Leçon 125 : Extensions de corps. Exemples et applications.

Clémentine Lemarié–Rieusset

2019

Table des matières

Les deux développements proposés sont, pour le premier, la construction des corps finis et les treillis des sous-corps des corps finis (Lemme 34, Théorèmes 35 et 36) et, pour le second, le théorème d'Artin (67) et son corollaire (68) qui sont utiles pour prouver le théorème de la correspondance de Galois. Ces deux développements sont prouvés dans ce mémoire, ainsi que le théorème de l'élément primitif (53), utilisé pour prouver le théorème d'Artin, et le fait que tout corps admet une extension algébriquement close (46), ainsi que son corollaire (47), le fait que tout corps admet une clôture algébrique.

Notation 1

$\mathbb{K}, \mathbb{L}$ *et* $\mathbb{M}$ *sont des corps.* $\mathrm{car}(\mathbb{K})$ *est la caractéristique de* $\mathbb{K}$*.*

1 Généralités

1.1 Définitions et premières propriétés

Définition 2

Une extension du corps $\mathbb{K}$ *est la donnée d'un corps* $\mathbb{L}$ *et d'un morphisme de corps* $\psi : \mathbb{K} \to \mathbb{L}$*.*

Tout morphisme de corps est injectif donc $\mathbb{K}$ s'injecte dans $\mathbb{L}$ via ψ. On identifiera donc souvent $\mathbb{K}$ à $\psi(\mathbb{K})$ et on verra $\mathbb{K}$ comme un sous-corps de $\mathbb{L}$.

Remarque 3

Il faudra tout de même garder ψ *à l'esprit, car par exemple si* p *est un nombre premier* $\begin{cases} \mathbb{Z}/p\mathbb{Z}(X) & \to & \mathbb{Z}/p\mathbb{Z}(X) \\ x & \mapsto & x^p \end{cases}$ *est un morphisme de corps non surjectif (donc* $\mathbb{Z}/p\mathbb{Z}(X)$ *peut être vu comme un sous-corps strict de lui-même).*

Définition 4

$\mathbb{L}$ *est une sous-extension de* $\mathbb{K} \subset \mathbb{M}$ *si* $\mathbb{L}$ *est un sous-corps de* $\mathbb{M}$ *contenant* $\mathbb{K}$*. Si* $\mathbb{K}$ *est un sous-corps de* $\mathbb{M}$ *et* $S \subset \mathbb{M}$ *alors* $\mathbb{K}(S)$ *est le plus petit sous-corps de* $\mathbb{M}$ *contenant* $\mathbb{K}$ *et* S*. Si* $S = \{x_1, \ldots, x_n\}$ *on note* $\mathbb{K}(x_1, \ldots, x_n)$ *pour* $\mathbb{K}(S)$*.*

$\mathbb{K}(S)$ est une sous-extension de $\mathbb{K} \subset \mathbb{M}$.

Définition 5

Le degré de l'extension $\mathbb{K} \subset \mathbb{L}$ *est la dimension de* $\mathbb{L}$ *en tant que* $\mathbb{K}$*-espace vectoriel et est noté* $[\mathbb{L} : \mathbb{K}]$*. On dit que* $\mathbb{K} \subset \mathbb{L}$ *est une extension finie si* $[\mathbb{L} : \mathbb{K}] < +\infty$*.*

Exemple 6

$\mathbb{K} \subset \mathbb{K}(X)$ *est une extension de degré infini (car* $(X^n, n \in \mathbb{N})$ *est libre).*
$\mathbb{Q} \subset \mathbb{R}$ *est une extension de degré infini (car* $\mathbb{Q}$ *est dénombrable et* $\mathbb{R}$ *n'est pas dénombrable).*
$\mathbb{R} \subset \mathbb{C}$ *est une extension de degré* 2 *(car* $\mathbb{C} = \{a + ib, a, b \in \mathbb{R}\}$ *et* $i \notin \mathbb{R}$*).*
$\mathbb{Z}/2\mathbb{Z} \subset \mathbb{Z}/2\mathbb{Z}[X]/(X^2 + X + 1)$ *est une extension de degré* 2*.*

Définition 7

Le sous-corps premier de $\mathbb{K}$ est le plus petit sous-corps de $\mathbb{K}$.

Proposition 8

i) Si $\text{car}(\mathbb{K}) = 0$ *alors le sous-corps premier de $\mathbb{K}$ est isomorphe à $\mathbb{Q}$.*
ii) Si $\text{car}(\mathbb{K}) = p > 0$ *(un nombre premier) alors le sous-corps premier de $\mathbb{K}$ est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.*

Tout corps est donc une extension de $\mathbb{Q}$ ou de $\mathbb{Z}/p\mathbb{Z}$ pour un p premier.

Corollaire 9

Si $\mathbb{K}$ est un corps fini alors $\mathbb{K}$ est de caractéristique un nombre premier p et le cardinal de $\mathbb{K}$ est p^n pour un certain $n \in \mathbb{N}^*$.

Théorème 10 (*de la base télescopique*)

Si $\mathbb{K} \subset \mathbb{L} \subset \mathbb{M}$ sont des corps tels que $(e_1, \ldots, e_n)$ est une $\mathbb{K}$-base de $\mathbb{L}$ et $(f_1, \ldots, f_m)$ est une $\mathbb{L}$-base de $\mathbb{M}$ alors $(e_i f_j)_{i \in \{1,\ldots,n\}, j \in \{1,\ldots,m\}}$ est une $\mathbb{K}$-base de $\mathbb{M}$.

Corollaire 11 (*multiplicativité des degrés*)

Si $\mathbb{K} \subset \mathbb{L} \subset \mathbb{M}$ alors $[\mathbb{M} : \mathbb{K}] = [\mathbb{M} : \mathbb{L}][\mathbb{L} : \mathbb{K}]$ (avec la convention que pour tout $n \in \mathbb{N}^* \cup \{+\infty\}$ on a $+\infty \times n = n \times +\infty = +\infty$).

1.2 Extensions algébriques

Définition 12

Soient $\mathbb{K} \subset \mathbb{L}$. $x \in \mathbb{L}$ est algébrique sur $\mathbb{K}$ s'il existe $P \in \mathbb{K}[X] \setminus \{0\}$ tel que $P(x) = 0$. Il existe alors un unique $\Pi_{\mathbb{K},x} \in \mathbb{K}[X]$ unitaire tel que l'idéal de $\mathbb{K}[X]$ engendré par $\Pi_{\mathbb{K},x}$ est $\{P \in \mathbb{K}[X], P(x) = 0\}$ (car $\mathbb{K}[X]$ est principal) ; $\Pi_{\mathbb{K},x}$ est le polynôme minimal de x sur $\mathbb{K}$. Si x n'est pas algébrique sur $\mathbb{K}$ alors on dit que x est transcendant sur $\mathbb{K}$.

Remarque 13

$\Pi_{\mathbb{K},x}$ est irréductible sur $\mathbb{K}$.

Définition 14

$\mathbb{K} \subset \mathbb{L}$ est une extension algébrique si tout élément de $\mathbb{L}$ est algébrique sur $\mathbb{K}$.

