

* Etude de $\mathbb{Z}[i]$, Théorème des deux carrés: leçons 121, 122, 127

[Perrin, II 6]

On note $\Sigma = \{n \in \mathbb{N}, \exists a, b \in \mathbb{N}, n = a^2 + b^2\}$ et $\mathbb{Z}[i] = \{a + ib, a, b \in \mathbb{Z}\}$.

$N: z \mapsto z\bar{z}$ la norme sur $\mathbb{Z}[i]$. On a pour $n \in \mathbb{N}$: $n \in \Sigma \Leftrightarrow \exists z \in \mathbb{Z}[i], n = N(z)$

(En particulier: Σ stable par multiplication)

lemme 1:

$$z \in \mathbb{Z}[i]^{\times} \Leftrightarrow N(z) = 1 \Leftrightarrow z \in \{\pm 1, \pm i\}$$

Lemme 1: $\mathbb{Z}[i]$ est un anneau euclidien pour le norme N .Th:Soit $p \in \mathcal{P}$:1) $p \in \mathcal{E} \Leftrightarrow p$ n'est pas irréd. dans $\mathbb{Z}[i]$ 2) $p \in \mathcal{E} \Leftrightarrow p=2$ ou $p \equiv 1[4]$ Soit $n \in \mathbb{N}^* \setminus \mathcal{P}$: $n = \prod_{p \in \mathcal{P}} p^{r_p(n)}$ 3) $n \in \mathcal{E} \Leftrightarrow \forall p \in \mathcal{P}: r_p(n) \in 2\mathbb{N}$.Par ailleurs, les irréd. de $\mathbb{Z}[i]$ sont aux inversibles près:

- les $p \in \mathcal{P}$ avec $p \equiv 3[4]$
- les $z \in \mathbb{Z}[i]$ avec $N(z) \in \mathcal{P}$.

peut-être mettre que ça dans le par.

preuve du lemme 1:• $z \in \{\pm 1, \pm i\} \Rightarrow z \in \mathbb{Z}[i]^\times$: ok.• Si $z \in \mathbb{Z}[i]^\times$: $N(z)N(z^{-1})=1 \leadsto N(z)=1$.

• Si $z = a+ib \in \mathbb{Z}[i]$ vérifie $N(z)=1$. $a^2+b^2=1$ donc l'un des deux vaut ± 1 et l'autre 0
 $\leadsto z \in \{\pm 1, \pm i\}$

preuve du lemme 2:Soient $z, z' \in \mathbb{Z}[i] \setminus \{0\}$: $\frac{z}{z'} = a+iv = \underbrace{qn+in}_{=:q} + s+it$ avec $m, n \in \mathbb{Z}$, $s, t \in \mathbb{R}$, $|s|, |t| \leq \frac{1}{2}$.

$$r := z'(s+it) = z - qz' \in \mathbb{Z}[i] \quad \text{et} \quad N(r) = |z'|^2 |s+it|^2 = N(z')(s^2+t^2) \leq \frac{1}{2} N(z') < N(z')$$

preuve du Th:1) $\odot$: ok $\odot$ Si $p = zz'$ avec $N(z), N(z') > 1$, alors: $p^2 = N(p) = N(z)N(z')$ Par unicité de la décomz en facteurs premiers dans $\mathbb{Z}$ et le fait que $N(z), N(z') > 1$, on a:

$$p = N(z) = N(z') \leadsto p \in \mathcal{E}$$

2) Les carrés sont congrus à 0 ou 1 mod 4 et donc les éléments de $\mathcal{E}$ sont congrus à 0, 1 ou 2 mod 4. On a donc facilement l'implication $\odot$.

⊕ Soit $p \in \mathcal{S}(42)$ tq $p \equiv 1[4]$

On veut mq $p \in \mathcal{I}$, par la question préc. il suffit de mq p n'est pas irréd. dans $\mathbb{Z}[i]$.

Or, par le lemme 2, $\mathbb{Z}[i]$ est euclidien donc principal donc il suffit de mq p n'est pas premier.

On cherche donc $z, z' \in \mathbb{Z}[i]$ tq $p \nmid z$, $p \nmid z'$ et $p \mid zz'$.

Il suffit en fait de mq $-1 \in (\mathbb{F}_p^\times)^2$. En effet, si c'est le cas, alors $\exists a \in \mathbb{Z}$ tq:

$$p \mid a^2 + 1 = (a+i)(a-i)$$

Or, $p \nmid a+i \Rightarrow p \nmid i$ (en identifiant la partie imaginaire)

De même, $p \nmid a-i$ est impossible.

