Vincent Beck

Corps

Dans toute cette feuille d'exercice à l'exception de l'exercice 9, les corps sont commutatifs.

0 Extension de corps.

Définition 1 – Extension de corps. Soit k un corps. Une *extension de* k est un couple (K, i) où K est un corps et $i : k \to \mathrm{K}$ un morphisme d'anneaux unitaires. Évidemment, on omet presque systématiquement le i et on note $(\mathrm{K} : k)$ pour dire que K est une extension de k.

Pour les gens qui connaissent la notion de k-algèbre, une extension de k est une k-algèbre qui est un corps.

Exemple 2 $\mathbb{C}$ est une extension de $\mathbb{R}$, $\mathbb{R}(\mathrm{T})$ est une extension de $\mathbb{R}$. Si k est un sous-corps de K alors K est une extension de k et le morphisme associé est simplement l'inclusion.

Exercice 1 – Conséquences élémentaires. Soit (K, i) une extension de k.

a) Montrer que i est un morphisme **injectif** d'anneaux.

b) Montrer comment tout polynôme à coefficient dans k peut-être vu comme un polynôme à coefficient dans K.

c) Construire sur K une structure de k-espace vectoriel. C'est toujours cette structure qui est considéré dans cette feuille.

d) Montrer que tout corps de caractéristique nulle (resp. p) est extension de $\mathbb{Q}$ (resp. $\mathbb{F}_p$) de façon unique.

Définition 3 – Dimension. Dans cette feuille, si E est un k-espace vectoriel, on note $[\mathrm{E} : k] = \dim_k(\mathrm{E})$.

Exercice 2 – Multiplicativité des degrés.

a) Soit K une extension de k et E un K-espace vectoriel. Munir E d'une structure de k-espace vectoriel. Montrer que $[\mathrm{E} : k] = [\mathrm{E} : \mathrm{K}][\mathrm{K} : k]$.

b) Quelle est la dimension de $\mathbb{C}^n$ sur $\mathbb{R}$? Donner une $\mathbb{R}$-base de $\mathbb{C}^n$.

c) Soit $\mathrm{K} = k(x)$ où $x \in \mathrm{K}$ est algébrique sur k de degré impair. Montrer que $\mathrm{K} = k(\alpha^2)$.

d) Soient p, q deux nombres premiers. Pour quels valeurs de p et q a-t-on $\mathbb{Q}(\sqrt{p}) \subset \mathbb{Q}(\sqrt[3]{q})$?

e) Soit p un nombre premier, k un corps et K une extension de k de degré p premier. Montrer que K est une extension monogène de k.

f) Soient k un corps et $\mathrm{P}, \mathrm{Q} \in \mathsf{k}[\mathrm{X}]$ irréductibles tels que $\deg(\mathrm{P})$ et $\deg(\mathrm{Q})$ sont premiers entre eux. Soit K le corps de rupture de Q. Montrer que P est irréductible dans $\mathrm{K}[\mathrm{X}]$.

g) Soient $(\mathrm{K} : k)$ une extension de corps et E, F deux sous-extensions de K. Montrer que $[\mathrm{EF} : k] \leqslant [\mathrm{E} : k][\mathrm{F} : k]$ avec égalité si $[\mathrm{E} : k]$ et $[\mathrm{F} : k]$ sont premiers entre eux.

h) Soient k un corps et $a \in k$. Soient $m, n \in \mathbb{N}$ non nuls et premiers entre eux. Montrer que :

$$\mathrm{X}^{mn} - a \text{ est irréductible sur } k \iff \mathrm{X}^n - a \text{ et } \mathrm{X}^m - a \text{ sont irréductibles sur } k.$$

i) Déterminer une $\mathbb{Q}$-base de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, montrer que $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$. Déterminer les automorphismes de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

j) Calculer $[\mathbb{Q}(j, \sqrt[5]{2}) : \mathbb{Q}]$. Montrer que $\mathbb{Q}(j)$ est le seul sous-corps de $\mathbb{Q}(j, \sqrt[5]{2})$ de degré 2 sur $\mathbb{Q}$.

Définition 4 – Morphisme d'extensions. Soient (K, i) et (L, j) deux extensions de k. Un *morphisme d'extensions de* k de (K, i) dans (L, j) est un morphisme d'anneaux (unitaires) $f : \mathrm{K} \to \mathrm{L}$ vérifiant $f \circ i = j$ (on dit aussi *morphisme de* k*-extensions* ou k-morphisme). Le diagramme suivant est commutatif

$$\begin{tikzcd} \mathrm{K} \arrow[rr, "f"] & & \mathrm{L} \\ & k \arrow[ul, "i"] \arrow[ur, "j"'] & \end{tikzcd}$$

Pour ceux qui connaissent la notion de k-algèbre, vérifier qu'entre deux extensions de k, morphismes de k-extensions et morphismes de k-algèbres coïncident.

Exercice 3 — Linéarité et morphisme d'extension.

a) Soient K et L deux extensions de k. Montrer qu'un morphisme d'extensions de K dans L est k-linéaire pour les structures définies dans la question **c** de l'exercice 1. Inversement, soit $f : \mathrm{K} \to \mathrm{L}$ un morphisme d'anneaux unitaires qui est k-linéaire pour les structures définies ci-dessus. Montrer que f est un morphisme de k-extensions.

b) Pourquoi un k-morphisme est-il nécessairement injectif ? En déduire que pour qu'il existe un morphisme de k-extensions de K dans L, il faut que $[\mathrm{L} : k] \geqslant [\mathrm{K} : k]$. La condition est-elle suffisante ?

c) Donner un exemple de k-morphisme non surjectif (voir aussi l'exercice 14).

Exercice 4 — Deux versions de $\mathbb{C}$. On considère l'ensemble $\mathbb{C}_1 := \mathbb{R}^2$ muni des lois $(x, y) + (x', y') = (x + x', y + y')$ et $(x, y)(x', y') = (xx' - yy', xy' + yx')$ et du morphisme $i_1 : x \in \mathbb{R} \mapsto (x, 0) \in \mathbb{C}_1$. Vérifier que c'est une extension de corps de $\mathbb{R}$. Vérifier que la structure naturelle d'espace vectoriel sur $\mathbb{R}$ de $\mathbb{C}_1$ coïncide avec la structure d'espace vectoriel donnée par la structure d'extension.

On considère l'extension $\mathbb{C}_2 := \mathbb{R}[\mathrm{X}]/(\mathrm{X}^2 + 1)$ de $\mathbb{R}$. Quel est le morphisme de $\mathbb{R}$ dans $\mathbb{C}_2$ sous-jacent à l'extension ?

Vérifier que $\mathbb{C}_1$ et $\mathbb{C}_2$ sont deux extensions isomorphes de $\mathbb{R}$.

Exercice 5 — Morphisme d'extensions. Soient K et L deux k-extensions et $f, g : \mathrm{K} \to \mathrm{L}$ deux morphismes de k-extensions.

a) L'ensembles des morphismes des morphismes de k-extensions de K dans L est-il stable par addition ? multiplication ?

b) Vérifier que si L' est une k-extension et $f' : \mathrm{L} \to \mathrm{L}'$ un morphisme de k-extensions alors $f' \circ f$ est un morphisme de k-extensions.

c) Montrer que $\{x \in \mathrm{K},\ f(x) = g(x)\}$ est une sous-extension de K.

d) En déduire que si $f : \mathrm{K} \to \mathrm{K}$ est un morphisme de corps alors $\mathrm{Ker}\,(f - \mathrm{id}_\mathrm{K}) = \{x \in \mathrm{K},\ f(x) = x\}$ est une sous-extension de K.

e) Montrer que tout endomorphisme σ du corps $\mathbb{R}$ est $\mathrm{id}_\mathbb{R}$ (on utilisera le fait que les éléments positifs de $\mathbb{R}$ sont les carrés (la positivité se traduit algébriquement) pour montrer que σ est croissant).

f) En déduire que les endomorphismes σ du corps $\mathbb{C}$ tel que $\sigma(\mathbb{R}) \subset \mathbb{R}$ sont $\mathrm{id}_\mathbb{C}$ et la conjugaison.

g) Déterminer les endomorphismes continus du corps $\mathbb{C}$.

h) Soient K un sous-corps de $\mathbb{C}$ et $\sigma : \mathrm{K} \to \mathbb{C}$ un morphisme de corps continu. Montrer que $\sigma = \mathrm{id}_\mathrm{K}$ ou que σ est la restriction à K de la conjugaison complexe.