Théorème 15

Toute extension finie est algébrique.

Théorème 16

Soit $x \in \mathbb{L}$ algébrique sur $\mathbb{K}$. Notons n le degré de $\Pi_{\mathbb{K},x}$.
i) $\mathbb{K}(x)$ est isomorphe au corps $\mathbb{K}[X]/(\Pi_{\mathbb{K},x})$.
ii) $(1, x, \ldots, x^{n-1})$ est une $\mathbb{K}$-base de $\mathbb{K}(x)$.
iii) Soit $y \in \mathbb{K}(x)$. y est algébrique sur $\mathbb{K}$ et le degré de $\Pi_{\mathbb{K},y}$ divise n.

Application 17

Si $x \in \mathbb{L} \setminus \{0\}$ est algébrique sur $\mathbb{K}$ alors $-x$ et x^{-1} sont algébriques sur $\mathbb{K}$.

Proposition 18

Si x est transcendant sur $\mathbb{K}$ alors $\mathbb{K}(x)$ est isomorphe à $\mathbb{K}(X)$. En particulier $[\mathbb{K}(x) : \mathbb{K}] = +\infty$.

Application 19

Si $x, y \in \mathbb{L}$ sont algébriques sur $\mathbb{K}$ alors $x + y$ et xy sont algébriques sur $\mathbb{K}$.

Exemple 20

Si $n \in \mathbb{N}^*$ et p premier alors $\sqrt[n]{p}$ est algébrique sur $\mathbb{Q}$ et $[\mathbb{Q}(\sqrt[n]{p}) : \mathbb{Q}] = n$.
i et j sont algébriques sur $\mathbb{Q}$ et $[\mathbb{Q}(i) : \mathbb{Q}] = 2 = [\mathbb{Q}(j) : \mathbb{Q}]$.
e et π sont transcendants sur $\mathbb{Q}$.

Proposition 21

Si $\mathbb{K} \subset \mathbb{L}$ et $\mathbb{L} \subset \mathbb{M}$ sont algébriques alors $\mathbb{K} \subset \mathbb{M}$ est algébrique.

Proposition 22

$\mathbb{K} \subset \mathbb{L}$ est une extension finie si et seulement s'il existe $n \in \mathbb{N}^*, x_1, \ldots, x_n \in \mathbb{L}$ algébriques sur $\mathbb{K}$ tels que $\mathbb{L} = \mathbb{K}(x_1, \ldots, x_n)$.

Définition 23

$\mathbb{L}$ est une clôture algébrique de $\mathbb{K}$ si $\mathbb{L}$ est une extension algébrique de $\mathbb{K}$ qui est algébriquement close.

Proposition 24

Si $\mathbb{L}$ est une extension de $\mathbb{K}$ algébriquement close alors $\{x \in \mathbb{L}, x$ est algébrique sur $\mathbb{K}\}$ est une clôture algébrique de $\mathbb{K}$.

Exemple 25

$\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$.
$\overline{\mathbb{Q}} = \{x \in \mathbb{C}, x$ est algébrique sur $\mathbb{Q}\}$ est une clôture algébrique de $\mathbb{Q}$.

Remarque 26

$[\overline{\mathbb{Q}} : \mathbb{Q}] = +\infty$ *car, en notant* $\{p_n, n \in \mathbb{N}^*\}$ *les nombres premiers,* $\mathbb{Q}(\{\sqrt{p_n}, n \in \mathbb{N}^*\})$ *est une sous-extension de* $\mathbb{Q} \subset \overline{\mathbb{Q}}$ *de degré infini sur* $\mathbb{Q}$.

2 Corps de rupture, corps de décomposition et applications

2.1 Définitions et premières propriétés

Définition 27

Soit $P \in \mathbb{K}[X]$ *irréductible.* $\mathbb{L}$ *est un corps de rupture de* P *sur* $\mathbb{K}$ *s'il existe* $x \in \mathbb{L}$ *tel que* $\mathbb{L} = \mathbb{K}(x)$ *et* $P(x) = 0$.

Proposition 28

Soit $P \in \mathbb{K}[X]$ *irréductible.*
i) $\mathbb{K}[X]/(P)$ *est un corps de rupture de* P *sur* $\mathbb{K}$.
ii) Deux corps de rupture de P *sur* $\mathbb{K}$ *sont isomorphes en tant que* $\mathbb{K}$*-algèbres.*

Exemple 29

$\mathbb{C}$ *est un corps de rupture de* $X^2 + 1$ *sur* $\mathbb{R}$.
$\mathbb{Q}(\sqrt[3]{2})$ *est un corps de rupture de* $X^3 - 2$ *sur* $\mathbb{Q}$.

Définition 30

Soit $P \in \mathbb{K}[X]$ *de degré* $n \geq 1$. $\mathbb{L}$ *est un corps de décomposition de* P *sur* $\mathbb{K}$ *s'il existe* $x_1, \ldots, x_n \in \mathbb{L}, c \in \mathbb{K}$ *tels que* $\mathbb{L} = \mathbb{K}(x_1, \ldots, x_n)$ *et dans* $\mathbb{L}[X]$ $P = c\prod_{i=1}^{n}(X - x_i)$.

Proposition 31

Soit $P \in \mathbb{K}[X]$ *de degré* $n \geq 1$.
i) P *admet un corps de décomposition sur* $\mathbb{K}$.
ii) Deux corps de décomposition de P *sur* $\mathbb{K}$ *sont isomorphes en tant que* $\mathbb{K}$*-algèbres.*

Exemple 32

$\mathbb{C}$ *est un corps de décomposition de* $X^2 + 1$ *sur* $\mathbb{R}$.
$\mathbb{Q}(\sqrt[3]{2}, j)$ *est un corps de décomposition de* $X^3 - 2$ *sur* $\mathbb{Q}$.

2.2 Applications aux corps finis

Lemme 33

Soit p un nombre premier. Soit $n \in \mathbb{N}^*$. Dans $\mathbb{Z}/p\mathbb{Z}[X]$ $X^{p^n} - X$ est le produit des polynômes irréductibles unitaires de $\mathbb{Z}/p\mathbb{Z}[X]$ de degré divisant n.

Le lemme et les deux théorèmes suivants font l'objet de mon premier développement.

Lemme 34

Soit p un nombre premier. Pour tout $n \in \mathbb{N}^*$ il existe un polynôme irréductible unitaire de degré n dans $\mathbb{Z}/p\mathbb{Z}[X]$.

Preuve :

Pour tout $d \in \mathbb{N}^*$ notons $\mathcal{P}_d$ l'ensemble des polynômes irréductibles unitaires de degré d dans $\mathbb{Z}/p\mathbb{Z}[X]$. D'après le Lemme 33 on a pour tout $n \in \mathbb{N}^*$:

$$X^{p^n} - X = \prod_{d|n} \prod_{P \in \mathcal{P}_d} P.$$

En regardant les degrés on a donc pour tout $n \in \mathbb{N}^*$: $p^n = \sum_{d|n} d\,|\mathcal{P}_d|$.
Avec la formule d'inversion de Möbius on a donc pour tout $n \in \mathbb{N}^*$:

$$n\,|\mathcal{P}_n| = \sum_{d|n} p^{\frac{n}{d}} \mu(d) \text{ où } \mu(d) = \begin{cases} 0 & \text{si } d \text{ a un facteur carré} \\ (-1)^k & \text{si } d \text{ est le produit de } k \\ & \text{nombres premiers distincts} \end{cases}.$$

Soit $n \in \mathbb{N}^*$. Notons q le produit des facteurs premiers de n.

