Algèbre Commutative 2023/2024
T.D.2

Exercice 1: On dit qu'un anneau commutatif A est local s'il possède un unique idéal maximal. Soit A un anneau local int ègre dont l'unique idéal maximal $\mathfrak{m}$ est principal, engendré par π.

(1) On suppose que $\cap_{n\geq 1}\mathfrak{m}^n = 0$. Montrer que tout $0 \neq a \in A$ s'écrit sous la forme $a = u\pi^n$ avec $u \in A^\times$, $n \geq 0$ et que cette écriture est unique. En déduire que A est principal (donc en particulier noetherien).

(2) On suppose que A est noetherien. Montrer que pour tout idéal $I \subset A$, $\mathfrak{m}I = I$ implique $I = 0$. En déduire que $\cap_{n\geq 1}\mathfrak{m}^n = 0$.

(1) Comme $a \notin \cap_{n\geq 1}\mathfrak{m}^n = 0$, il existe un unique $n \geq 0$ tel que $a \in \mathfrak{m}^n \setminus \mathfrak{m}^{n+1}$ *i.e.* $a = u\pi^n$ avec $u \in A \setminus \mathfrak{m} = A^\times$. Supposons de plus que A est intègre. Ecrivons $a = u\pi^n = v\pi^m$ avec $n \geq m$, ce qui implique (A est intègre) $1 = v^{-1}u\pi^{n-m}$ donc $n = m$ et $u = v$.
Maintenant (on ne suppose plus que A est intègre), si $0 \subsetneq I \subsetneq A$ est un idéal non trivial de A on se fixe $m \geq 1$ minimal tel que $\pi^m \in A$. On a évidemment $A\pi^m \subset I$. Inversement, tout $a \in I$ s'écrit sous la forme $a = u\pi^n$ avec $u \in A^\times$, $n \geq 0$ donc $\pi^n = u^{-1}a \in I$. Par minimalité de m cela implique $n \geq m$ donc $I \subset A\pi^m$.

(2) Comme A est noetherien, I est de type fini. Soit donc $a_1, \ldots, a_r \in I$ un système de longueur minimale de générateurs de I comme idéal. La condition $\mathfrak{m}I = I$ implique en particulier qu'il existe $\alpha_1, \ldots, \alpha_r \in A$ telq que $a_r = \pi(\alpha_1 a_1 + \cdots + \alpha_r a_r)$ ou, encore, $(1 - \pi\alpha_r)a_r = \alpha_1 a_1 + \cdots + \alpha_{r-1}a_{r-1}$. Mais comme $(1 - \pi\alpha_r) \in A \setminus \mathfrak{m} = A^\times$, on en déduit $a_r = ((1 - \pi\alpha_r))^{-1}(\alpha_1 a_1 + \cdots + \alpha_{r-1}a_{r-1})$, ce qui contredit la minimalité de r. La seconde partie de la question résulte de la première en prenant $I = \cap_{n\geq 0}\mathfrak{m}$.

Exercice 2: Soit A un anneau commutatif.

(1) Soit $a \in A$ et $I \subset A$ un idéal. Montrer que si les idéaux $I + Aa$ et $(I : Aa) := \{x \in A \mid ax \in I\}$ sont de type fini alors I est de type fini.

(2) [Utilise Zorn] Montrer que A est noetherien si et seulement si tous ses idéaux premiers sont de type fini.

(1) Soit $x_i + a_i a$ ($x_i \in I$, $a_i \in A$), $i = 1, \ldots, r$ un système de générateurs de l'idéal $I + Aa$ et $y_1, \ldots, y_s \in (I : Aa)$ un système de générateurs de l'idéal $(I : Aa)$. En particulier, $ay_i \in I$, $i = 1, \ldots, s$. Soit maintenant $x \in I$. Comme $I \subset I + Aa$, on peut écrire $x = \sum_{1\leq i\leq r}\alpha_i(x_i + ay_i)$ ou, encore, $x - \sum_{1\leq i\leq r}\alpha_i x_i = (\sum_{1\leq i\leq r}\alpha_i y_i)a$. Comme $x - \sum_{1\leq i\leq r}\alpha_i x_i \in I$, on a $\sum_{1\leq i\leq r}\alpha_i y_i \in (I : Aa)$ donc on peut écrire $\sum_{1\leq i\leq r}\alpha_i y_i = \sum_{1\leq i\leq s}\beta_i y_i$. En réinjectant cela dans l'écriture de x, on obtient $x = \sum_{1\leq i\leq r}\alpha_i x_i + \sum_{1\leq i\leq s}\beta_i a y_i$. Cela montre que $I \subset \sum_{1\leq i\leq r}Ax_i + \sum_{1\leq i\leq s}Aay_i$. Inversement, comme $x_1, \ldots, x_r, ay_1, \ldots, ay_s \in I$, on a $\sum_{1\leq i\leq r}Ax_i + \sum_{1\leq i\leq s}Aay_i \subset I$.
Rem. Les A-modules n'ont pas encore été traités en cours mais quand on l'aura fait, on pourra raisonner comme suit. En considérant le morphisme de A-modules $L_a : A \to A$, $x \mapsto ax$, on a $(I : Aa) := L_a^{-1}(I)$ et $L_a((I : Aa)) = I \cap Aa$; en particulier, si $(I : Aa)$ est de type fini alors $I \cap Aa$ l'est aussi. De plus, on a la suite exacte courte de A-modules $0 \to I \cap Aa \to I \to I/(I \cap Aa) \to 0$ avec $I/(I \cap Aa) \xrightarrow{\sim} (I + Aa)/Aa \twoheadleftarrow I + Aa$. En particulier, si $I + Aa$ est de type fini alors $I/(I \cap Aa)$ est de type fini. On conclut par le fait général (et élémentaire) que dans une suite exacte courte de A-modules $0 \to M' \to M \to M'' \to 0$, M est de type fini ssi M' et M'' sont de type fini.

(2) Le sens $\Rightarrow$ est immédiat. Pour le sens $\Leftarrow$, on raisonne par l'absurde en observant que l'ensemble $\mathcal{E}$ des idéaux de A qui ne sont pas de type fini est ordonné inductif donc, s'il est non vide, par Zorn, il possède un élément maximal I pour $\subset$. Par hypothèse, I n'est pas premier. Observons que $I \subset I + Aa$ et $I \subset (I : Aa)$. Si on peut trouver $a \in A$ de sorte que $I \subsetneq I + Aa$ et $I \subsetneq (I : Aa)$ on aura gagné car, par maximalité de I, cela imposera que $I + Aa$ et $(I : Aa)$ sont tous deux de type fini donc, par la question 1., que I lui-même est de type fini, contredisant la définition de $\mathcal{E}$. Mais comme I n'est pas premier, il existe $a, b \in A$ tels que $a, b \notin I$ mais $ab \in I$. Or $a \notin I$ assure $I \subsetneq I + Aa$ tandis que $ab \in I$ assure $b \in (I : Aa)$ donc, puisque $b \notin I$, $I \subsetneq (I : Aa)$.