Exercice 6

a) Existe-t-il un morphisme de $\mathbb{R}$-extensions de $\mathbb{R}(\mathrm{T})$ dans $\mathbb{C}$?

b) Existe-t-il un morphisme de $\mathbb{R}$-extensions de $\mathbb{C}$ dans $\mathbb{R}(\mathrm{T})$?

c) Existe-t-il un morphisme d'extensions de $\mathbb{Q}(\sqrt{2})$ dans $\mathbb{Q}(\sqrt[3]{2})$?

d) Plus généralement pour quelles valeurs de $n \in \mathbb{N}$, existe-t-il un morphisme d'extensions de $\mathbb{Q}(\sqrt{2})$ dans $\mathbb{Q}(\sqrt[n]{2})$?

e) Montrer que tout morphisme de corps entre deux corps de caractéristique nulle (resp. p) est un morphisme de $\mathbb{Q}$-extensions (resp. $\mathbb{F}_p$-extensions).

Exercice 7 — Lemme de Dedekind.

a) Soit M un monoïde unitaire (non nécessairement commutatif) et K un corps. Montrer que l'ensemble des morphismes de monoïdes unitaires de M dans $\mathrm{K}^\times$ est une famille libre de l'espace vectoriel des fonctions de M dans K (on pourra vérifier considérer une relation de dépendance linéaire de longueur minimale).

b) En déduire que les fonctions $x \mapsto \exp(ax)$ sont linéairement indépendantes en tant que fonction de $\mathbb{R}$ dans $\mathbb{R}$.

c) En déduire aussi que si les λ_i sont des nombres complexes deux à deux distincts alors les suites $({\lambda_i}^n)_{n\in\mathbb{N}}$ forment une famille libre de l'ensemble des suites à valeurs complexes.

d) Soit K, L deux extensions de k. Montrer que l'ensemble des morphismes de k-extensions forme une famille libre du L-espace vectoriel des applications k-linéaires de K dans L.

e) Soit E un k-espace vectoriel et L une extension de k. Déterminer la dimension du L-espace vectoriel des applications k-linéaires de E dans L.

f) En déduire que si K est une extension finie de k alors le nombre de k-morphismes de K dans L est inférieur ou égal à $[\mathrm{K} : k]$.

g) Soit σ un k-automorphisme d'une extension K de k. On suppose que σ est d'ordre fini n dans le groupe des k-automorphismes de K. Montrer que le polynôme minimal de σ est $\mathrm{X}^n - 1$. Déterminer les invariants de similitude de σ.

h) On s'intéresse au cas où $\sigma = \mathrm{F}$ est le morphisme de Frobenius, $k = \mathbb{F}_p$ et $\mathrm{K} = \mathbb{F}_{p^n}$. Quel est l'ordre de F ? En déduire qu'il existe une $\mathbb{F}_p$-base de $\mathbb{F}_q$ dans laquelle la matrice de F est celle d'un n-cycle.

Définition 5 — Sous-extension. Soit k un corps et (K, i) une extension de k. Une sous-k-extension de (K, i) est un sous-corps L de K contenant $i(k)$. Le couple (L, i) est alors une extension de k et l'inclusion de L dans K est un morphisme d'extensions.

Pour ceux qui connaissent la notion de k-algèbre, vérifier qu'un sous-extension de K est une sous-k-algèbre qui est un corps.

Exercice 8 — Sous-extension.

a) Montrer qu'une sous-k-extension L de K est un sous-espace vectoriel de k. Montrer que la structure de k-espace vectoriel induite par la structure d'extension coïncide avec la structure d'espace vectoriel induite par le fait d'être un sous-espace vectoriel de K.

b) Inversement, soit L un sous-corps de K qui est un sous-k-espace vectoriel de K. Vérifier que L est une sous-extension de K.

c) Vérifier qu'une intersection de sous-k-extensions de K est une sous-k-extension de K. En déduire une notion de sous-k-extension engendrée par une partie A de K. On la note $k(\mathrm{A})$.

d) Vérifier que $k(\mathrm{A})$ est le plus petit sous-corps de K contenant k et A et que

$$k(\mathrm{A}) = \{\mathrm{P}(a_1, \ldots, a_n)/\mathrm{Q}(a_1, \ldots, a_n), \qquad n \in \mathbb{N},\ a_1, \ldots, a_n \in \mathrm{A},\ \mathrm{P}, \mathrm{Q} \in k[\mathrm{X}_1, \ldots, \mathrm{X}_n],\ \mathrm{Q}(a_1, \ldots, a_n) \neq 0\}$$

e) On prendra garde à ne pas confondre $k(\mathrm{A})$ avec $k[\mathrm{A}]$ qui est par définition la sous-algèbre engendrée par A ou encore le plus petit sous-anneau de K contenant A et k. On vérifiera que

$$k[\mathrm{A}] = \{\mathrm{P}(a_1, \ldots, a_n),\ n \in \mathbb{N},\ a_1, \ldots, a_n \in \mathrm{A},\ \mathrm{P} \in k[\mathrm{X}_1, \ldots, \mathrm{X}_n]\}$$

Voir aussi la caractérisation de l'algébricité à l'exercice 10.

Exercice 9 — Théorème de Wedderburn. On considère $(\mathrm{A}, +, \cdot)$ un ensemble muni de deux lois telles que $(\mathrm{A}, +)$ soit un groupe, $\cdot$ soit associative (on ne suppose pas que $\cdot$ admet un élément neutre). On suppose que la loi $\cdot$ est distributive par rapport à $+$. On dit que A est un *pseudo-anneau* (il manque juste l'existence de l'élément neutre pour $\cdot$ pour avoir un anneau).

Dans toute la suite A désigne un pseudo-anneau **fini** tel que tout élément non nul $a \in \mathrm{A}$ soit un non-diviseur de 0 à gauche (si $ax = 0$ alors $x = 0$). On va montrer que A est un corps commutatif : c'est le théorème de Wedderburn.

a) Montrer que A est un anneau (on pourra considérer l'application $x \mapsto ax$) et que tout élément non nul de A est non diviseur de 0 à droite.

b) Montrer que la caractéristique de A est un nombre premier p. En déduire une structure de $\mathbb{F}_p$-espace vectoriel sur A.

c) Montrer que tout élément non nul de A est inversible dans A. Finalement A est un anneau à division (ou corps gauche ou corps non nécessairement commutatif).

Il s'agit à présent de montrer la commutativité.

d) On considère $\mathrm{ZA} = \{x \in \mathrm{A}, \quad \forall\, a \in \mathrm{A},\ xa = ax\}$. Montrer que ZA est un sous-corps (commutatif) de A. Construire une structure de ZA-espace vectoriel sur A et de $\mathbb{F}_p$-espace vectoriel sur A. On note $[\mathrm{A} : \mathrm{ZA}] = n$ et $q = |\mathrm{ZA}|$.

e) En faisant agir $\mathrm{ZA}^\times$ par conjugaison sur $\mathrm{A} \smallsetminus \{0\}$. Déterminer des entiers d_{x_i} divisant n et distincts de n tels que

$$q^n - 1 = q - 1 + \sum_{x_i} \frac{q^n - 1}{q^{d_{x_i}} - 1} \tag{1}$$

où les x_i représentent une famille de représentant des orbites non ponctuelles de l'action.

f) En déduire que $\Phi_n(q) \mid (q - 1)$.

g) Par un simple dessin, montrer que si $n > 1$ et $q \geqslant 2$ alors $\Phi_n(q) > (q - 1)^{\varphi(n)}$.

h) En déduire que $n = 1$ dans l'égalité (**1**).

i) Conclure.

