Théorème des deux carrés

Réf: Perrin, Cours d'Algèbre p. 56.
X. Gourdon, Algèbre p. 49.

L'objectif est de trouver l'ensemble des $n \in \mathbb{N}$ tel qu'il existe $(n_1, n_2) \in \mathbb{N}$ tq :

$$n = n_1^2 + n_2^2$$

Pour cela on note $\Sigma = \{ n \in \mathbb{N} \mid n = n_1^2 + n_2^2 , (n_1, n_2) \in \mathbb{N}^2 \}$.

Remarque : 1 - Soit n tq $n \equiv 3[4]$ alors $n \notin \Sigma$, en effet si n_1 est pair $n_1^2 \equiv 0[4]$

n_2 est impair $n_1^2 \equiv 1[4]$

donc $n_1^2 + n_2^2 \equiv 0, 1, 2[4]$ pour $(n_1, n_2) \in \mathbb{N}$.

2 - Soit $n = n_1^2 + n_2$ alors $n = (n_1 + i n_2)(n_1 - i n_2)$

C'est pourquoi on s'intéresse à $\mathbb{Z}[i] = \{ a + ib \in \mathbb{C} \mid a, b \in \mathbb{N} \}$ car on a :

$$n \in \Sigma \iff \exists z \in \mathbb{Z}[i], \ n = |z|^2 \text{ (norme de } \mathbb{C}).$$

Théorème :

1) $\mathbb{Z}[i]$ est euclidien pour le stathme $N(z) = a^2 + b^2$ donc principal et $\mathbb{Z}[i]^\times = \{ \pm 1, \pm i \}$.
2) Les irréductibles de $\mathbb{Z}[i]$ sont à un inversible près :
   - les $p \in \mathbb{Z}$ premiers tels que $p \equiv 3[4]$
   - les $a + ib \in \mathbb{Z}[i]$ tels que $a^2 + b^2$ est premier

Application :

1) Soit p premier alors p s'écrit comme la somme de deux carrés ssi $p = 2$ ou $p \equiv 1[4]$.
2) Soit $n \in \mathbb{N}^*$, $n \neq 1$ tel que $n = \prod_{p \in \mathcal{P}} p^{\nu_p(n)}$ alors $n \in \Sigma$ est la somme de deux carrés ssi $\nu_p(n)$ est pair pour tout $p \equiv 3[4]$.

Preuve 1)

Étape 1 : $\mathbb{Z}[i]^\times = \{ \pm 1, \pm i \}$.

Soit $z \in \mathbb{Z}[i]^\times$ alors il existe $z' \in \mathbb{Z}[i]$ tel que : $zz' = 1$.

Ainsi $N(z)N(z') = 1$ or $\forall z'' \in \mathbb{Z}[i]$, $N(z'') \in \mathbb{N}$ donc $N(z) = N(z') = 1$.

Or si on écrit $z=a+ib$ alors $N(z)=a^2+b^2$ comme $(a,b)\in\mathbb{N}$ on a:

$$a=0 \text{ et } b=\pm 1 \quad \text{ou} \quad a=\pm 1 \text{ et } b=0$$

i.e $z\in\{\pm 1,\pm i\}$.

Réciproquement $\{\pm 1,\pm i\}$ sont inversibles dans $\mathbb{Z}[i]$.

Etape 2: $\mathbb{Z}[i]$ est euclidien.

Soient $z,t\in\mathbb{Z}[i]\setminus\{0\}$, on commence par étudier $\frac{z}{t}\in\mathbb{C}$.

On écrit $\frac{z}{t}=x+iy$ alors il existe $a,b\in\mathbb{Z}$ tel que:

$$|x-a|\leq\frac{1}{2} \text{ et } |y-b|\leq\frac{1}{2}.$$

Alors si on note $q=a+ib$ on a:

$$\left|\frac{z}{t}-q\right|^2=(x-a)^2+(y-b)^2\leq\frac{1}{2}<1$$

On pose alors $r=z-qt\in\mathbb{Z}[i]$ car $\mathbb{Z}[i]$ est un anneau.

