Théorème des deux carrés :

I Le développement

Le but de ce développement est de démontrer le théorème des deux carrés dans l'anneau $\mathbb{Z}[i]$. Ce résultat est utile car il sert à trouver les irréductibles de $\mathbb{Z}[i]$ (aux inversibles près).

On désigne $\mathcal{P}$ l'ensemble des nombres premiers (au sens usuel). Si $p \in \mathcal{P}$ et $n \in \mathbb{N}^*$, on note $v_p(n)$ la valuation p-adique de l'entier n. On note également $N : \mathbb{Z}[i] \longrightarrow \mathbb{N}$ l'application définie par $N(z) = |z|^2$ ainsi que l'ensemble $\Sigma = \{n \in \mathbb{N} \text{ tq } \exists (a,b) \in \mathbb{N}^2 \text{ tq } n = a^2 + b^2\}$.

On commence tout d'abord par démontrer le lemme suivant :

Lemme 1 : [Perrin, p.57]
Soit $p \in \mathcal{P}$.
Les assertions suivantes sont équivalentes :
$*$ $p \in \Sigma$. $*$ L'élément p n'est pas irréductible dans $\mathbb{Z}[i]$.
$*$ On a $p = 2$ ou $p \equiv 1$ [4]

Preuve :
Soit p un nombre premier (au sens usuel).
$*$ Supposons que $p \in \Sigma$:
Il existe alors $(a,b) \in \mathbb{N}^2$ tel que $p = a^2 + b^2 = (a+ib)(a-ib)$. On ne peut avoir $a = 0$ ou $b = 0$ car sinon p qui est un nombre premier serait nul ou un carré. Donc $a \pm ib \notin \mathbb{Z}[i]^\times$ (car $\mathbb{Z}[i]^\times = \{-i; i; -1; 1\}$), de sorte que p n'est pas irréductible.

$*$ Supposons que p n'est pas irréductible dans $\mathbb{Z}[i]$:
Il existe deux nombres $z, \omega \in \mathbb{Z}[i]$ non inversibles tels que $p = z\omega$. On a alors :

$$p^2 = N(p) = N(z\omega) = N(z)N(\omega)$$

Comme z et ω ne sont pas des inversibles de $\mathbb{Z}[i]$, on a alors $N(z) \neq 1$ et $N(\omega) \neq 1$ et comme p est un nombre premier, on en déduit que $N(z) = N(\omega) = p$. Ainsi, en écrivant $z = a + ib$ avec $(a,b) \in \mathbb{Z}$, on obtient $p = N(z) = a^2 + b^2 \in \Sigma$.

$*$ Comme l'anneau $\mathbb{Z}[i]$ est principal, p est réductible si, et seulement si, l'idéal (p) n'est pas premier, ce qui équivaut à $\mathbb{Z}[i]/(p)$ n'est pas intègre. Or, on a les isomorphimes suivants par le troisième théorème d'isomorphisme :

$$\mathbb{Z}[i]/(p) \cong \left(\mathbb{Z}[X]/(X^2+1)\right)/(p) \cong \mathbb{Z}[X]/(p, X^2+1) \cong \mathbb{F}_p[X]/(X^2+1)$$

Ce dernier anneau n'est pas intègre, si et seulement si, X^2+1 est réductible dans l'anneau $\mathbb{F}_p[X]$, ce qui équivaut à ce que -1 soit un carré dans $\mathbb{F}_p$. Cette dernière condition est équivalente à $p = 2$ ou $p \equiv 1$ [4], d'où le résultat.

On a donc démontré le lemme par implications circulaires.

■

Théorème 2 : Théorème des deux carrés [Perrin, p.58] :
Soit $n \in \mathbb{N}^*$.
$n \in \Sigma$ si, et seulement si, pour tout $p \in \mathcal{P}$ vérifiant $p \equiv 3$ [4], l'entier $v_p(n)$ est pair.