1 Algébricité.

Exercice 10 — Définition des éléments algébriques. Soient k un corps, K une extension de k et $x \in \mathrm{K}$.

a) Montrer qu'il existe un unique morphisme de k-algèbres $\varphi_x \colon k[\mathrm{X}] \to \mathrm{K}$ tel que $\varphi_x(\mathrm{X}) = x$. Les éléments de $\operatorname{Ker} \varphi_x$ sont appelés les *polynômes annulateurs de x*.

b) Montrer que les conditions suivantes sont équivalentes

(i) La famille $(x^k, k \in \mathbb{N})$ est liée sur k ;
(ii) Il existe $\mathrm{P} \in k[\mathrm{X}] \smallsetminus \{0\}$ tel que $\mathrm{P}(x) = 0$;
(iii) φ_x n'est pas injectif ;
(iv) $k[x] = k(x)$;
(v) $[k[x] : k] < +\infty$;
(vi) $[k(x) : k] < +\infty$;
(vii) $k[\mathrm{X}]/\operatorname{Ker} \varphi_x$ est un corps ;
$(viii)$ Il existe une sous-algèbre L de K contenant x telle que $[\mathrm{L} : k] < +\infty$;
(ix) Il existe une sous-extension L de K contenant x telle que $[\mathrm{L} : k] < +\infty$;

Un tel x est dit *algébrique sur k* et $[k(x) : k]$ s'appelle le *degré de x sur k*.

c) On suppose que x est algébrique sur k. Montrer que $\operatorname{Ker}(\varphi_x)$ admet une unique générateur unitaire noté $\pi_x \in k[\mathrm{X}]$. On dit que π_x est le *polynôme minimal de x sur k*.

d) Montrer que π_x est irréductible.

e) Soit $\mathrm{P} \in k[\mathrm{X}]$ un polynôme annulateur de x irréductible. Montrer qu'il existe $\lambda \in k^\times$ tel que $\mathrm{P} = \lambda \pi_x$. *Autrement dit, pour trouver le polynôme minimal, il suffit de trouver un polynôme irréductible et annulateur à coefficient dans k.*

f) Montrer que $k[\mathrm{X}]/(\pi_x) \overset{k\text{-alg.}}{\simeq} k(x)$ et $[k(x) : k] = \deg \mu_x$.

g) Sur $\mathbb{Q}$, montrer que les éléments suivants sont algébriques et calculer leur polynôme minimal : $\sqrt{2}$, $\sqrt{4 + 2\sqrt{2}}$ (même question sur $\mathbb{Q}(\sqrt{2})$), $\sqrt[3]{2}$.

Exercice 11 — Élément transcendant. Soit (K, i) une extension de k et $x \in \mathrm{K}$. Montrer que les propriétés suivantes sont équivalentes

(i) La famille $(x^k,\ k \in \mathbb{N})$ est libre sur k ;
(ii) Si $\mathrm{P}(x) = 0$ avec $\mathrm{P} \in k[\mathrm{X}]$ alors $\mathrm{P} = 0$;
(iii) φ_x est injectif ;
(iv) $k[\mathrm{X}] \overset{k\text{-alg.}}{\simeq} k[x]$;
(v) $k(\mathrm{X}) \overset{k\text{-ext.}}{\simeq} k(x)$;
(vi) $k(x) \neq k[x]$;
(vii) $k[x] \subsetneq k(x)$;
$(viii)$ $[k[x] : k] = +\infty$;
(ix) $[k(x) : k] = +\infty$.

Un tel x est dit *transcendant sur k*.

Exercice 12 — Extensions algébriques. Soit L une extension de k. L'extension de corps $(\mathrm{L} : k)$ est dite *algébrique* si tout élément de L est algébrique sur k.

a) Montrer que l'ensemble K des éléments de L qui sont algébriques sur k est une sous-extension de L. On dit que K est la *fermeture algébrique de k dans* L.

b) Vérifier que $(\mathrm{L} : k)$ est algébrique si et seulement si L est la fermeture algébrique de k dans lui-même.

c) Montrer que L est algébrique sur k si et seulement si L est engendrée sur k par des éléments algébriques.

d) Montrer que si $(\mathrm{L} : k)$ est *finie* (c'est-à-dire $[\mathrm{L} : k] < \infty$), alors elle est algébrique.

e) Étudier la réciproque : une extension algébrique est-elle finie ?

f) Montrer que si $\mathrm{L} = k(\alpha_1, \ldots, \alpha_n)$ et si $\alpha_1, \ldots, \alpha_n$ sont algébriques sur k alors $(\mathrm{L} : k)$ est finie, donc algébrique.

g) *Transitivité de l'algébricité.* Soit L' une extension de L. Montrer que $(\mathrm{L}' : k)$ est algébrique si et seulement si $(\mathrm{L}' : \mathrm{L})$ et $(\mathrm{L} : k)$ algébrique. *Cette propriété est fondamentale. Il* **faut** *savoir la démontrer.*

h) Soient I un ensemble et $\{M_i\}_{i\in I}$ une famille de sous-extension de L contenant k. Soit M le sous-corps de L engendré par $\bigcup_{i\in I} M_i$. Montrer que si chaque $(M_i : k)$ est algébrique, alors $(M : k)$ est algébrique.

Exercice 13 Comparer

(i) $\mathbb{R}[i]$ et $\mathbb{R}(i)$
(ii) $\mathbb{Q}[i]$ et $\mathbb{Q}(i)$
(iii) $\mathbb{R}[T^2]$ et $\mathbb{R}(T^2)$
(iv) $\mathbb{Q}[\pi]$ et $\mathbb{Q}(\pi)$
(v) $\mathbb{Q}[\sqrt{2}]$ et $\mathbb{Q}(\sqrt{2})$
(vi) $\mathbb{Q}[e]$ et $\mathbb{Q}(e)$

Exercice 14 — Algébricité et finitude. Soient $(K : k)$ une extension algébrique et $\sigma : K \to K$ un endomorphisme de k-extension. Montrer que σ est un automorphisme. Que se passe-t-il si on ne suppose plus $(K : k)$ algébrique.

Exercice 15 — Fractions rationelles et changement de corps. Soit $(K : k)$ une extension. Pour rendre l'exercice moins technique, on pourra traiter uniquement le cas $n = 1$.

a) Montrer que $(K(X_1, \dots, X_n) : k(X_1, \dots, X_n))$ est une extension algébrique si et seulement si $(K : k)$ l'est.

b) Déterminer la fermeture algébrique de k dans $K(X_1, \dots, X_n)$. Soit $x \in K(X_1, \dots, X_n)$. En déduire que si $(K : k)$ est algébrique, alors $x \in K$ si et seulement si x est algébrique sur k.

c) On suppose que $(K : k)$ est une extension algébrique. En déduire qu'on peut définir un morphisme de groupes

$$\Psi : \begin{cases} \mathrm{Aut}_{k(X_1,\dots,X_n)}(K(X_1, \dots, X_n)) \longrightarrow \mathrm{Aut}_k(K) \\ \qquad\qquad \sigma \qquad\qquad\qquad\qquad \longmapsto \sigma_K \end{cases}$$

où σ_K désigne la restriction de σ à K. Montrer que Ψ est bijectif (on pourra utiliser la propriété universelle des polynômes pour construire l'inverse de Ψ).

d) On suppose que $(K : k)$ est finie. Montrer que $(K(X_1, \dots, X_n) : k(X_1, \dots, X_n))$ l'est aussi et comparer $[K(X_1, \dots, X_n) : k(X_1, \dots, X_n)]$ et $[K : k]$. En déduire que si $(K(X_1, \dots, X_n) : k(X_1, \dots, X_n))$ alors $(K : k)$. Comparer le polynôme minimal de $x \in K$ sur k et le polynôme minimal de x sur $k(X_1, \dots, X_n)$.

Pour ceux qui en savent plus.

e) Montrer que $(K : k)$ est une extension séparable si et seulement si $(K(X_1, \dots, X_n) : k(X_1, \dots, X_n))$ l'est aussi.

f) Montrer que $(K : k)$ est une extension normale si et seulement si $(K(X_1, \dots, X_n) : k(X_1, \dots, X_n))$ l'est aussi.

g) En déduire que $(K : k)$ est une extension galoisienne si et seulement si $(K(X_1, \dots, X_n) : k(X_1, \dots, X_n))$ l'est aussi. Retrouver alors le résultat de la question **d** : $[K : k] = [K(X_1, \dots, X_n) : k(X_1, \dots, X_n)]$.

