Correction TD6

Exercice 8.
Partie 1
On commence par remarquer que, pour $z, z' \in \mathbb{Z}[i]$, on a $N(zz') = N(z)N(z')$ (autrement dit notre stathme est multiplicatif, ce qui n'est pas le cas de tous les stathmes). Ensuite, on a vu que les inversibles de $\mathbb{Z}[i]$ sont $\{\pm 1, \pm i\}$, c'est-à-dire exactement les éléments z de $\mathbb{Z}[i]$ tels que $N(z) = 1$. Ensuite, on a
$(a) \Rightarrow (b)$ Si p est réductible dans $\mathbb{Z}[i]$, alors on peut poser $p = zz'$ avec $z, z' \in \mathbb{Z}[i]$ non inversibles tous les deux. On a alors $N(z) \neq 1$ et $N(z') \neq 1$. Comme $p = p + i0$, on a $N(p) = p^2$, et donc

$$p^2 = N(p) = N(zz') = N(z)N(z').$$

Comme $N(z)$ et $N(z')$ sont deux entiers positifs différents de 1, l'égalité ci-dessus entraîne $N(z) = N(z') = p$ par unicité de la décomposition d'un entier en produit de facteurs premiers. On peut alors poser $\alpha := z$ et on obtient (b).
$(b) \Rightarrow (c)$. Soit $\alpha \in \mathbb{Z}[i]$ tel que $N(\alpha) = p$. On pose $\alpha = x + iy$ avec $x, y \in \mathbb{Z}$, et on obtient que $p = N(\alpha) = x^2 + y^2$ s'écrit bien comme somme de deux carrés de nombres entiers, d'où (c).
$(c) \Rightarrow (a)$. Soient n, m deux entiers tels que $p = n^2 + m^2$. On a $p = (n + im)(n - im)$ s'écrit comme produit de deux éléments de $\mathbb{Z}[i]$, et aucun de ces deux éléments n'est inversible (leurs stathmes sont tous deux égaux à $p \neq 1$). On a donc que p est réductible dans $\mathbb{Z}[i]$, d'où (a).

Partie 2
1.a) On a $\mathbb{Z}[X] \subset \mathbb{Q}[X]$. Comme $\mathbb{Q}[X]$ est un corps, on peut considérer la division euclidienne de $P(X)$ par X^2+1 dans $\mathbb{Q}[X]$. On obtient qu'il existe $Q, R \in \mathbb{Q}[X]$ tels que $P(X) = Q(X)(X^2+1) + R(X)$ avec $\deg(R(X)) < 2$. De plus, R et Q sont uniques. On peut obtenir Q et R par l'algorithme de division euclidienne des polynômes. Comme $X^2 + 1$ est unitaire (son coefficient dominant est 1), l'algorithme de division euclidienne des polynômes montre que $Q, R \in \mathbb{Z}[X]$. On obtient alors qu'il existe une unique écriture $P(X) = Q(X)(X^2+1) + R(X)$ avec $Q, R \in \mathbb{Z}[X]$ et $\deg(R(X)) \leqslant 1$, donc $R(X) = ax + b$ avec $a, b \in \mathbb{Z}$.
b) Comme dans la question précédente, on pose

$$P(X) = Q(X)(X^2+1) + aX + b$$

Comme $Q(X)(X^2+1) \in (X^2+1, p)$, on a que

$$P(X) \in (X^2+1, p) \Leftrightarrow P(X) - Q(X)(X^2+1) = aX + b \in (X^2+1, p)$$

Si p divise a et b, alors $aX + b \in (p) \subset (X^2+1, p)$ comme somme de deux éléments de (p). Réciproquement, si $aX + b \in (X^2+1, p)$, alors il existe des polynômes $M(X), N(X)$ tels que

$$M(X)(X^2+1) + pN(X) = aX + b.$$

Comme X^2+1 est de degré 2, ceci n'est possible que si $M(X)$ est nul, on aurait donc $aX + b = pN(X)$, ce qui entraîne $\deg(N) \leqslant 1$ et $N(X) = n_1X + n_2$. On a alors $a = pn_1$ et $b = pn_2$ et p divise a et b, d'où le résultat.
Ensuite, concernant $\operatorname{Ker} f$, on a $P \in \operatorname{Ker} f$ si et seulement si $P(i) = 0$ modulo p, autrement dit si et seulement si $P(i) \in (p) \subset \mathbb{Z}[i]$. On a

$$P(i) = Q(i)(i^2+1) + ai + b = ai + b \in (p) \Leftrightarrow p|a \text{ et } p|b$$

d'où le résultat : $P(X) \in \operatorname{Ker} f$ si et seulement si $p|a$ et $p|b$, ce qui équivaut à $P(X) \in (X^2+1, p)$.
c). On montre que le morphisme f est surjectif. En effet, soit $z + (p) \in \mathbb{Z}[i]/(p)$, il existe $a, b \in \mathbb{Z}$ tels que