De plus

$$|r|^2=\left|t\left(\frac{z}{t}-q\right)\right|^2=|t|^2\left|\frac{z}{t}-q\right|^2<|t|^2 \text{ donc } N(r)<N(t).$$

On a bien écrit $z=qt+r$ avec $N(r)<N(t)$.

□

Preuve Application

1) On a déjà vu que si $p\equiv 3[4]$ alors $p\notin\square$ donc $\Rightarrow$ est déjà montré.

Pour la réciproque on utilise le Lemme suivant.

Lemme: On a pour p premier:

$$p\in\square \iff p \text{ n'est pas irréductible dans } \mathbb{Z}[i]$$

Preuve: $\Rightarrow$: Si $p\in\square$ alors $p=a^2+b^2$ donc $p=(a+ib)(a-ib)$ dans $\mathbb{Z}[i]$ avec $a+ib\notin\{\pm 1,\pm i\}$
$a-ib\notin\{\pm 1,\pm i\}$

$\Leftarrow$: Si $p=zz'$ avec $z,z'\notin\{\pm 1,\pm i\}$. On a: $N(p)=N(z)N(z')=p^2$ et comme $N(z)\neq 1$, $N(z')\neq 1$.

Alors on peut supposer $N(z)=p$ donc $p\in\square$

□

Pour finir la preuve on utilise que $\mathbb{Z}[i]$ est principal donc factoriel ainsi p est non irréductible est équivalent à ce que $\langle p \rangle = p\mathbb{Z}[i]$ est non premier.
Donc que le quotient $\mathbb{Z}[i]/\langle p \rangle$ est non intègre.

Pour étudier ce quotient on utilise le théorème d'isomorphisme et que :

$$\mathbb{Z}[i] \simeq \mathbb{Z}[X]/\langle X^2+1 \rangle \quad \text{(par division euclidienne)}$$

Qui nous donne :

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

Ainsi $\mathbb{Z}[i]/\langle p \rangle$ est non intègre $\Leftrightarrow$ $\mathbb{F}_p[X]/\langle X^2+1 \rangle$ est non intègre $\Leftrightarrow$ X^2+1 ne soit pas irréductible dans $\mathbb{F}_p[X]$
$\Leftrightarrow$ X^2+1 à une racine dans $\mathbb{F}_p$.

En résumé on a montré l'équivalence suivante :

$$p \in \Gamma \Leftrightarrow -1 \text{ est un carré mod } p.$$

Or on sait que -1 est un carré mod p ssi $p = 2$ ou $p \equiv 1[4]$.

⚠ Soit $n \in \mathbb{N}^*$ et $n \neq 1$.

$\Leftarrow$ Si $v_p(n)$ est pair pour $p \equiv 3[4]$ alors :

$$n = \prod_{p \in \mathcal{P}} p^{v_p(n)} = \prod_{\substack{p \in \mathcal{P} \\ p=1[4]}} p^{v_p(n)} \prod_{\substack{p \in \mathcal{P} \\ p \equiv 3[4]}} \left(p^2\right)^{\frac{v_p(n)}{2}} \quad 2^{v_2(n)}$$

En utilisant que si $p = 1[4]$ alors $p \in \Gamma$
$2 \in \Gamma$ et Γ stable par produit on a $n \in \Gamma$.

si $p = 3[4]$ alors $p^2 \in \Gamma$

$\Rightarrow$ Supposons $n \in \Gamma$ alors $n = a^2+b^2 = (a+ib)(a-ib)$.
Soit $p \in \mathcal{P}$ tq $p \equiv 3[4]$, tq $v_p(n) \neq 0$.
Alors $p \mid n = a^2+b^2$ donc p divise $(a+ib)(a-ib)$ dans $\mathbb{Z}[i]$.
or par le lemme p est irréductible donc $p \mid a+ib$ ou $p \mid a-ib$.
Dans les deux cas comme $p \in \mathbb{N}$ on a $p \mid a$ et $p \mid b$.
donc $p^2 \mid a^2+b^2 = n$

De plus si on écrit $a = pa'$ et $b = pb'$ alors

$$\frac{n}{p^2} = a'^2 + b'^2 \in \mathbb{Z}$$

et $v_p\left(\frac{n}{p^2}\right) = v_p(n) - 2$.