Soit d un diviseur de n tel que $\mu(d) \neq 0$. On a alors $d|q$ donc il existe $k \in \mathbb{N}^*$ tel que $q = kd$. Ainsi $\frac{n}{d} = k\frac{n}{kd} = k\frac{n}{q}$ donc $p^{\frac{n}{d}} = (p^{\frac{n}{q}})^k = p^{\frac{n}{q}}(p^{\frac{n}{q}})^{k-1}$.
Si de plus $d \neq q$ alors $k \geq 2$ donc $p^{\frac{n}{d}} = p^{2\frac{n}{q}}(p^{\frac{n}{q}})^{k-2}$.
Ainsi $n\,|\mathcal{P}_n| \equiv p^{\frac{n}{q}}\mu(q)$ ($\mod p^{2\frac{n}{q}}$) or $\mu(q) \in \{-1, 1\}$ et $0 < p^{\frac{n}{q}} < p^{2\frac{n}{q}}$ donc $n\,|\mathcal{P}_n| \not\equiv 0$ ($\mod p^{2\frac{n}{q}}$) donc $n|\mathcal{P}_n| \neq 0$ donc $|\mathcal{P}_n| \neq 0$.

Il existe donc un polynôme irréductible unitaire de degré n dans $\mathbb{Z}/p\mathbb{Z}[X]$.
□

Théorème 35

Soit p un nombre premier. Soit $n \in \mathbb{N}^*$. Il existe un corps de cardinal p^n, unique à isomorphisme de $\mathbb{Z}/p\mathbb{Z}$-algèbres près. C'est un corps de décomposition de $X^{p^n} - X$ sur $\mathbb{Z}/p\mathbb{Z}$. On note un tel corps $\mathbb{F}_{p^n}$.

Preuve :

D'après le Lemme 34 il existe un polynôme irréductible unitaire P de degré n dans $\mathbb{Z}/p\mathbb{Z}[X]$. $\mathbb{Z}/p\mathbb{Z}[X]/(P)$ est un corps de degré n sur $\mathbb{Z}/p\mathbb{Z}$ donc de cardinal p^n.

Soit $\mathbb{K}$ un corps de cardinal p^n. $|\mathbb{K}^*| = p^n - 1$ donc pour tout $x \in \mathbb{K}^* x^{p^n-1} = 1$ donc $x^{p^n} = x$ or $0^{p^n} = 0$ donc tout élément de $\mathbb{K}$ est racine de $X^{p^n} - X$. Or $X^{p^n} - X$ est de degré p^n et $\mathbb{K}$ est un corps donc $X^{p^n} - X$ est scindé sur $\mathbb{K}$ (car $|\mathbb{K}| = p^n$). De plus $\mathbb{K} = \mathbb{Z}/p\mathbb{Z}(\mathbb{K})$ (et $\mathbb{K}$ n'est constitué que de racines de $X^{p^n} - X$) donc $\mathbb{K}$ est un corps de décomposition de $X^{p^n} - X$ sur $\mathbb{Z}/p\mathbb{Z}$, d'où l'unicité à isomorphisme de $\mathbb{Z}/p\mathbb{Z}$-algèbres près. □

Théorème 36

Soient p un nombre premier, $n \in \mathbb{N}^*$, m un diviseur de n. $\mathbb{F}_{p^n}$ a un unique sous-corps de cardinal p^m. Réciproquement tout sous-corps de $\mathbb{F}_{p^n}$ a un cardinal de la forme p^d avec d un diviseur de n.

Preuve :

$\mathbb{F}_{p^n}$ est un corps de décomposition de $X^{p^n} - X$ sur $\mathbb{Z}/p\mathbb{Z}$ et $X^{p^m} - X$ divise $X^{p^n} - X$ (car m divise n) donc $X^{p^m} - X$ est scindé sur $\mathbb{F}_{p^n}$. D'après le théorème précédent, l'ensemble des racines de $X^{p^m} - X$ dans $\mathbb{F}_{p^n}$ est l'unique sous-corps de cardinal p^m de $\mathbb{F}_{p^n}$.

Soit $\mathbb{K}$ un sous-corps de $\mathbb{F}_{p^n}$. $\mathbb{K}$ est un corps fini de caractéristique p (car $\mathbb{F}_{p^n}$ l'est) donc $|\mathbb{K}| = p^d$ pour un certain $d \in \mathbb{N}^*$. De plus $(\mathbb{K}^*, \times)$ est un sous-groupe de $((\mathbb{F}_{p^n})^*, \times)$ donc $|\mathbb{K}^*|$ divise $|(\mathbb{F}_{p^n})^*|$ donc $p^d - 1$ divise $p^n - 1$ donc d divise n. □

Remarque 37

Si $P \in \mathbb{Z}/p\mathbb{Z}[X]$ est un polynôme irréductible alors tout corps de rupture de P sur $\mathbb{Z}/p\mathbb{Z}$ est un corps de décomposition de P sur $\mathbb{Z}/p\mathbb{Z}$.

Exemple 38

$\mathbb{F}_4 = \mathbb{Z}/2\mathbb{Z}[X]/(X^2 + X + 1)$, $\mathbb{F}_8 = \mathbb{Z}/2\mathbb{Z}[X]/(X^3 + X + 1)$,
$\mathbb{F}_{16} = \mathbb{Z}/2\mathbb{Z}[X]/(X^4 + X + 1)$, $\mathbb{F}_9 = \mathbb{Z}/3\mathbb{Z}[X]/(X^2 - X - 1)$.

Exemple 39

$\mathbb{F}_5$ *et* $\mathbb{F}_{125}$ *sont les sous-corps de* $\mathbb{F}_{125}$.
$\mathbb{F}_5$, $\mathbb{F}_{25}$ *et* $\mathbb{F}_{625}$ *sont les sous-corps de* $\mathbb{F}_{625}$.

Théorème 40

Soit p un nombre premier. Soit $n \in \mathbb{N}^*$. $\bigcup_{k\in\mathbb{N}^*} \mathbb{F}_{p^{k!}}$ *est une clôture algébrique de* $\mathbb{Z}/p\mathbb{Z}$.

2.3 Applications à l'irréductibilité

Proposition 41

Soit $P \in \mathbb{K}[X]$ de degré $n \geq 1$. P est irréductible si et seulement si pour toute extension $\mathbb{L}$ de $\mathbb{K}$ vérifiant $2[\mathbb{L} : \mathbb{K}] \leq n$, P n'a aucune racine dans $\mathbb{L}$.

Application 42

$X^4+X+1 \in \mathbb{Z}/2\mathbb{Z}[X]$ *est irréductible car il n'a pas de racine dans* $\mathbb{Z}/2\mathbb{Z}$ *ni dans* $\mathbb{Z}/2\mathbb{Z}[X]/(X^2+X+1)$.

