Feuille de TD n° 1

Exercice 1

a) Soit $y = e^{\frac{2i\pi}{5}}$. Vérifier que

$$(X - (y + y^{-1}))(X - (y^2 + y^{-2})) = X^2 + X - 1$$

et en déduire une expression de $2\cos\left(\frac{2\pi}{5}\right) = y + y^{-1}$ avec des radicaux.

b) Déterminer $[\mathbb{Q}\left(\cos(\frac{2\pi}{5})\right) : \mathbb{Q}]$ et justifier l'existence d'un automorphisme du corps $\mathbb{Q}\left(\cos(\frac{2\pi}{5})\right)$ qui envoie $\cos\left(\frac{2\pi}{5}\right)$ sur $\cos\left(\frac{4\pi}{5}\right)$.

Exercice 2 Racines des polynômes de degré 3

a) Montrer que sur un corps $\mathbb{K}$ quelconque un polynôme de degré 2 ou 3 est irréductible si et seulement s'il n'a pas de racine.

b) En déduire que les polynômes $X^3 - X - 1$, $X^3 - 3X + 1$ sont irréductibles sur $\mathbb{Q}$.

c) Montrer que l'unique racine réelle de $X^3 - X - 1$ est :

$$\sqrt[3]{\frac{1}{2} + \frac{1}{2}\sqrt{\frac{23}{27}}} + \sqrt[3]{\frac{1}{2} - \frac{1}{2}\sqrt{\frac{23}{27}}} \ .$$

Indication : chercher une solution sous la forme $x = u + v$.

d) Montrer que les racines de $X^3 - 3X + 1$ sont $2\cos\left(\frac{2\pi}{9}\right)$, $2\cos\left(\frac{4\pi}{9}\right)$, $2\cos\left(\frac{8\pi}{9}\right)$. Vérifier que chacune de ces racines peut s'écrire

$$\sqrt[3]{j} + \frac{1}{\sqrt[3]{j}} \ .$$

Exercice 3

Vérifier que les anneaux suivants sont des corps :

a) $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ (p premier), $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[i]$, $\mathbb{C}(X, Y)$.

b) $\mathbb{C}((T)) = \{\sum_{n \geq n_0} a_n T \ : \ n_0 \in \mathbb{Z}, {}^\forall n \geq n_0, \ a_n \in \mathbb{C}\}$.

c) $\mathbb{Z}[i]/7$, $\mathbb{Z}[\sqrt{2}]/3$, $\left\{ \begin{pmatrix} a & 2b \\ b & a \end{pmatrix} \ : \ b \in \mathbb{F}_5 \right\}$ sont des corps finis à $49, 9$ et 25 éléments.

Exercice 4 Polynôme minimal

a) Soit $P \in K[X]$. Montrer que $K[X]/(P)$ est un $K-$espace vectoriel de dimension $d = \deg P$ (*une base est donnée par les* $X^k \bmod P$, $0 \leq k < \deg P$).

b) Soit $K \leq E$ une extension de corps. Soit $x \in E$. Montrer que sont équivalentes :

(i) il existe $0 \neq P \in K[X]$ tel que $P(x) = 0$;

(ii) $\dim_K K[x]$ est finie ;

(iii) $K[x] = K(x)$.

Dans ce cas, on dit que x est *algébrique sur* K.

c) Montrer que si $K \leq L$ sont des corps et si $x, y \in L$ sont algébriques sur K, alors $x + y$, xy et x/y aussi (si $y \neq 0$).

d) Montrer que $e^{2i\pi/103}$ est algébrique sur $\mathbb{Q}$, $\cos(2\pi/7)$ aussi, $\sum_{k\geq 0} \frac{1\times\ldots\times(2k-1)}{2\times\ldots\times(2k)} t^k$ est algébrique sur $\mathbb{C}(t)$ (*indication : en effet c'est* $(1-t)^{-1/2}$). Déterminer à chaque fois leur polynôme minimal !

e) Trouver le polynôme minimal de $\sqrt[3]{2} + j$ sur $\mathbb{Q}$ *(indication : trouver d'abord un polynôme rationnel de degré* 6 *qui annule* $\alpha = \sqrt[3]{2} + j$ *puis montrer que* $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt[3]{2}, j)$ *en considérant le pgcd des polynômes* $X^2 + X + 1$ *et* $(\alpha - X)^3 - 2$*).*

Exercice 5

Soit $x = \sqrt{2 + \sqrt{2}}$.

a) Déterminer le polynôme minimal P de x sur $\mathbb{Q}$.

b) Déterminer toutes les racines de P.

c) Montrer que le groupe $\mathrm{Aut}\mathbb{Q}(x)$ est cyclique d'ordre 4 engendré par l'automorphisme $\theta : x \mapsto \sqrt{2 - \sqrt{2}}$.

Exercice 6

a) Déterminer toutes les extensions algébriques de $\mathbb{C}$.

b) Montrer que toute extension algébrique de $\mathbb{R}$ est isomorphe à $\mathbb{C}$.

Exercice 7 Soit $\mathbb{K}$ un corps et $f : \mathbb{Q} \to \mathbb{K}$ un morphisme de corps. Montrer que $\mathbb{K}$ est de caractéristique nulle et que f est l'identité (sous-entendu $\mathbb{Q}$ est contenu dans tout corps de caractéristique nulle).

a) Déterminer tous les automorphismes des corps $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{R}$

b) Déterminer tous les automorphismes continus de $\mathbb{C}$.

c) Soit $\mathbb{K} \leq \mathbb{L}$ une extension algébrique. Montrer que tout endomorphisme $\mathbb{K}-$linéaire du corps $\mathbb{L}$ est un automorphisme !