Exercice 3: Soit A un anneau commutatif. On dit qu'un idéal I de A est irréductible si pour tout idéaux I_1, I_2 de A, $I = I_1 \cap I_2$ implique $I = I_1$ ou $I = I_2$. On suppose de plus A noetherien. Montrer que

(1) tout idéal $I \subset A$ est intersection d'un nombre fini d'idéaux irréductibles;

(2) pour tout idéal $I \subset A$ irréductible, $\sqrt{I}$ est premier;

(3) tout idéal radiciel $I \subset A$ est intersection d'un nombre fini d'idéaux premiers;

(4) A ne possède un nombre fini d'idéaux premiers minimaux pour $\subset$.

(1) Sinon, l'ensemble $\mathcal{E}$ des idéaux de A qui ne sont pas intersections d'un nombre fini d'idéaux irréductibles est non-vide. Comme A est noetherien, il a admet donc un élément maximal I pour l'inclusion. Comme I n'est pas irréducitble, $I = I_1 \cap I_2$ avec $I \subsetneq I_1, I_2$ des idéaux de A. Mais par maximalité de I, I_1 et I_2 sont tous deux intersection d'un nombre fini d'idéaux irréductibles de A, ce qui contredit $I \in \mathcal{E}$. Donc $\mathcal{E} = \emptyset$.

(2) En considérant $\mathrm{p}_I : A \twoheadrightarrow A/I$, on peut supposer que $I = \{0\}$ (utiliser que A/I est encore noetherien, que l'image d'un idéal irréductible de A contenant I est irréductible, que $p_I^{-1}(\sqrt{0}) = \sqrt{I}$ et $p_I^{-1}(spec(A/I)) \subset spec(A)$). Soit donc $a, b \in A$ tel que $(ab)^n = 0$ pour un certain $n \geq 1$. Supposons $b \notin \sqrt{0}$. Pour simplifier, réécrivons $a := a^n$, $b := b^n$ et notons

$$I_n := \{\alpha \in A \mid \alpha a^n = 0\}.$$

On vérifie que I_n est un idéal de A et que $I_n \subset I_{n+1}$. Comme A est noetherien, il existe $N \geq 1$ tel que $I_n = I_{n+1}$, $n \geq N$. J'affirme que $Aa^N \cap Ab = 0$. Sinon, il existe $0 \neq \beta b = \alpha a^N \in Aa^N \cap Ab$ donc $0 = \beta ab = \alpha a^{N+1}$ i.e. $\alpha \in I_{N+1} = I_N$ i.e. $\beta b = \alpha a^N = 0$: contradiction. Mais comme on a supposé 0 irréductible et que $Ab \neq 0$, cela impose $a^N = 0$ donc que a est nilpotent. On a gagné.

(3) Commençons par observer que la racine commute avec l'intersection finie: Soit $J, J_1, \ldots, J_r \subset A$ des idéaux tels que $J = J_1 \cap \cdots \cap J_r$. L'inclusion $\sqrt{J} \subset \sqrt{J_1} \cap \cdots \cap \sqrt{J_r}$ est claire. Pour l'incusion réciproque, si $a \in \sqrt{J_1} \cap \cdots \cap \sqrt{J_r}$, pour $i = 1, \ldots, r$, il existe $n_i \geq 1$ tel que $a^{n_i} \in J_i$. Donc avec $n :=\max\{n_1, \ldots, n_r\}$ on a $a^n \in J_1 \cap \cdots \cap J_r = J$ *i.e.* $a \in \sqrt{J}$. D'après (1) pour tout idéal I de A il existe des idéaux $I_1, \ldots, I_r$ irréductibles de A tels que $I = I_1 \cap \cdots \cap I_r$. D'après ce qu'on vient d'observer $I = \sqrt{I} = \sqrt{I_1} \cap \cdots \cap \sqrt{I_r}$ et, d'après (2) $\sqrt{I_1}, \ldots, \sqrt{I_r}$ sont premiers.

(4) D'après (3), $\sqrt{0} = \cap_{\mathfrak{p} \in spec(A)} \mathfrak{p}$ est intersection d'un nombre fini $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ d'idéaux premiers de A. Donc pour tout $\mathfrak{p} \in spec(A)$, $\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r \subset \mathfrak{p}$. Mais comme $\mathfrak{p}$ est premier, d'après l'Exercice 10 du TD 1, cela implique qu'il existe $1 \leq i \leq r$ tel que $\mathfrak{p}_i \subset \mathfrak{p}$. Les idéaux premiers minimaux de A pour $\subset$ sont donc contenus dans les $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$.

Exercice 4: Montrer que $A[X]$ est principal si et seulement si A est un corps.

Si A est un corps, $A[X]$ est euclidien donc principal. Inversement, comme $A[X]/X \tilde{\to} A$, il suffit de montrer que $XA[X]$ est un idéal maximal de $A[X]$. Mais comme $A[X]$ est principal, il suffit de montrer

que X est irréductible dans $A[X]$. Ecrivons donc $X = PQ$ dans $A[X]$. En prenant les degrés on a $1 = deg(X) = deg(P) + deg(Q)$ avec $deg(P) \leq deg(Q)$, où la deuxième égalité utilise que A est intègre. Donc, nécessairement $deg(P) = 0$ et $deg(Q) = 1$. En écrivant $P = a_0$, $Q = b_0 + b_1X$, la condition $X = PQ$ se réécrit alors en $a_0b_0 = 0$, $a_0b_1 = 1$. En particulier, $a_0 \in A^\times \subset A[X]^\times$. C'est bien ce que l'on voulait montrer.

Exercice 5: Si K est un corps, on note $K(X_1, \ldots, X_n) := Frac(K[X_1, \ldots, X_n])$. Montrer que si A est un anneau intègre de corps des fractions K alors $Frac(A[X_1, \ldots, X_n]) = K(X_1, \ldots, X_n)$.

Par prop. univ de $A[X_1, \ldots, X_n]$ appliquée à $A \hookrightarrow K \hookrightarrow K[X_1, \ldots, X_n] \hookrightarrow K(X_1, \ldots, X_n)$ il existe un unique morphsisme de A-algèbres $\phi : A[X_1, \ldots, X_n) \to K(X_1, \ldots, X_n)$ tel que $\phi(X_i) = X_i$, $i = 1, \ldots, n$. On vérfiie immédiatement que $\phi : A[X_1, \ldots, X_n) \to K(X_1, \ldots, X_n)$ donc, comme $K(X_1, \ldots, X_n)$ est un corps, $\phi : A[X_1, \ldots, X_n) \to K(X_1, \ldots, X_n)$ se localise en un morphisme $\phi : Frac(A[X_1, \ldots, X_n]) \to K(X_1, \ldots, X_n)$. Comme $Frac(A[X_1, \ldots, X_n])$ est un corps, $\phi : Frac(A[X_1, \ldots, X_n]) \to K(X_1, \ldots, X_n)$ est injectif. Par ailleurs, pour tout $F = P/Q \in K(X_1, \ldots, X_n)$ avec $P, Q \in K[X_1, \ldots, X_n]$, on peut mettre les coefficients de P, Q au même dénominateurs *i.e.* il existe $0 \neq a, b \in A$ tels que $aP, bQ \in A[X_1, \ldots, X_n]$. Mais alors, $F = P/Q = b/aaP/bQ = \phi(b/a)\phi(aP/bQ)$ donc $\phi : Frac(A[X_1, \ldots, X_n]) \to K(X_1, \ldots, X_n)$ est aussi surjectif.