Proposition 43

Soit $P \in \mathbb{K}[X]$ irréductible de degré n. Si $\mathbb{L}$ est une extension de $\mathbb{K}$ de degré m premier avec n alors P est irréductible dans $\mathbb{L}[X]$.

Contre-exemple 44

$X^4+1 \in \mathbb{Q}[X]$ *est irréductible et* $X^4+1 = (X^2-i)(X^2+i)$ *dans* $\mathbb{Q}(i)[X]$.

Application 45

$X^4+1 \in \mathbb{Q}[X]$ *est irréductible et* $3 \wedge 4 = 1$ *donc* X^4+1 *est irréductible dans* $\mathbb{Q}(\sqrt[3]{2})[X]$.

2.4 Applications aux clôtures algébriques

Théorème 46

Tout corps admet une extension algébriquement close.

Preuve :

Soit $\mathbb{K}$ un corps. Notons $A := \mathbb{K}[\{X_f, f \in \mathbb{K}[X] \setminus \mathbb{K}\}]$ (c'est-à-dire que $A = \mathbb{K}^{(\mathbb{N}^{(\mathbb{K}[X]\setminus\mathbb{K})})}$ (l'ensemble des fonctions à support fini de $\mathbb{N}^{(\mathbb{K}[X]\setminus\mathbb{K})}$ dans $\mathbb{K}$, où $\mathbb{N}^{(\mathbb{K}[X]\setminus\mathbb{K})}$ est l'ensemble des fonctions à support fini de $\mathbb{K}[X] \setminus \mathbb{K}$ dans $\mathbb{N}$) muni de l'addition usuelle, du produit par un scalaire usuel et du

produit qui est l'unique application bilinéaire valant $X_{f_1}^{m_1+n_1} \dots X_{f_k}^{m_k+n_k}$ en $(X_{f_1}^{m_1} \dots X_{f_k}^{m_k}, X_{f_1}^{n_1} \dots X_{f_k}^{n_k})$, qui en font une algèbre unitaire commutative).

Notons I l'idéal de A engendré par $\{f(X_f), f \in \mathbb{K}[X] \setminus \mathbb{K}\}$ (ACACAC). Montrons que $I \neq A$.
Supposons $1 \in I$. Il existe $n \in \mathbb{N}^*, f_1, \dots, f_n \in \mathbb{K}[X] \setminus \mathbb{K}, g_1, \dots, g_n \in A$ tels que $\sum_{i=1}^{n} g_i f_i(X_{f_i}) = 1$.
Pour tout $i \in \{1, \dots, n\}$ soit α_i une racine de $f_i(X_{f_i})$ dans un corps de décomposition de $f_i(X_{f_i})$ sur $\mathbb{K}(\alpha_1, \dots, \alpha_{i-1})$ ($\mathbb{K}$ si $i = 1$ par convention).
Notons $\mathbb{L} = \mathbb{K}(\alpha_1, \dots, \alpha_n)$. Notons $B = \mathbb{L}[\{X_f, f \in \mathbb{K}[X] \setminus \mathbb{K}\}]$.
$\sum_{i=1}^{n} g_i f_i(\alpha_i) = 0$ ce qui contredit $\sum_{i=1}^{n} g_i f_i(X_{f_i}) = 1$ dans B.
Ainsi $1 \notin I$ donc $I \neq A$.
I est donc contenu dans un idéal maximal M de A.
Posons $E_1 = A/M$. E_1 est un corps (car M est maximal) et est une extension de $\mathbb{K}$ (car en composant le morphisme canonique de $\mathbb{K}$ dans A et le morphisme canonique π de A dans E_1 on a un morphisme de $\mathbb{K}$ dans E_1).

Soit $f \in \mathbb{K}[X] \setminus \mathbb{K}$. $\pi(X_f) \in E_1$ est racine de f (car $\pi(f(X_f)) = 0$ car $f(X_f) \in I \subset M$).

On construit de même, pour tout $k \in \mathbb{N}^*$, une extension E_{k+1} de E_k telle que tout polynôme de $E_k[X] \setminus E_k$ a une racine dans E_{k+1}.

Posons $E_0 = \mathbb{K}$ et $E = \bigcup_{k \in \mathbb{N}} E_k$.

Définissons $+ : E \times E \to E$ et $\times : E \times E \to E$ par $y + x = x + y = \psi(x) + y$ et $y \times x = x \times y = \psi(x) \times y$ si $x \in E_k$ (avec $k \in \mathbb{N}$), $y \in E_{k+r}$ (avec $r \in \mathbb{N}$) et $\psi : E_k \to E_{k+r}$ est la composée des morphismes construits plus hauts (et le troisième $+$ (respectivement $\times$) est la loi additive (respectivement multiplicative) de E_{k+r}). On peut vérifier que $(E, +, \times)$ est un surcorps de $(\mathbb{K}, +, \times)$.

Soit $P \in E[X] \setminus E$. P a un nombre fini de coefficients donc il existe $k \in \mathbb{N}$ tel que P peut être vu comme un polynôme de $E_k[X] \setminus E_k$ (en passant par les morphismes définis plus haut). P a donc une racine dans $E_{k+1} \subset E$.

E est donc algébriquement clos. □

Corollaire 47

Tout corps admet une clôture algébrique.

Preuve :

Soit $\mathbb{K}$ un corps. D'après le Théorème 46, il existe une extension $\mathbb{L}$ de $\mathbb{K}$ qui est algébriquement close. D'après la Proposition 24, l'ensemble $\{x \in \mathbb{L},\ x \text{ est algébrique sur } \mathbb{K}\}$ est une clôture algébrique de $\mathbb{K}$. □

Théorème 48

Deux clôtures algébriques de $\mathbb{K}$ sont isomorphes en tant que $\mathbb{K}$-algèbres.

3 Extensions normales, séparables, galoisiennes

3.1 Définitions et premières propriétés

Définition 49

L'extension $\mathbb{K} \subset \mathbb{L}$ est normale si elle est algébrique et si tout polynôme irréductible de $\mathbb{K}[X]$ qui admet une racine dans $\mathbb{L}$ est scindé dans $\mathbb{L}[X]$.
$x \in \mathbb{L}$ est séparable sur $\mathbb{K}$ s'il est algébrique sur $\mathbb{K}$ et si son polynôme minimal sur $\mathbb{K}$ est à racines simples dans un de ses corps de décomposition sur $\mathbb{K}$. L'extension $\mathbb{K} \subset \mathbb{L}$ est séparable si tout élément de $\mathbb{L}$ est séparable sur $\mathbb{K}$.
Un corps est parfait si toutes ses extensions algébriques sont séparables.
Une extension est galoisienne si elle est normale et séparable.

Exemple 50

Toute extension algébrique de $\mathbb{Z}/p\mathbb{Z}$ est normale (cf. Rq 37).
Les clôtures algébriques sont normales.
Les corps de caractéristique nulle sont parfaits.
$\mathbb{Q} \subset \overline{\mathbb{Q}}$ et $\mathbb{R} \subset \mathbb{C}$ sont galoisiennes.

Contre-exemple 51

$\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$ n'est pas normale (considérer $X^3 - 2$).

