Théorème des deux carrés

Recasage : 121 / 122 / 126

Référence : Perrin p.56

On note $\Sigma = \left\{ n \in \mathbb{N} \mid n = a^2 + b^2 \right\}$

On définit l'anneau des entiers de Gauss $\mathbb{Z}[i] = \left\{ a, b \in \mathbb{Z} \mid a + ib \right\}$ on montrera que cette anneau est Euclidien (donc Principal) et que ses inversibles sont $\left\{1; -1\right\}$. De plus cette anneau dispose d'une norme N , en effet si $z \in \mathbb{Z}[i]$ $N(z) = a^2 + b^2$. On vérifiera qu'il s'agit d'une norme multiplicative.

Lemme 1

Soit p premier alors : $p \in \Sigma \iff p$ n'est pas irréductible dans $\mathbb{Z}[i]$

Preuve.

($\Longrightarrow$) Si $p = a^2 + b^2$ on a $p = (a + ib)(a - ib)$ de plus a, b sont non nuls donc $a + ib$ et $a - ib$ ne sont pas des inversibles de $\mathbb{Z}[i]$ de ce fait p n'est pas irréductible.

($\Longleftarrow$) Si $p = zz'$ avec z et z' non inversible dans $\mathbb{Z}[i]$ alors on a $p^2 = N(p) = N(zz') = N(z)N(z')$ et comme $N(z) \neq 1$ alors $N(z) = p$. Mais si $z \in \mathbb{Z}[i]$ alors $z = a + ib$ et donc $N(z) = a^2 + b^2$ et donc $p \in \Sigma$.

Théorème 1 (Deux carrés)

Soit $p \in \mathbb{N}$ un nombre premier alors $p \in \Sigma \iff p = 2$ ou $p \equiv 1[4]$

Preuve.

▶ On comme par démontrer que $p \in \Sigma \iff -1$ est un carré dans $\mathbb{F}_p^*$. D'après ce qui précède et le fait que $\mathbb{Z}[i]$ principal (donc il y a équivalence entre premier et irréductible) :

$$\begin{aligned} p \in \Sigma &\iff p \text{ n'est pas irréductible dans } \mathbb{Z}[i] \\ &\iff (p) \text{ n'est pas premier dans } \mathbb{Z}[i] \\ &\iff \frac{\mathbb{Z}[i]}{(p)} \text{ n'est pas intègre} \end{aligned}$$

Mais $\dfrac{\mathbb{Z}[i]}{(p)} \simeq \dfrac{\mathbb{Z}[X]}{(X^2+1)}$ par division euclidienne et premier théorème d'isomorphisme. De plus on a :

$$\frac{\mathbb{Z}[i]}{(p)} \simeq \frac{\mathbb{Z}[X]}{(p, X^2+1)} \simeq \frac{\mathbb{F}_p[X]}{(X^2+1)}$$

On obtient donc :

$$\begin{aligned} p \in \Sigma &\iff \frac{\mathbb{F}_p[X]}{(X^2+1)} \text{ n'est pas intègre} \\ &\iff (X^2+1) \text{ n'est pas premier} \\ &\iff X^2+1 \text{ n'est pas irréductible dans } \mathbb{F}_p[X] \\ &\iff X^2+1 \text{ a une racine dans } \mathbb{F}_p \qquad (\text{Car } X^2+1 \text{ est de degré 2}) \\ &\iff -1 \text{ est un carré dans } \mathbb{F}_p^* \end{aligned}$$

▶ On montre à présent l'équivalent -1 est un carré dans $\mathbb{F}_p^* \iff p = 2$ ou $p \equiv 1[4]$.

— Si $p = 2$ alors $-1 = 1 = 1^2$ donc -1 est un carré dans $\mathbb{F}_2^*$

— Si $p > 2$ on considère alors les ensembles $A = \Big\{x \in \mathbb{F}_p^* \mid x = y^2\Big\}$ et $B = \Big\{x \in \mathbb{F}_p^* \mid x^{\frac{p-1}{2}} = 1\Big\}$. Montrons que $A = B$ par inclusion et égalité des cardinaux.

Soit $x \in A$, montrons que $x \in B$; par définition $\exists y \in \mathbb{F}_p^*$ tel que $x = y^2$. Mais par théorème de Lagrange $y^{p-1} = 1$ donc $x^{\frac{p-1}{2}} = y^{p-1} = 1$ ainsi $x \in B$.

On considère l'application $\varphi : \begin{array}{ccc} \mathbb{F}_p^* & \longrightarrow & \mathbb{F}_p^* \\ x & \longmapsto & x^2 \end{array}$ ainsi $\text{Im}(\varphi) = A$ et $\text{Ker}(\varphi) = \big\{-1; 1\big\}$ ainsi en vertu du premier théorème d'isomorphisme on obtient $A \simeq \dfrac{F_p^*}{\big\{-1, 1\big\}}$ ce qui nous donne que $|A| = \dfrac{p-1}{2}$. De plus $|B| \leq \frac{p-1}{2}$ car le polynôme $X^{\frac{p-1}{2}}$ à au plus $\dfrac{p-1}{2}$ racines et comme $A \subset$ il vient que $|A| = |B|$ et donc $A = B$.

On a donc -1 qui est un carré dans $\mathbb{F}_p^*$ si et seulement si $x^{\frac{p-1}{2}} = 1$ c'est à dire si qu'il existe $k \in \mathbb{Z}$ tel que $\dfrac{p-1}{2} = 2k$ ce qui veut dire que $p = 4k+1$ et donc $p \equiv 1[4]$. Ce qui achève la preuve.

■

On démontre ici les propriétés annoncés sur l'anneau $\mathbb{Z}[i]$

Lemme 2

L'anneau $\mathbb{Z}[i]$ est euclidien pour le stahtme N.

Preuve.

Soit $z, t \in \mathbb{Z}[i]$ non nuls alors $\dfrac{z}{t} = x + iy$ avec $x, y \in \mathbb{R}$. On note alors $q = a + ib$ avec a l'entier le plus proche de x et b l'entier le plus proche de y . Ainsi :

$$N\Big(\frac{z}{t} - q\Big) = N\Big(x + iy - a - ib\Big) = N\Big(x - a + i(y-b)\Big) = (x-a)^2 + (y-b)^2 \leq \frac{1}{2} < 1$$

Ainsi en posant $r = z - qt$ on a $z = qt + r$ avec $z, q, t \in \mathbb{Z}[i]$ et de plus on a $N(r) < N(t)$. Ainsi l'anneau $\mathbb{Z}[i]$ est Euclidien.

■