Exercice 6: Soit k un corps et $A = k[X_1, \ldots, X_4]/X_1X_2 - X_3X_4$. On note $x_i \in A$ l'image de X_i par la projection canonique $p : k[X_1, \ldots, X_4] \to A$, $i = 1, \ldots, 4$.

(1) Montrer que le morphisme canonique d'anneaux $\phi : k[X_3, X_4] \to A$, $X_i \mapsto x_i$, $i = 3, 4$ est injectif;

(2) Montrer que tout $a \in A$ s'écrit de façon unique sous la forme $a = a_0 + x_1a_1(x_1) + x_2a_2(x_2)$ avec $a_0 \in k[x_3, x_4]$, $a_1, a_2 \in k[x_3, x_4][T]$;

(3) Construire un morphisme injectif d'anneaux $A \hookrightarrow k[X_3, X_4][T, T^{-1}]$ et en déduire que A est intègre.

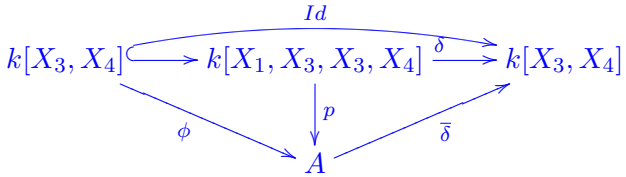
(4) Montrer que les x_i, $i = 1, \ldots, 4$ sont irréductibles et deux à deux non associés dans A;

(5) En déduire que A n'est pas factoriel.

(1) Par prop. univ. de $k[X_3, X_4][X_1, X_2,]$ il existe un unique morphisme de $k[X_3, X_4]$-algèbres

$$\delta : k[X_1, X_3, X_3, X_4] \to k[X_3, X_4]$$

tel que $\delta(X_1) = X_3$, $\delta(X_2) = X_4$. Comme $X_1X_2 - X_3X_4 \subset \ker(\delta)$, on en déduit une factorisation



Comme $\delta \circ \phi = Id$ on a, en particulier, que ϕ est injectif.

(2) On peut écrire tout $P \in k[X_1, X_3, X_3, X_4]$ dans $k[X_3, X_4][X_1, X_2]$ sous la forme

$$P = \sum_{n\geq 0} a_{(n,n)}(X_1X_2)^n + \sum_{0\leq n_1<n_2} a_{(n_1,n_2)}(X_1X_2)^{n_1}X_2^{n_2-n_1} + \sum_{0\leq n_2<n_1} a_{(n_1,n_2)}(X_1X_2)^{n_2}X_1^{n_1-n_2}$$

donc

$$p(P) = \sum_{n\geq 0} p(a_{(n,n)})(x_3x_4)^n + \sum_{0\leq n_1<n_2} p(a_{(n_1,n_2)})(x_3x_4)^{n_1}x_2^{n_2-n_1} + \sum_{0\leq n_2<n_1} p(a_{(n_1,n_2)})(x_3x_4)^{n_2}x_1^{n_1-n_2}$$

est bien de la forme demandée. Pour l'unicité, il suffit de montrer que pour tout $P = a_0 + X_1a_1(X_1) + X_2a_2(X_2) \in k[X_1, X_3, X_3, X_4]$ avec $a_0 \in k[X_3, X_4]$, $a_1 \in k[X_3, X_4][X_1]$, $a_2 \in k[X_3, X_4][X_2]$, $X_1X_2 - X_3X_4|P$ implique $P = 0$. Supposons donc qu'il existe $Q = \sum_{n\geq 0}(X_1X_2)^nQ_n$ avec $Q_n = a_{n,0} +$

$X_1a_{n,1}(X_1)+X_2a_{n,2}(X_2)$ et $a_{n,0}\in k[X_3,X_4]$, $a_{n,1}\in k[X_3,X_4][X_1]$, $a_{n,2}\in k[X_3,X_4][X_2]$, $n\geq 0$ tel que tel que $P=(X_1X_2-X_3X_4)Q$. En développant on obtient $P=-X_3X_4Q_0$ et $\sum_{n\geq 1}(Q_{n-1}-X_3X_4Q_n)(X_1X_2^n)=0$ ou encore, $P=-X_3X_4Q_0$ et $Q_{n-1}=X_3X_4Q_n$, $n\geq 1$. Mais comme $Q_n=0$, $n\gg 0$, cela implique $Q_n=0$, $n\geq 0$ donc $P=0$.

(3) Par prop. univ de $k[X_3,X_4][X_1,X_2]$ il existe un unique morphisme $\psi: k[X_1,X_3,X_3,X_4]\to k[X_3,X_4][T,T^{-1}]$ de $k[X_3,X_4]$-algèbres tel que $\psi(X_1)=T$ et $\psi(X_2)=X_3X_4T^{-1}$. Clairement $X_1X_2-X_3X_4\in\ker(\psi)$ donc $\psi: k[X_1,X_3,X_3,X_4]\to k[X_3,X_4][T,T^{-1}]$ se factorise en

$$\begin{array}{ccc} k[X_1,X_3,X_3,X_4] & \xrightarrow{\psi} & k[X_3,X_4][T,T^{-1}] \\ {\scriptstyle p}\downarrow & \nearrow_{\overline{\psi}} & \\ A & & \end{array}$$

Et, pour tout $a=a_0+x_1a_1(x_1)+x_2a_2(x_2)\in A$,

$$a_0(X_3,X_4)+Ta_1(X_3,X_4,T)+X_3X_4T^{-1}a_2(X_3,X_4,T^{-1})=\overline{\psi}(a)=0$$

se réécrit dans $k[X_3,X_4][T,T^{-1}]$, en posant $a_1(X_3,X_4,T)=\sum_{n\geq 0}a_{1,n}T^n$, $a_2(X_3,X_4,T^{-1})=\sum_{n\geq 0}a_{2,n}T^{-n}$ sous la forme

$$a_0+\sum_{n\geq 1}a_{1,n-1}T^n+\sum_{n\geq 1}X_3X_4a_{n-1,2}T^{-n}=0$$

d'où $a_0=0$, $a_{1,n-1}=0$, $a_{2,n-1}=0$, $n\geq 0$ *i.e.* $a_0=a_1=a_2=0$. Cela montre que $\overline{\psi}: A\to k[X_3,X_4][T,T^{-1}]$ est injectif donc que A est intègre.

