TD 8 : corrigé

13. Théorème des deux carrés et irréductibles de $\mathbb{Z}[i]$ (TD 7)

1. Déjà, on peut factoriser une somme de deux carrés dans $\mathbb{Z}[i]$: $a^2+b^2=(a-ib)(a+ib)$. En outre, on a vu lors du TD précédent que les seuls irréductibles de $\mathbb{Z}[i]$ sont ± 1 et $\pm i$. Ainsi, si le nombre premier p s'écrit $p=a^2+b^2$, la décomposition $p=(a-ib)(a+ib)$ ne contient pas d'irréductibles (sinon, on aurait $|p|=1$, ce qui est absurde) et p est bien réductible dans $\mathbb{Z}[i]$.

Pour la réciproque, on rappelle que le carré du module définit une application multiplicative $\mathrm{N} : \mathbb{Z}[i] \to \mathbb{N}$ (la « norme » des arithméticiens). Ainsi, une décomposition du nombre premier $p=(a+ib)(c+id)$ dans $\mathbb{Z}[i]$ donnerait une décomposition

$$p^2 = \mathrm{N}(p) = \mathrm{N}(a+ib)\,\mathrm{N}(c+id) = (a^2+b^2)(c^2+d^2)$$

où ni $a+ib$ ni $c+id$ n'est nul ou inversible. Les facteurs (a^2+b^2) et (c^2+d^2) sont donc >1 et la primalité de p implique : $p=a^2+b^2=c^2+d^2$ et p se décompose bien comme une somme de deux carrés.

2. On a un morphisme d'évaluation

$$\mathrm{év}_i : \begin{array}{ccc} \mathbb{Z}[\mathrm{X}] & \to & \mathbb{C} \\ \mathrm{P} & \mapsto & \mathrm{P}(i) \end{array}$$

auquel on va chercher à appliquer le théorème d'isomorphisme. L'image de $\mathrm{év}_i$ est l'ensemble des nombres complexes obtenus à partir de $\mathbb{Z}$ et de i par sommes et produits. Puisque $\mathbb{Z}[i]$ est un sous-anneau de $\mathbb{C}$, on a clairement $\operatorname{im}\mathrm{év}_i = \mathbb{Z}[i]$.

Le noyau de $\mathrm{év}_i$ est l'ensemble $\left\{ \mathrm{P} \in \mathbb{Z}[\mathrm{X}] \,\middle|\, \mathrm{P}(i)=0 \right\}$. Notons que tout polynôme réel s'annulant en i s'annule également en $-i$. On peut alors, d'après l'exercice 2 de la feuille de TD 7, effectuer la division euclidienne de tout polynôme $\mathrm{P} \in \mathbb{Z}[\mathrm{X}]$ par le polynôme unitaire $(\mathrm{X}-i)(\mathrm{X}+i)=\mathrm{X}^2-1 \in \mathbb{Z}[\mathrm{X}]$: $\mathrm{P}=(\mathrm{X}^2+1)\mathrm{Q}+\mathrm{R}$, avec $\deg \mathrm{R} \leqslant 1$. Puisque aucun polynôme réel de degré $\leqslant 1$, à part le polynôme nul, ne s'annule en i, on obtient donc

$$\mathrm{P}(i)=0 \Leftrightarrow \exists \mathrm{Q} \in \mathbb{Z}[\mathrm{X}] : \mathrm{P}=(\mathrm{X}^2+1)\mathrm{Q},$$

c'est-à-dire l'égalité $\ker \mathrm{év}_i = (\mathrm{X}^2+1)$. D'après le théorème d'isomorphisme, on a donc un isomorphisme :

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

L'exercice 6 de la feuille de TD 7 implique que, lorsque l'on quotiente un anneau par un idéal (x,y), l'anneau quotient est isomorphe au quotient de $\mathrm{A}/(x)$ par l'idéal $(\overline{y}) \lhd \mathrm{A}/(x)$ engendré par l'image $\overline{y}$ de y par l'application canonique $\mathrm{A} \to \mathrm{A}/(x)$. Par symétrie, il est donc également isomorphe à l'anneau obtenu en échangeant les rôles de x et y. Cela fournit donc,

dans le cas de l'idéal $(p, X^2+1) \lhd \mathbb{Z}[X]$, une suite d'isomorphismes :

$$\begin{aligned}
\mathbb{Z}[i]/(p) &\simeq (\mathbb{Z}[X]/(X^2+1))/(p) \qquad \text{d'après le point précédent} \\
&\simeq \mathbb{Z}[X]/(X^2+1, p) \\
&\simeq (\mathbb{Z}[X]/(p))/(X^2+1) \\
&\simeq \mathbb{F}_p[X]/(X^2+1).
\end{aligned}$$