Preuve :
Soit $n = \prod_{p \in \mathcal{P}} p^{v_p(n)} \in \mathbb{N}^*$ (décomposition en facteur premier).
$*$ Supposons que $v_p(n)$ est pair pour tout nombre premier p vérifiant $p \equiv 3$ [4] :
On a alors $n = 2^{v_2(n)} \prod_{\substack{p \in \mathcal{P} \\ p \equiv 1 \ [4]}} p^{v_p(n)} \prod_{\substack{p \in \mathcal{P} \\ p \equiv 3 \ [4]}} \left(p^{\frac{v_p(n)}{2}}\right)^2$. Or, puisque $2 \in \Sigma$, que les carrés des entiers naturels appartiennent à Σ et que Σ est stable par multiplication, on en déduit que $n \in \Sigma$.

$*$ Supposons que $n \in \Sigma$:
On fixe un nombre premier $p \in \mathcal{P}$ tel que $p \equiv 3$ [4].
On montre par récurrence sur $k \in \mathbb{N}$ la propriété suivante :

$$\mathcal{P}_k : \text{"Pour tout } n \in \Sigma\backslash\{0\} \text{ avec } v_p(n) \leq k, \text{ l'entier } v_p(n) \text{ est pair"}$$

- Initialisation pour $k = 0$:
La propriété $\mathcal{P}_0$ est vérifiée (car tous les $v_p(n)$ sont nuls, donc pairs).
La propriété est donc bien initialisée.

- Hérédité :
On considère $k \in \mathbb{N}$ et on suppose que la propriété est vraie au rang k. Montrons que la propriété est encore vraie au rang $k+1$:

Soit $n \in \Sigma\backslash\{0\}$ tel que $v_p(n) \leq k+1$.
On peut supposer que p divise n sinon le résultat est évident (car $v_p(n) = 0$).
Comme $n \in \Sigma\backslash\{0\}$, il existe $(a,b) \in \mathbb{N}^2\backslash\{(0,0)\}$ tel que $n = a^2 + b^2$ et on peut écrire $n = a^2 + b^2 = (a+ib)(a-ib)$. De plus, par le lemme précédent, on en déduit que p est irréductible dans $\mathbb{Z}[i]$ (car $p \equiv 3$ [4]), donc premier car l'anneau $\mathbb{Z}[i]$ est principal.
On en déduit que p divise $a+ib$ ou $a-ib$ dans $\mathbb{Z}[i]$, donc p divise a et b car $p \in \mathbb{Z}$.
Ainsi, p divise $a+ib$ et p divise $a-ib$ (car p divise a et b).

Finalement, p^2 divise n et donc on peut appliquer l'hypothèse de récurrence à $\frac{n}{p^2}$.
En effet, on a :

$$\frac{n}{p^2} = \left(\frac{a}{p}\right)^2 + \left(\frac{b}{p}\right)^2 \text{ avec } \frac{a}{p}, \frac{b}{p} \in \mathbb{Z} \text{ (par ce qui précède)}$$

On en conclut que l'entier $v_p(n) = v_p\left(\frac{n}{p^2}\right) + 2$ est pair, donc $\mathcal{P}_{k+1}$ est vraie.
La propriété est donc héréditaire.

Finalement, on a donc montré la propriété par récurrence.

Ainsi, on a démontré le théorème des deux carrés.

■

II Remarques sur le développement

II.1 Résultat(s) utilisé(s)

Dans le développement, on a utilisé 3 résultats importants :

Lemme 3 : [Perrin, p.56]
L'ensemble Σ est stable par multiplication.