En raisonnant par récurrence $\frac{n}{p^{2\ell}} \in \mathbb{Z}$ où $\ell = \left\lfloor \frac{v_p(n)}{2} \right\rfloor$

et $v_p\left(\frac{n}{p^{2\ell}}\right) = v_p(n) - 2\left\lfloor \frac{v_p(n)}{2} \right\rfloor$.

Si $v_p(n)$ est impair alors $v_p\left(\frac{n}{p^{2\ell}}\right) = 1$ donc p divise $\frac{n}{p^{2\ell}}$ et $\frac{n}{p^{2\ell}} \in \mathbb{Z}$ parce que précède p^2 divise $\frac{n}{p^{2\ell}}$.
Ce qui est absurde car $2\ell + 2 > v_p(n)$.

Ainsi $v_p(n)$ est pair et $v_p\left(\frac{n}{p^{2\ell}}\right) = 0$.

□

Quelque résultat que l'on utilise.

Lemme: p. 75.

Soit p premier, $p \neq 2$ alors -1 est un carré dans $\mathbb{F}_p$ ssi $p \equiv 1 [4]$.

Preuve:

$$-1 \in \mathbb{F}_p^{*2} \iff (-1)^{\frac{p-1}{2}} = 1 \iff \frac{p-1}{2} \text{ pair} \iff p \equiv 1 [4].$$

□

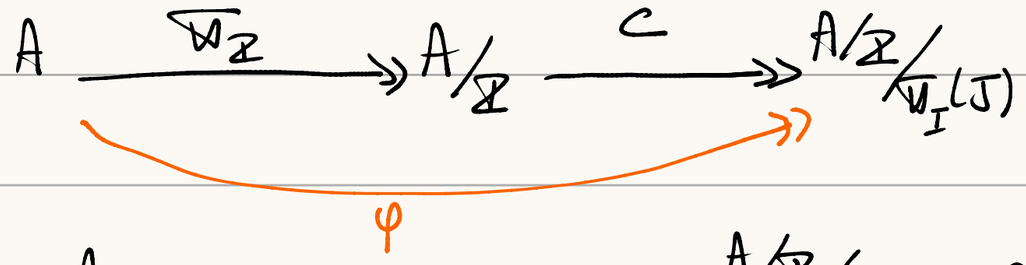
Lemme: Soit A un anneau et $\mathcal{I}, \mathcal{J}$ deux idéaux de A.

On note $\pi_{\mathcal{I}} : A \longrightarrow A/\mathcal{I}$ et $\pi_{\mathcal{J}} : A \longrightarrow A/\mathcal{J}$ alors on a:

$$\frac{A/\mathcal{I}}{\pi_{\mathcal{I}}(\mathcal{J})} \simeq A/\langle \mathcal{I}, \mathcal{J} \rangle \simeq \frac{A/\mathcal{J}}{\pi_{\mathcal{J}}(\mathcal{I})}.$$

Preuve : Par symétrie il nous suffit de montrer l'isomorphisme de droite.

Pour cela on définit le morphisme d'anneau :



i.e $\varphi : A \longrightarrow A/I/\pi_I(J)$ qui est surjectif.

$x \longmapsto c(\pi_I(x))$

Il nous suffit de montrer que $\ker(\varphi) = \langle I, J \rangle$.

- Soit $x \in I$

  $\varphi(x) = c(\pi_I(x)) = c(0) = 0$

  Soit $y \in J$

  $\varphi(y) = c(\pi_I(y)) = 0$ car $\pi_I(y) \in \pi_J(y) = \ker(c)$.

Donc $\langle I, J \rangle \subset \ker(\varphi)$.

- Soit $x \in \ker(\varphi)$ alors $c(\pi_I(x)) = 0$.

  donc $\pi_I(x) \in \pi_I(J)$.

  donc $\exists y \in J$ tel que $x - y \in I$.

Donc $x \in \langle I, J \rangle = I + J$.

$\pi_I : A \longrightarrow A/I$ surjectif et $\ker(\pi_I) = I$.

□