Exercice 16 — Automorphisme de $k(X)$. Soient k un corps et $k(X)$ le corps des fractions rationnelles sur k. Pour $F \in k(X)$, on écrit $F = P/Q$ avec $P, Q \in k[X]$ et P et Q premier entre eux et on pose $\deg F = \max(\deg P, \deg Q)$.

a) Montrer que, si F n'est pas une constante, alors $[k(X) : k(F)] = \deg F$.

b) Décrire une bijection entre les endomorphismes de la k-algèbre $k(X)$ et les fractions rationnelles non constante.

c) Déduire de la question **a** que tout k-automorphisme de $k(X)$ est déterminé par une fraction rationnelle F vérifiant $\deg F = 1$.

d) Montrer que le groupe G des k-automorphismes de $k(X)$ est isomorphe à $\mathrm{PGL}(2, k) = \mathrm{GL}(2, k)/k^\times \mathrm{id}$.

e) Montrer G est engendré par les automorphismes déterminés par les fractions rationnelles $X + b$ $(b \in k)$, aX $(a \in k^\times)$ et X^{-1}.

f) On suppose que k est infini. Montrer que G est infini et déterminer $k(X)^G$.

g) Montrer que l'extension $\mathbb{C}(X^3+1/X^3) \subset \mathbb{C}(X)$ est galoisienne, déterminer son groupe de Galois, les extensions intermédiaires et des éléments primitifs pour chacune.

h) Montrer que les automorphismes déterminer par $X \mapsto 1/X$ et $X \mapsto 1 - X$ engendré un sous-groupe fini H de G. Déterminer les éléments de H et la classe d'isomorphisme de H. Déterminer une expression factorisée du polynôme minimal de X sur $k(X)^H$. En calculer le terme en T^3 ou le terme en T^4, en déduire une fraction rationnelle F telle que $k(X)^H = k(F)$.

Dans la suite, on suppose que k est fini de cardinal q.

i) Déterminer l'ordre de G.

j) Montrer que $k(X)^G = k(F)$ pour $F = (X^{q^2} - X)^{q+1}/(X^q - X)^{q^2+1}$.

k) Soit H_1 le sous-groupe de G formé par les automorphismes déterminées par les fractions rationnelles $aX + b$ ($a \in k^\times$, $b \in k$). Montrer que $k(X)^{H_1} = k(Y)$ où $Y = (X^q - X)^{q-1}$.

l) Soit H_2 le sous-groupe de G formé par les automorphismes déterminées par les fractions rationnelles $X + b$ ($b \in k$). Montrer que $k(X)^{H_2} = k(Z)$ où $Z = X^q - X$.

m) Soit H_3 le sous-groupe de G formé par les automorphismes déterminées par les fractions rationnelles aX ($a \in k^\times$). Montrer que $k(X)^{H_3} = k(T)$ où $T = X^{q-1}$.

n) Soit H_4 le sous-groupe de G formé par les automorphismes déterminées par les fractions rationnelles X et X^{-1}. Montrer que $k(X)^{H_4} = k(U)$ où $U = X + 1/X$.

2 Corps de rupture.

Le polynôme $X^2 + 1 \in \mathbb{R}[X]$ n'a pas de racine dans $\mathbb{R}$. Pour remédier à ce problème, on crée le corps $\mathbb{C} := \mathbb{R}[X]/(X^2 + 1)$. Dans $\mathbb{C}$, le polynôme $T^2 + 1$ a une racine qui est la classe de X.

On se pose alors la question suivante. Étant donné $P \in k[X]$ un polynôme, peut-on trouver un corps (une extension de k) dans lequel P a une racine ? Dans quelle mesure, une telle extension est-elle unique ?

Si P n'est pas irréductible, on écrit $P = P_1P_2$ avec P_1, P_2 non inversible. Il suffit de trouver une racine de P_1 ou de P_2. Ainsi, en continuant la factorisation, il suffit de trouver des racines aux polynômes irréductibles sur k. Cette même factorisation en irréductibles montre que si P n'est pas irréductible, il n'y a aucune chance d'obtenir une quelconque propriété d'unicité du corps dans lequel P a une racine. Par exemple, sur $\mathbb{R}$, avec $P = X(X^2 + 1)$, $\mathbb{R}$ et $\mathbb{C}$ sont deux corps dans lesquels P admet une racine. De même, si on n'impose pas un propriété de minimalité de l'extension cherchée, aucune chance d'avoir unicité : les extensions $\mathbb{Q}(\sqrt{2})$ et $\mathbb{C}$ contiennent toutes les deux des racines de $P = X^2 - 2$.

Exercice 17 — Corps de rupture. Soit $P \in k[X]$ **irréductible**. On appelle *corps de rupture* de P sur k un couple formée d'une extension $(L : k)$ et d'un élément $x \in L$ vérifiant $P(x) = 0$ (on veut trouver une racine de P) et $L = k(x)$ (c'est la condition de minimalité).

a) Soit $P \in k[X]$ irréductible. Montrer que P admet un corps de rupture (on pourra considérer $k[X]/(P)$).

Soient $P \in k[X]$ irréductible et $k(x)$ un corps de rupture de P. Soit L un corps et $\iota\colon k \to L$ un morphisme de corps. On notera $\iota(P) \in L[X]$ le polynôme obtenu à partir de P en appliquant ι aux coefficients (l'application $P \mapsto \iota(P)$ est un morphisme de k-algèbre).

b) Montrer que pour tout morphisme d'extensions $j\colon \mathsf{k}(x) \to L$, l'image de x est une racine de $\iota(P)$.

c) Montrer que pour toute racine $y \in L$ de $\iota(P)$, il existe un unique morphisme d'extensions de $k(x)$ dans L envoyant x sur y.

d) En déduire que l'application

$$\begin{cases} \{\text{Prolongement de } \iota \text{ en un morphisme de corps } k(x) \to L\} \longrightarrow \{\text{Racines de P dans L}\} \\ \qquad\qquad \sigma \qquad\qquad\qquad\qquad\qquad\qquad \longmapsto \sigma(x) \end{cases}$$

est bien définie et est une bijection.

e) En déduire que si $L = k(y)$ est un corps de rupture pour P avec $P(y) = 0$ alors il existe un unique k-isomorphisme σ de $k(x)$ sur L tel que $\sigma(x) = y$. En particulier, deux corps de rupture de P sont isomorphes.

Exercice 18 — Extension monogène et corps de rupture.

a) Soit $K = k(x)$ une extension monogène de k avec x algébrique sur k. Montrer que K est un corps de rupture (c'est-à-dire qu'il existe un polynôme P irréductible sur k tel que K soit le corps de rupture de P).

b) Quel est le corps de rupture de $X^2 + 1$ sur $\mathbb{Q}, \mathbb{R}, \mathbb{C}$? Les questions posées ont-elles un sens ?

c) Montrer que $P = X^3 - 2$ est irréductible sur $\mathbb{Q}$. Combien P admet-il de corps de rupture dans $\mathbb{C}$?

Exercice 19 — Calculs dans des corps de rupture.

a) Soit $P = X^3 + X^2 + X + 2 \in \mathbb{Q}[X]$. Montrer que P est irréductible sur $\mathbb{Q}$. Soit $\alpha \in \mathbb{C}$ une racine de P. Écrire $(\alpha^2 + \alpha + 1)(\alpha^2 + \alpha)$ et $1/(\alpha - 1)$ dans la base $(1, \alpha, \alpha^2)$ de $\mathbb{Q}(\alpha)$ sur $\mathbb{Q}$.

b) Soit $P = X^3 + 2X^2 + 2X + 2 \in \mathbb{Q}[X]$. Montrer que P est irréductible sur $\mathbb{Q}$. Soit $\alpha \in \mathbb{C}$ une racine de P. Écrire $(\alpha^2 - \alpha + 1)(\alpha^2 + 2\alpha + 1)$ et $1/(3\alpha^2 + \alpha + 5)$ dans la base $(1, \alpha, \alpha^2)$ de $\mathbb{Q}(\alpha)$ sur $\mathbb{Q}$.

c) Soit $P = X^6 + X^3 + 1 \in \mathbb{Q}[X]$. Montrer que P est irréductible sur $\mathbb{Q}$ et que P divise $X^9 - 1$. Soit $\alpha \in \mathbb{C}$ une racine de P. Écrire $(\alpha^5 - \alpha - 2)(\alpha^4 + 1)$ et $1/(\alpha^5 + \alpha + 1)$ dans la base $(1, \ldots, \alpha^5)$ de $\mathbb{Q}(\alpha)$ sur $\mathbb{Q}$. Trouver tous les morphismes de corps $\mathbb{Q}(\alpha) \to \mathbb{C}$.