Théorème 52

Soit $\mathbb{K} \subset \mathbb{L}$ une extension finie. $\mathbb{K} \subset \mathbb{L}$ est normale si et seulement si $\mathbb{L}$ est un corps de décomposition d'un polynôme de $\mathbb{K}[X]$ sur $\mathbb{K}$.

Théorème 53 (*de l'élément primitif*)

Soit $\mathbb{K} \subset \mathbb{L}$ une extension finie séparable. Il existe $x \in \mathbb{L}$ tel que $\mathbb{L} = \mathbb{K}(x)$.

Preuve :

Si $\mathbb{K}$ est fini alors $\mathbb{L}$ aussi (car l'extension est finie) donc $\mathbb{L}^*$ est cyclique. Soit x un générateur de $\mathbb{L}^*$. Tout élément non nul de $\mathbb{L}$ est une puissance de x donc $\mathbb{L} = \mathbb{K}(x)$.

Supposons $\mathbb{K}$ infini. En raisonnant par récurrence (et en utilisant la Proposition 22), il suffit de montrer que si $\mathbb{L} = \mathbb{K}(x, y)$ est séparable sur $\mathbb{K}$ alors il existe $z \in \mathbb{L}$ tel que $\mathbb{L} = \mathbb{K}(z)$.

Notons $x_1, \ldots, x_n$ (respectivement $y_1, \ldots, y_m$) les racines (disctinctes par séparabilité) de $\Pi_{\mathbb{K},x}$ (respectivement $\Pi_{\mathbb{K},y}$) dans une clôture algébrique de $\mathbb{L}$, avec $x_1 = x$ et $y_1 = y$.

L'ensemble $A = \{-\frac{x_i - x}{y_j - y}, i \in \{1, \ldots, n\}, j \in \{2, \ldots, m\}\}$ est fini et $\mathbb{K}^*$ est infini donc il existe $c \in \mathbb{K}^* \cap A^c$. Pour tous $i \in \{1, \ldots, n\}, j \in \{2, \ldots, m\}$ $x_i + cy_j \neq x + cy$ donc $x + cy - cy_j \notin \{x_1, \ldots, x_n\}$.

Posons $z = x + cy$. Montrons que $\mathbb{L} = \mathbb{K}(z)$.

Notons P le polynôme $\Pi_{\mathbb{K},x}(z - cX)$. Les polynômes P et $\Pi_{\mathbb{K},y}$ sont à coefficients dans $\mathbb{K}(z)$ donc leur pgcd est à coefficients dans $\mathbb{K}(z)$.

Or leur pgcd est $X - y$ (car y est racine de P et de $\Pi_{\mathbb{K},y}$ et aucune des autres racines de $\Pi_{\mathbb{K},y}$ n'est racine de P car pour tout $j \in \{2, \ldots, m\}$ on a $P(y_j) = \Pi_{\mathbb{K},x}(z - cy_j) = \Pi_{\mathbb{K},x}(x + cy - cy_j) \neq 0$ car $x + cy - cy_j \notin \{x_1, \ldots, x_n\}$) donc $X - y \in \mathbb{K}(z)[X]$.

Ainsi $y \in \mathbb{K}(z)$ puis $x = cy - z \in \mathbb{K}(z)$ d'où $\mathbb{K}(x, y) \subset \mathbb{K}(z)$ or $\mathbb{L} = \mathbb{K}(x, y)$ donc $\mathbb{L} = \mathbb{K}(z)$. □

Exemple 54

$\mathbb{Q}(\sqrt[3]{2}, j) = \mathbb{Q}(\sqrt[3]{2} + j)$, $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

Notation 55

Soient $\mathbb{L}$ et $\mathbb{M}$ des surcorps de $\mathbb{K}$. $\mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \mathbb{M})$ *est l'ensemble des morphismes de $\mathbb{K}$-algèbres de $\mathbb{L}$ dans $\mathbb{M}$.*

Théorème 56

Soient $\mathbb{K} \subset \mathbb{L}$ une extension finie et Ω une clôture algébrique de $\mathbb{K}$. Le cardinal de $\mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \Omega)$ *est compris entre* 1 *et* $[\mathbb{L} : \mathbb{K}]$ *et il y a équivalence entre :*
i) $\mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \Omega)$ *est de cardinal* $[\mathbb{L} : \mathbb{K}]$ *;*

ii) il existe $n \in \mathbb{N}^*, x_1, \dots, x_n \in \mathbb{L}$ *séparables sur* $\mathbb{K}$ *tels que* $\mathbb{L} = \mathbb{K}(x_1, \dots, x_n)$ *;*
iii) $\mathbb{K} \subset \mathbb{L}$ *est séparable.*

Théorème 57

Soient p *un nombre premier et* $\mathbb{K}$ *un corps de caractéristique* p*.* $\mathbb{K}$ *est parfait si et seulement si le morphisme de Frobenius* $\begin{cases} \mathbb{K} & \to & \mathbb{K} \\ x & \mapsto & x^p \end{cases}$ *est surjectif.*

Application 58

Les corps finis sont parfaits. $\mathbb{Z}/p\mathbb{Z}(X)$ *n'est pas parfait.*

3.2 Théorie de Galois

Définition 59

Soit $\mathbb{K} \subset \mathbb{L}$ *une extension finie. Le groupe de Galois de* $\mathbb{K} \subset \mathbb{L}$ *est le groupe des automorphismes de* $\mathbb{K}$*-algèbre de* $\mathbb{L}$ *et est noté* $\mathrm{Gal}(\mathbb{K}, \mathbb{L})$*.*

Proposition 60

Soient $\mathbb{K} \subset \mathbb{L}$ *une extension finie,* $\sigma \in \mathrm{Gal}(\mathbb{K}, \mathbb{L}), n \in \mathbb{N}^*, P \in \mathbb{K}[X_1, \dots, X_n]$*. Pour tous* $x_1, \dots, x_n \in \mathbb{L}$ $\sigma(P(x_1, \dots, x_n)) = P(\sigma(x_1), \dots, \sigma(x_n))$*.*

Application 61

$\mathrm{Gal}(\mathbb{R}, \mathbb{C})$ *a deux éléments : l'identité et la conjugaison.*
$\mathrm{Gal}(\mathbb{Q}, \mathbb{Q}(\sqrt[3]{2}))$ *n'a qu'un élément : l'identité.*

Proposition 62

Soit $\mathbb{K} \subset \mathbb{L}$ *une extension finie.* $|\mathrm{Gal}(\mathbb{K}, \mathbb{L})| \leq [\mathbb{L} : \mathbb{K}]$*.*

Théorème 63

Soient $\mathbb{K} \subset \mathbb{L}$ *une extension finie et* Ω *une clôture algébrique de* $\mathbb{L}$*. Il y a équivalence entre :*
i) $\mathbb{K} \subset \mathbb{L}$ *est galoisienne ;*
ii) $\mathrm{Gal}(\mathbb{K}, \mathbb{L})$ *est d'ordre* $[\mathbb{L} : \mathbb{K}]$ *;*
iii) $\mathbb{K} \subset \mathbb{L}$ *est séparable et* $\mathrm{Gal}(\mathbb{K}, \mathbb{L}) = \mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \Omega)$*.*

Application 64

$\mathrm{Gal}(\mathbb{Q}, \mathbb{Q}(\sqrt[3]{2}, j))$ *est isomorphe à* $\mathcal{S}_3$*.*

Notation 65

Soient $\mathbb{L}$ un corps et G un sous-groupe fini du groupe des automorphismes de $\mathbb{L}$. $\mathbb{L}^G = \{x \in \mathbb{L}, \forall \sigma \in G\ \sigma(x) = x\}$.

