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

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 1.3 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 1.4 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 1.5

1. Déterminer les automorphismes du corps $\mathbb{Q}$.
2. Déterminer les automorphismes du corps $\mathbb{Q}(\sqrt{2})$
3. Déterminer les automorphismes du corps $\mathbb{R}$. (On pourra montrer que tout automorphisme de $\mathbb{R}$ est strictement croissant et utiliser la densité de $\mathbb{Q}$ dans $\mathbb{R}$.)
4. Déterminer le groupe de Galois de $\mathbb{C}$ sur $\mathbb{R}$, $\text{Gal}(\mathbb{C}/\mathbb{R}) := \text{Aut}_{\mathbb{R}}(\mathbb{C})$.

Exercice 1.6 Soient K est un corps et $K(X)$ le corps des fractions rationnelles à coéfficients dans K. Soit $G := \text{Aut}_K(K(X))$ le groupe de Galois de $K(X)$ sur K.

1. Vérifier que pour $a \in K$, l'application qui à $F(X) \in K(X)$ associe $F(X + a)$ est un automorphisme de $K(X)$.
2. En déduire que si K est infini alors G est infini.
3. Soit $\text{Fix}(G) := \{F \in K(X) | \sigma(F) = F, \ \forall \sigma \in G\}$ le corps fixe de G. Montrer que si K est infini alors $\text{Fix}(G) = K$.

Exercice 1.7 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 1.8 Soit A un anneau.

1. Montrer qu'il existe un unique homomorphisme d'anneaux f de $\mathbb{Z}$ dans A.
   On appelle *caractéristque* 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 1.9 Soit K un corps fini à q éléments.

1. Montrer qu'il existe un nombre premier p et un entier $f \geq 1$ tels que $q = p^f$.
2. Montrer que :
$$X^q - X = \prod_{x \in K} (X - x).$$
3. Soit σ le morphisme de Frobenius de K, *i.e.* $\sigma(x) = x^p$ pour tout $x \in K$. Prouver que $\sigma \in \mathrm{Aut}_{\mathbb{F}_p}(K)$ et que σ est d'ordre f. (On verra par la suite que σ est un générateur de $\mathrm{Aut}_{\mathbb{F}_p}(K)$).
4. Soit $x \in K$. Montrer que $x \in \mathbb{F}_p$ si et seulement si $x^p = x$.
   En déduire que pour $P(X) \in K[X]$, $P(X) \in \mathbb{F}_p[X]$ si et seulement si $P(X)^p = P(X^p)$.

Exercice 1.10 Soient K un corps et P un polynôme dans $K[X]$.

1. Vérifier que si $\mathrm{carac}(K) = 0$, alors $P'(X) = 0$ si et seulement si P est constant, et que si $\mathrm{carac}(K) = p > 0$, 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 1.11 Soit K un corps fini à q éléments de caractéristique p impair.

1. Montrer que l'application
$$\begin{array}{rccc} \varphi & : & K^\times & \to & K^\times \\ & & x & \mapsto & x^2 \end{array}$$
est un morphisme de groupes et que $\mathrm{Im}\varphi$ est d'indice 2 dans $K^\times$.

2. Soit $x \in K^\times$; montrer que x est un carré dans K si et seulement si $x^{(q-1)/2} = 1$.
3. Montrer que -1 est un carré dans K si et seulement si $q \equiv 1 \pmod 4$.
4. a) Soit L un corps contenant K sur lequel X^4+1 est scindé. Soit $\alpha \in L$ une racine de X^4+1. Vérifier que :
$$\left(\alpha + \alpha^{-1}\right)^2 = 2.$$

   b) En déduire que 2 est un carré dans K si et seulement si $q \equiv \pm 1 \pmod 8$. (On admettra qu'il existe toujours un corps L contenant K sur lequel X^4+1 est scindé.)

Exercice 1.12 Soit p un nombre premier. Factoriser sur $\mathbb{Q}$ le polynôme $X^p - 1$.

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
$$b^p = (-a)^m.$$
2. En utilisant l'identité de Bezout, en déduire que $X^p - a$ a une racine dans K.

Exercice 1.14

1. Factoriser X^4+1 sur $\mathbb{F}_p$ (avec p nombre premier). Distinguer les cas : $p = 2$, $p \equiv 1 \pmod 8$, $p \equiv -3 \pmod 8$, $p \equiv -1$ ou $3 \pmod 8$ et on utilisera l'exercice 1.11.
2. Montrer que X^4+1 est irréductible sur $\mathbb{Q}$.

Exercice 1.15 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 1.16 Soit p un nombre premier et K un corps fini de caractéristique différente de p.

1. Soit P un facteur irréductible dans $K[X]$ du polynôme
$$\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + 1.$$
   Considérons le corps $L = K[X]/(P)$ et soit $\alpha = \overline{X}$ la classe de X dans L.
   Montrer que α est d'ordre p dans $L^\times$ et en déduire que :
$$\mathrm{card}(K)^d \equiv 1 \pmod p$$
   où $d = \deg P$.

2. On suppose que $\overline{\mathrm{card}(K)}$ engendre le groupe $\mathbb{F}_p^\times$. Montrer que Φ_p est irréductible sur K.
3. En déduire que si q est un nombre premier tel que $\overline{q}$ engendre $\mathbb{F}_p^\times$, alors Φ_p est irréductible sur $\mathbb{F}_q$.
4. Soient p et q deux nombres premiers. On suppose que $q \neq 2$, $p \equiv -1 \pmod 3$ et que $\overline{q}$ engendre $\mathbb{F}_p^\times$. Montrer que $X^{p+1} - X + q$ est irréductible sur $\mathbb{Q}$. (Indication : réduire modulo q et modulo 2 et utiliser la question précédente.)
   Application : Montrer que $X^{18} - X + 3$ est irréductible sur $\mathbb{Q}$.

Exercice 1.17 (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).