L'anneau $\mathbf{Z}[i]$ et le théorème des deux carrés.

On définit

$$\mathbf{Z}[i] := \{a + ib \in \mathbf{C},\ a, b \in \mathbf{Z}\}$$

l'anneau des *entiers de Gauss* muni de l'automorphsime de conjugaison et de la « norme » hérités de $\mathbf{C}$:

$$\begin{array}{rcl} \sigma : \mathbf{Z}[i] & \longrightarrow & \mathbf{Z}[i] \\ z = a + ib & \longmapsto & \overline{z} = a - ib \end{array} \quad \text{et} \quad \begin{array}{rcl} N : \mathbf{Z}[i] & \longrightarrow & \mathbf{N} \\ z = a + ib & \longmapsto & z\overline{z} = a^2 + b^2 \end{array}$$

De l'étude de $\mathbf{Z}[i]$, on va déduire le théorème des deux carrés dont le but est de préciser l'ensemble :

$$\Sigma := \{n \in \mathbf{N},\ \ n = a^2 + b^2,\ a, b \in \mathbf{N}\}.$$

Propriétés. *On liste ici les propriétés structurelles de* $\mathbf{Z}[i]$ *:*

(i) L'anneau $\mathbf{Z}[i]$ *est un anneau intègre.*

(ii) Les inversibles de $\mathbf{Z}[i]$ *sont connus :* $\mathbf{Z}[i]^\times = \{\pm 1, \pm i\} = \{z \in \mathbf{Z}[i],\ \ N(z) = 1\}$.

(iii) L'anneau $\mathbf{Z}[i]$ *est euclidien, donc principal, pour le stathme* N.

Preuve. Dans l'ordre :

(i) C'est un sous-anneau de $\mathbf{C}$ qui est intègre.

(ii) Si $z = a + ib \in \mathbf{Z}[i]^\times$, alors on note son inverse z' et puisque la norme est à valeurs dans $\mathbf{N}$:

$$N(z)N(z') = 1 \implies N(z) = N(z') = 1$$

de sorte que $a^2 + b^2 = 1$ et $z \in \{\pm 1, \pm i\}$. Réciproquement ces éléments sont bien inversibles.

(iii) C'est presque de l'analyse : si $z, t \in \mathbf{Z}[i] \setminus \{0\}$, alors on commence par écrire dans $\mathbf{C}$:

$$\frac{z}{t} = x + iy \in \mathbf{C} \ \text{ et } \ q = a + ib \in \mathbf{Z}[i] \ \text{ avec } \ |x - a| \leq \frac{1}{2} \ \text{ et } \ |y - b| \leq \frac{1}{2}.$$

Par construction, $|z/t - q| \leq \sqrt{1/4 + 1/4} = \sqrt{2}/2 < 1$ et le reste de la *division euclidienne* de z par t est :

$$r = z - qt \in \mathbf{Z}[i] \ \text{ et } \ |r| = |t||z/t - q| < |t|.$$

On a trouvé $q, r \in \mathbf{Z}[i]$ tels que $z = qt + r$ et $N(r) < N(t)$.

□

Le théorème des deux carrés est en fait peu ou prou une reformulation arithmétique de ce que sont les irréductibles de $\mathbf{Z}[i]$. Comme ça n'est pas l'objectif ici, on renvoie à la fin pour un théorème qui les décrit précisément (mais la preuve n'utilise rien de plus que ce qui va suivre). Notons qu'il ne faut pas confondre *nombre premier* et *entier vu dans dans* $\mathbf{Z}[i]$ *qui s'avère être premier dans cet anneau.* Comme l'anneau est euclidien donc factoriel, on ne parlera pas d'éléments premiers mais seulement d'irréductibles.

Lemme. *Soit* $p \in \mathbf{N}$ *un nombre premier. On a :*

$$p \in \Sigma \iff p \text{ n'est pas irréductible dans } \mathbf{Z}[i].$$

PREUVE. Si $p = a^2 + b^2$, alors $p = (a + ib)(a - ib)$ et $a, b \neq 0$ donc $p \in \mathbf{Z}[i]$ n'est pas irréductible. Réciproquement, si $p = zz'$ avec z, z' non inversibles, alors $N(p) = N(z)N(z') = p^2$ et nécessairement $N(z) = N(z') = p$ donc $p \in \Sigma$. □

Théorème. *Soit $p \in \mathbf{N}$ un nombre premier. On a :*

$$p \in \Sigma \iff p = 2 \text{ ou } p \equiv 1 \text{ (mod. 4)}.$$

PREUVE. La condition est nécéssaire car un carré modulo 4 vaut 0 ou 1 et $2 = 1+1$. Il reste à montrer le sens direct. Compte-tenu du lemme précédent, il suffit de supposer que p n'est pas irréductible, c'est à dire, dans un anneau factoriel, que l'idéal (p) n'est pas premier, ou encore que le quotient $\mathbf{Z}[i]/(p)$ n'est pas intègre. D'abord, on se convainc que :