Exercice 20 — Polynômes minimaux. Trouver le degré et le polynôme minimal sur $\mathbb{Q}$ de : $j\sqrt{2}$, $\sqrt{2}+\sqrt{3}$, $i+\sqrt{2}$, $j+\sqrt{3}$, $i+j$.

3 Corps de décomposition.

Étant donné un polynôme P à coefficients dans k, on sait construire une extension de k dans lequel P a une racine. On cherche maintenant à agrandir encore le corps pour scinder le polynôme P : existe-t-il une extension de k dans laquelle P est scindé. Dans quelle mesure une telle extension est-elle unique ? Bien entendu, une extension d'une extension dans laquelle P est scindé est encore une extension dans laquelle P est scindé. Ainsi, on ne peut espérer de résultats d'unicité qu'en demandant des propriétés de minimalité sur l'extension dans laquelle P est scindé.

Exercice 21 — Corps de décomposition. Soient k un corps $\mathrm{P} \in k[\mathrm{X}]$. Un *corps de décomposition* de P sur k est une extension L de k telle que P est scindé dans L (on veut bien toutes les racines de P) et L est engendré sur k par l'ensemble des racines de P dans L (c'est la condition de minimalité).

a) Montrer qu'il existe toujours un corps de décomposition et que c'est une extension finie dont le degré divise $(\deg \mathrm{P})!$.

b) Soient k' un corps, $\iota\colon k \to k'$ une extension et $\mathrm{Q} \in k'[\mathrm{X}]$ le polynôme obtenu à partir de P en appliquant ι aux coefficients. Soit L (resp. L′) un corps de décomposition de P sur k (resp. une extension de k' dans laquelle P est scindé). Montrer qu'il existe un morphisme de k-extensions $\mathrm{L} \to \mathrm{L}'$.

c) En déduire que si L, L' sont deux corps de décomposition de P sur k, alors il existe un isomorphisme de k-extensions $\mathrm{L} \to \mathrm{L}'$.

Attention, on remarquera qu'on n'a pas unicité dans le morphisme d'extension de L dans L′ ou dans l'isomorphisme entre corps de décomposition. On pourra comparer avec le cas du corps de rupture. La théorie de Galois résulte de cette non-unicité.

Exercice 22 — Comparaison du corps de rupture et du corps de décomposition.

a) Soit P un polynôme de degré 2. Comparer son corps de rupture et son corps de décomposition.

b) Soient $\mathrm{P} \in k[\mathrm{X}]$ et K une extension de k dans laquelle P est scindé. Montrer qu'il existe une unique sous-extension de K qui est un corps de décomposition de P sur k. A-t-on un résultat analogue pour les corps de rupture ?

c) Soit $\mathrm{P} = \mathrm{X}^4 - 9$. Calculer le corps de décomposition de P sur $\mathbb{Q}$. Quel est son degré ?

d) Soit $\mathrm{P} = \mathrm{X}^3 - 2$. Montrer que P est irréductible sur $\mathbb{Q}$. Calculer le corps de décomposition de P sur $\mathbb{Q}$. Quel est son degré ? Comparer avec le degré du corps de rupture. Déterminer les corps de rupture de P dans $\mathbb{C}$.

e) Mêmes questions avec $\mathrm{P} = \mathrm{X}^4 - 2$.

f) Soit $\zeta \in \mathbb{C}$ une racine primitive 5e de l'unité. Montrer que ζ est algébrique sur $\mathbb{Q}$ et calculer son polynôme minimal P. Quel est le corps de décomposition de P sur $\mathbb{Q}$?

Exercice 23 — Extension et carré. Soient K un corps de caractéristique différente de 2 et $\alpha_1, \ldots, \alpha_n$ des éléments de K tels que pour toute famille $\nu = (\nu_1, \ldots, \nu_n) \in \{0,1\}^n$, l'élément

$$\alpha_\nu := {\alpha_1}^{\nu_1} \cdots {\alpha_n}^{\nu_n}$$

n'est pas un carré dans K. On considère L un corps de décomposition sur K de $(\mathrm{X}^2 - \alpha_1) \cdots (\mathrm{X}^2 - \alpha_n) \in \mathrm{K}[\mathrm{X}]$ et on note $\beta_i = \sqrt{\alpha_i} \in \mathrm{L}$ une racine de $\mathrm{X}^2 - \alpha_i$. Pour $\nu = (\nu_1, \ldots, \nu_n) \in \{0,1\}^n$, on pose

$$\beta_\nu := {\beta_1}^{\nu_1} \cdots {\beta_n}^{\nu_n}$$

a) Montrer que $[\mathrm{L} : \mathrm{K}] = 2^n$ et que la famille $(\beta_\nu)_{\nu \in \{0,1\}^n}$ est une K-base de L.

b) Décrire un isomorphisme explicite entre le groupe multiplicatif $\{-1,1\}^n$ et $\mathrm{Aut}_{\mathrm{K}}(\mathrm{L})$. En déduire que les éléments de L fixes par tous les éléments de $\mathrm{Aut}_{\mathrm{K}}(\mathrm{L})$ sont les éléments de K.

c) Pour $f \in \{-1,1\}^n$, on pose $\theta_f = \sum_{i=1}^{n} f(i)\beta_i$. Montrer que

$$\mathrm{P}(\mathrm{X}) = \prod_{f \in \{-1,1\}^n} (\mathrm{X} - \theta_f) \in \mathrm{K}[\mathrm{X}]$$

et est irréductible sur K. En déduire que $\mathrm{L} = \mathrm{K}(\theta_f)$.

d) Montrer que le résultat s'applique avec $k = \mathbb{Q}$ et les α_i des nombres premiers distincts. En déduire que si $\mathrm{N} \geqslant 2$ alors $1 + \sqrt{2} + \cdots + \sqrt{\mathrm{N}} \notin \mathbb{Q}$.

3 Corps algébriquement clos.

Exercice 24 — Corps algébriquement clos.

a) Soit k un corps. Les propositions suivantes sont équivalentes

(i) Tout polynôme non constant à coefficients dans k admet une racine dans k
(ii) Les éléments irréductibles de $k[\mathrm{X}]$ sont les polynômes de degré 1
(iii) Tout polynôme non constant est produit de polynômes de degré 1
(iv) Si (K, i) est une extension algébrique de k alors i est un isomorphisme.

Un corps vérifiant ces propriétés est dit *algébriquement clos*.

b) Montrer que $\mathbb{C}$ est algébriquement clos.

c) Montrer que l'ensemble des éléments de $\mathbb{C}$ algébriques sur $\mathbb{Q}$ est un corps algébriquement clos.

Définition 6 — Clôture algébrique. Soit k un corps. Une *clôture algébrique de k* est une extension (K, i) de k où K est algébriquement clos et (K, i) est algébrique sur k.

Exercice 25 — Clôture algébrique.

a) Montrer que $\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$ mais pas de $\mathbb{Q}$ (par un argument de cardinalité **et** en exhibant un élément de $\mathbb{C}$ non algébrique sur $\mathbb{Q}$).

b) Montrer que l'ensemble des éléments de $\mathbb{C}$ algébriques sur $\mathbb{Q}$ est une clôture algébrique de $\mathbb{Q}$.

c) En admettant le théorème de Steinitz : tout corps admet une extension algébriquement close. Montrer que tout corps k admet une clôture algébrique (on pourra considérer l'ensemble des éléments algébriques sur k d'une extension algébriquement close de k).

Exercice 26 — Le lemme de prolongement. Soient (K, i) une extension **algébrique** de k et (K', j) une extension algébriquement close.

a) On suppose $[\mathrm{K} : k] < +\infty$. Montrer, par récurrence sur $[\mathrm{K} : k]$, qu'il existe un k-morphisme de (K, i) dans (K', j) (on pourra commencer par traiter le cas où $k(x)$ est monogène).

b) En utilisant le lemme de Zorn, montrer qu'il existe un k-morphisme de (K, i) dans (K', j) (on pourra considérer l'ensemble **non vide** des couples (L, σ) où L est une sous-extension de K et σ un k-morphisme de L dans K').

c) En déduire que deux clôtures algébriques de k sont k-isomorphes (on pourra utiliser l'exercice 14).

