II.— Extensions algébriques et morphismes de corps

Exercice 1 *Combien les polynômes t^2-1 et t^2+1 ont-ils de solutions sur $\mathbb{F}_2$, $\mathbb{F}_3$, $\mathbb{F}_7$, $\mathbb{Z}/24\mathbb{Z}$, $\mathbb{H}$ (le corps des quaternions†) ?*

Exercice 2 *a) Soit k un corps et G un sous-groupe fini de k^*. Montrer que G est cyclique. (Indication : Soit n l'ordre de G : i) si φ est l'indicateur d'Euler, alors : $\sum_{d|n}\varphi(d)=n$; ii) si n_d est le nombre d'éléments d'ordre d, $\sum_{d|n} n_d = n$).*

b) Soit G un sous-groupe de $\mathbb{C}^*$. On suppose qu'il existe $n>0$ tel que tous les éléments de G sont d'ordre $\leq n$. Montrer que G est cyclique.

c) Donner un exemple de sous-groupe infini de $\mathbb{C}^*$ où tous les éléments sont d'ordre fini.

d) Quels sont les sous-groupes finis de $\mathbb{C}^*$? et de $\mathbb{R}^*$?

e) Montrer directement que $\mathbb{F}_7^*$ est cyclique.

Exercice 3 *Soit $z\in\mathbb{C}$. a) Montrer que sont équivalentes :*

i) l'anneau $\mathbb{Q}[z]$ est un corps ;

ii) il existe un polynôme rationnel non nul qui annule z ;

iii) le $\mathbb{Q}-$espace vectoriel $\mathbb{Q}[z]$ est de dimension finie.

Si l'une de ces conditions est vérifiée, on dit que z est algébrique sur $\mathbb{Q}$.

b) Montrer que l'ensemble des nombres complexes algébriques sur $\mathbb{Q}$ est un sous-corps de $\mathbb{C}$. On le note $\overline{\mathbb{Q}}$. En admettant que $\mathbb{C}$ est algébriquement clos, montrer que $\overline{\mathbb{Q}}$ est lui aussi algébriquement clos.

Exercice 4 *a) Soit k un corps. Si $P\in k[t]$. Montrer que P est irréductible sur $k \Leftrightarrow k[t]/(P)$ est un corps.*

b) Montrer que l'anneau $\mathbb{F}_2[t]/(t^2+t+1)$ est un corps. Quel est son cardinal ?

c) Montrer que l'anneau

$$\mathbb{F} := \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \ : \ a,b\in\mathbb{F}_5 \right\}$$

est un corps commutatif. Quel est son cardinal ?

---

†. Le corps des quaternions est un corps *non commutatif* engendré comme sous-$\mathbb{R}-$espace vectoriel des matrices réelles d'ordre 2 par $1 := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ $I := \begin{pmatrix} i & \\ & -i \end{pmatrix}$ $J := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ $K := \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$.

Exercice 5 *Soit m un idéal maximal de $\mathbb{Z}[t]$. Montrer que $\mathbb{Z}[t]/m$ est un corps fini. Donner un exemple.*

Exercice 6

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 7 Irréductibilité du polynôme $X^n - X - 1$

Pour tout polynôme $P \in \mathbb{C}[X]$, on notera, chaque fois que cela a un sens :

$$\mathscr{S}(P) := \sum_{z \text{ racine de P}} (z - \frac{1}{z}) \ .$$

Notons $F := X^n - X - 1$. a) Montrer que F a n racines distinctes et calculer $\mathscr{S}(F)$.

Soit maintenant $D \in \mathbb{Q}[X]$ est un diviseur unitaire de F.

b) Montrer que $D \in \mathbb{Z}[X]$.

c) Montrer que $\mathscr{S}(D)$ a un sens et que c'est un entier.

d) Soit $z = re^{it}$ ($r > 0$ et $t \in \mathbb{R}$) une racine de D. Montrer que :

$$r^{2n} = r^2 + 1 + 2r\cos t$$

et en déduire que $r \neq 1$.

e) Montrer que $2Re(z - \frac{1}{z}) > \frac{1}{r^2} - 1$.

f) Soient $z_1, ..., z_d$ les racines de D. Calculer $\prod_{i=1}^{d} |z_i|$.

g) Montrer que $\mathscr{S}(D) \geq 1$.

h) Conclusion ?

Exercice 8 *Soient $a_1, ..., a_n$ n entiers distincts. On va montrer que le polynôme $P = (t - a_1)...(t - a_n) - 1$ est irréductible dans $\mathbb{Z}[t]$.*

a) On suppose que $P = FG$ pour deux polynômes entiers unitaires. Montrer que pour tout i, $F(a_i) + G(a_i) = 0$.

b) Aboutir à une contradiction si $n > \deg F, \deg G$.

c) Conclure.

Exercice 9

1. Quelles sont les extensions de degré fini 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 10 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 11 (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 12 *Soient $K := \mathbb{Q}(t), K_1 := \mathbb{Q}(t^2), K_2 := \mathbb{Q}(t^2 - t)$.*

Montrer que K est algébrique sur K_1, algébrique sur K_2 mais non sur $K_1 \cap K_2$. Indication : vérifier que $\mathbb{K}_1 \cap K_2 = \mathbb{Q}$.