(4) Par symétrie, il suffit de voir que x_3 n'est pas irréductible. Ecrivons $x_3=p(P_1)p(P_2)$ dans A donc $X_3=\overline{\psi}(x_3)=P_1(T,X_3X_4T^{-1},X_3,X_4)P_2(T,X_3X_4T^{-1},X_3,X_4)$ dans $k[X_3,X_4][T,T^{-1}]$. Mais comme $k[X_3,X_4]$ est intègre, on en déduit

$$0=val_T(X_3)=val_T(P_1(T,X_3X_4T^{-1},X_3,X_4))+val(P_2(T,X_3X_4T^{-1},X_3,X_4))$$

$$0=deg_T(X_3)=deg_T(P_1(T,X_3X_4T^{-1},X_3,X_4))+deg(P_2(T,X_3X_4T^{-1},X_3,X_4))$$

donc, $val_T(P_i(T,X_3X_4T^{-1},X_3,X_4))=deg_T(P_i(T,X_3X_4T^{-1},X_3,X_4))=0$ ou encore $P_i(T,X_3X_4T^{-1},X_3,X_4)\in k[X_3,X_4]$, $i=1,2$. Mais alors, comme $k[X_3,X_4]$ est factoriel et X_3 irréductible (car premier) dans $k[X_3,X_4]$, cela impose $P_1(T,X_3X_4T^{-1},X_3,X_4)\in k[X_3,X_4]^\times=k^\times$ (ou $P_2(T,X_3X_4T^{-1},X_3,X_4)\in k[X_3,X_4]^\times=k^\times$) donc $p(P_1)=\overline{\psi}^{-1}(P_1(T,X_3X_4T^{-1},X_3,X_4))\in k^\times$ (ou ...). Le même argument montre que x_3,x_4 (donc par symmétrie x_1,x_2) ne sont pas associés dans A. Il rest à voir que c'est aussi le cas pour x_1,x_3 (donc par symmétrie x_1,x_4, x_2,x_3, x_2,x_4). Ecrivons $x_3=(a_0+x_1a_1(x_1)+x_2a_2(x_2))x_1=x_1(a_0+x_1a_1(x_1))-x_3x_4a_{2,0}-x_2(x_3x_4\sum_{n\geq 1}a_{2,n}x_2^{n-1})$. Par la question 2., cela impose $a_0=a_1=a_2=0$.

(5) Le fait que $x_1x_2=x_3x_4$ dans A et la question 5. montre qu'on n'a pas unicité de la décomposition en produit d'irréductible donc que A est intègre noetherien mais non factoriel. (On pourrait aussi observer que $A/x_1\tilde{\to}k[X_2,X_3,X_4]/X_3X_4$ n'est pas intègre donc x_1 est irréductible mais pas premier.

Exercice 7: (Entiers de Gauss) L'anneau des entiers de Gauss est, par définition, le sous-anneau $\mathbb{Z}[i]\subset\mathbb{C}$ engendré par $i:=\sqrt{-1}$. Notons $\mathcal{P}_{\mathbb{Z}}\subset\mathcal{P}$ l'ensemble des nombres premiers ≥ 2 et

$$\Sigma:=\{n\in\mathbb{N}\mid\exists a,b\in\mathbb{N},\ n=a^2+b^2\}.$$

(1) Montrer qu'on a un isomorphisme canonique d'anneaux $\mathbb{Z}[T]/T^2+1\tilde{\to}\mathbb{Z}[i]$.

Notons $N:\mathbb{Z}[i]\to\mathbb{N}$, $z\mapsto z\overline{z}$.

(2) Montrer que $N:\mathbb{Z}[i]\to\mathbb{N}$ est un morphisme de monoïdes et montrer que $\mathbb{Z}[i]^\times=\{z\in\mathbb{Z}[i]\mid N(z)=1\}=\{\pm 1,\pm i\}$;

(3) Montrer que $N:\mathbb{Z}[i]\to\mathbb{N}$ munit $\mathbb{Z}[i]$ d'un stathme euclidien;

(4) Montrer que pour tout $p \in \mathcal{P}_{\mathbb{Z}}$ les PSSE.

(i) p est irréductible dans $\mathbb{Z}[i]$;
(ii) $p \equiv 3[4]$;
(iii) p n'est pas somme de deux carrés dans $\mathbb{Z}$.

(5) Montrer que les éléments irréductibles de $\mathbb{Z}[i]$ sont - modulo $\mathbb{Z}[i]^\times$ - les éléments $p \in \mathbb{Z}$ tels que $p \equiv 3[4]$; $z \in \mathbb{Z}[i]$ tels que $N(z) \in \mathcal{P}_{\mathbb{Z}}$.

(6) Montrer qu'un entier $n \in \mathbb{N}$ est somme de deux carrés ssi pour tout $p \equiv 3[4]$, $2|\nu_p(n)$.

(1) Par prop. univ. de $\mathbb{Z}[X]$ appliquée à $(\mathbb{Z}[i], i)$, il existe un unique morphisme d'anneaux $\phi : \mathbb{Z}[X] \to \mathbb{Z}[i]$, $X \mapsto i$. Par définition de $\mathbb{Z}[i]$, ce morphisme est surjectif et, comme $i^2+1=0$, on a $(X^2+1)\mathbb{Z}[X] \subset \mathbb{Z}[i]$. Cette inclusion est en fait une égalité. En effet, comme 1 est inversible dans $\mathbb{Z}$, pour tout $P \in \mathbb{Z}[X]$, on peut effectuer la division euclidienne de P par X^2+1 dans $\mathbb{Z}[X]$: il existe $Q, R \in \mathbb{Z}[X]$ tel que $P = (X^2+1)Q + R$ avec $R = 0$ ou $R \neq 0$ et $deg(R) \leq 1$. En particulier, si $P \in \ker(\phi)$, $P(i) = R(i) = 0$ ce qui impose $R = 0$.

(2) La première partie de la question résulte de $|zz'| = |z||z'|$, $z, z' \in \mathbb{C}$ et $|1| = 1$. Pour la seconde partie de la question, on a clairement $N^{-1}(1) = \{\pm 1, \pm i\} \subset \mathbb{Z}[i]^\times$. Inversement, pour tout $z = a + ib \in \mathbb{Z}[i]$, $z \in \mathbb{Z}[i]^\times$ ssi il existe $z' \in \mathbb{Z}[i]$ tel que $zz' = 1$ donc en particulier $N(z)N(z') : N(zz') = N(1) = 1$. Mais comme $N(z), N(z') \in \mathbb{Z}_{\geq 0}$, cela impose $N(z) = N(z') = 1$. Or $N(z) = a^2 + b^2 = 1$ ssi $z = \pm 1, \pm i$.

