Corps

Exercice 1 [Vrai-faux spécial morphisme].

1. Un morphisme de corps est injectif.
2. L'identité est le seul morphisme de corps de $\mathbb{Q}$ dans lui même.
3. L'identité est le seul morphisme de corps de $\mathbb{R}$ dans lui même.
4. L'identité est le seul morphisme de corps de $\mathbb{C}$ dans lui même.

Exercice 2 [Vrai-faux spécial extension de corps].

1. $\mathbb{Q}$ admet un sous-corps autre que lui-même.
2. La cloture algébrique de $\mathbb{Q}$ est un ensemble dénombrable.
3. $\mathbb{C}$ admet une extention de corps K tel que $[K, \mathbb{C}] = n$ pour un certain $n > 1$.
4. $\mathbb{C}$ admet une extention de corps.
5. Le corps des fractions rationnelles $\mathbb{C}(t)$ est algébriquement clos.
6. Il existe un sous-corps K de $\mathbb{R}$ tel que $[\mathbb{R} : K] = 2$.
7. Il existe une extension K de $\mathbb{F}_2$ tel que $[K : \mathbb{F}_2] = 2$.
8. Il existe une extension K de $\mathbb{F}_2$ tel que $|K| = 6$.

Exercice 3 [Extension et degré].

1. Soit K un corps et L une extension de K de degré fini. Soit H_1, H_2 des corps tels que $K \subset H_i$ pour $i = 1, 2$. Montrer que si $[H_1 : K]$ et $[H_2 : K]$ sont premiers entre eux, alors $H_1 \cap H_2 = K$.
2. Soit K un corps et L une extension de K de degré premier. Montrer que, pour tout $\alpha \in L \setminus K$, on a $K(\alpha) = L$.

Exercice 4 [Corps finis].

1. Soit A un anneau intègre commutatif fini. Démontrer que A est un corps.
2. Dans toute la suite K est un corps fini. Calculer
$$\prod_{x \in K^\times} x.$$
3. Montrer qu'il existe un entier p premier tel le plus petit sous-corps de K est isomorphe à$\mathbb{Z}/p\mathbb{Z}$.
4. Montrer que le cardinal de K est une puissance de p, on pourra munir K d'une structure de $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel.
5. A quel groupe est isomorphe $(K, +)$?
6. Montrer que le groupe multiplicatif d'un corps fini est cyclique. On montrera qu'il existe dans $K^\times$ un élément d'ordre égal à m, le ppcm des ordres des éléments de $K^\times$ puis que m est plus grand que le cardinal de $K^\times$.

Exercice 5 [Corps du type $\mathbb{Q}[\sqrt{d}]$]. 1. Soit $d \in \mathbb{N}$ tel que $\sqrt{d} \notin \mathbb{Q}$. On note

$$\mathbb{Q}[\sqrt{d}] = \{a + b\sqrt{d}; (a, b) \in \mathbb{Q}^2\}.$$

Démontrer que $(\mathbb{Q}[\sqrt{d}], +, \times)$ est un corps.

2. Démontrer que -1 est une somme de deux carrés dans $\mathbb{Q}[i\sqrt{2}]$. En déduire que les corps $\mathbb{Q}[\sqrt{2}]$ et $\mathbb{Q}[i\sqrt{2}]$ ne sont pas isomorphes.
3. Soit $\alpha, \beta \in \mathbb{N}$ tels que $\sqrt{\alpha}$ et $\sqrt{\beta}$ sont irrationnels. Donner une condition nécessaire et suffisante pour que $\mathbb{Q}[\sqrt{\alpha}]$ et $[\sqrt{\beta}]$ soient isomorphes.

Exercice 6. 1. Soit K un corps de caractéristique différente de 2. Soient a et b qui ne sont pas des carrés de K. Montrer que $K(\sqrt{a}, \sqrt{b})$ est de degré 4 sur K si ab n'est pas des carrés de K et de degré 2 sinon.

2. Soit $L = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$. En déduire $[L : Q]$.
3. Montrer que $L = \mathbb{Q}[\sqrt{2} + \sqrt{3}]$.

Exercice 7 [Appartenance à un corps]. 1. Le nombre $\sqrt[7]{2}$ est-il dans $\mathbb{Q}[\sqrt[7]{3}]$?

2. Le nombre $1 + \sqrt[3]{2}$ est-il un carré dans $\mathbb{Q}[\sqrt[3]{2}]$?

Exercice 8. Montrer que les deux polynômes $X^2 - 3$ et $X^2 - 2X - 2$ sont irréductibles sur $\mathbb{Q}$ et distincts mais ont même corps de décomposition.

