2.16 Théorème des deux carrés

Référence : D. Perrin, *Cours d'Algèbre*, Ellispes, 1996.

Leçons concernées : 120, 121, 122, 126.

On introduit $\mathbb{Z}[i] := \{a + ib, a, b \in \mathbb{Z}\}$ l'anneau des entiers de Gauss et on pose $\Sigma := \{n \in \mathbb{N}^* \mid n = a^2 + b^2,\ a, b \in \mathbb{N}\}$. On pose également

$$N : \begin{array}{ccc} \mathbb{Z}[i] & \to & \mathbb{N} \\ z = a + ib & \mapsto & z\overline{z} = a^2 + b^2 \end{array}$$

où, pour $z = a + ib \in \mathbb{Z}[i]$, $\overline{z} = a - ib$.

Proposition 1. *Les inversibles de $\mathbb{Z}[i]$ sont $\{\pm 1, \pm i\}$, de sorte que $z \in \mathbb{Z}[i]^* \Leftrightarrow N(z) = 1$*

Démonstration. Il est clair que ces éléments sont inversibles, réciproquement, si $z = a+ib$ est inversible, alors il existe $z' \in \mathbb{Z}[i]$ tel que $zz' = 1$, et donc $N(zz') = N(z)N(z') = N(1) = 1$ dans $\mathbb{N}$, donc $N(z) = N(z') = 1$. On a donc $a^2 + b^2 = 1$, donc ($a = \pm 1$ et $b = 0$) ou ($a = 0$ et $b = \pm 1$) ce qui nous fournit les quatre éléments annoncés. □

Théorème 2. *On a, pour p premier,*

(i) $\mathbb{Z}[i]$ est euclidien, donc principal.

(ii) $p \in \Sigma \Leftrightarrow p$ n'est pas irréductible dans $\mathbb{Z}[i] \Leftrightarrow p = 2$ ou $p \equiv 1 \mod 4$.

Démonstration. Pour la preuve du point (i), on montre que $\mathbb{Z}[i]$ est euclidien relativement à N. Soit $z, t \in \mathbb{Z}[i]\backslash\{0\}$, on considère $z/t = x + iy \in \mathbb{C}$, et on prend $q = a + ib$ avec $a, b \in \mathbb{Z}$ tels que a et b soient les entiers les plus proches de x et y, ainsi, $|x-a| \leqslant 1/2$ et $|y-b| \leqslant 1/2$ et donc $|z/t - q| \leqslant \sqrt{2}/2 < 1$ (c'est plus clair sur un dessin) d'où $|z - tq| < |t|$. Si on pose $r := z - tq$, on a $z = tq + r$ dans $\mathbb{Z}[i]$ et en passant au carré dans $|r| < |t|$, on obtient $N(r) < N(t)$.

On montre alors la première équivalence du point (ii) : pour le sens direct, si $p = a^2 + b^2$, alors $p = (a + ib)(a - ib)$ dans $\mathbb{Z}[i]$ et puisque a et b sont non nuls, $a + ib$ et $a - ib$ ne sont pas inversibles dans $\mathbb{Z}[i]$ et donc p n'est pas irréductible.

Réciproquement, si $p = zz'$ avec $z, z' \notin \mathbb{Z}[i]^*$, $N(p) = p^2 = N(z)N(z')$ et puisque p est premier et $N(z), N(z') \neq 1$, $N(z) = N(z') = p$ et donc $p \in \Sigma$.

