UNIVERSITÉ DE RENNES 1

Théorie des nombres

Interrogation 1 — Corrigé

Exercice 1

1 *Quel est l'anneau des entiers de $\mathbb{Q}(i)$? Est-il euclidien ? principal ? factoriel ? (Il n'est pas demandé de fournir une preuve détaillée).*

L'anneau des entiers d'un corps quadratique $\mathbb{Q}(\sqrt{d})$ (pour d un entier relatif sans facteur carré) est :

- $\mathbb{Z}[\sqrt{d}]$ si $d \not\equiv 1 \pmod 4$;
- $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ si $d \equiv 1 \pmod 4$.

Ici, $d = -1$ donc on est dans le premier cas. L'anneau des entiers de $\mathbb{Q}(i)$ est $\mathbb{Z}[i]$.

L'anneau des entiers d'un corps quadratique imaginaire (c'est-à-dire $d < 0$) est euclidien pour $d \in \{-1, -2, -3, -7, -11\}$ (et seulement pour ces entiers négatifs), donc en particulier $\mathbb{Z}[i]$ est euclidien.

Comme tout anneau euclidien est principal et tout anneau principal est factoriel, donc $\mathbb{Z}[i]$ est principal et factoriel.

2 *Dans la suite, p désignera un nombre premier impair. Montrer que si $p \equiv 3 \pmod 4$ alors p n'est pas somme de deux carrés (d'entiers naturels).*

Les carrés dans $\mathbb{Z}/4\mathbb{Z}$ sont : $0^2 \equiv 0$, $1^2 \equiv 1$, $2^2 \equiv 0$ et $3^2 \equiv 1$. On en déduit que la somme de deux carrés peut être congrue à 0, 1 ou 2 modulo 4, mais pas à 3.

Si $p \equiv 3 \pmod 4$, p ne peut donc pas être somme de deux carrés.

3 *Montrer que p est somme de deux carrés si et seulement s'il est la norme d'un élément $a + ib$ de $\mathbb{Z}[i]$.*

Si $(a, b) \in \mathbb{Z}^2$, on a $N_{\mathbb{Q}(i)/\mathbb{Q}}(a + ib) = (a + ib)(a - ib) = a^2 + b^2$, donc

$$\begin{aligned} \exists (a,b) \in \mathbb{Z}^2 \quad p = a^2 + b^2 &\iff \exists (a,b) \in \mathbb{Z}^2 \quad N_{\mathbb{Q}(i)/\mathbb{Q}}(a+ib) \\ &\iff \exists (a+ib) \in \mathbb{Z}[i] \quad N_{\mathbb{Q}(i)/\mathbb{Q}}(a+ib). \end{aligned}$$

4 *Montrer que dans ce cas $(a + ib)|p$ dans $\mathbb{Z}[i]$, et que $a + ib$ est irréductible dans $\mathbb{Z}[i]$.*

Comme $p = N_{\mathbb{Q}(i)/\mathbb{Q}}(a + ib) = (a + ib)(a - ib)$, on a bien $(a + ib)|p$.

Rappelons qu'un élément $x + iy$ de $\mathbb{Z}[i]$ est inversible si et seulement si sa norme est inversible dans $\mathbb{Z}$, et donc si et seulement si elle est égale à 1, puisque les inversibles de $\mathbb{Z}$ sont 1 et -1, et $norm(x + iy) = x^2 + y^2 \in \mathbb{N}$. En effet, si $u = x + iy$ est inversible, on a $N_{\mathbb{Q}(i)/\mathbb{Q}}(u)\, N_{\mathbb{Q}(i)/\mathbb{Q}}(u^{-1}) = N_{\mathbb{Q}(i)/\mathbb{Q}}(uu^{-1}) = N_{\mathbb{Q}(i)/\mathbb{Q}}(1) = 1$, avec

$(N_{\mathbb{Q}(i)/\mathbb{Q}}(u), N_{\mathbb{Q}(i)/\mathbb{Q}}(u^{-1})) \in \mathbb{Z}^2$, donc $N_{\mathbb{Q}(i)/\mathbb{Q}}(u)$ est inversible dans $\mathbb{Z}$, et réciproquement si $N_{\mathbb{Q}(i)/\mathbb{Q}}(x+iy) = 1$, on a $(x+iy)(x-iy) = 1$ donc $x+iy$ est inversible dans $\mathbb{Z}[i]$.

