Leçons :
121, 122, 127

Lemme 1 :
Σ est stable par produit

Lemme 2 : $p \in P$
$p \in \Sigma$ ssi n n'est pas irr. dans $\mathbb{Z}[i]$

Théorème 1 :
$p \in P$. $p \in \Sigma$ ssi $p = 1 [4]$ ou $p = 2$

Théorème 2 :
$n = \prod_{p \in P} p^{v_p(n)}$. $n \in \Sigma$ ssi $v_p(n)$ est pair pour $p = 3 [4]$

V2

Références
[PERS] Cours d'algèbre, Perrin.

$\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$, $\Sigma = \{n \in \mathbb{N} \mid \exists a, b \in \mathbb{N},\ n = a^2 + b^2\}$, $N : \mathbb{Z}[i] \to \mathbb{N}$, $a + ib \mapsto a^2 + b^2$

Montrons le lemme 1 [PERS] p. 56 (ne pas faire)

Par déf. de N on a : $n \in \Sigma$ ssi il existe $z \in \mathbb{Z}[i]$ tq $n = N(z)$

Prenons $n, n' \in \Sigma$ et $z, z' \in \mathbb{Z}[i]$ tq $n = N(z)$, $n' = N(z')$

$n n' = N(z) N(z')$
$= N(zz')$ ↓ car N est multiplicative
$zz' \in \Sigma$

Donc Σ est stable par produit. □

Montrons le lemme 2 [PERS] p. 57 (Grimm)

- **Montrons $\Rightarrow$:**

Prenons $p \in \Sigma$, donc $p = a^2 + b^2$ où $a, b \in \mathbb{N}^*$ (car $p \in P$)
$= (a + ib)(a - ib)$

Donc $a \pm ib \in \mathbb{Z}[i]^\times$, car $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$ ⚠ je l'ai mit juste après

Donc p n'est pas irréductible.

- **Montrons $\Leftarrow$:** à faire à la fin si il reste du temps

On va déjà montrer $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$ [PERS] p. 56

A mettre avant ⚠

Prenons $z \in \mathbb{Z}[i]^\times$ tq $z = a+ib$.

Il existe $z' \in \mathbb{Z}[i]$ tq $zz' = 1$

Donc $N(zz') = N(z)N(z')$

$= 1$ ($\in \mathbb{N}$, $\neq 0$, $\in \mathbb{N}$)

Donc $N(z) = 1$.

Donc $a^2 + b^2 = 1$ donc soit $a = 0$ ou $b = 0$ et l'autre vaut ± 1

D'où le résultat.

Montrons l'implication réciproque :

Prenons p qui n'est pas irréductible, ie $p = zz'$ où $z, z' \notin \mathbb{Z}[i]^\times$

$N(p) = N(z)N(z')$ et $N(p) = p\bar{p} = p^2$

Puisque $z, z' \notin \mathbb{Z}[i]^\times$ on a $N(z)$ et $N(z') \neq 1$

On en déduit que $p = N(z) = N(z')$, donc $p \in \Sigma$.

D'où le résultat car $p \in P$.

□

Pour montrer le théorème 1, on va montrer pour $p \in P$: [PERR] p.57 4min

$p = 1 [4]$ ou $p = 2$ ssi p non irr.

Et avec le lemme on aura bien le thm.

- Montrer que p est non irr. ssi $\frac{\mathbb{Z}[i]}{(p)}$ n'est pas intègre

On a que $\mathbb{Z}[i]$ est Euclidien donc factoriel.

p est non irr. ssi (p) est non premier

ssi $\frac{\mathbb{Z}[i]}{(p)}$ n'est pas intègre

- Montrer que $\frac{\mathbb{Z}[i]}{(p)} \simeq \frac{\mathbb{F}_p[X]}{(X^2+1)}$:

On a que $\mathbb{Z}[i] \simeq \frac{\mathbb{Z}[X]}{(X^2+1)}$ $\quad \left(\frac{\mathbb{Z}[X]}{(X^2+1)}\right)/(p)$

Donc $\frac{\mathbb{Z}[i]}{(p)} \simeq \frac{\mathbb{Z}[X]}{(X^2+1, p)}$

$\simeq \frac{\mathbb{Z}[X]}{(p)}/(X^2+1)$

$\simeq \frac{\mathbb{F}_p[X]}{(X^2+1)}$

↓ à savoir faire bien justifier

je l'ai fait dans mon cahier de brouillon

Donc p non irr. ssi x^2+1 non irr. dans $\mathbb{F}_p[X]$

ssi x^2+1 a une racine dans $\mathbb{F}_p$

si $p \neq 2$ ↓ ssi $-1 \in (\mathbb{F}_p^\times)^2$ ssi $(-1)^{\frac{p-1}{2}} = 1$ ssi $\frac{p-1}{2}$ est pair ssi $p = 1$ [4] ← à savoir redémontrer

Si $p=2$ -1 est un carré !

D'où le résultat □

Montrons le dernier théorème [PER] p. 58

Montrons ⇐ (3 min)

Puisque Σ est stable par produit, il suffit de vérifier que chacun des facteurs de $n = \prod_{p \in \mathcal{P}} p^{v_p(n)}$ est dans Σ

→ Si $p=2$, c'est ok (le cas $p = 2$ [4] n'existe pas car p est 1er)

→ Si $p = 1$ [4], c'est ok avec le thm précédent

→ Si $p = 3$ [4], $v_p(n)$ est pair donc $p^{v_p(n)}$ est un carré

Montrons ⇒ : 3 min

Prenons $n = \prod_{p \in \mathcal{P}} p^{v_p(n)}$ dans Σ, écrivons $n = a^2 + b^2$

Vérifions que si $p = 3$ [4] alors $v_p(n)$ est pair :

On a que p est irréductible d'après le lemme 2 et le théorème 1.

Donc puisque $p \mid n$ on a $p \mid a - ib$ ou $p \mid a + ib$

Par ex., si $p \mid a+ib$ on a que $p \mid a$ et $p \mid b$

Donc $p \mid a - ib$ donc $p^2 \mid a^2 + b^2 = n$

Posons $n' = \frac{n}{p^2}$, réitérons l'opération jusqu'à ce que p^2 ne divise plus $\frac{n}{p^{2k}}$

On a donc $n = p^{2k} u$ avec u non divisible par p^2

Donc $v_p(n) = 2k$, d'où le résultat □