Proposition 66

Soient $\mathbb{L}$ un corps et G un sous-groupe fini du groupe des automorphismes de $\mathbb{L}$. $\mathbb{L}^G$ *est un sous-corps de* $\mathbb{L}$.

Le théorème et le corollaire suivants font l'objet de mon second développement.

Théorème 67 (*d'Artin*)

Soient $\mathbb{L}$ un corps et G un sous-groupe fini du groupe des automorphismes de $\mathbb{L}$. $[\mathbb{L} : \mathbb{L}^G]$ *est égal à l'ordre de G.*

Preuve :

Montrons tout d'abord que $\mathbb{L}^G \subset \mathbb{L}$ est séparable.

Soit $x \in \mathbb{L}$. Notons $O_x = \{\sigma(x), \sigma \in G\}$.

Posons $P = \prod_{y \in O_x} (X - y) \in \mathbb{L}[X]$. Montrons que $P \in \mathbb{L}^G[X]$.

Notons $O_x = \{y_1, \ldots, y_m\}$ (avec les y_i distincts) et pour tout $k \in \{1, \ldots, m\}$ $s_k = \sum_{1 \leq i_1 < \cdots < i_k \leq m} \prod_{j=1}^{k} y_{i_j}$ le k-ième polynôme symétrique élémentaire en les racines de P. Remarquons que tout $\sigma \in G$ induit une bijection de O_x sur lui-même, d'où pour tout $k \in \{1, \ldots, m\}$ $s_k \in \mathbb{L}^G$.

En notant $P = X^m + \sum_{i=0}^{m-1} a_i X^i$ on a donc pour tout $i \in \{0, \ldots, m-1\}$ $a_i = (-1)^{n-i} s_{n-i} \in \mathbb{L}^G$ (relations coefficients-racines).

Ainsi $P \in \mathbb{L}^G[X]$, or P est à racines simples et annule x, donc $\Pi_{\mathbb{L}^G,x}$ est à racines simples donc x est séparable sur $\mathbb{L}^G$. De plus, $\deg \Pi_{\mathbb{L}^G,x} \leq \deg P \leq |G|$.

$\mathbb{L}^G \subset \mathbb{L}$ est donc séparable.

Supposons que $\mathbb{L}^G \subset \mathbb{L}$ n'est pas finie. Il existe alors des sous-extensions finies $\mathbb{L}_i, i \in \mathbb{N}^*$ telles que pour tout $i \in \mathbb{N}^*$ $\mathbb{L}_i \subset \mathbb{L}_{i+1}$ et $[\mathbb{L}_i : \mathbb{L}^G] \underset{i \to +\infty}{\longrightarrow} +\infty$. Pour tout $i \in \mathbb{N}^*$ $\mathbb{L}^G \subset \mathbb{L}_i$ est séparable (car $\mathbb{L}^G \subset \mathbb{L}$ l'est) et finie donc, d'après le théorème de l'élément primitif, il existe $x_i \in \mathbb{L}_i$ tel que $\mathbb{L}_i =$

$\mathbb{L}^G(x_i)$. D'après ce qui a été montré plus haut, $\deg\Pi_{\mathbb{L}^G,x_i} \leq |G|$ or $[\mathbb{L}_i : \mathbb{L}^G] = \deg\Pi_{\mathbb{L}^G,x_i}$ donc $[\mathbb{L}_i : \mathbb{L}^G] \leq |G|$.

Ceci contredit $[\mathbb{L}_i : \mathbb{L}^G] \underset{i\to+\infty}{\longrightarrow} +\infty$. $\mathbb{L}^G \subset \mathbb{L}$ est donc finie.

Ainsi, $\mathbb{L}^G \subset \mathbb{L}$ est séparable et finie donc, d'après le théorème de l'élément primitif, il existe $x \in \mathbb{L}$ tel que $\mathbb{L} = \mathbb{L}^G(x)$. D'après ce qui a été montré plus haut, $\deg\Pi_{\mathbb{L}^G,x} \leq |G|$ or $[\mathbb{L} : \mathbb{L}^G] = \deg\Pi_{\mathbb{L}^G,x}$ donc $[\mathbb{L} : \mathbb{L}^G] \leq |G|$.

Or $G \subset \mathrm{Gal}(\mathbb{L}^G, \mathbb{L})$ (par définition de $\mathbb{L}^G$) et d'après la Proposition 62 $|\mathrm{Gal}(\mathbb{L}^G, \mathbb{L})| \leq [\mathbb{L} : \mathbb{L}^G]$ donc $G = \mathrm{Gal}(\mathbb{L}^G, \mathbb{L})$ et $|G| = [\mathbb{L} : \mathbb{L}^G]$. □

Corollaire 68

Soient $\mathbb{L}$ un corps et G un sous-groupe fini du groupe des automorphismes de $\mathbb{L}$. $\mathbb{L}^G \subset \mathbb{L}$ est une extension finie galoisienne de groupe de Galois G.

Preuve :

On a déjà montré que $\mathbb{L}^G \subset \mathbb{L}$ est une extension finie de groupe de Galois G et que $|G| = [\mathbb{L} : \mathbb{L}^G]$ donc on peut conclure avec le Théorème 63. □

Notation 69

Soit $\mathbb{K} \subset \mathbb{L}$ une extension finie. $\mathcal{K}(\mathbb{K}, \mathbb{L})$ est l'ensemble des sous-extensions de $\mathbb{K} \subset \mathbb{L}$ et $\mathcal{G}(\mathbb{K}, \mathbb{L})$ est l'ensemble des sous-groupes de $\mathrm{Gal}(\mathbb{K}, \mathbb{L})$.

