EPFL - Printemps 2023	Prof. Zs. Patakfalvi
Anneaux et Corps	**Exercices**
Corrigé – bonus 5	

Exercice bonus 5. Soit $n \geq 1$ un entier. On dit qu'une racine n-ième de l'unité ξ est primitive si n est le plus petit entier tel que $\xi^n = 1$. On pose,

$$\Phi_n(t) = \prod_{\substack{\xi \text{ racine} \\ \text{primitive} \\ n\text{-ième} \\ \text{de l'unité}}} (t - \xi) \in \mathbb{C}[t].$$

1. Montrer que $t^n - 1 = \prod_{d|n} \Phi_d(t)$ et que $\Phi_n(t) \in \mathbb{Z}[t]$.

2. Soit p un nombre premier et $n \geq 1$. En utilisant le critère d'Eisenstein et le changement de variable $t \mapsto t + 1$, montrer que $\Phi_{p^n}(t)$ est irréductible. (*c.f.* exemple 3.9.4.(2))

3. Soit $n \geq 1$ un entier et p un premier qui est premier avec n. On note ξ_n une racine primitive n-ième de l'unité. Soit $m(t) \in \mathbb{Q}[t]$ le polynôme minimal de ξ_n. Montrer que $m(t) \in \mathbb{Z}[t]$. Montrer que si ξ est une racine de $m(t)$, alors ξ^p est une racine de $m(t)$. En déduire que $m(t) = \Phi_n(t)$.

   Indication: on pourra montrer par l'absurde que si ξ^p n'est pas une racine de $m(t)$ alors $t^n - 1$ a une racine double modulo p, ce qui est absurde comme $(n, p) = 1$ (Voir Proposition 4.4.10).

4. Montrer qu'il existe une infinité de premiers p tel que $\Phi_n(t)$ a une racine dans $\mathbb{F}_p[t]$. En déduire qu'il existe une infinité de premiers p tel que $p \equiv 1 \mod n$.

   Indication: pour tout m suffisamment grand si un nombre premier p divise $\Phi_n(m!)$ alors $p > m$.

Solution.

1. Notons que comme le produit de toutes les racines n-ièmes de l'unité sont égales au produit des racines primitives d-ièmes pour $d \mid n$, on a

$$t^n - 1 = \prod_{d|n} \Phi_d(t).$$

   On montre par récurence sur n que $\Phi_n(t)$ a coefficients entiers. Pour $n = 1$, on a $\Phi_1(t) = (t - 1)$. Pour $n > 1$ notons que $\Phi_n(t)$ est le résultat de la division euclidienne dans $\mathbb{Z}[t]$ de $t^n - 1$ par $\prod_{d|n, d \neq n} \Phi_d(t)$ et ce dernier polynôme est bel et bien à coefficients entiers par récurence.

   Barème. 10 pts pour $t^n - 1 = \prod_{d|n} \Phi_d(t)$, et 10 pts pour montrer que les coefficients du polynôme sont entiers.

2. Notons tout d'abord que

$$t^p - 1 = (t - 1)\Phi_p(t),$$

   et donc que $\Phi_p(t) = t^{p-1} + t^{p-2} + \cdots + 1$. Notons également que

$$t^{p^n} - 1 = (t^{p^{n-1}} - 1)\Phi_{p^n}(t),$$

   et donc que $\Phi_{p^n}(t) = \Phi_p(t^{p^{n-1}})$. Notons que $\Phi_{p^n}(t+1) \equiv (\Phi_p(t+1))^{p^{n+1}} = t^{p^{n+1}} \mod p$ par le raisonnement de l'exemple 3.9.4.(2). Comme de plus le coefficient constant de $\Phi_{p^n}(t+1)$ est égal à p, le critère d'Einsenstein permet de conclure à l'irréductibilité de $\Phi_{p^n}(t)$.

   Barème. 10 pts pour montrer que $\Phi_{p^n}(t) = \Phi_p(t^{p^{n-1}})$. 10 pts pour conclure avec Eisenstein.

3. Écrivons $t^n - 1 = m(t)g(t)$ avec $g(t) \in \mathbb{Q}$. Comme $m(t)$ et $t^n - 1$ ont coefficients dominant 1, g aussi. Dès lors pour $c, d \in \mathbb{Z}$, on a

$$t^n - 1 = \frac{1}{c}(cm(t))\frac{1}{d}(dg(t)))$$

pour $cm(t), dg(t) \in \mathbb{Z}[t]$ primitifs. Par le lemme de Gauss (version II), on a $\frac{1}{cd} \in \mathbb{Z}^\times$. Donc $\frac{1}{d} = \pm c \in \mathbb{Z}$ et donc $c, d = \pm 1$. Ainsi $m(t) \in \mathbb{Z}[t]$.