Exercice 27 — Applications.

a) Soit K une extension **algébrique** de k. Montrer que K et k ont même clôture algébrique.

b) À l'aide du théorème de Steinitz, démontrer le théorème d'existence et l'unicité du corps de décomposition.

c) Soit k une clôture algébrique de $\mathbb{F}_p$. Montrer que k contient un unique sous-corps à p^n pour tout $n \in \mathbb{N}^*$. On le note $\mathbb{F}_{p^n}$ Montrer que $k = \cup_{n \in \mathbb{N}^*} \mathbb{F}_{p^n}$. En déduire que tout élément non nul de $\mathbb{F}_p$ est une racine de l'unité.

4 Corps finis.

Exercice 28 — Cube et corps fini. Soit K un corps fini de caractéristique p et $|\mathrm{K}|$ son cardinal.

a) On suppose $p \neq 2$. Montrer l'équivalence

(i) Tout élément de K est un cube ;
(ii) -3 n'est pas un carré dans K.

b) On suppose $p = 3$. Quelle est la situation ?

c) On suppose $p = 2$. Quelle est la situation ?

Exercice 29 — Sous-corps d'un corps fini. Déterminer les sous-corps $\mathbb{F}_{2^6} = \mathbb{F}_{64}$.

Exercice 30 — Polynôme irréductible sur un corps fini.

a) Quels sont les polynômes irréductibles sur $\mathbb{F}_2$ de degré 1, 2 et 3, 4 ?

b) Quels sont les polynômes irréductibles sur $\mathbb{F}_3$ de degré 1, 2 et 3 ?

c) Factoriser sur $\mathbb{F}_2$ les polynômes suivants $\mathrm{X}^4 + \mathrm{X}^2 + 1$, $\mathrm{X}^5 + \mathrm{X}^4 + 1$.

d) Factoriser sur $\mathbb{F}_3$ le polynôme $\mathrm{X}^4 + 1$.

e) Factoriser sur $\mathbb{F}_p$ le polynôme $\mathrm{X}^p - \mathrm{X} + 1$.

f) Pour quelles valeurs de $q = p^n$, $X^4 + 1$ est-il scindé sur $\mathbb{F}_q$?

Exercice 31 — Calcul dans les corps finis.

a) Calculer s'il existe l'inverse de $X^2 + 1$ dans $\mathbb{F}_2[X]/(X^5 + X^2 + 1)$.

b) L'anneau $\mathbb{F}_2[X]/(X^5 + X^2 + 1)$ est-il un corps ?

c) Montrer que $\mathbb{F}_5[X]/(X^2+X+2)$ et $\mathbb{F}_5[X]/(X^2+2)$ sont des corps. Quel est leur cardinal ? On note α (resp. β) la classe de X dans $\mathbb{F}_5[X]/(X^2 + X + 2)$ (resp. dans $\mathbb{F}_5[X]/(X^2 + 2)$) Définit-on un morphisme de $\mathbb{F}_5$-algèbres en posant $\varphi(\alpha) = \beta^6$ (resp. $\varphi(\alpha) = 2\beta + 2$) ? Si oui, est-ce un isomorphisme ?

Exercice 32 — Racines de l'unité. Soient p un nombre premier, $n \in \mathbb{N}^*$ et $q = p^n$.

a) Montrer que $X^2 + X + 1$ est irréductible sur $\mathbb{F}_q$ si et seulement si $q = -1[3]$ (on pourra distinguer le cas où $p = 3$ et $p \neq 3$ et remarquer que $(X^2 + X + 1)(X - 1) = X^3 - 1$).

b) Montrer que $X^2 + 1$ est irréductible sur $\mathbb{F}_q$ si et seulement si $q = -1[4]$ (on pourra distinguer le cas où $p = 2$ et $p \neq 2$ et remarquer que $(X^2 + 1)(X^2 - 1) = X^4 - 1$).

c) En déduire que si $q = -1[12]$ alors $\mathbb{F}_q[X]/X^2 + X + 1$ et $\mathbb{F}_q[X]/X^2 + 1$ sont isomorphes et décrire de façon explicite un isomorphisme entre les deux.

Exercice 33 — Cyclotomie dans les corps finis. On rappelle les propriétés suivantes des polynômes cyclotomiques sur $\mathbb{Q}$ (les redémontrer en cas de doute) :

$$\Phi_n \in \mathbb{Z}[X], \qquad \deg(\Phi_n) = \varphi(n), \qquad X^n - 1 = \prod_{d|n} \Phi_d$$

a) Soient k un corps de caractéristique p premier et $n \in \mathbb{N}$. Existe-t-il une extension de k contenant des racines **primitives** n^{e} de l'unité ? (on pourra écrire $n = p^r m$ avec $m \wedge p = 1$).

Soit q une puissance d'un entier premier p et soit $n \geqslant 1$ un entier, premier à p. On pose $k = \mathbb{F}_q$. On notera r l'ordre de q dans $(\mathbb{Z}/n\mathbb{Z})^*$. Pour tout entier d, on notera $\Phi_d \in \mathbb{F}_p[X]$ le polynôme obtenu à partir de $\Phi_d \in \mathbb{Z}[X]$ en réduisant les coefficients modulo p. On fixe $P \in \mathbb{F}_q[X]$ un facteur irréductible de Φ_n et de degré noté s. On fixe également $x \in \mathbb{F}_q[X]/(P)$ une racine de P. On pose $K = \mathbb{F}_q[X]/(P)$.

b) Montrer que $X^n - 1 \in k[X]$ est sans facteur carré. Montrer que les racines de $\Phi_n \in k[X]$ dans k sont exactement les racines primitives n^{e} de 1 dans k (c'est-à-dire les éléments de $k^\times$ qui sont d'ordre exactement n).

c) Montrer que $x^{q^s - 1} = 1$. En déduire que n divise $q^s - 1$ puis que $s \geqslant r$.

d) Montrer que $x^{q^r} = x$. En déduire que $s \leqslant r$ puis que $r = s$.

e) En déduire que la décomposition de $\Phi_n \in k[X]$ est un produit de polynômes irréductibles tous de degré r. Montrer que $\Phi_n \in \mathbb{F}_q[X]$ est irréductible si et seulement si q engendre $(\mathbb{Z}/n\mathbb{Z})^*$.

f) Établir une méthode pour calculer dans un corps fini (par exemple dans $\mathbb{F}_9$, dans $\mathbb{F}_{16}$).

Exercice 34 — Algorithme de Berlekamp : un développement classique. Soit p un entier premier et $q = p^n$. On considère $P \in \mathbb{F}_q[X]$ un polynôme de degré d. On pose $V = \mathbb{F}_q[X]/(P)$ et $W = \{f \in V,\ f^q = f\}$.

a) Montrer que l'application

$$\begin{cases} V \longrightarrow V \\ h \longmapsto h^q - h \end{cases}$$

est une application $\mathbb{F}_q$-linéaire. En déduire que W est un sous-espace vectoriel de V.

b) Supposons que P est sans facteur carré et écrivons $P = P_1 \cdots P_\ell$ comme produit de polynômes irréductibles de $\mathbb{F}_q[X]$ deux à deux non associés. Montrer que W est isomorphe, en tant que $\mathbb{F}_q$-espace vectoriel, à

$$\prod_{i=1}^{\ell} \{f \in \mathbb{F}_q[X]/(P_i), \quad f^q = f\}.$$

En déduire que la dimension de W est ℓ. En déduire un critère d'irréductibilité sur $\mathbb{F}_q[X]$.

c) On conserve les hypothèses et notations de la question précédente et on suppose que $\ell > 1$. Montrer qu'il existe $h \in W \smallsetminus \{0\}$ ainsi que $H \in \mathbb{F}_q[X]$ relevant h et tel que $\deg(H) < \deg(P)$ et H est non constant. Pour $\alpha \in \mathbb{F}_q$, posons $H_\alpha = \operatorname{pgcd}(H - \alpha, P)$. Montrer que les H_α sont premiers entre eux deux à deux et que

$$P = \prod_{\alpha \in \mathbb{F}_q} H_\alpha.$$

Qu'en conclure ? En déduire un algorithme de factorisation de P.

d) Supposons à présent que $\mathrm{P} = {\mathrm{P}_1}^{n_1} \cdots {\mathrm{P}_\ell}^{n_\ell}$ avec $\mathrm{P}_1, \ldots, \mathrm{P}_\ell$ polynômes irréductibles de $\mathbb{F}_q[\mathrm{X}]$ deux à deux distincts et $n_1, \ldots, n_\ell \geqslant 1$. À quelle condition, la factorisation $\mathrm{P} = \mathrm{pgcd}\,(\mathrm{P}, \mathrm{P}') \cdot (\mathrm{P}/\mathrm{pgcd}\,(\mathrm{P}, \mathrm{P}'))$ (qui s'obtient par l'algorithme d'Euclide) fournit-elle une vraie factorisation de P (c'est-à-dire que les deux facteurs sont non triviaux). En particulier, on montrera $\mathrm{P} = \mathrm{pgcd}\,(\mathrm{P}, \mathrm{P}')$ si et seulement si $\mathrm{P}' = 0$ si et seulement si il existe $\mathrm{Q} \in \mathbb{F}_q[\mathrm{X}]$ tel que $\mathrm{P} = \mathrm{Q}^p$ (et on donnera une méthode de construction de Q, expliquer pourquoi cette méthode est particulière simple sur $\mathbb{F}_p$). En déduire un algorithme de factorisation de P.