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

Ensuite, on utilise un théorème d'isomorphisme pour montrer :

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

Et dire que ce dernier anneau n'est pas intègre signifie que $X^2 + 1$ n'est pas irréductible dans $\mathbf{F}_p[X]$, ce qui équivalent (c'est un polynôme de degré 2) à dire que que $X^2 + 1$ a une racine dans $\mathbf{F}_p$. Finalement,

$$p \in \Sigma \iff -1 \in \mathbf{F}_p^{\times 2}.$$

Mais on connait une caractérisation des carrés dans les corps finis : si $p > 2$

$$-1 \in \mathbf{F}_p^{\times 2} \iff (-1)^{\frac{p-1}{2}} = 1 \iff \frac{p-1}{2} \text{ pair} \iff p \equiv 1 \text{ (mod. 4)}.$$

et bien sûr -1 est un carré dans $\mathbf{F}_2$. □

On vient de terminer la description de l'ensemble des des nombres premiers appartenant à Σ. Le théorème des deux carrés dans toute sa généralité en découle, modulo la factorialité de $\mathbf{Z}$.

Théorème (des deux carrés)**.** *Soit $n \in \mathbf{N}$, $n \geq 2$. Alors*

$$n \in \Sigma \iff v_p(n) \text{ pair pour } p \equiv 3 \text{ (mod. 4)}.$$

PREUVE. Comme Σ est stable par multiplication et qu'un carré est toujours dans Σ, le théorème précédent donne le sens réciproque. Pour le sens direct, on fixe $p \equiv 3$ (mod. 4) et on procède par récurrence sur $v_p(n)$. En voici les arguments :

- Si $v_p(n) = 0$ alors c'est fini.
- Si $v_p(n) \geq 1$, alors $p | a^2 + b^2 = (a + ib)(a - ib)$. Mais par le théorème précédent, $p \notin \Sigma$ et le lemme indique que p est irréductible dans $\mathbf{Z}[i]$. Disons par exemple que p divise $a + ib$ dans $\mathbf{Z}[i]$.
- Comme p est entier, $p|a$ et $p|b$ donc $p^2|n$ et on peut même écrire :

  $$\frac{n}{p^2} = a'^2 + b'^2 \in \Sigma \text{ et } v_p\left(\frac{n}{p^2}\right) = v_p(n) - 2 \text{ est pair par hypothèse de récurrence.}$$

  Finalement $v_p(n)$ est aussi pair et on a fini.

□

Quelques compléments et précisions.

- D'abord, on a par les mêmes arguments une description précise des irréductibles de $\mathbf{Z}[i]$:

  Théorème (Irréductibles de $\mathbf{Z}[i]$)**.** *Les irréductibles de* $\mathbf{Z}[i]$ *sont aux inversibles près :*

  (i) Les nombres premiers $p \in \mathbf{N}$ *avec* $p \equiv 3$ (*mod.* 4)*.*

  (ii) Les entiers de Gauss $a + ib$ *dont la norme* $a^2 + b^2$ *est un nombre premier* p*. Dans ce cas, on a* $p = 2$ *ou* $p \equiv 1$ (*mod.* 4)*.*

  Notons qu'il existe une preuve un peu plus pédestre dans [Jeanneret, Lines].

- Le théorème d'isomorphisme en question dans la preuve est le suivant :

  Théorème (d'isomorphisme)**.** *Soient* A *un anneau commutatif unitaire et* I *un idéal de* A*. Alors, les idéaux de* A/I *sont de la forme* J/I *où* J *est un idéal de* A *tel que* $I \subset J$ *et dans ce cas on a un isomorphisme :*

  $$\frac{A/I}{J/I} \simeq \frac{A}{J}.$$

  La preuve repose sans doute sur le théorème de correspondance des idéaux qui donne une bijection entre l'ensemble des idéaux de A contenant I et l'ensemble des idéaux de A/I. Ici, on applique le théorème avec $A = \mathbf{Z}[X]$ et $I = (p) \subset (X^2 + 1, p) = J$ et $I = (X^2 + 1) \subset (X^2 + 1, p) = J$.

- On a aussi passé sous silence le fait que $Z[X]/(p) \simeq \mathbf{F}_p[X]$, qui repose sur le théorème d'isomorphisme « standard ».

- La caractérisation des carrés dans les corps fini repose sur l'étude du nombre de racines du polynôme $X^{\frac{q-1}{2}} - 1$.

Références.

D. Perrin, *Cours d'Algèbre*
A. Jeanneret, D. Lines, *Invitation à l'Algèbre*

120 Anneaux $\mathbf{Z}/n\mathbf{Z}$. Applications.
121 Nombres premiers. Applications.
122 Anneaux principaux. Applications.
126 Exemples d'équations diophantiennes.