Preuve :
Soient $n, n' \in \Sigma$.
Il existe alors $a, b, c, d \in \mathbb{N}$ tels que $n = a^2 + b^2$ et $n' = c^2 + d^2$.
On a donc :

$$nn' = \left(a^2+b^2\right)\left(c^2+d^2\right) = N(a+ib)N(c+id) = N((ac-bc)+i(ad+bc)) = (ac-bd)^2+(ad+bc)^2$$

■

Proposition 4 : [Perrin, p.56]
L'ensemble des éléments inversibles de $\mathbb{Z}[i]$ est donné par :

$$\mathbb{Z}[i]^\times = \{z \in \mathbb{Z}[i] \text{ tq } N(z) = 1\} = \{-i; i; -1; 1\}$$

Preuve :
$*$ Soit $z \in \mathbb{Z}[i]^\times$.
Il existe alors $\omega \in \mathbb{Z}[i]$ tel que $z\omega = 1$.
On a alors le relation $N(z)N(\omega) = N(z\omega) = N(1) = 1$ dans $\mathbb{N}$, donc $N(z) = 1$.

$*$ Soit $z \in \mathbb{Z}[i]$ tel que $N(z) = 1$.
On a alors $N(z) = z\overline{z} = 1$ et puisque $\overline{z} \in \mathbb{Z}[i]$, on obtient que $\overline{z}$ est l'inverse de z dans $\mathbb{Z}[i]$, d'où $z \in \mathbb{Z}[i]^\times$.

$*$ Enfin, on a l'égalité entre les deux derniers ensembles puisque l'inclusion du dernier vers le deuxième est immédiate (simple calcul) et réciproquement, les seules solutions de l'équation $N(z) = N(a+ib) = a^2+b^2 = 1$ sont $-i, i, -1$ et 1.

Finalement, on a les égalités d'ensembles.

■

Lemme 5 : [Perrin, p.75]
Soit $p \in \mathcal{P}$.
-1 est un carré dans $\mathbb{F}_p$ si, et seulement si, $p = 2$ ou $p \equiv 1\ [4]$.

Preuve :
Soit $p \in \mathcal{P}$.
$*$ Si $p = 2$, alors $\overline{-1} = \overline{1} = \overline{1}^2$ dans $\mathbb{F}_2$ et on a le résultat. On peut donc supposer $p > 2$ dans la suite.

$*$ L'ensemble des carrés de $\mathbb{F}_p^*$ est l'image du morphisme de groupes $f : \mathbb{F}_p^* \longrightarrow \mathbb{F}_p^*$ défini par $f(x) = x^2$. Or, comme $\mathrm{Ker}(f) = \{-1; 1\}$, on obtient par le premier théorème d'isomorphisme qu'il y a $\frac{p-1}{2}$ carrés dans $\mathbb{F}_p^*$.
On en déduit que les carrés de $\mathbb{F}_p^*$ sont exactement les racines du polynôme $X^{\frac{p-1}{1}} - \overline{1} \in \mathbb{F}_p[X]$. On en conclut que -1 est un carré dans $\mathbb{F}_p^*$ si, et seulement si, $(-1)^{\frac{p-1}{2}} = 1$, c'est-à-dire $p \equiv 1$ [4].

On a donc démontré l'équivalence désirée.

■

II.2 Pour aller plus loin...

II.2.1 Les irréductibles de $\mathbb{Z}[i]$

Grâce au théorème des deux carrés, nous sommes désormais capable de donner les irréductibles de $\mathbb{Z}[i]$ (aux inversibles près) :

Proposition 6 : [Perrin, p.58]
Les irréductibles de $\mathbb{Z}[i]$ sont exactement, aux éléments inversibles près :
$*$ Les entiers premiers $p \in \mathbb{N}$ tels que $p \equiv 3$ [4].
$*$ Les entiers de Gauss $a + ib$ dont la norme est un nombre premier.

Preuve :
$*$ D'après le lemme, les nombres premiers $p \in \mathbb{N}$ vérifiant la relation $p \equiv 3$ [4] sont irréductibles dans $\mathbb{Z}[i]$.

