Devoir Maison L3 Algèbre

I. HONORE, 25 septembre 2016

Problème

Notations et définitions :

Voici les notations et les définitions des objets dont nous avons besoin pour ce problème.

1. Le long de ce problème, nous prendrons $(K, +, .)$ un corps avec 0_K l'élément neutre pour la loi "+" et 1_K l'élément neutre pour la loi "." .
2. On dit qu'un sous-corps est **premier** s'il ne contient aucun sous-corps distinct de lui-même. Un élément d'un anneau est dit **premier** si l'idéal engendré est premier.
3. On appelle **caractéristique** d'un corps le plus petit entier strictement positif n tel que $n.1_K = 0_K$. S'il n'existe pas de tel n fini, nous dirons que la **caractéristique** est nulle, i.e. $n = 0$.
4. On dit que $x \in K$ est une **racine n-ième de l'unité** pour $n \in \mathbb{N}$ si l'on a $x^n = 1$. On dit également que x est une **racine de l'unité** s'il existe $n \in \mathbb{N}$ tel que x soit une racine n-ième de l'unité.
5. Nous noterons $U(K)$ l'ensemble des racines de l'unité de K et pour $n \in \mathbb{N}$, $U_n(K)$ l'ensemble des racines n-ième de l'unité de K.
6. On dit que $x \in K$ est une **racine n-ième primitive de l'unité** pour $n \in \mathbb{N}$ si l'on a $x^m = 1 \Rightarrow n|m$.
7. On rappelle que l'indicatrice d'Euler est la fonction :

$$\begin{array}{rcl} \varphi : \mathbb{N}^* & \to & \mathbb{N}^* \\ n & \mapsto & Card(\{m \in \mathbb{N}^* | m \leq n \text{ et m premier avec n }\}) \end{array}$$

8. Nous noterons Z le **centre** de K, pour tout $x \in K$, Z_x sera le sous-ensemble des éléments de K qui commutent avec x, nous prendrons de plus $q \in \mathbb{N}$ telle que $q = Card(Z)$. Nous supposerons connue la propriété : " *Soit L un sous-corps de K (corps fini), alors il existe $s \in \mathbb{N}$ tel que $Card(K) = Card(L)^s$* ".
9. Pour K un corps fini, dans la dernière partie, nous noterons $n \in \mathbb{N}$ tel que :

$$Card(K) = q^n$$

*Le but du devoir est de montrer le théorème de Wedderburn "***Tout corps fini est commutatif***".*

Partie 1 : Étude de la caractéristique d'un corps.

a. Montrer que les éléments premiers de $\mathbb{Z}$ sont les nombres premier.

b. On considère l'application $\varphi : n \mapsto n.1_K$. Montrer que φ est un morphisme d'anneaux entre $(\mathbb{Z}, +, \times)$ et $(K, +, .)$.

c. Que dire de $\mathbb{Z}/\text{Ker}(\varphi)$ et $\text{Im}(\varphi)$?

d. Montrer que la caractéristique d'un corps est soit nulle, soit un nombre premier.

e. Montrer qu'un nombre $p \in \mathbb{N}$ est premier si et seulement s'il divise $\binom{p}{k}$ pour tout $k \in [\![1; p-1]\!]$.

f. On suppose que K est un corps qui a pour caractéristique $p > 0$. Montrer que l'application $x \longleftrightarrow x^p$ est un isomorphisme de K.
Indication : Remarquer que $(x + y)^p = x^p + y^p$ avec $x, y \in K$.

Partie 2 : Étude des racines de l'Unité .

Dans cette partie, nous supposerons K commutatif. Nour prendrons $p > 0$ la caractéristique de K.

a. Montrer que $U(K)$ forme un sous groupe multiplicatif de $K\backslash\{0\}$.

b. Montrer que les racines de l'unité sont des éléments d'ordre fini du groupe multiplicatif $K\backslash\{0\}$.

c. Si x est une racine de l'unité dans K alors sont ordre n'est pas divisible par p.

d. Pour tout entier $m > 0$ il n'existe pas dans K de racine p^m-ième de l'unité autre que 1.

e. Soit $n \in \mathbb{N}$, montrer que le groupe $U_n(K)$ est un groupe cyclique d'ordre n.

