Problème

Notations et rappels

Si k est un corps commutatif tout élément de $k[t]$ se factorise de manière unique sous la forme d'un produit de polynômes irréductibles. Si $f(t) = cp_1^{n_1} \dots p_l^{n_l}$ est une telle factorisation pour $f(t) \in k[t]$ ($n_i > 0$, p_i irréductibles,$0 \neq c \in k$), on note $r(f) := p_1 \dots p_l$. Si $f,g \in k[t]$, on note (f,g) le pgcd de f et g et $f|g$ pour signifier que f divise g. la dérivée de $f(t) \in k[t]$ est notée f' et $deg(f)$ désigne le degré de $f \in k[t]$.

Dans la première partie on prouve un résultat qui montre que si des polynômes $A,B,C \in k[t]$ sont tels que $A + B = C$, alors le nombre de facteurs premiers de ABC ne peut pas être trop petit.

Dans la deuxième partie on utilise le résultat établit en I) pour montrer que le "grand" théorème de Fermat est vrai pour les polynômes dans $\mathbb{C}[t]$. On donne ensuite une deuxième preuve de ce résultat indépendante de la première partie.

Dans la troisième partie on applique à nouveau la première partie pour prouver qu'une certaine équation n'a pas de solutions dans $\mathbb{C}(t)$.

Partie I

Soit k un corps commutatif

A)

1. $m,a,b \in k[t]$ tel que $(a,m) = 1$, montrer que $m|ab$ implique $m|b$.
2. Montrer que si $a|m$, $b|m$ et $(a,b) = 1$ alors $ab|m$.
3. Montrer que $\frac{f}{r(f)}|f'$.

B) On suppose que $A,B,C \in k[t]$ sont des polynômes non nuls tels que $A + B + C = 0$, $(A,B,C) = 1$ et $deg(A) \geq deg(r(ABC))$.

1. Montrer que $(A,B) = (B,C) = (A,C) = 1$.
2. Montrer que $C'B - CB' = AB' - A'B$.
3. Montrer que $\frac{A}{r(A)} \frac{B}{r(B)} \frac{C}{r(C)} \mid C'B - B'C$.
4. Montrer que $deg \frac{ABC}{r(ABC)} > deg(C'B - CB')$.
5. Conclure que l'on doit avoir $A' = B' = C' = 0$.

C)

1. Montrer que si le corps k est de caractéristique nulle et si $A,B,C \in k[t]$ sont des polynômes non constants tels que $A+B+C = 0$ et $(A,B,C) = 1$ alors
$$max\{deg(A),deg(B),deg(C)\} \leq deg(r(ABC)) - 1$$
2. Montrer que cette dernière égalité n'est pas vraie si le corps n'est pas de caractéristique nulle.

Partie II

A)

1. Montrer que pour $n > 2$, il n'existe pas de polynômes $X,Y,Z \in \mathbb{C}[t]$ dont l'un au moins est de degré ≥ 1 et tels que $X^n + Y^n = Z^n$. (aide montrer que l'on peut supposer X,Y,Z premiers entre eux et utiliser la première partie pour prouver que $ndeg(X) \leq deg(X) + deg(Y) + deg(Z) - 1$).
2. Trouver un triplet $(X,Y,Z) \in \mathbb{C}[t] \setminus \mathbb{C}$ tel que $X^2 + Y^2 = Z^2$.

B) On va redémontrer le résultat en II, A,1 ci dessus indépendamment de la première partie. On pose $\epsilon = e^{2i\pi/n}$ et on suppose que $a,b,c \in \mathbb{C}[t]$ sont tels que $a^n + b^n = c^n$ où $n > 2$. et l'un au moins des polynômes a,b,c est de degré ≥ 1.

1. Montrer que l'on peut supposer n premier et $(a,b,c) = 1$.
2. Montrer que $a^n + b^n = (a+b)(a+b\epsilon)\dots(a+b\epsilon^{n-1})$. (remarquer que 2 et le seul premier pair).
3. Montrer que $(a + b\epsilon^r, a + b\epsilon^s) = 1$ si $r \neq s$ $(1 \leq r,s \leq n-1)$.
4. Montrer que pour tout $i \in \{1,\dots,n-1\}$ il existe $f_i(t) \in \mathbb{C}[t]$ tels que $a + b\epsilon^i = f_i^n$.
5. Montrer que $a = \frac{f_1^n - \epsilon f_0^n}{1-\epsilon}$, $b = \frac{f_1^n - f_0^n}{\epsilon - 1}$ et $f_2^n = (\epsilon+1)f_1^n - \epsilon f_0^n$.
6. On pose $a_1 = (\sqrt[n]{\epsilon+1})f_1$ et $b_1 = -\sqrt[n]{\epsilon} f_0$, montrer que le triplet (a_1,b_1,f_2) satisfait l'équation $X^n + Y^n = Z^n$.
7. On pose $N := max\{deg(a),deg(b),deg(c)\}$ montrer que
$$max\{deg(a_1),deg(b_1),deg(f_2)\} \leq \frac{N}{n}$$
.
8. Conclure qu'il n'existe pas de polynômes $X,Y,Z \in \mathbb{C}[t]$ dont l'un au moins est de degré ≥ 1 et tels que $X^n + Y^n = Z^n$.

Partie III

Soient $x,y \in \mathbb{C}(t)$ tels que $y^2 = x^3 + x$. On pose $x = \frac{m}{M}$ $y = \frac{n}{N}$ où $m,N,m,n \in \mathbb{C}[t]$ et $(m,M) = 1 = (n,N)$.

1. Montrer que $M^3 = cN^2$ pour un ceratin $0 \neq c \in \mathbb{C}$. En déduire que l'on peut supposer que $M^3 = N^2$. On fait cette hypothèse pour la suite...
2. Montrer qu'il existe $e \in \mathbb{C}[t]$ tel que $M = e^2$ et $N = e^3$.
3. Montrer que $n^2 = m(m^2 + e^4)$ et en déduire qu'il existe $u \in \mathbb{C}[t]$ tel que $m = u^2$.
4. Montrer qu'il existe $z \in \mathbb{C}[t]$ tel que $u^4 + e^4 = z^2$et utiliser la partie I) pour conclure que l'équation $y^2 = x^3 + x$ n'a pas de solution non triviale dans $\mathbb{C}(t)$.