DM02 à rendre lundi 07/10/2024

Cyclicité de $\mathbb{K}^*$ lorsque $\mathbb{K}$ est un corps fini

On rappelle que $\varphi : \mathbb{N}^* \to \mathbb{N}^*$ désigne l'indicatrice d'Euler, c'est-à-dire que pour tout $n \in \mathbb{N}^*$:

$$\varphi(n) = Card\{k \in [\![1, n]\!],\ pgcd(k, n) = 1\}.$$

Première partie :
Soit n un entier naturel. On note $\mathcal{D}_n$ l'ensemble des entiers naturels qui divisent n. On souhaite montrer que pour tout entier n strictement positif on a l'égalité $n = \sum\limits_{d \in \mathcal{D}_n} \varphi(d)$.

On pose $f(n) = \sum\limits_{d \in \mathcal{D}_n} \varphi(d)$.

1. Soit p un nombre premier. Pour tout entier $i \in \mathbb{N}^*$, calculer $\varphi(p^i)$.
   En déduire la valeur $f(p^k)$ pour tout entier k strictement positif.
2. Soient m_1 et m_2 deux entiers naturels non nuls premiers entre eux. Montrer que l'application
   $$P : \left\{ \begin{array}{ccc} \mathcal{D}_{m_1} \times \mathcal{D}_{m_2} & \longrightarrow & \mathcal{D}_{m_1 m_2} \\ (d_1, d_2) & \longmapsto & d_1 d_2 \end{array} \right.$$
   est bien définie et qu'elle est bijective.
3. En déduire que lorsque m_1 et m_2 sont deux entiers naturels non nuls premiers entre eux on a la relation $f(m_1)f(m_2) = f(m_1 m_2)$.
4. Montrer que pour tout entier n strictement positif on a l'égalité $n = \sum\limits_{d \in \mathcal{D}_n} \varphi(d)$.

Deuxième partie :
Soit $\mathbb{K}$ un corps **quelconque** (fini ou infini). On note $\mathbb{K}[X]$ l'anneau des polynômes à coefficients dans $\mathbb{K}$ et à une indéterminée X.
On admet que $(\mathbb{K}[X], +, \cdot)$ est un anneau commutatif et intègre, et l'on définit la notion de degré de manière habituelle, et on dispose des propriétés classiques (par ex $\deg(PQ) = \deg(P) + \deg(Q)$, etc.).

5. Etant donné un polynôme $P \in \mathbb{K}[X]$, on note $\tilde{P} : \left\{ \begin{array}{ccc} \mathbb{K} & \longrightarrow & \mathbb{K} \\ x & \longmapsto & P(x) \end{array} \right.$ sa fonction polynôme associée.
   Montrer que $\theta : \left\{ \begin{array}{ccc} \mathbb{K}[X] & \longrightarrow & \mathbb{K}^{\mathbb{K}} \\ P & \longmapsto & \tilde{P} \end{array} \right.$ est un morphisme d'anneaux.
6. Si $\mathbb{K}$ est de cardinal infini, montrer que θ est injectif.
   Dans ce cas, on peut identifier un polynôme et sa fonction polynôme associée.
7. En prenant l'exemple $\mathbb{K} = \mathbb{Z}/2\mathbb{Z}$, montrer que le morphisme θ n'est plus nécessairement injectif lorsque $\mathbb{K}$ est fini.
8. On revient au cas où $\mathbb{K}$ est un corps quelconque.
   (a) Montrer que le théorème de la division euclidienne dans $\mathbb{K}[X]$ reste vrai (reprendre la démonstration faite en MP2I).
   (b) En déduire que pour tout $P \in \mathbb{K}[X]$ et tout $a \in \mathbb{K}$, a est racine de P si et seulement si $X - a$ divise P.
   (c) En déduire que si $P \in \mathbb{K}[X]$ est un polynôme de degré $d \in \mathbb{N}^*$, alors P possède au plus d racines.

Troisième partie :
Soit $(\mathbb{K}, +, \cdot)$ un corps de cardinal fini égal à $c+1$ (avec $c \in \mathbb{N}^*$). L'ensemble des éléments inversibles de $\mathbb{K}$ est $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$ et on souhaite montrer que le groupe $(\mathbb{K}^*, \cdot)$ de cardinal c est cyclique.
Pour tout entier d de $\mathcal{D}_c$, on note $N(d)$ le nombre d'éléments de $(\mathbb{K}^*, \cdot)$ qui sont d'ordre d.

9. Déterminer la valeur de $\sum\limits_{d \in \mathcal{D}_c} N(d)$.
10. Soit d un élément de $\mathcal{D}_c$.
    (a) On suppose qu'il existe un élément x d'ordre d dans $\mathbb{K}^*$ et on note H le sous-groupe de $(\mathbb{K}^*, \cdot)$ engendré par x. En introduisant un polynôme judicieux, montrer que tout élément d'ordre d de $\mathbb{K}^*$ est dans H.
    (b) Si x est d'ordre d dans $\mathbb{K}^*$, déterminer l'ordre de x^k dans $\mathbb{K}^*$ pour tout $k \in \mathbb{N}^*$.
    (c) Montrer que pour tous les éléments d de $\mathcal{D}_c$ on l'inégalité $N(d) \leq \varphi(d)$.
11. Montrer que pour tout entier d de $\mathcal{D}_c$, on a l'égalité $N(d) = \varphi(d)$.
12. En déduire que $(\mathbb{K}^*, \cdot)$ est un groupe cyclique.