(3) Soit $x, y \in \mathbb{Z}[i]$ avec $x \neq 0$. On cherche $q, r \in \mathbb{Z}[i]$ tels que $y = qx + r$ et $r = 0$ ou $N(r) < N(x)$. Or en écrivant $y = qx + r$ sous la forme $y/x = q + r/x$ et en observant que $N(r/x) = N(r)/N(x)$ (dans $\mathbb{Q}$), on voit qu'il suffit de trouver $q \in \mathbb{Z}[i]$ tel que $N(y/x - q) < 1$. Dans $\mathbb{Q}[i]$ on a $y/x = \alpha + i\beta$ et on peut toujours trouver $\alpha_0, \beta_0 \in \mathbb{Z}$ tels que $|\alpha - \alpha_0|, |\beta - \beta_0| \leq 1/2$. Donc $q = \alpha_0 + i\beta_0$ et $r = y - qx$ conviennent.

(4) Notons que $p \not\equiv 3[4]$ est un carré ($2 = 1 + 1$). On peut donc supposer $p > 2$ dans ce qui suit. (ii) $\Rightarrow$ (iii): si $a^2 + b^2 = p \equiv 3[4]$ par réduction modulo 4 on aurait $\overline{a}^2 + \overline{b}^2 = \overline{3}$ mais $\overline{3}$ n'est pas somme de deux carrés dans $\mathbb{Z}/4$.
(iii) $\Rightarrow$ (i): si p n'est pas irréductible dans $\mathbb{Z}[i]$, on peut écrire $p = zz'$ avec $z, z' \in \mathbb{Z}[i] \setminus \mathbb{Z}[i]^\times$ donc $p^2 = N(z)N(z')$ avec $N(z), N(z') \neq 1$. Par factorialité de $\mathbb{Z}$, cela impose $N(z) = N(z') = p$.
(i) $\Rightarrow$ (ii): comme $\mathbb{Z}[i]$ est (euclidien donc) principal, p est irréductible dans $\mathbb{Z}[i]$ ssi $\mathbb{Z}[i]/p$ est un corps. Mais on a

$$\mathbb{Z}[i]/p \xleftarrow{\sim} (\mathbb{Z}[X]/(X^2+1))/p \xrightarrow{\sim} \mathbb{Z}[X]/(p\mathbb{Z}[X] + (X^2+1)\mathbb{Z}[X]) \xrightarrow{\sim} \mathbb{F}_p[X]/(X^2+1).$$

Donc $\mathbb{Z}[i]/p$ est un corps ssi X^2+1 est irréductible dans $\mathbb{F}_p[X]$ *i.e.* ssi -1 n'est pas un carré dans $\mathbb{F}_p$. Supposons $p > 2$. J'affirme que

$$-1 \in (\mathbb{F}_p^\times)^2 \Leftrightarrow (-1)^{\frac{p-1}{2}} = 1 \Leftrightarrow p \equiv 1[4].$$

La deuxième équivalence est claire. Pour la première, comme $\mathbb{F}_p^\times \to \mathbb{F}_p^\times$, $x \mapsto x^2$ est un morphisme de groupes de noyau $\mathbb{Z}/2$ (on utilise $p > 2$), $(\mathbb{F}_p^\times)^2 \subset \mathbb{F}_p^\times$ est un sous-groupe d'indice 2 donc de cardinal $\frac{p-1}{2}$. En particulier, $-1 \in (\mathbb{F}_p^\times)^2$ implique $(-1)^{\frac{p-1}{2}} \equiv 1[p]$, ce qui équivaut à $(-1)^{\frac{p-1}{2}} = 1$ (toujours parce que $p > 2$). Cela montre le sens $\Rightarrow$ de la première implication. Inversement, le polynôme $T^{\frac{p-1}{2}} - 1$ a au plus $\frac{p-1}{2}$ racines distinctes dans $\mathbb{F}_p$ donc ses racines sont en fait exactement les éléments de $(\mathbb{F}_p^\times)^2$. Autrement dit pour $x \in \mathbb{F}_p^\times$, $x \in (\mathrm{F}_p^\times)^2$ si et seulement si $x^{\frac{p-1}{2}} = 1$ et on applique cela à $x = -1$.

(5) Notons $\mathcal{P}$ les éléments de $\mathbb{Z}[i]$ qui sont de l'une des deux formes suivantes: $p \in \mathcal{P}_{\mathbb{Z}}$ tels que $p \equiv 3[4]$; $z \in \mathbb{Z}[i]$ tels que $N(z) \in \mathcal{P}_{\mathbb{Z}}$.
On a vu que ceux du premier type sont irréductible dans $\mathbb{Z}[i]$ dans la question précédente. Pour ceux du second type, $z = xy$ dans $\mathbb{Z}[i]$ implique $N(z) = N(x)N(y)$ donc par factorialité de $\mathbb{Z}$ et comme $N(z)$ est premier dans $\mathbb{Z}$, $N(x) = 1$ (*i.e.* $x \in \mathbb{Z}[i]^\times$) ou $N(y) = 1$ (*i.e.* $y \in \mathbb{Z}[i]^\times$). Inversement, si $z \in \mathbb{Z}[i]$ est irréductible, on se fixe un diviseur premier p de $N(z)$ dans $\mathbb{Z}$. Mais $p|N(z) = z\overline{z}$. Si $p \equiv 3[4]$ on sait

que p est irréductible dans $\mathbb{Z}[i]$ donc $p|z$ ou $p|\overline{z}$ mais comme z, $\overline{z}$ sont aussi irréductibles, cela impose $p = z = \overline{z}$. Si $p \equiv 1[4]$, on sait que $p = a^2 + b^2 = (a+ib)(a-ib)$ avec $a \pm ib \notin \mathbb{Z}[i]^\times$ donc, par factorialité de $\mathbb{Z}[i]$ et comme z, $\overline{z}$ sont irréductibles, cela impose $z = a+ib$ (ou $z = a-ib$). En particulier, $N(z) = p$.