Soit ξ une racine quelconque de $m(t)$ et par l'absurde supposons que ξ^p ne soit pas une racine de $m(t)$. Alors si $t^n - 1 = m(t)f(t)$ on a que ξ^p est une racine de $f(t)$. Comme $m(t)$ est irréductible dans $\mathbb{Q}[t]$, notons que c'est aussi le poolynôme minimal de ξ. Dès lors $m(t)|f(t^p)$ dans $\mathbb{Q}[t]$ et donc dans $\mathbb{Z}[t]$ comme ces polynômes sont primitifs. En réduisant modulo p (ce qu'on dénote par $\overline{(-)}$ dans la suite), on voit alors que $\overline{m(t)}|\overline{f(t^p)} = (\overline{f(t)})^p$. Dès lors, $\overline{m(t)}$ et $\overline{f(t)}$ ont une racine commune, car les racines (sans compter les multiplicités) de $\overline{f(t)}$ et $(\overline{f(t)})^p$ sont les mêmes. Mais comme $\overline{t^n - 1} = \overline{m(t)f(t)}$ n'as pas de racine multiple comme $(n, p) = 1$, on obtient une contradiction.

Notons que toute racine primitive n-ième de l'unité est de la forme $\xi_n^{p_1 \cdots p_r}$ avec $(p_i, n) = 1$. On obtient par récurence sur r que toute racine primitive n-ième de l'unité est une racine de $m(t)$ et donc que $\Phi_n(t) = m(t)$.

Barème. 10 pts pour montrer que $m(t)$ est à coefficients entiers. 20 pts pour montrer si ξ est une racine de $m(t)$ alors, ξ^p aussi. 5 pts pour $\Phi_n(t) = m(t)$.

4. Soit m suffisamment grand pour que $\Phi_n(m!) \neq 0, 1, -1$. Soit alors p premier tel que $p \mid \Phi_n(m!)$. Alors $p \mid (m!)^n - 1$. Si $p \leq m$, on aurait $p \mid 1$, ce qui est absurde. Ainsi, il suit qu'il existe une infinité de premiers tel que $\overline{\Phi_n(t)} \in \mathbb{F}_p[t]$ a une racine dans $\mathbb{F}_p$. En effet, on peut prendre un $m' \geq p$ puis appliquer à nouveau l'argument pour m' pour trouver un premier $p' > m' \geq p$ et ainsi de suite pour construire une suite infinie croissante de premiers où $\overline{\Phi_n(t)}$ s'annule.

Notons que n est fixé et donc sans perte de généralité $(p, n) = 1$. Notons k le corps de décomposition de $\overline{t^n - 1} \in \mathbb{F}_p[t]$. On montre par récurence croissante sur les diviseurs d de n que les racines de $\overline{\Phi_d(t)}$ dans k sont exactement les racines primitives d-ième de l'unité. Pour $d = 1$, l'assertion est vérifiée car $\overline{\Phi_1(t)} = \overline{t - 1}$. Traitions le pas d'induction. Comme $(p, d) = 1$ le polynôme $\overline{t^d - 1} \in \mathbb{F}_p[t]$ n'a pas de racines multiples. Ainsi le sous-groupe multiplicatif des racines d-ième de l'unité est de cardinal d. Comme tous les éléments de ce sous-groupe multiplicatif sont des racines de $t^e - 1$ pour e l'exposant du groupe, on a forcément $d = e$ sinon $t^e - 1$ aurait trop de racines. Dés lors ce sous-groupe est cyclique d'ordre d. Grâce à la récurence les racines de $\overline{\Phi_{d'}(t)}$ pour tout diviseur $d' \neq d$ de d sont les racines primitives d'-ième de l'unité, c'est à dire les éléments multiplicatifs d'ordre d'. Par suite, en utilisant la formule du point 1., les racines de $\overline{\Phi_d(t)}$ sont forcément les éléments restants du groupe cyclique formé par les racines de $t^d - 1$, c'est à dire les éléments d'ordre d.

Dès lors si $\overline{\Phi_n(t)} \in \mathbb{F}_p[t]$ a une racine dans $\mathbb{F}_p$, cela implique qu'il existe une racine primitive n-ième de l'unité dans $\mathbb{F}_p$. En particulier, par Lagrange, $n \mid p - 1$, et donc que $p \equiv 1 \mod n$.

Barème. 10 pts pour montrer qu'il y a a une infinité de premiers tel que $\overline{\Phi_n(t)} \in \mathbb{F}_p[t]$ a une racine dans $\mathbb{F}_p$. 10 pts pour montrer que les racines de $\overline{\Phi_n(t)}$ sont des racines primitives de l'unité (noter que l'hypothèse $(p, n) = 1$ est importante pour cela.) 5 pts pour conclure avec Lagrange.