Proposition 70

Soit $\mathbb{K} \subset \mathbb{L}$ une extension finie. $\begin{cases} \mathcal{K}(\mathbb{K},\mathbb{L}) & \to & \mathcal{G}(\mathbb{K},\mathbb{L}) \\ \mathbb{M} & \mapsto & \mathrm{Gal}(\mathbb{M},\mathbb{L}) \end{cases}$ *et* $\begin{cases} \mathcal{G}(\mathbb{K},\mathbb{L}) & \to & \mathcal{K}(\mathbb{K},\mathbb{L}) \\ H & \mapsto & \mathbb{L}^H \end{cases}$ *sont bien définies et renversent les inclusions.*

Théorème 71 (*correspondance de Galois*)

Soit $\mathbb{K} \subset \mathbb{L}$ une extension finie galoisienne. $\begin{cases} \mathcal{K}(\mathbb{K},\mathbb{L}) & \to & \mathcal{G}(\mathbb{K},\mathbb{L}) \\ \mathbb{M} & \mapsto & \mathrm{Gal}(\mathbb{M},\mathbb{L}) \end{cases}$ *et* $\begin{cases} \mathcal{G}(\mathbb{K},\mathbb{L}) & \to & \mathcal{K}(\mathbb{K},\mathbb{L}) \\ H & \mapsto & \mathbb{L}^H \end{cases}$ *sont des bijections réciproques l'une de l'autre. De plus, pour tout $\mathbb{M} \in \mathcal{K}(\mathbb{K}, \mathbb{L})$, $\mathrm{Gal}(\mathbb{M}, \mathbb{L})$ est distingué dans $\mathrm{Gal}(\mathbb{K}, \mathbb{L})$ si et seulement si $\mathbb{K} \subset \mathbb{M}$ est galoisienne, et on a alors :*

$$\mathrm{Gal}(\mathbb{K}, \mathbb{M}) \simeq \mathrm{Gal}(\mathbb{K}, \mathbb{L})/\mathrm{Gal}(\mathbb{M}, \mathbb{L}).$$

Application 72

Le groupe de Galois de l'extension finie galoisienne $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}, j)$ est

isomorphe à $\mathcal{S}_3$ donc $\mathbb{Q}, \mathbb{Q}(j), \mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(j\sqrt[3]{2}), \mathbb{Q}(j^2\sqrt[3]{2}), \mathbb{Q}(\sqrt[3]{2}, j)$ sont les seules sous-extensions de $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{(2)}, j)$ et on retrouve que $\mathbb{Q} \subset \mathbb{Q}(j)$ est galoisienne alors que $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}), \mathbb{Q} \subset \mathbb{Q}(j\sqrt[3]{2}), \mathbb{Q} \subset \mathbb{Q}(j^2\sqrt[3]{2})$ ne le sont pas.

4 Questions posées et réponses

Question 1

Montrer que si $\mathbb{K} \subset \mathbb{L}$ est une extension finie séparable alors $|\operatorname{Gal}(\mathbb{K}, \mathbb{L})| \leq [\mathbb{L} : \mathbb{K}]$.

Réponse :

Le théorème de l'élément primitif stipule qu'il existe $x \in \mathbb{L}$ tel que $\mathbb{L} = \mathbb{K}(x)$. On a ainsi $[\mathbb{L} : \mathbb{K}] = \deg \Pi_{\mathbb{K},x}$ or la Proposition 60 nous donne que pour tout $\sigma \in \operatorname{Gal}(\mathbb{K}, \mathbb{L})$ $\sigma(x)$ est une racine de $\Pi_{\mathbb{K},x}$, et si $\sigma \neq \tau \in \operatorname{Gal}(\mathbb{K}, \mathbb{L})$ alors $\sigma(x) \neq \tau(x)$ (car $\mathbb{L} = \mathbb{K}(x)$), d'où $|\operatorname{Gal}(\mathbb{K}, \mathbb{L})| \leq [\mathbb{L} : \mathbb{K}]$.

Remarque : pour démontrer la Proposition 62 (qui n'a pas d'hypothèse de séparabilité) on utilise le théorème 56 (plus précisément, le fait que si Ω est une clôture algébrique de $\mathbb{L}$ (et donc de $\mathbb{K}$ car $\mathbb{K} \subset \mathbb{L}$ est finie) alors $|\operatorname{Hom}_{\mathbb{K}}(\mathbb{L}, \Omega)| \leq [\mathbb{L} : \mathbb{K}]$).

Question 2

Que donne le théorème d'Artin si on l'applique à $\mathbb{L} = \mathbb{Q}(\sqrt[3]{2})$ et $G = \operatorname{Gal}(\mathbb{Q}, \mathbb{Q}(\sqrt[3]{2}))$?

Réponse :

$\operatorname{Gal}(\mathbb{Q}, \mathbb{Q}(\sqrt[3]{2})) = \{Id\}$ (car si $\sigma \in \operatorname{Gal}(\mathbb{Q}, \mathbb{Q}(\sqrt[3]{2}))$ alors $\sigma(\sqrt[3]{2}) \in \{\sqrt[3]{2}, j\sqrt[3]{2}, j^2\sqrt[3]{2}\} \cap \mathbb{Q}(\sqrt[3]{2}) = \{\sqrt[3]{2}\}$ (cf. Proposition 60 appliquée à $X^3 - 2$) et σ est déterminée par $\sigma(\sqrt[3]{2})$) donc ici $\mathbb{L}^G = \mathbb{L}$ et le théorème d'Artin et son corollaire nous donnent les faits évidents que $[\mathbb{L} : \mathbb{L}] = 1$ et $\mathbb{L} \subset \mathbb{L}$ est galoisienne.

Question 3

Que donne le théorème d'Artin si on l'applique à $\mathbb{L} = \mathbb{Z}/p\mathbb{Z}(t^{\frac{1}{p}})$ et $G = \operatorname{Gal}(\mathbb{Z}/p\mathbb{Z}(t), \mathbb{Z}/p\mathbb{Z}(t^{\frac{1}{p}}))$ (où t est transcendant sur $\mathbb{Z}/p\mathbb{Z}$) ?

Réponse :

$\operatorname{Gal}(\mathbb{Z}/p\mathbb{Z}(t), \mathbb{Z}/p\mathbb{Z}(t^{\frac{1}{p}})) = \{Id\}$ (car si $\sigma \in \operatorname{Gal}(\mathbb{Z}/p\mathbb{Z}(t), \mathbb{Z}/p\mathbb{Z}(t^{\frac{1}{p}}))$ alors $\sigma(t^{\frac{1}{p}}) \in \{t^{\frac{1}{p}}\}$ (cf. Proposition 60 appliquée à $X^p - t = (X - t^{\frac{1}{p}})^p$ en carac-

téristique p) et σ est déterminée par $\sigma(t^{\frac{1}{p}})$) donc ici $\mathbb{L}^G = \mathbb{L}$ et le théorème d'Artin et son corollaire nous donnent les faits évidents que $[\mathbb{L} : \mathbb{L}] = 1$ et $\mathbb{L} \subset \mathbb{L}$ est galoisienne.

Question 4

Donner une extension finie non séparable. Indice : $\mathbb{Z}/p\mathbb{Z}(X,Y) \subset \mathbb{Z}/p\mathbb{Z}(X^{\frac{1}{p}}, Y^{\frac{1}{p}})$.

Réponse :

Montrons tout d'abord que l'extension $\mathbb{Z}/p\mathbb{Z}(X,Y) \subset \mathbb{Z}/p\mathbb{Z}(X^{\frac{1}{p}}, Y^{\frac{1}{p}})$ est de degré p^2. Par multiplicativité des degrés, il suffit de montrer que $\mathbb{Z}/p\mathbb{Z}(X,Y) \subset \mathbb{Z}/p\mathbb{Z}(X^{\frac{1}{p}}, Y)$ et $\mathbb{Z}/p\mathbb{Z}(X^{\frac{1}{p}}, Y) \subset \mathbb{Z}/p\mathbb{Z}(X^{\frac{1}{p}}, Y^{\frac{1}{p}})$ sont de degré p. C'est bien le cas car les polynômes minimaux associés à ces extensions sont respectivement $T^p - X$ (annule $X^{\frac{1}{p}}$ et est irréductible par le critère d'Eisenstein (avec l'élément premier X)) et $T^p - Y$ (annule $Y^{\frac{1}{p}}$ et est irréductible par le critère d'Eisenstein (avec l'élément premier Y)).