$z + (p) = a + ib + (p)$. On a alors $z + (p) = f(aX + b)$ par définition, et donc $z + (p) \in \operatorname{Im} f$. Ceci étant vrai pour tout élément de $\mathbb{Z}[i]/(p)$, on trouve $\operatorname{Im} f = \mathbb{Z}[i]/(p)$. Le résultat est alors une conséquence tu théorème de factorisation canonique : le morphisme f induit un isomorphisme entre

$$\mathbb{Z}[X]/(X^2+1, p) = \mathbb{Z}[X]/\operatorname{Ker} f \simeq \operatorname{Im} f = \mathbb{Z}[i]/(p).$$

2. On rappelle la notation $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ (vu comme corps). On considère le morphisme $g_1 : \mathbb{Z}[X] \to \mathbb{F}_p[X]$ envoyant un polynôme $P(X) = \sum_{i=0}^n a_i X^i$ sur $\sum_{i=0}^n \pi(a_i) X^i$, où $\pi : \mathbb{Z} \to \mathbb{F}_p$ est la projection canonique. On vérifie facilement que g_1 est un morphisme d'anneaux. On considère ensuite la composition g de g_1 avec la projection canonique $\mathbb{F}_p[X] \to \mathbb{F}_p[X]/(X^2+1)$.
En considérant l'écriture $P(X) = Q(X)(X^2+1) + aX + b$ de la question 1. On trouve $g(P(X)) = \pi(a)X + \pi(b)$, qui est égal à 0 si et seulement si $\pi(a) = \pi(b) = 0$, autrement dit si p divise a et b. Le noyau de g est donc (X^2+1, p), et comme g est surjectif, on trouve également que g induit un isomorphisme

$$\mathbb{Z}[X]/(X^2+1, p) = \mathbb{Z}[X]/\operatorname{Ker} g \simeq \operatorname{Im} g = \mathbb{F}_p[X]/(X^2+1).$$

3. En mettant bout à bout les questions précédentes, on obtient un isomorphisme d'anneaux

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

Comme ces anneaux sont isomorphes, le premier est intègre si et seulement si le second est intègre. Comme $\mathbb{Z}[i]$ est euclidien (donc principal et factoriel), on a l'équivalence

$$p \text{ réductible dans } \mathbb{Z}[i] \Leftrightarrow (p) \text{ idéal non premier de } \mathbb{Z}[i].$$

Cette dernière propriété est équivalente à

$$\mathbb{Z}[i]/(p) \text{ non intègre} \Leftrightarrow \mathbb{F}_p[X]/(X^2+1) \text{ non intègre} \Leftrightarrow (X^2+1) \text{ idéal non premier de } \mathbb{F}_p[X].$$

Comme $\mathbb{F}_p$ est un corps, $\mathbb{F}_p[X]$ est euclidien donc principal, cette dernière propriété est donc équivalente à X^2+1 réductible dans $\mathbb{F}_p[X]$. Comme X^2+1 est de degré 2, il est irréductible si et seulement si il n'a pas de racines dans $\mathbb{F}_p[X]$ (ATTENTION : ce critère ne vaut que pour les polynômes de degré 2 ou 3). Au total, on a donc

$$p \text{ réductible dans } \mathbb{Z}[i] \Leftrightarrow X^2+1 \text{ admet une racine dans } \mathbb{F}_p.$$

Partie 3 Cette partie est l'objet de l'exercice 5 de la feuille 7. On le corrigera à ce moment là.

Partie 4
Par la partie 1, on a

$$p \text{ s'écrit comme somme de deux carrés} \Leftrightarrow p \text{ réductible dans } \mathbb{Z}[i].$$

Par la partie 2, on a

$$\begin{aligned} p \text{ réductible dans } \mathbb{Z}[i] &\Leftrightarrow \mathbb{Z}[i]/(p) \text{ non intègre} \\ &\Leftrightarrow \mathbb{F}_p[X]/(X^2+1) \text{ non intègre} \\ &\Leftrightarrow X^2+1 \text{ a une de racine dans } \mathbb{F}_p \\ &\Leftrightarrow -1 \text{ est un carré dans } \mathbb{F}_p. \end{aligned}$$

Par la partie 3, on a

$$-1 \text{ est un carré dans } \mathbb{F}_p \Leftrightarrow p = 2 \text{ ou } (-1)^{\frac{p-1}{2}} = 1.$$

Enfin, on a $(-1)^{\frac{p-1}{2}} = 1$ si et seulement si $\frac{p-1}{2}$ est pair, autrement dit que $p \equiv 1[4]$. En concaténant toutes ces équivalences, on obtient

$$p \text{ s'écrit comme somme de deux carrés} \Leftrightarrow p = 2 \text{ ou } p \equiv 1[4].$$