Exercice 9 [Irréductibilité]. Soit p un nombre premier impair.

1. Montrer que $X^4 + 1$ est irréductible de $\mathbb{Z}[X]$.
2. Montrer que si $p > 2$ est premier alors $p^2 - 1$ est un multiple de 8.
3. Soit $p > 2$ premier, montrer que $X^4 + 1$ admet une racine dans $\mathbb{F}_{p^2}$.
4. Montrer que $X^4 + 1$ n'est jamais irréductible modulo p.

Exercice 10 [Extension de corps fini]. 1. Calculer $[\mathbb{F}_8 : \mathbb{F}_4]$ et $[\mathbb{F}_{16} : \mathbb{F}_4]$.

2. Montrer les isomorphismes suivants

$$\mathbb{F}_8 \simeq \mathbb{F}_2[X]/(X^3 + X + 1), \qquad \mathbb{F}_{25} \simeq \mathbb{F}_5[X]/(X^2 - 2), \qquad \mathbb{F}_{49} \simeq \mathbb{F}_7[X]/(X^2 + 1).$$

Exercice 11 [Irréductibilité sur les corps fini]. Montrer que :

1. $X^2 + X + 1$ est le seul polynôme de degré 2 irréductible sur $\mathbb{F}_2$;
2. $X^3 + X + 1$ et $X^3 + X^2 + 1$ sont les seuls polynômes de degré 3 irréductible sur $\mathbb{F}_2$;
3. $X^2 + 1$, $X^2 - X - 1$ et $X^2 + X - 1$ sont les seuls polynômes unitaires de degré 2 irréductible sur $\mathbb{F}_3$.
4. Combien y-a-t-il de polynômes unitaires irréductible de degrés 4 (resp. 3) sur $\mathbb{F}_2$ (resp. $\mathbb{F}_3$) ?

Exercice 12. Soit A un anneau intègre. On rappelle que A est un anneau euclidien s'il existe $\nu : A^* \to \mathbb{N}$ tel que

— Pour tout $a \in A$ et pour tout $b \in A^*$, il existe $(q, r) \in A^2$ tels que $a = bq + r$ avec $r = 0$ ou $\nu(r) < \nu(b)$.

— Pour tout $a, b \in A^*$ si a divise b alors $\nu(a) \leq \nu(b)$.

Partie A

1. Donner un exemple d'anneau euclidien pour lequel le couple (q, r) n'est pas unique.
2. Montrer que $\nu(ab) = \nu(a)$ si et seulement si b est inversible. (on pourra faire la division euclidienne de a par ab.
3. En déduire que tout élément non nul et non inversible d'un anneau euclidien est un produit d'éléments irréductibles.

Partie B Dans toute la suite, on suppose que le couple (q, r) de la définition d'anneau euclidien est unique et que A n'est pas un corps. Le but de cette partie est de montrer que A est isomorphe à $\mathbb{K}[X]$ où $\mathbb{K}$ est un corps.

1. Justifier que quitte à modifier ν, on peut supposer que $\nu(A^*) = \mathbb{N}$.
2. Soit $a, b \in A^*$. Montrer que $\nu(a + b) \leq \max(\nu(a), \nu(b))$.
3. Justifier que $\{a \in A : \nu(a) = 0\} \cup \{0\}$ est un corps que l'on notera $\mathbb{K}$.
4. Justifier que si $\nu(b) < \nu(a)$ alors $\nu(a + b) = \nu(a)$.
5. Soit $x \in A$ tel que $\nu(x) = 1$. Soit $n \geq 1$ tel que $\nu(x^n) = n$. Soit $a \in A$ tel que $\nu(a) = n$. Montrer qu'il existe $P \in \mathbb{K}_n[X]$ tel que $a = P(x)$.
6. En déduire que, pour tout $n \geq 1$, $\nu(x^n) = n$.
7. En déduire qu'il existe un isomorphisme d'anneau entre $A[X]$ et $\mathbb{K}[X]$.

Exercice 13 [Paradoxe de Sierpinski-Mazurkiewicz]. Soit u un nombre complexe transcendant de module 1. Soit

$$\begin{aligned} E &= \{P(u); P \in \mathbb{N}[X]\} \\ A &= \{(XQ)(u); Q \in \mathbb{N}[X]\} \\ B &= \{(R+1)(u); R \in \mathbb{N}[X]\}. \end{aligned}$$

1. Démontrer que (A, B) forme une partition de E.
2. En déduire qu'il existe un ensemble contenu dans le plan dont il existe une partition en deux parties qui sont isométriques à l'ensemble initial !