Supposons $\mathbb{Z}/p\mathbb{Z}(X,Y) \subset \mathbb{Z}/p\mathbb{Z}(X^{\frac{1}{p}}, Y^{\frac{1}{p}})$ séparable. Comme elle est finie, d'après le théorème de l'élément primitif il existe $\alpha \in \mathbb{Z}/p\mathbb{Z}(X^{\frac{1}{p}}, Y^{\frac{1}{p}})$ tel que $\mathbb{Z}/p\mathbb{Z}(X^{\frac{1}{p}}, Y^{\frac{1}{p}}) = \mathbb{Z}/p\mathbb{Z}(X,Y)(\alpha)$. Le degré de $\mathbb{Z}/p\mathbb{Z}(X,Y) \subset \mathbb{Z}/p\mathbb{Z}(X^{\frac{1}{p}}, Y^{\frac{1}{p}})$ est donc égal au degré de $\Pi_{\mathbb{Z}/p\mathbb{Z}(X,Y),\alpha}$, d'où (avec ce qui précède) $\deg\Pi_{\mathbb{Z}/p\mathbb{Z}(X,Y),\alpha} = p^2$, ce qui est impossible car α est racine de $T^p - \alpha^p \in \mathbb{Z}/p\mathbb{Z}(X,Y)[T]$ (cette appartenance vient du fait qu'on est en caractéristique p :

$$(\sum_{i,j} a_{i,j}(X^{\frac{1}{p}})^i(Y^{\frac{1}{p}})^j)^p = \sum_{i,j} a_{i,j}^p X^i Y^j \in \mathbb{Z}/p\mathbb{Z}(X,Y)).$$

Question 5

Soient en caractéristique nulle une extension finie $\mathbb{K} \subset \mathbb{L}$, Ω une clôture algébrique de $\mathbb{K}$ et $x \in \mathbb{L}$. Notons $H = \mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \Omega)$. Montrer que les deux définitions suivantes de la norme de x sont équivalentes :

- la norme de x est le déterminant de $m_x : \begin{cases} \mathbb{L} & \to & \mathbb{L} \\ y & \mapsto & xy \end{cases}$;

- la norme de x est $\prod_{\sigma \in H} \sigma(x)$.

Réponse :

Remarquons tout d'abord que si $\mathbb{L} = \mathbb{K}(x)$ alors dans la base $(1, x, \ldots, x^{[\mathbb{L}:\mathbb{K}]-1})$ la matrice de m_x est une matrice compagnon, donc le polynôme caractéristique de m_x est égal à son polynôme minimal, d'où le résultat.

Dans le cas général, soit $y \in \mathbb{L}$ tel que $\mathbb{L} = \mathbb{K}(y)$ (il existe par le théorème de l'élément primitif, car $\mathbb{K} \subset \mathbb{L}$ est finie et séparable (car en caractéristique nulle)). Il existe un polynôme $P \in \mathbb{K}[X]$ tel que $x = P(y)$.

Ainsi $m_x = P(m_y)$ donc les racines du polynôme caractéristique de m_x sont les images par P des racines du polynôme caractéristique de m_y donc, avec le cas précédent et les faits que $P \in \mathbb{K}[X]$ et $P(y) = x$ on a :

$$\det(m_x) = \prod_{\sigma \in H} P(\sigma(y)) = \prod_{\sigma \in H} \sigma(P(y)) = \prod_{\sigma \in H} \sigma(x).$$

Remarque : on peut aussi montrer que les deux définitions suivantes de la trace de x sont équivalentes :

- la trace de x est la trace de m_x : $\begin{cases} \mathbb{L} & \to & \mathbb{L} \\ y & \mapsto & xy \end{cases}$;

- la trace de x est $\sum_{\sigma \in H} \sigma(x)$.

Question 6

Soient p premier, $\mathbb{K}$ un corps de caractéristique p et $a \in \mathbb{K}$. Montrer que $X^p - X - a$ est scindé sur $\mathbb{K}$ ou irréductible dans $\mathbb{K}[X]$.

Réponse :

Supposons tout d'abord que $X^p - X - a$ a une racine $b \in \mathbb{K}$.

Soit $c \in \mathbb{Z}/p\mathbb{Z} \subset \mathbb{K}$ (car $\mathbb{K}$ est de caractéristique p). $(b+c)^p - (b+c) - a = b^p + c^p - b - c - a = b^p - b - a = 0$ (car tout élément de $\mathbb{Z}/p\mathbb{Z}$ est racine de $X^p - X$ et b est racine de $X^p - X - a$).

Ainsi $b + \mathbb{Z}/p\mathbb{Z}$ est inclus dans l'ensemble des racines de $X^p - X - a$ dans $\mathbb{K}$, or $\mathbb{K}$ est un corps et $X^p - X - a$ est de degré p, donc $X^p - X - a$ est scindé sur $\mathbb{K}$ (car $b + \mathbb{Z}/p\mathbb{Z}$ est de cardinal p).

Supposons désormais que $X^p - X - a$ n'a pas de racine dans $\mathbb{K}$.

Soit $\mathbb{L}$ un corps de rupture d'un facteur irréductible unitaire P de $X^p - X - a$.

Soit $b \in \mathbb{L}$ racine de P. Dans $\mathbb{L}[X]$ $X^p - X - a = \prod_{c \in \mathbb{Z}/p\mathbb{Z}} (X - (b + c))$ donc il existe $I \subset \mathbb{Z}/p\mathbb{Z}$ tel que $P = \prod_{c \in I} (X - (b + c))$.

Notons $P = X^n + \sum_k a_k X^k$. On a $a_{n-1} = -\sum_{c \in I} (b + c) = -|I| b - \sum_{c \in I} c$.

Ainsi $-|I|b = a_{n-1} + \sum_{c \in I} c \in \mathbb{K}$ or $b \notin \mathbb{K}$ donc $|I| \equiv 0(\mod p)$.

Or $0 \leq |I| \leq p$ (car $I \subset \mathbb{Z}/p\mathbb{Z}$) et $|I| \neq 0$ car P est irréductible donc de degré au moins 1, donc $|I| = p$ et $I = \mathbb{Z}/p\mathbb{Z}$ donc P est de degré p donc $P = X^p - X - a$ donc $X^p - X - a$ est irréductible.

5 Bibliographie

Calais J., Extensions de corps, 2006, Ellipses, Paris.

Chambert-Loir A., Algèbre corporelle, 2005, Éditions de l'École Polytechnique, Palaiseau.

Cox D., Galois Theory, Second Edition, 2012, John Wiley & Sons, Inc., Hoboken, New Jersey.

Lidl R., Niederreiter H., Introduction to finite fields and their applications, Revised edition, 1994, Cambridge University Press, Cambridge.

Perrin D., Cours d'algèbre, 1996, Ellipses, Paris.