1. Anneaux, Corps et Polynômes

Convention : les anneaux et corps qui suivent sont tous supposés commutatifs.

Exercice 1.1 Combien les polynômes X^2-1 et X^2+1 ont-ils de solutions sur $\mathbb{R}$, $\mathbb{F}_2$, $\mathbb{F}_3$, $\mathbb{F}_7$ et $\mathbb{Z}/24\mathbb{Z}$?

Exercice 1.2 Le polynôme X^4+X^2+1 est-il irréductible sur $\mathbb{F}_2$? Même question avec le polynôme X^4+X+1.

Exercice 1.3

1. Soit $P(X) \in \mathbb{Z}[X]$ un polynôme unitaire. Montrer que si $x \in \mathbb{Q}$ est une racine non nulle de P, alors $x \in \mathbb{Z}$ et x divise $P(0)$ dans $\mathbb{Z}$.
   Application : factoriser $X^4+X^3-X^2+X+2$ sur $\mathbb{Q}$.
2. Soient P et Q deux polynômes unitaires dans $\mathbb{Q}[X]$. Montrer que si
$$P(X) \cdot Q(X) \in \mathbb{Z}[X],$$
   alors P et Q sont dans $\mathbb{Z}[X]$

Exercice 1.4

1. Montrer que le polynôme X^5+X^3+1 est irréductible sur $\mathbb{F}_2$
2. En déduire que le polynôme $2009X^5+1000X^4+3X^3+2X^2+1$ est irréductible sur $\mathbb{Q}$.

Exercice 1.5 Soit K un corps, et soient $m, n \geq 1$ deux entiers. On note r le reste de la division euclidienne de m par n. Montrer que X^r-1 est le reste de la division euclidienne dans $K[X]$ de X^m-1 par X^n-1.
En déduire que le PGCD de X^m-1 et X^n-1 est X^d-1 où $d = \text{pgcd}(m,n)$.

Exercice 1.6 Soient K et L deux corps tels que $K \subset L$. Soient $P(X), Q(X) \in K[X]$. Montrer que P et Q sont premiers entre eux dans $K[X]$ si et seulement ils sont premiers entre eux dans $L[X]$.
En déduire que si P et Q sont deux polynômes de $\mathbb{R}[X]$ alors P et Q sont premiers entre-eux dans $\mathbb{R}[X]$ si et seulement si ils n'ont aucune racine complexe commune.

Exercice 1.7 Soit p un nombre premier. Factoriser sur $\mathbb{Q}$ le polynôme X^p-1.

Exercice 1.8 Soit z un nombre complexe (ou réel). On dit que z est un nombre *algébrique* (sur $\mathbb{Q}$), si z est racine d'un polynôme rationnel non nul.

Montrer que les propriétés suivantes sont équivalentes :

1. L'anneau $\mathbb{Q}[z]$ est un corps.
2. Le $\mathbb{Q}$-espace vectoriel $\mathbb{Q}[z]$ est de dimension finie.

3. z est algébrique sur $\mathbb{Q}$.

Exercice 1.9 Soit A un anneau.

1. Montrer qu'il existe un unique homomorphisme d'anneaux f de $\mathbb{Z}$ dans A.
   On appelle *caractéristique* de A l'entier naturel c tel que $\ker(f) = c\mathbb{Z}$.
2. Montrer que si A est intègre alors la caractéristique de A est nulle ou un nombre premier.
3. Montrer que si A est fini alors c divise le cardinal de A.
4. Que peut-on dire sur c si A est un corps fini ?

Exercice 1.10 Montrer qu'un corps fini est un $\mathbb{F}_p$-espace vectoriel pour un nombre premier p. En déduire que tout corps fini a pour cardinalité p^m pour un nombre premier p et un enitier $m \geq 1$.

Exercice 1.11
1. Soit K un corps et G un sous-groupe fini de $(K^*, \times)$. Montrer que G est cyclique. (On pourra utiliser l'indicatrice d'Euler et la formule $\Sigma_{d|n}\phi(d) = n$).
2. Soit K un corps et G un sous-groupe de $(K^*, \times)$. On suppose qu'il existe $n > 0$ tel que tous les éléments de G sont d'ordre $\leq n$. Montrer que G est cyclique.
3. Quels sont les sous-groupes finis de $(\mathbb{C}^*, \times)$ et de $(\mathbb{R}^*, \times)$?

Exercice 1.12 Soient K un corps et P un polynôme dans $K[X]$.

1. Vérifier que si $\text{carac}(K) = 0$, alors $P'(X) = 0$ si et seulement si P est constant, et que si $\text{carac}(K) = p > 0$, alors $P'(X) = 0$ si et seulement si $P(X) \in K[X^p]$.
2. On suppose par la suite P irréductible sur K et $\deg P > 0$. Montrer que si K est de caractéristique nulle ou si K est fini, alors $P'(X) \neq 0$.
3. Soient L un corps contenant K et $x \in L$ une racine de P. Montrer que x est racine simple de P si et seulement si $P'(x) \neq 0$.
4. Soit k un corps de caractéristique $p > 0$ et prenons $A = k[Y^p]$ et $B = k[Y]$. Montrer que $P(X) = X^p - Y^p$ est irréductible sur A et que Y est racine de P d'ordre de multiplicité p dans B.

Exercice 1.13 Soient p un nombre premier impair, K un corps et $a \in K$. On suppose que $X^p - a$ n'est pas irréductible sur K. Soit $P(X)$ un facteur unitaire propre de $X^p - a$ dans $K[X]$. On pose $b = P(0)$.

1. Montrer qu'il existe un entier m avec $0 < m < p$ tel que
$$b^p = (-a)^m.$$
   (On admettera que K est contenu dans un corps algébriquement clos et considérera les racines de P dans ce corps algébriquement clos)
2. En utilisant l'identité de Bezout, en déduire que $X^p - a$ a une racine dans K.

Exercice 1.14 Soit p un nombre premier impair, soit q un diviseur premier de $p-1$. Soit a un entier, $p \nmid a$, tel que la classe $\bar{a}$ de a modulo p engendre le groupe $\mathbb{F}_p^\times$. Montrer que tout polynôme de la forme

$$X^q + p\left(\sum_{i=1}^{q-1} \lambda_i X^i\right) - a,$$

avec $\lambda_i \in \mathbb{Z}$, est irréductible sur $\mathbb{Q}$. (Indication : réduire modulo p et utiliser l'exercice 1.13.)
Application : démontrer l'irréductibilité sur $\mathbb{Q}$ du polynôme $X^7 - 29X^4 + 2$.

Exercice 1.15 (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 :

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

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 :

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

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).