Ici, comme $N_{\mathbb{Q}(i)/\mathbb{Q}}(a+ib) = p \neq 1$, $a+ib$ n'est pas inversible dans $\mathbb{Z}[i]$.

Supposons maintenant que $a+ib = xy$, avec $(x,y) \in \mathbb{Z}[i]^2$. Par multiplicativité de la norme, on a alors $N_{\mathbb{Q}(i)/\mathbb{Q}}(x)\, N_{\mathbb{Q}(i)/\mathbb{Q}}(y) = N_{\mathbb{Q}(i)/\mathbb{Q}}(a+ib) = p$, or $N_{\mathbb{Q}(i)/\mathbb{Q}}(x)$ et $N_{\mathbb{Q}(i)/\mathbb{Q}}(y)$ sont des entiers naturels, et p est un nombre premier, donc $(N_{\mathbb{Q}(i)/\mathbb{Q}}(x), N_{\mathbb{Q}(i)/\mathbb{Q}}(y)) = (1,p)$ ou $(N_{\mathbb{Q}(i)/\mathbb{Q}}(x), N_{\mathbb{Q}(i)/\mathbb{Q}}(y)) = (p,1)$. Dans le premier cas, $N_{\mathbb{Q}(i)/\mathbb{Q}}(x) = 1$ donc x est inversible, et dans le second, $N_{\mathbb{Q}(i)/\mathbb{Q}}(y) = 1$ donc y est inversible.

On trouve donc que $a+ib$ est irréductible dans $\mathbb{Z}[i]$.

5 *En déduire que p est somme de deux carrés si et seulement s'il est réductible dans $\mathbb{Z}[i]$.*

Si p est somme de deux carré, on est dans la situation des deux questions précédentes, donc $p = (a+ib)(a-ib) = a^2+b^2$, avec $(a,b) \in \mathbb{Z}^2$. On a donc $N_{\mathbb{Q}(i)/\mathbb{Q}}(a+ib) = p$ et $N_{\mathbb{Q}(i)/\mathbb{Q}}(a-ib) = a^2+(-b)^2 = p$, donc $a+ib$ et $a-ib$ sont non inversibles. Donc p est réductible.

Réciproquement, si p est réductible, on peut écrire $p = xy$, avec $(x,y) \in \mathbb{Z}[i]^2$, et x et y non inversibles dans $\mathbb{Z}[i]$. Comme $p = xy$, on a $N_{\mathbb{Q}(i)/\mathbb{Q}}(x)\, N_{\mathbb{Q}(i)/\mathbb{Q}}(y) = N_{\mathbb{Q}(i)/\mathbb{Q}}(p) = p^2$, or x et y sont non inversibles dans $N_{\mathbb{Q}(i)/\mathbb{Q}}(x) \neq 1$ et $N_{\mathbb{Q}(i)/\mathbb{Q}}(y) \neq 1$. Comme $N_{\mathbb{Q}(i)/\mathbb{Q}}(x)$ et $N_{\mathbb{Q}(i)/\mathbb{Q}}(y)$ sont des entiers naturels, on a nécessairement $(N_{\mathbb{Q}(i)/\mathbb{Q}}(x), N_{\mathbb{Q}(i)/\mathbb{Q}}(y)) = (p,p)$. D'après la question 3, p est donc alors somme de deux carrés.

6 *Si p est irréductible dans $\mathbb{Z}[i]$, montrer que l'idéal (p) est premier. Que peut-on en déduire au sujet de l'anneau quotient $\mathbb{Z}[i]/(p)$?*

Comme p est irréductible dans $\mathbb{Z}[i]$ et comme l'anneau $\mathbb{Z}[i]$ est factoriel, l'idéal (p) est premier. (C'est le lemme d'Euclide, qui découle l'unicité de la factorisation : si $p|xy$, comme p est irréductible, p apparaît dans la décomposition en produit d'irréductibles de xy donc dans celle de x ou dans celle de y).