(6) On note $\Sigma = N(\mathbb{Z}[i])$ l'ensemble des nombres qui sont sommes de deux carrés. Notons que Σ est stable par produit par (1). Soit

$$n = \prod_{p \not\equiv 3[4]} p^{\mu_p(n)} \prod_{p \equiv 3[4]} p^{\nu_p(n)}$$

la décomposition de n en produit de facteurs irréductibles. Par (4); $p \not\equiv 3[4] \Rightarrow p \in \Sigma$. Comme Σ est stable par produit, on en déduit que $2|\nu_p(n)$, $p \equiv 3[4] \Rightarrow n \in \Sigma$. Inversement, si $n = a^2 + b^2 = z\overline{z} \in \Sigma$, en écrivant la décomposition de z en produit d'irréductibles dans $\mathbb{Z}[i]$

$$z = \prod_{q \equiv 3[4]} q^{\nu_q(z)} \prod_{N(q) \in \mathcal{P}_\mathbb{Z}} q^{\nu_q(z)}$$

on a

$$\overline{z} = \prod_{q \equiv 3[4]} q^{\nu_q(z)} \prod_{N(q) \in \mathcal{P}_\mathbb{Z}} \overline{q}^{\nu_q(z)}$$

donc

$$n = \prod_{q \equiv 3[4]} q^{2\nu_q(z)} \prod_{N(q) \in \mathcal{P}_\mathbb{Z}} N(z)^{\nu_q(z)}.$$

Comme les $N(q)$ sont par définition des éléments de Σ, par (4) on sait que $N(q) \not\equiv 3[4]$. Donc, par factorialité de $\mathbb{Z}$, on a bien que si $p \equiv 3[4]$, $\nu_p(n) = 2\nu_p(z)$.

Exercice 8: L'objectif de cet exercice est de montrer que l'anneau $\mathbb{Z}[\frac{1+i\sqrt{19}}{2}]$ est principal mais non euclidien.

(1) Soit A un anneau euclidien. Montrer qu'il existe un élément $a \in A$, $a \notin A^\times$ tel que l'application $p_{Aa} : A^\times \cup \{0\} \to A/Aa$ soit surjective.

Dans ce qui suit, on note $\alpha := \frac{1+i\sqrt{19}}{2}$ et $\overline{\alpha} := \frac{1-i\sqrt{19}}{2}$, $A := \mathbb{Z}[\alpha] \subset \mathbb{C}$.

(2) Montrer qu'on a un isomorphisme canonique d'anneaux $\mathbb{Z}[X]/X^2 - X + 5 \tilde{\to} A$;

(3) Montrer que $A/2A$ et $A/3A$ sont des corps;

(4) Déterminer $A^\times$ et en déduire que A n'est pas euclidien;

(5) Montrer que pour tout $0 \neq a, b \in A$ il existe $q, r \in A$ tels que $r = 0$ ou $|r| < |b|$ et soit $a = qb + r$ soit $2a = qb + r$;

(6) En déduire que A est principal.

(1) Soit $0 \neq a \in A \setminus A^\times$ et de stathme $\sigma(a) \geq 0$ minimal. Alors pour tout $b \in A$ il existe un $q, r \in A$ tel que $b = qa + r$ et $r = 0$ ou $\sigma(r) < \sigma(a)$. Mais par minimalité de $\sigma(a)$, si $r \neq 0$ on doit avoir $r \in A^\times$.

(2) Se traite exactement comme la question (1) de l'Exercice 7.

(3) D'après la question (2), $A/2A \tilde{\to} \mathbb{Z}[X]/((X^2-X+5)\mathbb{Z}[X]+2\mathbb{Z}[X]) \tilde{\to} \mathbb{F}_2[X]/X^2+X+1$ qui est bien un corps puisque X^2+X+1 est irréductible dans $\mathbb{F}_2[X]$ et que $\mathbb{F}_2[X]$ est principal. De même $A/3A \tilde{\to} \mathbb{F}_2[X]/X^2 - X - 1$ est un corps puisque $X^2 - X - 1$ est irréductible dans $\mathbb{F}_3[X]$.

(4) Le morphisme de monoïdes multiplicatifs $|-|^2 : (\mathbb{C}, \cdot) \to (\mathbb{N}, \cdot)$, $z \mapsto z\overline{z}$ induit par restriction un morphisme de monoïdes $N : (A, \cdot) \to (\mathbb{N}, \cdot)$. En particulier, pour tout $x = a + \alpha b \in A^\times$, $a^2 + ab + 5b^2 = N(x) = 1$, ce qui n'est possible que si $b = 0$ et $a = \pm 1$. Donc $A^\times = \{\pm 1\}$. D'après la question (1), si A était euclidien, il existerait $a \in A$, $a \notin A^\times$ tel que A/Aa soit de cardinal 2 ou 3. Dans le premier cas, A/Aa serait de caractéristique 2 donc $2A \subset Aa$ et $A/2A \twoheadrightarrow A/Aa$. Mais comme $A/2A$ est un corps,

ses seuls idéaux sont 0 ou $A/2A$, ce qui impose $A/2A \tilde{\to} A/Aa$. Mais $A/2A \tilde{\to} \mathbb{F}_2[X]/X^2+X+1$ est de cardinal $4>2$. Dans le second cas, A/Aa serait de caractéristique 3 donc $3A \subset Aa$ et $A/3A \twoheadrightarrow A/Aa$. Mais comme $A/3A$ est un corps, ses seuls idéaux sont 0 ou $A/3A$, ce qui impose $A/3A \tilde{\to} A/Aa$. Mais $A/3A \tilde{\to} \mathbb{F}_2[X]/X^2-X-1$ est de cardinal $9>3$.

(5)

(6) Soit $0 \subsetneq I \subsetneq A$ un idéal de A et $0 \neq a \in I$ tel $|a| = min|I|$. On a bien sûr $Aa \subset I$ et, d'après la question (4), $2I \subset Aa$. Supposons $Aa \subsetneq I$ donc il existe $\alpha \in I$ tel que $\alpha \notin Aa$. Comme $2\alpha \in Aa$, on peut écrire $2\alpha = qa \in 2A$. D'après la question (5) cela impose $q \in 2A$ ou $a \in 2A$. Mais comme $\alpha \notin Aa$, on a forcément $a \in 2A$. Ecrivons donc $a = 2b$. On a alors $2Ab \subsetneq I \subset Ab$. Comme A est intègre, le morphisme de multiplication par b $L_b : A \to A$ est injectif. On vérifie en outre que $L_b^{-1}(I) \subset A$ est encore un idéal de A. On a donc $2A \subsetneq L_b^{-1}(I) \subset A$. Mais comme $A/2A$ est un corps, cela force $L_b^{-1}(I) = A$ donc $I = Ab$: contradiction. Donc $Aa = I$.

Exercice 9. On dit qu'un anneau A intègre de corps des fraction K est intégralement clos si

$$A = \{x \in K \mid \exists\ P_x = T^d + \sum_{0 \leq n \leq d-1} a_n T^n \in A[X] \text{ tel que } P_x(x) = 0\}.$$

Montrer qu'un anneau factoriel est intégralement clos.

Soit $x \in K$ et supposons qu'il existe $P_x = T^d + \sum_{0 \leq n \leq d-1} a_n T^n \in A[X]$ tel que $P_x(x) = 0$. Ecrivons $x = ab^{-1}$ avec $a, b \in A$ sans facteurs irréductibles communs. On veut montrer que $b \in A^\times$. Supposons le contraire *i.e.* il existe $p \in P_A$ tel que $p|b$. La condition $P_x(x) = 0$ se réécrit $a^d = -\sum_{0 \leq n \leq d-1} a_n a^n b^{d-n}$. Mais $p|b \Rightarrow p| -\sum_{0 \leq n \leq d-1} a_n a^n b^{d-n} = a^d \Rightarrow p|a$: contradiction.