On montre maintenant la seconde équivalence. Puisque $\mathbb{Z}[i]$ est principal donc factoriel, p est irréductible dans $\mathbb{Z}[i]$ si et seulement si l'idéal $(p) = p\mathbb{Z}[i]$ est premier. On utilise alors les isomorphismes suivants : on sait que $\mathbb{Z}[i] \cong \mathbb{Z}[X]/(X^2 + 1)$. D'autre part,

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

d'après le troisième théorème d'isomorphisme. On obtient que (p) est premier dans $\mathbb{Z}[i]$ si et seulement si (X^2+1) est premier dans $\mathbb{F}_p[X]$, or (X^2+1) est premier dans $\mathbb{F}_p[X]$ si et seulement si (X^2+1) n'a pas de racine dans $\mathbb{F}_p[X]$ si et seulement si -1 n'est pas un carré modulo p. Or cette dernière condition est caractérisée par $p \equiv 3 \mod 4$, ce qui achève la démonstration du théorème. □

On peut maintenant conclure sur l'ensemble Σ :

Proposition 3. *On a $n \in \Sigma$ si et seulement si pour tout p premier tel que $p \equiv 3 \mod 4$, $\nu_p(n)$ est pair.*

Démonstration. On sait que $n \in \Sigma$ si et seulement si $\exists z \in \mathbb{Z}[i]$ tel que $n = N(z)$, et donc par multiplicativité de N on obtient la fait que Σ est stable par multiplication. Le sens réciproque s'obtient alors facilement avec le théorème 2.

Réciproquement, soit $p \equiv 3 \mod 4$. On montre par récurrence sur $k \in \mathbb{N}$ que pour tout $n \in \Sigma$ tel que $\nu_p(n) \leqslant k$, $\nu_p(n)$ est pair. Si $k = 0$, c'est clair. Sinon, soit $n \in \Sigma$ tel que $\nu_p(n) \leqslant k \in \mathbb{N}^*$. Si $\nu_p(n) = 0$ le résultat est clair, sinon $p \mid n = a^2 + b^2 = (a+ib)(a-ib)$, or p est irréductible dans $\mathbb{Z}[i]$ principal, donc $p \mid (a+ib)$ ou $p \mid (a-ib)$, disons que $p \mid (a+ib)$. Alors $p \mid a$ et $p \mid b$, ainsi $a = pa'$ et $b = pb'$, donc $n = p^2(a'^2 + b'^2)$ et donc $\frac{n}{p^2} \in \Sigma$. Or $\nu_p(\frac{n}{p^2}) = \nu_p(n) - 2$ et $\nu_p(\frac{n}{p^2})$ est pair par hypothèse de récurrence, donc $\nu_p(n)$ aussi, ce qui conclut la preuve. □

On montre maintenant la série d'isomorphismes donnée à la fin de la preuve du théorème.

Théorème 4 (Troisième théorème d'isomorphisme)**.** *Soit A un anneau, et soit I, J deux idéaux de A tels que $I \subset J$. Alors en tant qu'anneaux,*

$$(A/I)/(J/I) \cong A/J.$$

Démonstration. On note $\pi : A \to A/I$ le morphisme surjectif canonique. Puisque $I \subset J$, $\pi(J) = J/I$ et est un idéal de A/I. D'autre part, puisque $I \subset J$, on peut factoriser $\pi_2 : A \to A/J$ par I et obtenir le morphisme surjectif $\varphi : A/I \to A/J$, dont le noyau est exactement J/I, et donc par le premier théorème d'isomorphisme, $(A/I)/(J/I) \cong A/J$. □

On peut alors montrer :

Proposition 5. *Pour p premier on a*

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

Démonstration. On montre par exemple $\mathbb{Z}[X]/(X^2+1))/(p) \cong \mathbb{Z}[X]/(p, X^2+1)$ grâce au premier théorème d'isomorphisme appliqué à $A = \mathbb{Z}[X]$, $J = (p, X^2+1)$ et $I = (X^2+1)$ en remarquant que $(p, X^2+1)/(X^2+1) = (p)$. Le dernier isomorphisme s'obtient facilement avec le premier théorème d'isomorphisme. □

Remarque : on peut ne pas faire la première proposition sur la détermination des inversibles, et ne faire la proposition 3 que si il reste du temps. La partie sur le troisième théorème d'isomorphisme sert à se préparer à une éventuelle question sur ce point.