3. L'isomorphisme démontré à la question précédente implique que $\mathbb{Z}[i]/(p)$ est un corps si et seulement si $\mathbb{F}_p[X]/(X^2+1)$ l'est. Ainsi, (p) est un idéal maximal de l'anneau principal $\mathbb{Z}[i]$ si et seulement si (X^2+1) est un idéal maximal de l'anneau principal $\mathbb{F}_p[X]$. Or, on a vu au TD précédent que, dans un anneau principal, (x) est maximal si et seulement si x est irréductible. On a donc démontré l'équivalence

$$p \text{ irréductible dans } \mathbb{Z}[i] \Leftrightarrow X^2+1 \text{ irréductible dans } \mathbb{F}_p[X].$$

Or, un polynôme de degré 2 est irréductible si et seulement s'il n'admet pas de racine. L'irréductibilité de p dans $\mathbb{Z}[i]$ est donc équivalente au fait que -1 n'est pas un carré dans $\mathbb{F}_p$, dont on a déjà vu qu'il était équivalent à la congruence $p \equiv 3 \mod 4$. (En fait, dans l'exercice sur le caractère de Legendre, on avait exclu le cas $p=2$, dans lequel $-1=1$ est bien évidemment un carré et qui est évidemment la somme de deux carrés : $2 = 1^2+1^2$.)

4. Irréductibles dans $\mathbb{Z}[i]$, suite

1. Tout d'abord, tout élément de $\mathbb{Z}[i]$ divise un nombre entier non nul : $a+ib \in \mathbb{Z}[i]$ divise $(a+ib)(a-ib) = a^2+b^2$. Cet entier admet une décomposition en facteurs premiers $p_1^{\alpha_1} \cdots p_n^{\alpha_n}$, ce qui implique $p_1^{\alpha_1} \cdots p_n^{\alpha_n} \in (a+ib)$. Or, si $a+ib$ est irréductible, l'idéal $(a+ib)$ dans $\mathbb{Z}[i]$ est premier, donc il existe un k tel que $p_k \in (a+ib)$, ce qui implique que $a+ib$ divise p_k.
2. On a vu à l'exercice précédent que si p est irréductible, il s'écrit comme somme de deux carrés, ce qui donne une décomposition dans $\mathbb{Z}[i]$

$$p = a^2+b^2 = (a+ib)(a-ib).$$

On a alors $N(a+ib) = N(a-ib)$ et $N(a \pm ib)^2 = N(p) = p^2$, d'où $N(a \pm ib) = p$. Les éléments $a \pm ib$ sont alors irréductibles, comme tout élément de « norme » première. (Si z est de norme première q, toute décomposition $z = uv$ donne une décomposition dans $\mathbb{Z}$: $q = N(u)N(v)$, qui est donc fatalement triviale. On a alors $N(u) = 1$ ou $N(v) = 1$ et, puisque les irréductibles sont exactement les éléments de norme 1, u ou v était irréductible, ce qui prouve que z est irréductible).

On a donc trouvé une décomposition de p en deux irréductibles conjugués. On vérifie aisément que si $a+ib$ et $a-ib$ sont associés, on a $a=0$, $b=0$ (ces deux cas sont exclus, puisque ils impliqueraient que p est un carré) ou alors $a = \pm b$. Dans ce cas, p s'écrit $p = 2 \cdot a^2$, ce qui implique $p=2$. Ainsi, la seule décomposition en produit de deux irréductibles associés est (à multiplication par un inversible près) $2 = (1+i)(1-i)$.
3. La première question implique que les éléments irréductibles de $\mathbb{Z}[i]$ sont les éléments intervenant dans la décomposition en irréductibles des nombres premiers p. En rassemblant les questions des deux exercices, on a donc démontré que *les irréductibles de* $\mathbb{Z}[i]$ *sont les éléments associés aux nombres premiers p congrus à 3 modulo 4 ou aux entiers de Gauß* $a+ib$ *de norme* a^2+b^2 *première.*