Partie 3 : Polynômes cyclotomiques .

a. Soient n et m deux entiers et soit d leur PGCD. Le PGCD de $X^n - 1$ et $X^m - 1$ dans $K[X]$ est égal à $X^d - 1$.
Montrer que pour tout $n \in \mathbb{N}$, si la décomposition en produits de facteurs premiers s'écrit $\prod_{i=1}^{r} p_i^{k_i}$ avec p_i des nombres premiers distincts, r, et les (k_i) des entiers naturels alors :

$$\varphi(n) = n \prod_{i=1}^{r} (1 - \frac{1}{p_i})$$

b. En déduire pour un même $n \in \mathbb{N}$:

$$n = \sum_{d|n} \varphi(d)$$

c. Nous appelons polynôme cyclotomique pour $n \in \mathbb{N}^*$:

$$\Phi_n(X) = \prod_{i=1}^{\varphi(n)} (X - \zeta_i)$$

avec $(\zeta_i)_{1 \leq i \leq \varphi(n)}$ les racine n-ième primitive de l'unité.
Montrer que pour tout $n \in \mathbb{N}$:

$$X^n - 1 = \prod_{d|n; d \in]0;n[} \Phi_d(X).$$

d. Montrer que pour $m, n \in \mathbb{N}$ telle que pour $m|n$ et $m < n$ on ait dans $\mathbb{Z}[X]$:

$$\Phi_n(X) | \frac{X^n - 1}{X^m - 1}.$$

Partie 4 : Théorème de Wedderburn .

Le but du devoir est de montrer le théorème de Wedderburn " Tout corps fini est commutatif".

Pour se faire nous supposerons par l'absurde que $K \neq Z$.

a. Montrer que Z_x est un sous corps de Z.
Nous noterons l'opération de conjugaison "$*$", la loi qui à un sous-corps L de K et $x \in K$ donne :

$$L^* * x = \{yxy^{-1} | y \in L\}$$

b. Nous appelons **stabilisateur** de $x \in K$ l'ensemble des éléments de K qui laissent inchangé x par conjugaison :

$$stab(x) = \{y \in K | yxy^{-1} = x\}$$

Montrer que pour tout $y \in K^*$, il existe un entier $d(y)$ tel que :

$$Card(stab(y)) = q^{d(y)}$$

En déduire que que $d(y)|n$.

c. Montrer que $card(K^*x) = 1$ si et seulement si $x \in Z^*$. En déduire que pour $z_0 = 0, \ldots, z_q \in Z$ on a $Z = \bigcup_{0 \leq i \leq q-1} K^* * z_i$.

Nous supposerons la formule des classes : si K^* s'écrit comme réunion de $K^* * y_i$ avec les $y_i \in K^*$ et $i \in [1; p]$ pour $p \in \mathbb{N}^*$ alors :

$$Card(K) = \sum_{1 \leq i \leq p} \frac{Card(K^*)}{Card(stab(y_i)}$$

Nous supposerons que nous pouvons écrire $K^* \backslash Z$ comme réunions de $K^* * y_i$ avec les $y_i \in K^* \backslash Z$ et $i \in [1; r]$ pour $r \in \mathbb{N}^*$.

d. En déduire l'égalité :

$$q^n - 1 = q - 1 + \sum_{1 \leq i \leq r} \frac{q^n - 1}{q^{d(y_i)} - 1}$$

Posons le polynôme :

$$F(X) = X^n - 1 + \sum_{1 \leq i \leq r} \frac{X^n - 1}{X^{d(y_i)} - 1}$$

e. Montrer que $F \in \mathbb{Z}[X]$.

f. Montrer qu'il existe $Q \in \mathbb{Z}[X]$ telle que $F = Q\Phi_n$.

g. En déduire que :

$$|\Phi(q)| \leq q - 1$$

h. En déduire qu'il existe une racine $u \in \mathbb{C}$ telle que $|q - u| \leq q - 1$.

i. Montrer que $|q - u| > q - 1$. *Indication* : Faire un dessin...

j. En déduire que tout corps fini est commutatif (Théorème de Wedderburn).