Exercice 10: (Deux critères d'irréductibilité dans les anneaux de polynômes)

(1) **(Critère d'Eisenstein)**

(a) Soit A un anneau factoriel de corps des fractions K et $P = \sum_{n \geq 0} a_n X^n \in A[X]$. Montrer que s'il existe un irréductible p de A tel que $v_p(a_0) \leq 1$, $v_p(a_n) \geq 1$, $0 \leq n \leq deg(P)-1$ et $v_p(a_{deg(P)}) = 0$ alors P est irréductible dans $K[X]$.

(b) Montrer que $P \in K[X]$ est irréductible si et seulement si $P(X+1) \in K[X]$ est irréductible. En déduire que pour tout nombre premier p, le polynôme $\Phi_p(X) = X^{p-1} + \cdots + X + 1$ est irréductible dans $\mathbb{Q}[X]$.

(2) **(Critère de réduction)**

(a) Soit A, B des anneaux intègres et L le corps des fractions de B. Soit $\phi : A \to B$ un morphisme d'anneaux. On note encore $\phi = A[X] \to B[X]$ l'unique morphisme de A-algèbres $A[X] \to B[X]$, $X \mapsto X$ (pro. univ. de $A[X]$); explicitement $\phi(\sum_{n \geq 0} a_n X^n) = \sum_{n \geq 0} \phi(a_n) X^n)$. Soit $P \in A[X]$. Montrer que si $deg(\phi(P)) = deg(P)$ et $\phi(P)$ est irréductible dans $L[X]$ alors P ne peut s'écrire sous la forme $P = P_1 P_2$ avec $P_1, P_2 \in A[X]$ de degré ≥ 1.

(b) Montrer que $P = X^5 - 5X^2 - 6X - 1$ est irréductible dans $\mathbb{Q}[X]$.

(1) (a) Ecrivons $P = UV$ dans $K[X]$. Comme $P \in A[X]$, $C_A(P) \in A$ et quitte à remplacer U par $C_A(P)C_A(U)^{-1}U$, V par $C_A(V)^{-1}V$, on peut supposer que $U, V \in A[T]$ et $C_A(V) = 1$. Considérons l'unique morphisme de A-algèbres $\overline{(-)} : A[X] \to A/p[X]$ qui envoie X sur X. On a $\overline{a}_{deg(P)} X^{deg(P)} = \overline{P} = \overline{UV}$ dans $A/p[X]$. Comme A/p est intègre, cela impose $\overline{U} = \overline{u}_m X^m$, $\overline{V} = \overline{v}_n X^n$ avec $m+n = deg(P)$ et $\overline{u}_m \overline{v}_n = \overline{a}_{deg(P)}$. Supposons $m, n \geq 1$. Dans ce cas, comme $u_0 v_0 = a_0 \neq 0$ on doit avoir $0 \neq u_0, v_0$. Mais comme $\overline{u}_0 = \overline{v}_0$, cela impose $p^2 | a_0$: contradiction.

(b) On vérifie immédiatement que l'unique morphisme de k-algèbres $T : k[X] \to k[X]$ qui envoie X sur $X+1$ est un isomorphisme de k-algèbres. En particulier, pour tout $P \in k[X]$, P est irréductible dans $k[X]$ si et seulement si $T(P)(= P(X+1))$ est irréductible dans $k[X]$. Or $X^p - 1 = (X-1)\Phi_p(X)$ donc $(X+1)^p - 1 = X\Phi_p(X+1)$ donne $\Phi_p(X) = \sum_{1 \leq k \leq p} \binom{p}{k} X^{k-1}$ et on conclut par le critère d'Eisenstein en p.

(2) (a) Ecrivons $P = P_1P_2$ avec $P_1, P_2 \in A[X]$ et $deg(P_1) \leq deg(P_2)$. On veut montrer que $P_1 \in A$. Notons que par construction $deg(\phi(P)) \leq deg(P)$. Puisque $\phi : A[X] \to B[X]$ est un morphisme d'anneaux, on a $\phi(P) = \phi(P_1)\phi(P_2)$ dans $L[X]$. Puisque $\phi(P) \in L[X]$ est irréductible par hypothèse, on a $\phi(P_1) \in K$ ou $\phi(P_2) \in K$. Enfin, puisque

$$deg(P_1) + deg(P_2) \geq deg(\phi(P_1)) + deg(\phi(P_2)) = deg(\phi(P)) = deg(P) = deg(P_1) + deg(P_2),$$

on a $deg(\phi(P_i)) = deg(P_i)$, $i = 1, 2$. Donc (on a supposé $deg(P_1) \leq deg(P_2)$) $\phi(P_1) \in K$, ce qui implique $deg(P_1) = deg(\phi(P_1)) = 0$ donc $P_1 \in A$ comme annoncé.

(b) En considérant $\phi : \mathbb{Z} \twoheadrightarrow \mathbb{Z}/2$, on a $\phi(P) =: \overline{P} = X^5 + X^2 + 1$ dans $\mathbb{F}_2[X]$. Clairement $\overline{P}$ n'a pas de racine dans $\mathbb{F}_2$. Donc si $\overline{P}$ n'est pas irréductible, il s'écrit comme produit d'un polynôme P_1 de degré 2 et d'un polynôme P_2 de degré 3 tous deux sans racine dans $\mathbb{F}_2$. Cela force $P_1 = X^2 + X + 1$ et $P_3 = X^3 + X^2 + 1$ ou $P_3 = X^3 + X + 1$. Mais, dans ces cas, $P_1P_2 = X^5 + X + 1$ ou $P_1P_2 = X^5 + X^4 + 1$. Cela montre que $\overline{P}$ est irréductible dans $\mathbb{F}_2[X]$. Donc si $P = P_1P_2$ dans $\mathbb{Z}[X]$ avec $deg(P_1) \leq deg(P_2)$, on a forcément $P_1 \in \mathbb{Z}$. De plus,$C_{\mathbb{Z}}(P) = 1 = C_{\mathbb{Z}}(P_1)C_{\mathbb{Z}}(P_2) = P_1C_{\mathbb{Z}}(P_2))$ impose $P_1 = c_{\mathbb{Z}}(P_1) = \pm 1$. Cela montre que P est irréductible dans $\mathbb{Z}[X]$. Si $P = P_1P_2$ dans $\mathbb{Q}[X]$ avec $deg(P_1) \leq deg(P_2)$, on a $C_{\mathbb{Z}}(P_1)C_{\mathbb{Z}}(P_2) = C_{\mathbb{Z}}(P) = 1$ donc $P = P_1P_2 = \frac{P_1}{C_{\mathbb{Z}}(P_1)} \frac{P_2}{C_{\mathbb{Z}}(P_2)}$ avec, cette fois-ci, $\frac{P_1}{C_{\mathbb{Z}}(P_1)}, \frac{P_2}{C_{\mathbb{Z}}(P_2)} \in \mathbb{Z}[T]$. Donc $P_1 = C_{\mathbb{Z}}(P_1) \in \mathbb{Q}$. Cela montre bien que P est irréductible dans $\mathbb{Q}[X]$.

