1. Extensions de degré fini, extensions algébriques.

Exercice 1.1

1. Déterminer les morphismes de $\mathbb{Q}(i)$ dans $\mathbb{C}$.
2. Déterminer les morphismes de $\mathbb{Q}(j)$ dans $\mathbb{C}$.
3. Les corps $\mathbb{Q}(i)$ et $\mathbb{Q}(j)$ sont-ils isomorphes ?

Exercice 1.2

1. Montrer que $\mathbb{Q}(\sqrt{2}) \cap \mathbb{Q}(\sqrt{3}) = \mathbb{Q}$.
2. En déduire le degré de la $\mathbb{Q}$-extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.
3. Soit $\alpha = \sqrt{2} + \sqrt{3}$. Montrer que $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\alpha)$.
4. Déterminer le polynôme minimal P de α sur $\mathbb{Q}$ et toutes les racines de P.
5. Déterminer les automorphismes de $\mathbb{Q}(\alpha)$.
6. Soit K un sous-corps de $\mathbb{Q}(\alpha)$; en remarquant que le polynôme minimal de α sur K divise P 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 1.3 (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 1.4 Soit α un élément algébrique sur K tel que $[K(\alpha) : K]$ est impair. Montrer que $K(\alpha) = K(\alpha^2)$.

Exercice 1.5

1. Quelles sont les extensions de degré finis de $\mathbb{R}$ et de $\mathbb{C}$?
2. Montrer que pour tout entier $n \geq 1$, il existe une extension de $\mathbb{Q}$ de degré n.

Exercice 1.6

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 1.7 Soient K un corps contenu dans un corps algébriquement clos Ω et $P(X) \in K[X]$ un polynôme non constant de degré d.

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 1.8 Soit K un corps. On appelle *extension algébrique* de K une extension qui ne contient que des éléments algébriques sur K. On appelle *clôture algébrique* de K une extension algébrique de K qui est de plus algébriquement close.

1. Donner un exemple d'extension algébrique de $\mathbb{Q}$ qui n'est pas une extension de degré fini.
2. Montrer que si L est une extension algébrique de K et M est une extension algébrique de L alors M est une extension algébrique de K.
3. On suppose que K est contenu dans un corps algébriquement clos Ω. On note $\tilde{K}$ l'ensemble des éléments de Ω algébriques sur K. Montrer que $\tilde{K}$ est un corps et que c'est en fait une clôture algébrique de K.

Exercice 1.9 Soit K un corps fini ou dénombrable.

1. Quel est la cardinalité de $K[X]$?
2. En déduire que toute extension algébrique de K est fini ou dénombrable.

Exercice 1.10 (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 1.11 Soit K un corps et P un polynôme irréductible de $K[X]$ de degré n.

1. On dit qu'une extension L de K est un *corps de rupture* de P si elle est engendrée par L et une racine de P. Montrer qu'un tel corps de rupture existe toujours.

2. On dit qu'une extension L de K est un *corps de décomposition* de P s'il existe $c, \alpha_1, \alpha_2, ..., \alpha_n \in L$ tel que $L = K(\alpha_1, ..., \alpha_n)$ et $P = c(X - \alpha_1) \cdots (X - \alpha_n)$. Montrer qu'un tel corps de décomposition existe.

Exercice 1.12 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 un corps de décomposition de P sur K. Montrer que $[L : K]$ divise $\prod_{i=1}^{r} (d_i\,!)$.

Exercice 1.13 (Théorème de Steinitz) On va montrer que tout corps K a une clôture algébrique.

1. Supposons dans un premier temps que K est fini ou dénombrable. A l'aide d'une suite dénombrable d'extensions de degré fini montrer qu'il existe une extension algébrique K_1 de K contenant une racine pour chaque polynôme P sur K de degré non nul. En réitérant un nombre dénombrable de fois, en déduire l'existence d'une clôture algébrique de K.
2. Pour montrer le théorème de Steinitz sans utiliser l'hypothèse ci-dessus, on va utiliser le fait que tout idéal propre d'un anneau est contenu dans un idéal maximal. Ce fait découle du lemme de Zorn (lemme équivalent à l'axiome du choix).
   (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) À l'aide d'une suite de telles extensions, montrer qu'il existe une extension algébriquement close de K. Conclure.

Exercice 1.14 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 1.15 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 1.3 et 1.14.)

Exercice 1.16 (Résolution des équations cubiques)
Méthode de Cardan (1501-1576)/Tartaglia (1500-1557).

Soit l'équation

$$(E) \;\; z^3 + pz + q = 0$$

avec $p, q \in \mathbb{Q}$

1. Soient z_1, z_2, z_3 les 3 racines dans $\mathbb{C}$ de (E). Exprimer le *discriminant* $\Delta := (z_1 - z_2)^2(z_2 - z_3)^2(z_1 - z_3)^2$ en fonction de p et q. (Indication : développer $z^3 + pz + q = (z - z_1)(z - z_2)(z - z_3)$).
2. Montrer que :

$$\begin{array}{lcl} \Delta = 0 & \Longleftrightarrow & z^3 + pz + q \text{ a une racine réelle double} \\ \Delta > 0 & \Longleftrightarrow & z^3 + pz + q \text{ a 3 racines réelles simples} \\ \Delta < 0 & \Longleftrightarrow & z^3 + pz + q \text{ a 2 racines complexes conjuguées et 1 racine réelle} \end{array}$$

3. Montrer que si

$$\begin{cases} u^3 + v^3 = -q \\ uv = -\frac{p}{3} \end{cases}$$

alors $z = u + v$ est racine de $z^3 + pz + q$.

4. En déduire que si z_1 et z_2 sont les racines de :

$$z^2 + qz - \frac{p^3}{27}$$

et si u, v sont des racines cubiques de z_1 et z_2 telles que : $uv = -\frac{p}{3}$ alors :

$$u + v, \; ju + j^2v, \; j^2u + jv$$

sont les racines de $z^3 + pz + q$.

5. Résoudre $z^3 - z - 1 = 0$.
6. Déterminer un changement de variable permettant de passer de la résolution d'une équation générale du troisième degré de la forme

$$ax^3 + bx^2 + cx + d = 0$$

à celle d'une équation de la forme (E).