Montrons donc que $-1 \in (\mathbb{F}_p^\times)^2$:

$\varphi: \mathbb{F}_p^\times \rightarrow \{\pm 1\}$ est un morphisme de groupes surjectif (car $|\ker \varphi| = |\mathbb{Z}_p^\times(x^{p-1/2} - 1)| \leq p - \frac{p-1}{2}$)

Par Lagrange: $(\mathbb{F}_p^\times)^2 \subseteq \ker \varphi$ Or: $|\mathbb{F}_p^\times / \ker \varphi| = |\{\pm 1\}| = 2$ et $(\mathbb{F}_p^\times)^2 = \text{im}(\alpha \mapsto \alpha^2)$ donc:

$$|\mathbb{F}_p^\times / (\mathbb{F}_p^\times)^2| = |\ker \varphi| = 2$$

$$\leadsto (\mathbb{F}_p^\times)^2 = \ker \varphi$$

Donc: $-1 \in (\mathbb{F}_p^\times)^2 \Leftrightarrow (-1)^{p-1/2} = 1 \Leftrightarrow 2 \mid p-1 \Rightarrow 4 \mid p-1 \Rightarrow p \equiv 1[4]$.

On peut faire plus court si on admet $\mathbb{F}_p^\times$ cyclique.

3) d'implication ⊕ est donc grâce aux résultats précédents.

⊕: Soit $n \in \mathcal{S}(42, 1)$:

Soit $p \in$ un facteur premier de n , congru à 3 mod 4. (S'il n'y en a pas c'est ok)

On va mq: $p^2 \nmid n$ et $\frac{n}{p^2} \in \mathcal{I}$ ce qui permettra de conclure par récurrence (par exemple sur $\max\{v_p(n), p \equiv 3[4]\}$).

$n \in \mathcal{I}$ donc $n = N(z)$ avec $z \in \mathbb{Z}[i]$. On va mq $p \nmid z$ dans $\mathbb{Z}[i]$. Supposons que ce n'est pas le cas. Par les questions précédentes, p est irréd. dans $\mathbb{Z}[i]$ et donc $p \nmid z = 1$. Comme $\mathbb{Z}[i]$ est principal: $\exists u, v \in \mathbb{Z}[i]$, $pu + zv = 1 \leadsto 1 = p\bar{u} + \bar{z}\bar{v}$.

Donc: $z = pz\bar{u} + \bar{z}\bar{z}\bar{v} = pz\bar{u} + n\bar{v}$. Or, $p \mid n$ (dans $\mathbb{Z}$) donc $p \mid z$ (dans $\mathbb{Z}[i]$), ce qui contredit notre hypothèse initiale. Donc: $z = pz$ avec $x \in \mathbb{Z}[i]$.

$$\text{Et donc: } n = N(z) = p^2 \underbrace{N(x)}_{\in \mathcal{I}}$$

Dév. Alg. 11.

▽

preuve du par ailleurs.

On a déjà prouvé le point sur les nombres premiers.

Soit donc $z \in \mathbb{Z}[i]$ un elt. irred. non associé à un elt. de $\mathcal{P}$. Notons $n = N(z)$ et soit p un facteur premier de n . On veut montrer que $n=p$.

• d.l.g. $z \nmid p$:

En effet, dans le cas contraire, comme z est irred., on aurait $u, v \in \mathbb{Z}[i]$ tq. $pu + zv = 1$.

De la même manière que dans la quest. préc.: $p \mid z$, absurde car z irred. et z n'est pas associé à p .

• d.l.g. $\bar{z} \nmid p$:

la conjugaison donne un isomorphisme de $\mathbb{Z}[i]$ donc $\bar{z}$ est également irred. dans $\mathbb{Z}[i]$.

Or, $N(\bar{z}) = N(z) = n$, donc, par ce qu'on a fait avant: $\bar{z} \nmid p$.

• d.l.g. $z \nmid \bar{z}$:

Si $z = \bar{z}$, alors $z \in \mathbb{R} \cap \mathbb{Z}[i] = \mathbb{Z}$. Or, z est irred. dans $\mathbb{Z}[i]$ donc également dans $\mathbb{Z}$ (car $\mathbb{Z}[i]^\times \cap \mathbb{Z} = \mathbb{Z}^\times$), donc $z \in \mathcal{P}$, ce qui contredit notre hypothèse initiale.

Ainsi, comme z et $\bar{z}$ sont irred.: $n = z\bar{z} \mid p$. $\leadsto p = n\alpha$, avec $\alpha \in \mathbb{Z}[i]$.

$\alpha = \frac{p}{n} > 0$ donc $\alpha \in \mathbb{N}^*$

Par unicité de la décom. en facteurs premiers dans $\mathbb{Z}$: $p = n$.

La réciproque est immédiate grâce à la multiplicité de N .