2. Extensions algébriques, extensions normales, extensions séparables.

Exercice 2.1 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 2.2 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 2.3 (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 2.4 *Soit α un élément algébrique sur K tel que $[K(\alpha) : K]$ est impair. Montrer que $K(\alpha) = K(\alpha^2)$.*

Exercice 2.5

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 2.6 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 2.7 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 2.8 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 2.9 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 2.3 et 2.8.)

Exercice 2.10 (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 $t = x_1x_2$ 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 2.11 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 2.12 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 $L = K(x)$.

Exercice 2.13 Soit K un corps de caractéristique $p > 0$. Montrer que $K^p = \{x^p : x \in K\}$ est un sous-corps de K et que K/K^p est une extension normale.

Exercice 2.14 Soit q une puissance d'un nombre premier p, soit n un entier non divisible par p, $L = \mathbb{F}_q(Y)$ et $K = \mathbb{F}_q(Y^n)$.

1. Montrer que L/K est séparable.
2. Montrer que L/K est normale si et seulement si $q \equiv 1 \pmod{n}$.

Exercice 2.15 Soit L/K une extension algébrique, Ω une clôture algébrique de K contenant L. Le groupe G des K-automorphismes de Ω agit sur la Ω-algèbre $\Omega[X]$ par

$$\sigma\left(\sum_i \lambda_i X^i\right) = \sum_i \sigma(\lambda_i) X^i$$

où $\sigma \in G$ et $\sum_i \lambda_i X^i \in \Omega[X]$.

1. On suppose L/K normale. Soit $P \in K[X]$ irréductible sur K. Montrer que l'ensemble des facteurs irréductibles unitaires de P dans $L[X]$ est une G-orbite de $\Omega[X]$. En particulier, tous les facteurs irréductibles de P dans $L[X]$ ont même degré.
2. Réciproquement, supposons cette dernière condition vérifiée pour tout polynôme irréductible de $K[X]$. Prouver que L/K est normale.

Exercice 2.16 Soit p un nombre premier congru à ± 3 modulo 8. Montrer que pour tout quadruplet d'entiers relatifs $\alpha, \beta, \gamma, \delta$ avec $p \nmid \delta$, le polynôme

$$X^4 + p(\alpha X^3 + \beta X^2 + \gamma X + \delta)$$

est irréductible sur $\mathbb{Q}(\sqrt{2})$. (Indication : utiliser l'exercice précédent.)

Exercice 2.17 Soit K un corps fini, L une extension algébrique de K. Montrer que L/K est normale.

Exercice 2.18 Soit K un corps infini, Ω une clôture algébrique de K.

1. Soit $x, y \in \Omega$. On note P (resp. Q) le polynôme minimal de x (resp. y) sur K, $x_1 = x, x_2, \ldots, x_n$ (resp. $y_1 = y, y_2, \ldots, y_m$) les racines distinctes de P (resp. Q) dans Ω.
   a. Montrer qu'il existe $\lambda \in K^\times$ tel que
   $$\forall i \neq 1, \forall j \neq 1,\ \lambda x + y \neq \lambda x_i + y_j.$$
   On pose $z = \lambda x + y$.
   b. Montrer que $R(X) = Q(z - \lambda X)$ et $P(X)$ ont une seule racine commune dans Ω.
2. On suppose que x est séparable sur K. Calculer le polynôme minimal de x sur $K(z)$ et en déduire que $K(x, y) = K(z)$.
3. On suppose K parfait. Soient $x_1, x_2, \ldots, x_n \in \Omega$. Montrer qu'il existe $\lambda_1, \lambda_2, \ldots, \lambda_n$ dans K tels que :
   $$K(x_1, \ldots, x_n) = K\left(\lambda_1 x_1 + \cdots + \lambda_n x_n\right).$$

Exercice 2.19 On considère le polynôme de $\mathbb{Z}[X]$ suivant :

$$Q(X) = X^9 + 9X^8 - X^3 + 3X^2 - 3X + 11.$$

Soit p un nombre premier, on notera par la suite $\overline{Q}_p$ la réduction de Q modulo p.

1. Montrer que $X^3 - X - 1$ est irréductible dans $\mathbb{F}_3[X]$.
2. Décomposer $\overline{Q}_3$ en produit de polynômes irréductibles de $\mathbb{F}_3[X]$.
3. Soit $\alpha \in \bar{\mathbb{F}}_2$ une racine de $X^4 + X + 1$ où $\bar{\mathbb{F}}_2$ désigne une clôture algébrique de $\mathbb{F}_2$. Décrire l'orbite
   $$\{F^i(\alpha),\ i \geq 0\}$$
   où F désigne l'automorphisme de Frobenius de $\bar{\mathbb{F}}_2/\mathbb{F}_2$. En déduire que $X^4 + X + 1$ est irréductible sur $\mathbb{F}_2$.
4. Décomposer $\overline{Q}_2$ en produit de facteurs irréductibles de $\mathbb{F}_2[X]$.
5. Montrer que Q est irréductible sur $\mathbb{Q}$.