Exercice 11: (Polynômes cyclotomiques) Notons $\mu_n \subset \mathbb{C}$ l'ensemble des racines $n$ièmes de 1 et $\mathfrak{u}_n \subset \mu_n$ le sous-ensemble des générateurs de μ_n (les racines primitives n-ièmes de 1). Soit $\Phi_n = \prod_{u \in \mathfrak{u}_n}(T - u) \in \mathbb{C}[T]$ le $n$ième polynôme cylotomique.

(1) Montrer que $(X^n - 1) = \prod_{d|n} \Phi_d(X)$ dans $\mathbb{C}[X]$;

(2) Montrer que $\Phi_n \in \mathbb{Z}[X]$, $n \geq 2$;

(3) Soit $\zeta \in \mathfrak{u}_n$ et notons P le polynôme minimal de ζ sur $\mathbb{Q}$. On veut montrer que $P = \Phi_n$.

(a) Montrer qu'il suffit de prouver que si p est un nombre premier $\not| n$, ζ^p est aussi une racine de P.

(b) Supposons le contraire et notons Q le polynôme minimal de ζ^p sur $\mathbb{Q}$. Montrer que $\Phi_n = PQR$ dans $\mathbb{Q}[T]$ avec $P, Q, R \in \mathbb{Z}[T]$ unitaire.

(c) Montrer que $P|Q(T^p)$ dans $\mathbb{Z}[T]$ et en déduire que tout diviseur irréductible Π de la réduction modulo p $\overline{P}$ de P dans $\mathbb{F}_p[T]$ est aussi un diviseur irréductible de $\overline{Q}$ dans $\mathbb{F}_p[T]$.

(d) En déduire que $\Pi^2 | T^n - \overline{1}$ dans $\mathbb{F}_p[T]$ et conclure.

(1) Cela résulte de $\mu_n = \sqcup_{d|n} \mathfrak{u}_d$.

(2) Commençons par montrer que $\Phi_n \in \mathbb{Q}[X]$ pa rrécurrence sur n. Si $n = 1, 2$ c'est clair. Si $n \geq 3$, on a $X^n - 1 = \Phi_n \times \Psi_n$ avec $\Psi_n := \prod_{d|n, d<n} \Phi_d \in \mathbb{Z}[T]$ par hypothèse de récurrence. Comme $\Psi_n \in \mathbb{Z}[T]$ est unitaire, on peut effectuer la division euclidienne de $X^n - 1$ par Ψ_n dans $\mathbb{Z}[T]$: il existe $Q, R \in \mathbb{Z}[T]$ tels que $X^n - 1 = Q\Psi_n + R$ et $R = 0$ ou $R \neq 0$ et $deg(R) < deg(\Psi_n)$. Mais, dans ce cas, $X^n - 1 = Q\Psi_n + R$ et $X^n - 1 = \Phi_n\Psi_n$ sont aussi la division la division euclidienne de $X^n - 1$ par Ψ_n dans $\mathbb{C}[T]$. En outre,

dans $\mathbb{C}[X]$, on sait qu'on a unicité de Q et R dans la division euclidienne. On en déduit notamment $\Phi_n = Q \in \mathbb{Z}[T]$.

(3) (a) Comme $\mathfrak{u}_n = \{\zeta^m \mid (n,m) = 1\}$, $P(\zeta^p) = 0$, $p \in \mathcal{P}_\mathbb{Z}$, $p|n$ implique, par induction sur $v(m) = \sum_{p\in\mathcal{P}_\mathbb{Z}} v_p(m)$, $P(\zeta^m) = 0$, $(n,m) = 1$ donc $\Phi_n|P$. Inversement, comme $\Phi_n(\zeta) = 0$, on a $P|\Phi_n$. Donc $P = \Phi_n$ dans $\mathbb{Q}[T]$ (puisqu'ils sont tous deux unitaires).

(b) Supposons le contraire et notons Q le polynôme minimal de ζ^p sur $\mathbb{Q}$. Comme $P \neq Q$ et $P, Q|\Phi_n$ dans $\mathbb{Q}[T]$, $PQ|\Phi_n$ dans $\mathbb{Q}[T]$. On peut donc écrire $\Phi_n = PQR$ dans $\mathbb{Q}[T]$. Comme $\Phi_n \in \mathbb{Z}[T]$ et est unitaire, $C_\mathbb{Z}(\Phi_n) = 1$ alors que comme $P, Q, R \in \mathbb{Q}[T]$ sont unitaires, $C_\mathbb{Z}(P)^{-1}, C_\mathbb{Z}(Q)^{-1}, C_\mathbb{Z}(R)^{-1} \in \mathbb{Z}$. Donc $C_\mathbb{Z}(\Phi_n) = 1 = C_\mathbb{Z}(P)C_\mathbb{Z}(Q)C_\mathbb{Z}(R)$ impose $C_\mathbb{Z}(P) = C_\mathbb{Z}(Q) = C_\mathbb{Z}(R) = 1$ donc $P, Q, R \in \mathbb{Z}[T]$.

(c) Comme $Q(\zeta^p) = 0$, $P|Q(T^p)$ dans $\mathbb{Q}[T]$ *i.e.* il existe $R \in \mathbb{Q}[T]$ tel que $Q(T^p) = RP$. Comme $c_\mathbb{Z}(P) = c_\mathbb{Z}(Q) = 1$, on a en outre $c_\mathbb{Z}(R) = 1$ donc $R \in \mathbb{Z}[T]$. Soit Π un diviseur irréductible de la $\overline{P}$ dans $\mathbb{F}_p[T]$ alors $\Pi|\overline{Q}(T^p) = \overline{Q}(T)^p$ mais, par factorialitde $\mathbb{F}_p[T]$ cela implique $\Pi|\overline{Q}$.

(d) *In fine* on a $\Pi|\overline{P}$, $\Pi|\overline{Q}$ donc $\Pi^2|\overline{PQ}|T^n - \overline{1}$ dans $\mathbb{F}_p[T]$. On peut donc écrire $T^n - \overline{1} = \Pi^2\Xi$ dans $\mathbb{F}_p[T]$. En particulier, $nT^{n-1} = 2\Pi\Pi'\Xi + \Pi^2\Xi'$ donc $\Pi|T^n$ dans $\mathbb{F}_p[T]$ donc $\Pi|(T^n - \overline{1}) - T^n = \overline{1}$ dans $\mathbb{F}_p[T]$: contradiction.