbre, Chapitres 4 à 7, Masson, 1981.
- [BM] J. Briançon, Ph. Maisonobe, Éléments d'algèbre commutative (niveau M1), Ellipses, 2004.
- [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.
- [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.
- [Kri] J.-L. Krivine, Théorie des ensembles, Cassini, 1998.
- [Ku] E. Kunz, Introduction to commutative algebra and algebraic geometry, Birkhäuser, 1985.
- [La] S. Lang, Algebra, Addison-Wesley, 1965. Traduction française de la 3ème édition : *Algèbre*, Dunod, 2004.
- [Laf] J.-P. Lafon, Les formalismes fondamentaux de l'algèbre commutative, Hermann, 1974.
- [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.
- [SD] H.P.F. Swinnerton-Dyer, A brief guide to algebraic number theory, C.U.P., 2001.