Anneaux et Corps

Dans toute la suite, les anneaux sont supposés commutatifs unitaires, les corps sont supposés commutatifs.

Exercice 1. Soit $n \geq 2$ un nombre entier. Montrer que $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier.

Exercice 2.

1. Soit K un corps et $x \in K \backslash \{1\}$. Justifier que $1 + x + \cdots + x^{n-1} = (x^n - 1)/(x - 1)$.
2. Soit $a_n = 1 \ldots 1$ (n fois). Déterminer un entier $n > 0$ tel que 19 divise a_n. On pourra considérer $K = \mathbb{Z}/19\mathbb{Z}$ (remarque : aucun calcul n'est nécessaire pour répondre à cette question).
3. Déterminer le plus petit $n > 0$ pour lequel $19|a_n$ (ici les calculs doivent pouvoir se faire à la main. . .)

Exercice 3.

1. Trouver deux polynômes distincts dans $\mathbb{Z}/2\mathbb{Z}[X]$ qui définissent la même fonction de $\mathbb{Z}/2\mathbb{Z}$ vers $\mathbb{Z}/2\mathbb{Z}$.
2. Soit K un corps. Justifier à l'aide de la division euclidienne dans $K[X]$ que $a \in K$ est racine du polynome P si et seulement si $X - a$ divise P. En déduire qu'un polynôme de degré n admet au plus n racines distinctes.
3. Si K est un corps infini. Montrer que deux polynômes distincts dans $K[X]$ définissent des fonctions distinctes de K dans K.

Exercice 4.

1. Déterminer les racines du polynôme $P(X) = X^2 + X + 1$.
2. Le polynôme P divise-t-il $(X^8 + 1)^8 - X^8$?
3. Le polynôme P divise-t-il $(X^5 + 1)^5 - X^5$?

Exercice 5.

1. Montrer qu'il existe un unique morphisme d'anneau de $\mathbb{Z}$ vers un anneau donné A. Que dire de son noyau en général ? Et quand A est un corps ?
2. Soit A un anneau, et $B \subset A$. Est-il possible que B soit à la fois un idéal et un sous-anneau de A ?

Exercice 6. Déterminer tous les morphismes d'anneaux de $\mathbb{Z}$ dans $\mathbb{Z}$, puis de $\mathbb{Q}$ dans $\mathbb{Z}$, et finalement de $\mathbb{R}$ dans $\mathbb{Q}$.

Exercice 7. Soit K un corps, soient $A, B \in K[X]$ des polynômes non nuls. On appelle PGCD de A et B, un diviseur commun de A et B de degré maximal pour cette propriété.

1. Justifier qu'un PGCD existe, est il unique ?
2. On suppose que $B|A$, déterminer tous les PGCD de A et B.
3. On suppose que B ne divise pas A. On pose $A = BQ + R$ avec $\deg(R) < \deg(B)$ la division euclidienne de A par B. Montrer que A et B ont mêmes PGCD que B et R. En déduire un algorithme pour déterminer les PGCD de deux polynômes.
4. Déterminer les PGCD de $X^4 - X^3 + 2X^2 - X + 1$ et $X^3 + 1$.
5. Montrer que si D divise A et B, alors il divise forcément tous les PGCD de A et B.
6. Soit D un PGCD de A, B, montrer qu'il existe U, V des polynômes tels que $AU + BV = D$
7. Démontrer le théorème de Bezout : A, B sont premiers entre eux (*i.e.* n'ont pas de diviseurs communs autre que les constantes) si et seulement si il existe U, V tel que $AU + BV = 1$.

8. Déduire du théorème de Bezout le lemme de Gauss : si $A|BC$ et A, B sont premiers entre eux, alors $A|C$ (indic : on pourra multiplier l'identité de Bézout vue précédement par C).

Exercice 8. Soit K un corps et P un polynôme, on note $(P) = \{P.Q|\ Q \in K[X]\}$ l'idéal engendré par P. Justifier que $K[K]/(P)$ a naturellement une structure d'anneau. On suppose ici que P est irréductible, justifier que $L = K[X]/(P)$ est un corps. Pour un élément $x = [Q]$ de L déterminer explicitement x^{-1}.

Exercice 9.

1. En raisonnant par l'absurde, justifier que $\sqrt{2}$ est irrationnel.
2. Soit $m \in \mathbb{N}$ un entier qui n'est pas le carré d'un autre entier. Justifier que $\sqrt{m}$ est irrationnel.

Exercice 10. Si d est un entier relatif non-nul sans facteur carré et différent de 1, on note

$$\mathbb{Q}[\sqrt{d}] = \{a + b\sqrt{d}, a, b \in \mathbb{Q}\}.$$

1. Vérifier à la main que $\mathbb{Q}[\sqrt{d}]$ est un sous-corps de $\mathbb{C}$.
2. Parmis les trois corps $\mathbb{Q}[\imath]$, $\mathbb{Q}[\sqrt{2}]$ et $\mathbb{Q}[\sqrt{3}]$, lesquels sont isomorphes entre eux ?
3. Montrer que $\mathbb{Q}[\sqrt{d}] \simeq \mathbb{Q}[X]/(X^2 - d)$.
4. Soient $d, d' \in \mathbb{Z}$, distincts et sans facteurs carrés . Montrer qu'il n'y a pas de morphisme de corps de $\mathbb{Q}[\sqrt{d}]$ dans $\mathbb{Q}[\sqrt{d'}]$.