IV.— Théorème de l'élément primitif

Exercice 1 Soit α un élément algébrique sur K tel que $[K(\alpha):K]$ est impair. Montrer que $K(\alpha)=K(\alpha^2)$.

Exercice 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 $\mathbb{Q}(\sqrt{2},\sqrt{3})=\mathbb{Q}(\alpha)=\mathbb{Q}\oplus\mathbb{Q}\sqrt{2}\oplus\mathbb{Q}\sqrt{3}\oplus\mathbb{Q}\sqrt{6}$.
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 3

a) Déterminer le degré de l'extension $\mathbb{Q}(\sqrt{2},\sqrt[3]{3},\sqrt[5]{5})/\mathbb{Q}$.
b) Déterminer les plongements de $\mathbb{Q}(\sqrt{2},\sqrt[3]{3},\sqrt[5]{5})$ dans $\mathbb{C}$.
c) Trouver un élément primitif pour l'extension $\mathbb{Q}(\sqrt{2},\sqrt[3]{3},\sqrt[5]{5})/\mathbb{Q}$.

Exercice 4 Soit $\alpha:=\sqrt{2+\sqrt{2}}$.

a) Déterminer $f(X)\in\mathbb{Q}[X]$ le polynôme minimal de α sur $\mathbb{Q}$.
b) Montrer que le corps de décomposition de $f(X)$ sur $\mathbb{Q}$ est $\mathbb{Q}(\alpha)$.
c) Montrer que $\mathrm{Gal}_{\mathbb{Q}}(f)\simeq\mathbb{Z}/4\mathbb{Z}$.

Exercice 5 Soit $K\subseteq L$ une extension algébrique. On suppose que $L=K(x,y)$ avec $x,y\in L$ et y séparable sur K.

a) On suppose K infini. On note $x:=x_1,x_2,...,x_p$, $y:=y_1,...,y_q$ les racines de P_x et P_y les polynômes minimaux de x et y sur K (dans une clôture algébrique de L). Montrer qu'il existe $t\in K$ tel que les x_i+ty_j, $1\le i\le p$, $1\le j\le q$, soient deux à deux distincts.

b) On pose $z:=x+ty$. Quel est le pgcd des polynômes $P_x(z-tX)$ et $P_y(X)$.

c) Montrer que $L=K(z)$.

Exercice 6 Soit L/K une extension algébrique.

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.

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 7 (Séparabilité) On dit qu'un élément algébrique sur un corps k est séparable si son polynôme minimal est séparable. On dit qu'une extension algébrique K/k est séparable si tous ses éléments sont séparables sur k.

a) Soit k un corps. Soit $f \in k[X]$ un polynôme irréductible de degré n. Soit Ω une clôture algébrique de k. Montrer que les racines de f dans Ω sont toutes de multiplicité 1 si la caractéristique de k est nulle et sont toutes de la même multiplicité p^e, pour un certain e, si la caractéristique est $p > 0$.

b) Montrer que le nombre de racines de f est $\frac{n}{p^e} = \deg \frac{f}{\mathrm{pgcd}(f,f')}$. On appelle ce nombre le *degré réduit* de f.

c) Soit $x \in \Omega$. Montrer que le degré réduit du polynôme minimal de x sur k est aussi le nombre de $k-$plongements de $k(x)$ dans Ω.

d) Si L/k est une extension finie. Soit $j : k \to \Omega$ un plongement. On note $[L : k]_s$ le nombre de $k-$plongements de L dans Ω qui prolonge j. Montrer que $[L : k]_s$ ne dépend pas du j choisi.

e) Montrer que si $k \subseteq L \subseteq M$, alors : $[M : k]_s = [M : L]_s[L : k]_s$.

f) Montrer que si x est séparable algébrique sur k, alors l'extension $k(x)/k$ est séparable. En déduire que si x, y sont séparables algébriques sur k, alors $x + y$, xy aussi.

g) Soit k un corps dont toutes les extensions algébriques sont séparables. Montrer que k est de caractéristique nulle ou de caractéristique p avec $k^p = k$. Dans ce cas, on dit que k est un *corps parfait*.

Exercice 8 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 $L = K(x)$.
3. Montrer directement qu'il existe une infinité de corps entre K et L.