Rappels d'algèbre

Tous les anneaux considérés sont commutatifs.

Exercice 1 Construction de corps à partir d'un anneau. Dans cet exercice, A est un anneau et I un idéal de A.

1. Montrer que A est un corps si et seulement si ses idéaux sont triviaux.
2. Montrer que les idéaux de A/I sont les J/I, avec J idéal de A contenant I.
3. En déduire une condition nécessaire et suffisante sur I pour que A/I soit un corps.
4. Quels sont les idéaux de $A = \mathbb{Z}$? Quels sont ceux qui vérifient la condition ci-dessus ?
5. Même question pour l'anneau $A = \mathbb{K}[X]$ des polynômes sur un corps $\mathbb{K}$ quelconque.

Exercice 2 Corps de rupture, corps de décomposition. Soit $\mathbb{K}$ un corps, et P un polynôme sur $\mathbb{K}$.

1. On suppose dans un premier temps P irréductible. Construire une extension $\mathbb{L}$ de $\mathbb{K}$ vérifiant
   (a) P admet une racine α sur $\mathbb{L}$;
   (b) $\mathbb{L}$ est minimale pour cette propriété, i.e. $\mathbb{L}$ est engendrée par α.

   Une telle extension s'appelle un corps de rupture pour P sur $\mathbb{K}$.
2. Soit $\varphi\colon \mathbb{K} \to \mathbb{K}'$ un isomorphisme de corps, et soit $\mathbb{L}'$ un corps de rupture pour $\varphi(P)$. Montrer que $\mathbb{L}'$ est isomorphe à $\mathbb{L}$, et que l'isomorphisme peut même être choisi de manière à prolonger φ. Qu'obtient-on lorsque $\mathbb{K}' = \mathbb{K}$ et $\varphi = Id$?
3. On suppose désormais P quelconque. Montrer qu'il existe une extension $\mathbb{L}$ du corps $\mathbb{K}$, unique à $\mathbb{K}-$isomorphisme près, vérifiant :
   (a) P est scindé sur $\mathbb{L}$;
   (b) $\mathbb{L}$ est minimale pour cette propriété, i.e. les racines de P sur $\mathbb{L}$ engendrent $\mathbb{L}$.

   On l'appelle le corps de décomposition de P sur $\mathbb{K}$.

Exercice 3 Caractéristique, sous-corps premier, morphisme de Frobenius.

1. Soit $\varphi\colon A \to B$ un morphisme d'anneaux. Montrer que $\ker\varphi$ est un idéal de A, et que $A/\ker\varphi$ est isomorphe à $\operatorname{Im}\varphi$.
2. Que dit ce résultat lorsque $A = \mathbb{Z}$? Rappeler en particulier les notions de caractéristique (notée p) et de sous-corps premier d'un corps fini.

3. Montrer qu'un morphisme de corps est toujours injectif, et que les points fixes d'un automorphisme de corps forment un sous-corps.
4. Soit $\mathbb{K}$ un corps fini de caractéristique p, et soit $\varphi\colon \mathbb{K} \to \mathbb{K}$ défini par $\varphi(x) = x^p$. Montrer que φ est un automorphisme de corps. Quel corps forment ses point fixes ?

Exercice 4 Description d'un corps fini.

1. Soit $q = p^n$ avec p premier et $n \in \mathbb{N}^*$. On note $\mathbb{F}_q$ le corps de décomposition de $P = X^q - X$ sur $\mathbb{K} = \mathbb{Z}/p\mathbb{Z}$. Montrer que $\mathbb{F}_q$ a exactement q éléments.
2. Réciproquement, montrer que tout corps fini est isomorphe à un tel $\mathbb{F}_q$.
3. Montrer qu'il existe $\alpha \in \mathbb{F}_q$ tel que $\mathbb{F}_q = \{0\} \cup \{1, \alpha, \ldots, \alpha^{q-2}\}$. Un tel α est appelé élement primitif de $\mathbb{F}_q$.