D. Perrin Cours d'Algèbre p 56, 57, 58 (et 75 pour les compléments)

121 122 126

Développement : Théorème des deux carrés

On note $\mathbb{Z}[i] = \{a+ib \mid a,b \in \mathbb{Z}\}$ l'ensemble des entiers de Gauss.
On définit $\Sigma = \{n \in \mathbb{N},\ n = a^2+b^2 \ \ a,b \in \mathbb{N}\}$.

- **Proposition** : On a $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$.
- **Proposition** : Σ est stable par $\times$.
- **Proposition** : $\mathbb{Z}[i]$ est euclidien (muni de N) donc principal.
- **Théorème** : Soit $p \in \mathcal{P}$, alors $p \in \Sigma \iff p = 2$ ou $p \equiv 1 [4]$.

Preuve :

① Soit $z \in \mathbb{Z}[i]^\times$, $\exists z' \in \mathbb{Z}[i]^\times$, $zz' = 1$ d'où $N(zz') = N(z)N(z') = 1$.
Puisque $N(z), N(z') \in \mathbb{N}$, $N(z) = N(z') = 1$ et si $z = a+ib$, on a donc $a^2+b^2 = 1$, $(a,b) \in \mathbb{Z}^2$ donc $(a,b) = (\pm 1, 0)$ ou $(0, \pm 1)$ d'où le résultat.
On note au passage que $z \in \mathbb{Z}[i]^\times \iff N(z) = 1$ (réciproquement $\pm 1, \pm i \in \mathbb{Z}^\times [i]$, vérification rapide (l'inv est le conjugué)).

② $n \in \Sigma \iff \exists z \in \mathbb{Z}[i],\ n = N(z)$.
(N est multiplicative.) Alors si $n, n' \in \Sigma$, on a $n = N(z)$, $n' = N(z')$ donc $nn' = N(zz') \in \Sigma$

③ Soient $z, t \in \mathbb{Z}[i] \setminus \{0\}$. Pour faire la division euclidienne de z par t, on considère $\frac{z}{t} \in \mathbb{C}$. On approxime ensuite $\frac{z}{t}$ par un entier de Gauss q : si $\frac{z}{t} = x+iy$, on prend $q = a+ib$ où a et b sont les entiers le plus proches de x, y. On a ainsi $\left|\frac{z}{t} - q\right| = |(x-a)+i(y-b)| \leqslant \left|\frac{1+i}{2}\right| = \frac{\sqrt{2}}{2} < 1$ (car $|x-a|$ et $|y-b| \leqslant \frac{1}{2}$)
On pose alors $r = z - qt \in \mathbb{Z}[i]$ et on a $r = t\left(\frac{z}{t} - q\right)$ d'où $|r| = |t| \left|\frac{z}{t} - q\right| \overset{*}{<} |t|$ et en élevant au carré $N(r) = r\bar{r} = |r|^2 < N(t)$.
On a donc bien écrit $z = qt + r$ avec $N(r) < N(t)$.

Voir sujet agreg algèbre 2021

④ On montre le lemme : $p \in \Sigma \iff p$ n'est pas irréductible dans $\mathbb{Z}[i]$. donc p irréductible de $\mathbb{Z}[i]$
i) $\Rightarrow$ si $p = a^2+b^2$, alors $p = (a+ib)(a-ib)$ où $a, b \neq 0$ car $p \neq 1$ donc $a+ib, a-ib \notin \mathbb{Z}[i]^\times$ de sorte que p n'est pas irréductible.
ii) $\Leftarrow$ si $p = zz'$ avec $z, z' \notin \mathbb{Z}[i]^\times$, on a $N(p) = p^2 = N(z)N(z')$ donc $N(z) \in \{1, p, p^2\}$ mais $N(z) \neq 1$ et $\neq p^2$ sinon $N(z') = 1$ abs donc $N(z) = p = a^2+b^2 \in \Sigma$

⑤ Comme $\mathbb{Z}[i]$ est principal par ③, $\mathbb{Z}[i]$ est factoriel. Dire que p n'est pas irréductible c'est dire exactement que l'idéal principal $(p) = p\mathbb{Z}[i]$ est non premier donc que le quotient $\mathbb{Z}[i]/(p)$ est non intègre.
Pour étudier ce quotient on utilise l'isomaphise :

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

(Poser $\varphi : P \mapsto P(i)$ et montrer par div eucl que $\ker\varphi = (X^2+1)$.)

✳ On utilise aussi les isomaphismes suivants, qui résultent tous du thm d'isomaphisme :

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

et ce dernier n'est autre que $\mathbb{F}_p[X]/(X^2+1)$, où $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ désigne le corps à p éléments.
On donc montré les équivalences :
(p) non premier $\Leftrightarrow$ X^2+1 réductible dans $\mathbb{F}_p[X]$ car $\mathbb{F}_p[X]/(X^2+1)$ n'est pas intègre donc X^2+1 n'est pas irr $\Leftrightarrow$ X^2+1 a une racine dans $\mathbb{F}_p$
En résumé : $p \in \Sigma \Leftrightarrow -1 \in \mathbb{F}_p^{*2}$ ie $\exists \alpha \in \mathbb{F}_p,\ \alpha^2 = -1$ et $-1 \in \mathbb{F}_p^{*2}$
De plus -1 est un carré dans $\mathbb{F}_p$ ssi $p = 2$ ou $p \equiv 1 [4]$

Preuves complémentaires : Soit $p \in \mathcal{P} > 2$, mq $x \in \mathbb{F}_q^{*2} \Leftrightarrow x^{\frac{q-1}{2}} = 1$ où $q = p^m$ $m \in \mathbb{N}^*$.
On pose $X = \{x \in \mathbb{F}_q \mid x^{\frac{q-1}{2}} = 1\}$. On a $|X| \leq \frac{q-1}{2}$ (car un pol de $d° = \frac{q-1}{2}$ a au plus $\frac{q-1}{2}$ racines). D'autre part si $x \in \mathbb{F}_q^{*2}$ on a $x = y^2$ donc $x^{\frac{q-1}{2}} = y^{q-1} = 1$ car $y \in \mathbb{F}_q^*$ et donc $\mathbb{F}_q^{*2} \subset X$.
Pour une raison de cardinal, on a $X = \mathbb{F}_q^{*2}$. ↘ d'ordre $q-1$.

Montrons alors que -1 est un carré dans $\mathbb{F}_q$ ssi $q \equiv 1 [4]$.
$-1 \in \mathbb{F}_q^{*2} \Leftrightarrow (-1)^{\frac{q-1}{2}} = 1 \Leftrightarrow \frac{q-1}{2}$ pair $\Leftrightarrow q \equiv 1 [4]$.

✳ Prop : Soit A un anneau commutatif et I, J des idéaux de A. Alors

$$(A/I)/\pi_I(J) \simeq A/(I+J) \simeq (A/J)/\pi_J(I).$$

où π_I et π_J sont les projections de A dans A/I et A/J.
Preuve : Il suffit de montrer que $p \circ \pi_I$ où $p : A/I \to (A/I)/\pi_I(J)$ est surjectif de noyaux $I+J$. où visiblement p est la projection
Pour plus de détails voir dans mes documents