5 Extensions séparables.

Exercice 35 — Divisibilité et changement de corps. Soit K une extension du corps k et $\mathrm{U}, \mathrm{V} \in k[\mathrm{X}]$ avec $\mathrm{V} \neq 0$.

a) On considère $\mathrm{U} = \mathrm{V}\mathrm{Q}_k + \mathrm{R}_k$ la division euclidienne de U par V dans $k[\mathrm{X}]$ c'est-à-dire $\mathrm{Q}_k, \mathrm{R}_k \in k[\mathrm{X}]$ et $\deg \mathrm{R}_k < \deg \mathrm{V}$. De même, on considère $\mathrm{U} = \mathrm{V}\mathrm{Q}_\mathrm{K} + \mathrm{R}_\mathrm{K}$ la division euclidienne de U par V dans $k[\mathrm{X}]$ c'est-à-dire $\mathrm{Q}_\mathrm{K}, \mathrm{R}_\mathrm{K} \in \mathrm{K}[\mathrm{X}]$ et $\deg \mathrm{R}_\mathrm{K} < \deg \mathrm{V}$. Montrer que $\mathrm{Q}_k = \mathrm{Q}_\mathrm{K}$ et $\mathrm{R}_k = \mathrm{R}_\mathrm{K}$.

b) En déduire que $\mathrm{V} \mid \mathrm{U}$ dans $k[\mathrm{X}]$ si et seulement si $\mathrm{V} \mid \mathrm{U}$ dans $\mathrm{K}[\mathrm{X}]$.

c) En déduire que le pgcd de U et C ne dépend pas du corps : si $\mathrm{P}_k = \mathrm{pgcd}\,(\mathrm{U}, \mathrm{V})$ dans $k[\mathrm{X}]$ et $\mathrm{P}_\mathrm{K} = \mathrm{pgcd}\,(\mathrm{U}, \mathrm{V})$ dans $\mathrm{K}[\mathrm{X}]$ alors il existe $\lambda \in \mathrm{K}^\times$ tel que $\mathrm{P}_\mathrm{K} = \lambda \mathrm{P}_k$.

Exercice 36 — Dérivée d'un polynôme. Soit $\mathrm{P} = \sum_{i=0}^{n} a_i \mathrm{X}^i \in k[\mathrm{X}]$. On définit le *polynôme dérivé de* P par

$$\mathrm{P}' = \sum_{i=0}^{n} i a_i \mathrm{X}^{i-1} \in k[\mathrm{X}]\,.$$

a) Montrer que l'application

$$d\colon \begin{cases} k[\mathrm{X}] \longrightarrow k[\mathrm{X}] \\ \mathrm{P} \quad \longmapsto \mathrm{P}' \end{cases}$$

est k-linéaire et vérifie $(\mathrm{PQ})' = \mathrm{PQ}' + \mathrm{P}'\mathrm{Q}$ pour tous $\mathrm{P}, \mathrm{Q} \in k[\mathrm{X}]$.

b) Montrer que si $\mathrm{car} k = 0$ alors $\mathrm{Ker}\, d$ est l'ensemble des polynômes constant.

c) Montrer que si $\mathrm{car} k = p$ alors $\mathrm{Ker}\, d = k[\mathrm{X}^p]$.

d) Montrer que $(\mathrm{P}^n)' = n\mathrm{P}'\mathrm{P}^{n-1}$.

e) Soient $\mathrm{P}_1, \ldots, \mathrm{P}_r \in k[\mathrm{X}]$. Vérifier que $(\mathrm{P}_1 \cdots \mathrm{P}_r)' = \sum_{i=1}^{r} \mathrm{P}_i' \prod_{j \neq i} \mathrm{P}_j$

f) Calculer $({\mathrm{P}_1}^{n_1} \cdots {\mathrm{P}_r}^{n_r})'$.

g) Déterminer les applications k-linéaires D telles que $\mathrm{D}(\mathrm{PQ}) = \mathrm{P}\mathrm{D}(\mathrm{Q}) + \mathrm{D}(\mathrm{Q})\mathrm{P}$. Montrer qu'une telle application vérifie la formule de Leibniz

$$\mathrm{D}^r(\mathrm{PQ}) = \sum_{i=0}^{r} \binom{r}{i} \mathrm{D}^i(\mathrm{P})\mathrm{D}^{r-i}(\mathrm{Q})\,.$$

Exercice 37 — Dérivation et multiplicité de racines.

a) Soient $\mathrm{P} \in k[\mathrm{X}]$ et $a \in k$. Montrer que a est une racine multiple de P si et seulement si $\mathrm{P}(a) = \mathrm{P}'(a) = 0$ si et seulement si $(\mathrm{X} - a) \mid \mathrm{P}$ et $(\mathrm{X} - a) \mid \mathrm{P}'$.

b) Soient $\mathrm{P} \in k[\mathrm{X}]$, $a \in k$ et $n \in \mathbb{N}$. Montrer que si $(\mathrm{X} - a)^n \mid \mathrm{P}$ alors $\mathrm{P}(a) = \mathrm{P}'(a) = \cdots = \mathrm{P}^{(n-1)}(a) = 0$. Montrer que la réciproque est fausse en générale.

c) Montrer que la réciproque est vraie en caractéristique nulle.

Ainsi en toute généralité, la dérivation permet de lire les racines multiples mais pas la multiplicité des racines (sauf en caractéristique nulle).

Exercice 38 — Polynôme premier avec sa dérivée. Soient k un corps, $\mathrm{P} \in k[\mathrm{X}]$ non constant. On désigne par Ω une extension algébriquement close de k ; par K un corps de décomposition de P sur k et par L une extension de k.

a) Vérifier l'équivalence des propriétés suivantes

(i) $\mathrm{pgcd}\,(\mathrm{P}, \mathrm{P}') = 1$;

(ii) pour toute L, P et P′ sont sans racine commune ;

(*iii*) pour toute L algébrique, P et P′ sont sans racine commune ;
(*iv*) P et P′ n'ont pas de racine commune dans K ;
(*v*) P et P′ n'ont pas de racine commune dans Ω ;
(*vi*) pour toute L, P n'a que des racines simples dans L ;
(*vii*) pour toute L algébrique, P n'a que des racines simples dans L ;
(*viii*) P n'a que des racines simples dans K ;
(*ix*) P n'a que des racines simples dans Ω ;
(*x*) il existe L telle que P se factorise en un produit de polynôme de degré 1 **deux à deux distincts** dans L[X] ;
(*xi*) P se factorise en un produit de polynôme de degré 1 **deux à deux distincts** dans K[X] ;
(*xii*) P se factorise en un produit de polynôme de degré 1 **deux à deux distincts** dans Ω[X].

b) On suppose de plus que P est irréductible. Montrer que les propriétés précédentes sont équivalentes à

(*xiii*) $\mathrm{P}' \neq 0$;
(*xiv*) il existe une extension L de k tel que P ait une racine simple.

Un polynôme **irréductible** vérifiant ces propriétés équivalentes est dit *séparable*.