$*$ Soit $z \in \mathbb{Z}[i]$ tel que $N(z)$ soit un nombre premier.
Si on écrit $z = \omega_1\omega_2$ avec $(\omega_1, \omega_2) \in \mathbb{Z}[i]^2$, alors $N(z) = N(\omega_1)N(\omega_2)$ dans $\mathbb{N}$. Comme $N(z)$ est un nombre premier, on obtient $N(\omega_1) = 1$ ou $N(\omega_2) = 1$, donc ω_1 ou ω_2 est inversible dans $\mathbb{Z}[i]$.
Finalement, l'élément z est irréductible dans $\mathbb{Z}[i]$.

$*$ Réciproquement, soit $z \in \mathbb{Z}[i]$ non nul et non inversible.
Alors z divise l'élément $N(z) = z\overline{z} \in \mathbb{N}\backslash\{0; 1\}$.
Soit $p \in \mathbb{N}$ un diviseur premier de $N(z) \geq 2$.
- Si $p \equiv 3$ [4], alors p est irréductible dans $\mathbb{Z}[i]$.

- Si $p \not\equiv 3$ [4], alors d'après le théorème, il existe un couple $(a, b) \in \mathbb{N}^2$ tel que $p = a^2 + b^2 = (a + ib)(a - ib)$.

Par le sens direct, les nombres $a \pm ib$ sont irréductibles dans $\mathbb{Z}[i]$. On a montré que z divise un produit d'éléments irréductibles de la forme annoncée, donc il ne peut y avoir d'autres éléments irréductibles.

■

II.2.2 D'autres théorèmes sur les carrés

On peut se demander si tout entier est la somme de trois carrés d'entiers. Le résultat suivant apporte alors une réponse :

Théorème 7 : Théorème des trois carrés :
Un entier naturel est la somme de trois carrés d'entiers si, et seulement si, il n'est pas de la forme $4^k(8\ell + 7)$ avec $(k, \ell) \in \mathbb{N}^2$.

Remarque 8 :
L'ensemble $\Gamma = \left\{n \in \mathbb{N} \text{ tq } \exists (a, b, c) \in \mathbb{N}^3 \text{ tq } n = a^2 + b^2 + c^2\right\}$ n'est pas stable par produit contrairement à la situation précédente. En effet, on a par exemple :

$$(1^2 + 3^2 + 4^2)(2^2 + 3^2 + 5^2) = 26 \times 38 = 988 = 4(8 \times 30 + 7) \notin \Gamma$$

Pour finir, on a le résultat suivant, parfois appelé théorème de Lagrange :

Théorème 9 : Théorème des quatre carrés [Gourdon, p.54] :
Tout entier naturel est la somme de quatre carrés d'entiers.

Remarque 10 :
$*$ Si $(a, b, c, d) \in \mathbb{N}^4$, alors en utilisant la relation dans le corps des quaternions :

$$(a + bi + cj + dk)(a - bi - cj - dk) = a^2 + b^2 + c^2 + d^2$$

On remarque que l'ensemble $\Delta = \left\{n \in \mathbb{N} \text{ tq } \exists (a, b, c, d) \in \mathbb{N}^4 \text{ tq } n = a^2 + b^2 + c^2 + d^2\right\}$ est stable pour la multiplication.
$*$ On peut déduire le théorème des quatre carrés du théorème des trois carrés. En effet, il suffit de prouver que l'entier $4^k(8\ell + 7)$ est la somme de quatre carrés d'entiers pour tout $(k, \ell) \in \mathbb{N}^2$. Or on a la relation : $4^k(8\ell+7) = 4^k(8\ell+6)+\left(2^k\right)^2$, et par le théorème des trois carrés, le nombre $4^k(8\ell + 6)$ est une somme de trois carrés, d'où le résultat.

II.3 Recasages

Recasages : 121 - 122 - 127.

III Bibliographie

— Daniel Perrin, *Cours d'algèbre*.

— Xavier Gourdon, *Les maths en tête, Algèbre et Probabilités*.