ÉTUDE DE L'ANNEAU $\mathbb{Z}[i]$.

Thm: Les inversibles de $\mathbb{Z}[i]$ sont $\{\pm 1, \pm i\}$.

Les irréductibles de $\mathbb{Z}[i]$ sont $\begin{cases} \text{les } p\varepsilon \text{ avec } \varepsilon \in \mathbb{Z}[i]^\times \text{ et } p \equiv -1 \ [4] \text{ premier} \\ \text{les } \pi, \bar{\pi} \text{ tq. } \pi\bar{\pi} \text{ est premier avec } \pi\bar{\pi} \equiv 1 \ [4] \end{cases}$

Preuve:

Inversibles: On admet que $\mathbb{Z}[i]$ est euclidien pour le stathme $N(a+ib) := a^2+b^2$

On suppose $g \in \mathbb{Z}[i]$ inversible. Alors, $\exists w \in \mathbb{Z}[i]$ tq. $gw = 1$. ~~Alors~~ Donc, $N(g)N(w) = 1$. Comme $N(g) \in \mathbb{N}$, on a que $N(g) = 1$. Donc, $\mathbb{Z}[i]^\times \subseteq \{\pm 1, \pm i\}$. On vérifie réciproquement que tous les éléments sont inversibles et $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$. En particulier, $N(g) = 1 \Leftrightarrow g \in \mathbb{Z}[i]^\times$

Lemme (théorème des deux carrés) Soit $\Sigma = \{n = a^2+b^2 \text{ tq. } \exists a, b \in \mathbb{N}^2, n = a^2+b^2\}$. Notons $\mathcal{P}$ l'ensemble des nombres premiers de $\mathbb{N}$. $p \in \mathcal{P} \cap \Sigma \Leftrightarrow p = 2$ ou $p \equiv 1 \ [4]$.

Preuve: On a la chaîne d'équivalences:

$p \in \Sigma \overset{(1)}{\Leftrightarrow} p$ est réductible dans $\mathbb{Z}[i] \Leftrightarrow p$ non premier dans $\mathbb{Z}[i] \Leftrightarrow \frac{\mathbb{Z}[i]}{\langle p \rangle}$ non intègre.

Or, $\frac{\mathbb{Z}[i]}{\langle p \rangle}$ non intègre $\overset{(2)}{\Leftrightarrow} \frac{\mathbb{F}_p[X]}{\langle X^2+1 \rangle}$ non intègre $\Leftrightarrow X^2+1$ réductible dans $\mathbb{F}_p[X] \Leftrightarrow -1$ est un carré mod p

$\Leftrightarrow p \equiv 1 \ [4]$ ou $p = 2$.

(1) Si $p \in \Sigma$, alors $\exists a, b \in \mathbb{N}$ tq. $p = a^2+b^2 = (a+ib)(a-ib)$ et p est réductible dans $\mathbb{Z}[i]$.

Réciproquement, si $p = gw$ dans $\mathbb{Z}[i]$ avec $g, w \notin \mathbb{Z}[i]^\times$, alors $p^2 = N(g)N(w)$.

Donc, $N(g) = N(w) = p$ (sinon, g ou w serait inversible) donc, pour $g = a+ib$, on a que $a^2+b^2 = p$ et $p \in \Sigma$.

(2) On mq. $\frac{\mathbb{Z}[i]}{\langle p \rangle} \simeq \frac{\mathbb{Z}[X]}{\langle X^2+1, p \rangle} \simeq \frac{\mathbb{F}_p[X]}{\langle X^2+1 \rangle}$. On montre le premier, le deuxième se faisant de la même façon. On a que $\mathbb{Z}[i] \simeq \frac{\mathbb{Z}[X]}{\langle X^2+1 \rangle}$. On pose: $\varphi : \left(P \in \mathbb{Z}[X] \xmapsto{\pi_1} P \bmod X^2+1 \xmapsto{\pi_2} \overline{P} \bmod p \in \frac{\mathbb{Z}[X]/\langle X^2+1 \rangle}{\langle p \rangle}\right)$.

Si $P \in \ker \varphi$, alors, $\varphi(P) = \pi_2 \circ \pi_1(P) = 0$, donc $\pi_1(P) \in \ker \pi_2$, donc $\exists \bar{Q} \in \frac{\mathbb{Z}[X]}{\langle X^2+1 \rangle}$ tq. $\pi_1(P) = p\bar{Q}$. Donc $\exists R \in \mathbb{Z}[X]$ tq. $P = pQ(X) + (X^2+1)R(X)$, et $P \in \langle p, X^2+1 \rangle$. L'inclusion réciproque est claire et le thm d'isomorphisme donne la conclusion.

Irréductibles: Soit $\pi \in \mathbb{Z}[i]$ irréductible. Alors, $\langle \pi \rangle$ est maximal (car $\mathbb{Z}[i]$ principal) et l'idéal $\langle \pi \rangle \cap \mathbb{Z}$ est premier non trivial car $\pi\bar{\pi} = N(\pi) \in \mathbb{Z}$. Donc $\exists p \in \mathbb{Z}$ premier tq. $\langle \pi \rangle \cap \mathbb{Z} = p\mathbb{Z}$ par principalité de $\mathbb{Z}$. Comme $p \in \langle \pi \rangle$, $\pi | p$ dans $\mathbb{Z}[i]$ et $p = \pi\pi'$ avec $\pi' \in \mathbb{Z}[i]$. Comme $p^2 = N(p) = N(\pi)N(\pi')$ et $N(\pi) > 1$ (car non inversible), on a:

(1) Soit $N(\pi) = N(\pi') = p$ donc $p \in \Sigma$ et $p \equiv 1 \ [4]$ ou $p = 2$ et $\pi' = \bar{\pi}$. Rmq. $p = 2$ donne $\pm 1 \pm i$ irréductible.

(2) Soit $N(\pi) = p^2$ et $N(\pi') = 1$ donc $\pi' \in \mathbb{Z}[i]^\times$ et $\pi = p\varepsilon$, avec $\varepsilon \in \mathbb{Z}[i]^\times$.

Remarque :

▷ Un très joli développement, assez complet, monté à partir de plusieurs livres. Le thm des deux carrés est un grand classique, mais la caractérisation des irréductible de $\mathbb{Z}[i]$ est moins traditionnelle.
J'ai travaillé pour écourter le développement, et pouvoir bien traiter le dernier point (qui justifie encore plus le recasage dans la leçon sur les anneaux principaux). Il n'en demeure pas moins que le développement est assez long...

▷ Pas mal de choses à maîtriser, en fait, toutes les équivalences que l'on ne montre pas parce que c'est "facile"...