2. Extensions de corps : extensions de degré fini, extensions algébriques.

Exercice 2.1 1. Donner un exemple d'extension non algébrique de $\mathbb{Q}$. Donner un exemple d'extension algébrique de $\mathbb{Q}$ qui n'est pas une extension de degré fini.

2. Soit K un corps dénombrable. Que peut-on dire de la cardinialité d'une extension algébirque de K ?

Exercice 2.2 (Exemple de nombre transcendant)

1. Théorème de Liouville. Soit a un nombre algébrique réel sur $\mathbb{Q}$ de degré $n > 0$ (i.e. $[\mathbb{Q}(a) : \mathbb{Q}] = n$). Montrer qu'il existe un réel $c > 0$ tel que pour tout rationnel $\frac{p}{q}$, avec $q > 0$, on ait
$$\left| a - \frac{p}{q} \right| > \frac{c}{q^n}.$$
Indication : considérer un polynôme P irréductible de degré n dans $\mathbb{Z}[X]$ et annulant a et considérer $\delta > 0$ tel que P' ne s'annule pas sur $[a - \delta, a + \delta]$ et appliquer le théorème des accroissements finis pour le cas où $\left| a - \frac{p}{q} \right| \leq \delta$.

2. En déduire la transcendance de
$$a = \sum_{i>0} a_i 10^{-i!}$$
pour toute suite (a_i) d'entiers naturels compris entre 1 et 9.

Exercice 2.3 Soit P le polynôme $X^3 - 2$ de $\mathbb{Q}[X]$.

1. Déterminer un corps K de rupture sur $\mathbb{Q}$ de P. Que vaut $[K : \mathbb{Q}]$?
2. Décrire le corps L de racines sur $\mathbb{Q}$ de P. Calculer $[L : \mathbb{Q}]$.

Exercice 2.4 1. Soit K un corps et L une extension de K qui est algébriquement close. Notons $\tilde{K}$ l'ensemble des éléments algébriques sur K dans L. Montrer que $\tilde{K}$ est un corps, puis que $\tilde{K}$ est algébriquement clos.

2. Théorème de Steinitz. Soit K un corps. On va montrer qu'il existe une extension algébriquement close de K.
   (a) Soit pour chaque polynôme P sur K de degré non nul, une variable X_P et considérons l'idéal I engendré par les élements $P(X_P)$ de l'anneau $K[X_P : P]$. Montrer que I ne contient pas 1.
   (b) En déduire qu'il existe un idéal J maximal contenant I et qu'il existe une extension K_1 de K contenant une racine pour chaque polynôme P sur K de degré non nul.
   (c) Conclure à l'aide d'une suite de telles extensions.

3. En déduire que tout corps a une extension algébrique qui est algébriquement close. On appelle une telle extension une clôture algébrique de K. En utilisant le théorème de prolongement des morphismes à une extension algébrique (voir cours), on vérifie facilement que toutes les clôtures algébriques de K sont isomorphes.

Exercice 2.5 Soit $\alpha = \sqrt{2} + \sqrt{3} \in \mathbb{C}$.

1. Montrer que $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\alpha)$.
2. Quel est le polynôme minimal de α sur $\mathbb{Q}$? Même question sur $\mathbb{Q}(\sqrt{2})$ et $\mathbb{Q}(\sqrt{3})$.
3. Vérifier que α et α^{-1} sont conjugués sur $\mathbb{Q}$. Quel est le corps de racines de P_α sur $\mathbb{Q}$?
4. Soit K un sous-corps de $\mathbb{Q}(\alpha)$; en remarquant que le polynôme minimal de α sur K divise P_α dans $K[X]$, montrer que
$$K = \mathbb{Q},\ \mathbb{Q}(\sqrt{2}),\ \mathbb{Q}(\sqrt{3}),\ \mathbb{Q}(\sqrt{6}) \text{ ou } \mathbb{Q}(\alpha).$$

Exercice 2.6 (Extensions quadratiques de $\mathbb{Q}$) Soit K une extension de degré 2 sur $\mathbb{Q}$. Montrer que $K = \mathbb{Q}(\sqrt{a})$ où a est un entier sans facteur carré, *i.e.* tel qu'il n'existe pas de nombre premier p avec $p^2 \mid a$.

Exercice 2.7 *Soit α un élément algébrique sur K tel que $[K(\alpha) : K]$ est impair. Montrer que $K(\alpha) = K(\alpha^2)$.*

Exercice 2.8

1. Vérifier que le polynôme
$$P(X) = X^3 - 3X + 1$$
est irréductible sur $\mathbb{Q}$.
2. Soit $\alpha \in \mathbb{C}$ une racine de P ; montrer que $\alpha^2 - 2$ et $-\alpha^2 - \alpha + 2$ sont aussi racines de P. Quel est le corps des racines de P sur $\mathbb{Q}$?
3. Soit $\omega \in \mathbb{C}$ une racine de
$$X^6 + X^3 + 1.$$
Vérifier que $\omega^9 = 1$ et en déduire que $\omega + \omega^{-1}$ est racine de P. Quel est le polynôme minimal de ω sur $\mathbb{Q}(\alpha)$?
4. Prouver que $\mathbb{Q}(\alpha) = \mathbb{Q}(\omega) \cap \mathbb{R}$.