Exercice 39 — Polynôme séparable. Soit $\mathrm{P} \in k[\mathrm{X}]$ un polynôme irréductible.

a) Montrer que $\mathrm{P}' = 0$ ou $\mathrm{pgcd}\,(\mathrm{P}, \mathrm{P}') = 1$.

b) En déduire qu'en caractéristique nulle un polynôme irréductible est toujours séparable.

c) Montrer que s'il existe un polynôme $\mathrm{P} \in k[\mathrm{X}]$ irréductible qui n'est pas séparable alors $\mathrm{car} k = p$ est première et $k \neq k^{[p]} := \{x^p,\ x \in k\}$.

d) En déduire que sur un corps fini tout polynôme irréductible est séparable.

e) Soient k un corps de caractéristique p première et $a \in k \smallsetminus k^{[p]}$. Montrer que, pour tout $n \in \mathbb{N}$, le polynôme $\mathrm{P} = \mathrm{X}^{p^n} - a$ est irréductible sur k (on pourra factoriser P dans un corps de rupture de P) et n'est pas séparable si $n \geqslant 1$. En déduire une réciproque à la question **c**.

Définition 7 — Élément séparable. Soient K une extension de k et $x \in \mathrm{K}$. On dit que x est *séparable* sur k si le polynôme minimal de x sur k est séparable. Un élément séparable est algébrique.

Définition 8 — Extension algébrique. Soit K une extension de k. On dit que K est une *extension séparable de k* si toute élément de K est séparable sur k. Une extension séparable est algébrique.

Exercice 40 — Corps parfait.

a) Montrer que $\mathbb{F}_p(\mathrm{X}^p) \subset \mathbb{F}_p(\mathrm{X})$ est une extension non séparable.

Soit k un corps de caractéristique p. Si $p = 0$, on note $k^{[p]} := k$. Si p est premier, on note $k^{[p]} := \{x^p \in k,\ x \in k\}$. Soit Ω une clôture algébrique de k.

b) Montrer que les propositions suivantes sont équivalentes

(*i*) $k = k^{[p]}$;
(*ii*) tout élément irréductible de $k[\mathrm{X}]$ est séparable ;
(*iii*) tout extension algébrique de k est séparable ;
(*iv*) Ω est une extension séparable de k.

Un corps vérifiant ces conditions est appelé *corps parfait*.

c) Montrer qu'un corps fini, un corps algébriquement clos et un corps de caractéristique nulle sont parfait.

Exercice 41 — Le théorème de l'élément primitif en caractéristique nulle. Soit (L : K) une extension finie de caractéristique nulle. Supposons que $\mathrm{L} = \mathrm{K}[x, y]$ avec $x, y \in \mathrm{L}$. On considère P_x (resp. P_y) le polynôme minimal de x (resp. y) sur K et M le corps de décomposition de $\mathrm{P}_x\mathrm{P}_y$. Écrivons dans M[X]

$$\mathrm{P}_x = (\mathrm{X} - x) \prod_{i=2}^{m} (\mathrm{X} - x_i) \qquad \text{et} \qquad \mathrm{P}_y = (\mathrm{X} - y) \prod_{i=2}^{n} (\mathrm{X} - y_i).$$

a) Montrer qu'il existe $t \in \mathrm{K}^\times$ tel que pour $i \geqslant 1$ et $j \geqslant 2$ on ait $z := x + ty \neq x_i + ty_j$.

b) Posons $\mathrm{K}' = \mathrm{K}[z]$ et $\mathrm{F} = \mathrm{P}_x(z - t\mathrm{X}) \in \mathrm{K}'[\mathrm{X}]$. Montrer que $\mathrm{X} - y = \mathrm{pgcd}\,(\mathrm{F}, \mathrm{P}_y)$ (on utilisera le fait que les y_i et y sont deux à deux distincts).

c) En déduire que $y \in \mathrm{K}'$ puis que $\mathrm{L} = \mathrm{K}'$.

d) En déduire que toute extension finie en caractéristique nulle est monogène.

e) Exprimer $\mathbb{Q}[i, \sqrt{2}]$ (resp. $\mathbb{Q}[j, \sqrt{2}]$, resp. $\mathbb{Q}[i, j, \sqrt{2}]$) comme extension monogène de $\mathbb{Q}$.

f) Exprimer le corps de décomposition sur $\mathbb{Q}$ de $\mathrm{X}^3 - 2$ (resp. $\mathrm{X}^4 - 2$) comme extension monogène de $\mathbb{Q}$.

Exercice 42 — Degré séparable. Soit k un corps, K une extension **algébrique** de k et $j : k \to \Omega$ une extension algébriquement close.

a) Montrer que $|\mathrm{Hom}_{k-\mathrm{alg.}}(\mathrm{K}, \Omega)|$ ne dépend pas du couple (Ω, j) (on pourra se ramener à la clôture algébrique de k contenu dans Ω). On définit alors le *degré séparable de* K *sur* k et on note

$$[\mathrm{K} : k]_{\mathrm{s}} := |\mathrm{Hom}_{k-\mathrm{alg.}}(\mathrm{K}, \Omega)|$$

b) Soit L une extension algébrique de K. Montrer que $[\mathrm{L} : k]_{\mathrm{s}} = [\mathrm{L} : \mathrm{K}]_{\mathrm{s}}[\mathrm{K} : k]_{\mathrm{s}}$.

c) Soit $(k(x) : k)$ une extension algébrique monogène. Montrer que $[k(x) : k]_{\mathrm{s}}$ est le nombre de racine distinctes de P le polynôme minimal de x dans Ω. En déduire que $[k(x) : k]_{\mathrm{s}} \leqslant [k(x) : k] = \deg \mathrm{P}$.

d) Montrer l'équivalence des propriétés suivantes

(i) $[k(x) : k]_{\mathrm{s}} = [k(x) : k]$;
(ii) x est séparable sur k ;
(iii) P est séparable sur k ;
(iv) $k[\mathrm{X}]/(\mathrm{P}) \overset{k\text{-ext.}}{\simeq} k(x)$ est séparable sur k.

e) Soit K une extension finie de k. Montrer $[\mathrm{K} : k]_{\mathrm{s}} \leqslant [\mathrm{K} : k]$

f) Soit K une extension finie de k. Montrer $[\mathrm{K} : k]_{\mathrm{s}} = [\mathrm{K} : k]$ si et seulement si $(\mathrm{K} : k)$ est séparable.

g) Soit K une extension de k et L une extension de k. Alors $(\mathrm{L} : k)$ est séparable si et seulement si $(\mathrm{K} : k)$ est séparable et $(\mathrm{L} : \mathrm{K})$ séparable.

Exercice 43 — Des exemples.

a) Calculer le nombre de morphismes de corps $\mathbb{Q}(\sqrt[3]{2}, j) \to \mathbb{C}$.

b) Soit $\mathbb{F}_2(\mathrm{X})$ le corps des fractions rationnelles en une indéterminée à coefficients dans $\mathbb{F}_2$, soit Ω une clôture algébrique de $\mathbb{F}_2(\mathrm{X})$. Déterminer le nombre de morphismes de corps $\mathbb{F}_2(\mathrm{X}) \to \Omega$ prolongeant l'inclusion $\mathbb{F}_2(\mathrm{X}^2) \hookrightarrow \Omega$.

Exercice 44 — Le théorème de l'élément primitif. Soient $(\mathrm{L} : k)$ une extension finie de degré n et Ω une clôture algébrique de L.

a) Montrer qu'il existe $x \in \mathrm{L}$ sur lequel les k-morphismes de L dans Ω prennent des valeurs deux à deux distinctes (on pourra distinguer deux cas selon que k est fini ou non).

b) On suppose que $(\mathrm{L} : k)$ est séparable. Vérifier que la construction de x assure que $[k(x) : k]_{\mathrm{s}} = n$. En déduire que $\mathrm{L} = k(x)$.

Ainsi une extension séparable finie est monogène.

Exercice 45 — Un exemple d'extension non monogène. Soient p un nombre premier, k un corps de caractéristique p et X, Y deux indéterminées sur k. On considère $\mathrm{K} = k(\mathrm{X}, \mathrm{Y})$ et $\mathrm{L} = k(\mathrm{X}^p, \mathrm{Y}^p) \subset \mathrm{K}$.

a) Déterminer $[\mathrm{K} : \mathrm{L}]$.

b) Pour $x \in \mathrm{K}$, déterminer $[\mathrm{L}(x) : \mathrm{L}]$. En déduire que l'extension $\mathrm{L} \subset \mathrm{K}$ n'est pas monogène ni séparable.

c) Déterminer l'ensemble des éléments de K qui sont séparables sur L.