Exercice 8

a) Soit $f \in \mathbb{Q}(X)$ une fraction rationnelle non constante. Montrer que f n'est pas algébrique sur $\mathbb{Q}$.

b) Montrer que X est algébrique sur $\mathbb{Q}(f)$ de degré $\max\{\deg p, \deg q\}$ si $f = \frac{p}{q}$ pour deux polynômes $p, q \in \mathbb{Q}[X]$ premiers entre eux.

c) En déduire que les automorphismes du corps $\mathbb{Q}(X)$ sont donnés par les « changements de variable » $X \mapsto \frac{aX+b}{cX+d}$, où $a, b, c, d \in \mathbb{Q}$ sont tels que $ad - bc \neq 0$.

Exercice 9

a) Soit $\mathbb{K}$ et $\mathbb{L}$ deux corps tels que $\mathbb{K} \subset \mathbb{L}$. Soit $P_1, P_2 \in \mathbb{K}[X]$.
Montrer que le pgcd de P_1 et P_2 dans $\mathbb{L}[X]$ est le même que leur pgcd dans $\mathbb{K}[X]$.
En déduire que les polynômes P_1 et $P_2 \in \mathbb{K}[X]$ sont premiers entre eux si et seulement si il n'ont aucune racine commune dans toute extension de $\mathbb{K}$.

b) Soit $P \in \mathbb{K}[X]$ et $\mathbb{L} \supset \mathbb{K}$ une extension qui contient toutes les racines de P. Montrer que toutes les racines de P sont simples si et seulement si P est premier avec sa dérivée P'.

c) Application. Soit $\mathbb{F}_q$ est un corps fini de cardinal q. Vérifier que $q = p^n$ pour un certain nombre premier p et un $n \in \mathbb{N}_{>0}$. Supposons que le polynôme $X^{q^n} - X$ est scindé sur $\mathbb{K}$ une extension de $\mathbb{F}_q$. Montrer que $\{x \in \mathbb{K} \,:\, x^{q^n} = x\}$ est un corps de cardinal q^n.

d) Soit $\mathbb{K}$ un corps. Soit $P(X) \in \mathbb{K}[X]$ un polynôme irréductible. Montrer que $P' = 0 \Rightarrow P \in \mathbb{K}[X^p]$ où p est la caractéristique de $\mathbb{K}$. En déduire que si $\mathbb{K}$ est de caractéristique nulle ou un corps fini alors P n'a pas de racine multiple (dans n'importe quelle extension de $\mathbb{K}$).

Donner un exemple de polynôme irréductible sur un corps à racine multiple dans une extension.

Exercice 10

Soit $P(X) = a_0X^n + a_1X^{n-1} + \cdots + a_n \in \mathbb{Z}[X]$. Soit $\alpha = p/q \in \mathbb{Q}$ une racine rationnelle de P, avec $\text{pgcd}(p, q) = 1$.
Montrer que p divise a_n et q divise a_0. (En particulier, si $a_0 = 1$, toute racine rationnelle est entière.)

Exercice 11

a) Factoriser $X^4 + 1$ sur $\mathbb{R}$ et en déduire que $X^4 + 1$ est irréductible sur $\mathbb{Q}$.

b) Montrer que X^4+1 est réductible dans $\mathbb{Z}/p\mathbb{Z}$ quelque soit p premier.
Indication. Écrire $X^4+1 = (X^2+1)^2 - 2X^2 = (X^2-1)^2 + 2X^2$ *et montrer que* -1 *ou* 2 *ou* -2 *est un carré dans* $\mathbb{Z}/p\mathbb{Z}$.

Exercice 12

a) Soit p premier. Montrer que $X^{p-1} + X^{p-2} + ... + X + 1$ est irréductible sur $\mathbb{Q}$. Et si p n'est pas premier ?

b) Soit p premier. Montrer que $X^n + pX + p^2$ est irréductible.
(Utiliser la réduction mod p.)

c) Soit $a \in \mathbb{Z}$ et p un premier qui ne divise pas a. Montrer que $X^p - X + a$ est irréductible sur $\mathbb{Z}/p\mathbb{Z}$.
(Raisonner par absurde et considérer le corps de décomposition de ce polynôme sur $\mathbb{Z}/p\mathbb{Z}$.)

d) Soit p premier, $\mathbb{K}$ un corps. Montrer que $P(X) = X^p - a \in \mathbb{K}[X]$ est irréductible si et seulement si P n'a pas de racine dans $\mathbb{K}$.
Indication : considérer la factorisation de P dans le corps de décomposition de P.
En particulier, si $\mathbb{K} \subset \mathbb{R}$, P est irréductible sur $\mathbb{K}$ si et seulement si $a^{1/p}$ n'est pas dans $\mathbb{K}$.

Exercice 13 Algorithme pour déterminer les diviseurs d'un polynôme $P(X) \in \mathbb{Z}[X]$

a) Soit $g(X) \in \mathbb{Z}[X]$ divise $P(X)$, $\deg(g) = d$.
Alors $g(j)$ divise $P(j)$ pour $j = 0, \ldots, d$.

b) Etant donnés $a_0, ..., a_d \in \mathbb{Z}$ il existe un seul polynôme $g \in \mathbb{Q}[X]$ tels que $g(j) = a_j$, $j = 0, \ldots, d$.

c) Donner une méthode pour déterminer les diviseurs du polynôme $P(X)$.

Exercice 14 Soit $\mathbb{K} \subset \mathbb{L}$ une extension de degré n.
Montrer que le degré sur $\mathbb{K}$ de tout élément de $\mathbb{L}$ divise n.