Exercice 2.9 Soient K un corps et $P(X) \in K[X]$ un polynôme non constant de degré d. Notons Ω une clôture algébrique de K.

1. Soit α une racine de P dans Ω.
   a) Montrer que $[K(\alpha) : K] \leq d$.
   b) Prouver que $[K(\alpha) : K] = d$ si et seulement si P est irréductible sur K.
2. Soit $L \subset \Omega$ une extension de degré fini n sur K. On suppose que P est irréductible sur K et que n et $\deg P$ sont premiers entre eux. Montrer que P est irréductible sur L.
   Application : Soit $\alpha \in \mathbb{C}$ une racine de $X^7 - 6X + 3$, alors $X^{2000} + 10X^8 - 45$ est irréductible sur $\mathbb{Q}(\alpha)$.

Exercice 2.10 Soient K un corps et $P \in K[X]$ un polynôme non constant. Notons $d_1, d_2, \ldots, d_r$ les degrés de ses facteurs irréductibles sur K. Soit L le corps des racines de P sur K. Montrer que $[L : K]$ divise $\prod_{i=1}^{r} (d_i\,!)$.

Exercice 2.11 Soient p un nombre premier impair et Ω un corps algébriquement clos de caractéristique $\neq p$. Notons K le sous-corps premier de Ω.

1. Montrer qu'il existe $\omega \in \Omega$ avec $\omega^p = 1$ et $\omega \neq 1$.
2. Pour tout entier $x \in \mathbb{Z}$, on définit son symbole de Legendre (modulo p) par

$$\left(\frac{x}{p}\right) = \begin{cases} 0 & \text{si } x \text{ est un multiple de } p, \\ 1 & \text{si } x \text{ est un carré modulo } p, \\ -1 & \text{si } x \text{ est n'est pas un carré modulo } p. \end{cases}$$

a) On pose

$$s = \sum_{1 \leq x \leq p-1} \left(\frac{x}{p}\right) \omega^x.$$

Montrer que

$$s^2 = \sum_{1 \leq z \leq p-1} \left(\frac{z}{p}\right) \left(\sum_{1 \leq x \leq p-1} \omega^{x(1+z)} \right)$$

et en déduire que $s^2 = p \left(\frac{-1}{p}\right)$.

b) En déduire que

$$p \equiv 1 \pmod 4 \Rightarrow \sqrt{p} \in K(\omega)$$

et

$$p \equiv -1 \pmod 4 \Rightarrow \sqrt{-p} \in K(\omega).$$

Exercice 2.12 Le but de cet exercice est de montrer que toute extension quadratique de $\mathbb{Q}$ est contenu dans une extension cyclotomique de $\mathbb{Q}$.

Soit K une extension de degré 2 sur $\mathbb{Q}$. Montrer qu'il existe un entier $n \geq 1$ tel que $K \subset \mathbb{Q}(e^{2i\pi/n})$. (Utiliser les résultats des exercices 2.6 et 2.11.)

Exercice 2.13 (Elément algébrique de degré 4 qui n'est pas constructible)

1. Montrer que le polynôme $P(X) = X^4 - X - 1$ est irréductible sur $\mathbb{Q}$ et possède 4 racines distinctes x_1, x_2, x_3, x_4 dans $\mathbb{C}$.
2. Montrer que $u = x_1\,x_2 + x_3\,x_4$ est racine du polynôme $X^3 + 4X - 1$.
   (On pourra remarquer que $u = t - 1/t$ où $t = x_1 x_2$ et calculer $u^4 + 4u^2 - u$.)
3. En déduire que, pour tout i, x_i n'est pas constructible.
4. Montrer que $[\mathbb{Q}(x_1, x_2) : \mathbb{Q}] = 12$ et que si K est le corps des racines de P sur $\mathbb{Q}$, alors $[K : \mathbb{Q}] = 24$.

Exercice 2.14 Soit L/K une extension algébrique.

1. On suppose qu'il existe x tel que $L = K(x)$. Soit P le polynôme minimal de x sur K.
   a. Soit M un sous-corps de L, contenant K. Montrer qu'il existe un facteur unitaire Q de P dans $L[X]$ tel que M soit engendré sur K par les coefficients de Q.
   b. En déduire que l'extension L/K n'a qu'un nombre fini de sous-extensions.
2. Réciproquement, on suppose que l'extension L/K n'a qu'un nombre fini de sous-extensions.
   a. Montrer que $[L : K]$ est fini.
   b. Si K est fini, prouver qu'il existe x avec $L = K(x)$.
   c. Si K est infini, montrer que pour tout x, y dans L, il existe $\lambda \in K$ tel que $K(x, y) = K(x + \lambda y)$. En déduire qu'il existe x tel que $L = K(x)$.

Exercice 2.15 Soit p un nombre premier, $L = \mathbb{F}_p(X, Y)$ le corps des fractions rationnelles à deux variables. On pose $K = \mathbb{F}_p(X^p, Y^p) \subset L$.

1. Montrer que $[L : K] = p^2$, et que pour tout x dans L, $x^p \in K$.
2. En déduire qu'il n'existe pas de $x \in L$ tel que $L = K(x)$.