Comme l'idéal (p) est premier, le quotient $\mathbb{Z}[i]/(p)$ est un anneau intègre. (On peut remarquer que $\mathbb{Z}[i]/(p)$ est fini de cardinal p^2, donc c'est même un corps).

7 *Montrer que $\mathbb{Z}[i]/(p) \simeq \mathbb{F}_p[X]/(X^2+1)$.*

On considère l'application

$$\left\{ \begin{array}{ccc} \mathbb{Z}[X] & \longrightarrow & \mathbb{F}_p[X]/(X^2+1) \\ P(X) & \longmapsto & \overline{P}[X], \end{array} \right.$$

où $\overline{P}$ désigne le polynôme obtenu en réduisant modulo p les coefficients de P.

Cette application est clairement un morphisme d'anneaux, surjectif. Comme l'idéal (X^2+1) de $\mathbb{Z}[X]$ est inclus dans son noyau, elle induit un morphisme surjectif $\mathbb{Z}[i] \simeq \mathbb{Z}[X]/(X^2+1) \longrightarrow \mathbb{F}_p[X]/(X^2+1)$.

Les éléments $a+ib$ de $\mathbb{Z}[i]$ dont l'image dans $\mathbb{F}_p[X]/(X^2+1)$ est nulle sont ceux qui vérifient $(X^2+1)|(\overline{a}X+\overline{b})$, où $\overline{a}$ (respectivement $\overline{b}$) désigne la réduction de a (respectivement b) modulo p. Comme le degré de $\overline{a}X+\overline{b}$ est strictement plus petit que

celui de X^2+1, cela équivaut à ce que $\overline{a}X+\overline{b}=0$ dans $\mathbb{F}_p[X]$, c'est-à-dire $\overline{a}=\overline{b}=0$, donc à ce que a et b soient multiples de p, donc à $a+ib\in(p)$.

On en déduit donc un isomorphisme entre $\mathbb{Z}[i]/(p)$ et $\mathbb{F}_p[X]/(X^2+1)$.

8 *Montrer que $\mathbb{F}_p[X]/(X^2+1)$ est intègre si et seulement si -1 n'est pas un carré dans $\mathbb{F}_p$.*

Si -1 est un carré dans $\mathbb{F}_p$, posons $a\in\mathbb{F}_p$ tel que $a^2=-1$. On a alors $(X-a)(X+a)=X^2+1$, mais $(X^2+1)\nmid(X\pm a)$, donc $\mathbb{F}_p[X]/(X^2+1)$ n'est pas un anneau intègre.

Réciproquement, si -1 n'est pas un carré dans $\mathbb{F}_p$, alors le polynôme $X^2+1\in\mathbb{F}_p[X]$ n'a pas de racine dans $\mathbb{F}_p$. Comme il est de degré 2, il est donc irréductible dans $\mathbb{F}_p[X]$. L'anneau $\mathbb{F}_p[X]$ étant euclidien, donc factoriel, on en déduit que l'idéal (X^2+1) de $\mathbb{F}_p[X]$ est premier, et donc que $\mathbb{F}_p[X]/(X^2+1)$ est un anneau intègre.

9 *Montrer que -1 est un carré dans $\mathbb{F}_p$ si seulement si $p\equiv 1\pmod 4$. Conclure.*

Rappelons qu'un élément x de $\mathbb{F}_p^\times$ est un carré si et seulement si $x^{\frac{p-1}{2}}=1$. En effet :

- comme le polynôme X^2-1 a exactement deux racines, 1 et -1, dans $\mathbb{F}_p$, le noyau du morphisme de groupes $\mathbb{F}_p^\times\to\mathbb{F}_p^\times$, $u\mapsto u^2$ est $\{\pm1\}$, donc le nombre de carrés dans $\mathbb{F}_p^\times$ est égal au cardinal de $\mathbb{F}_p^\times/\{\pm1\}$, c'est-à-dire $\frac{p-1}{2}$;
- ces $\frac{p-1}{2}$ carrés sont tous des racines du polynôme $X^{\frac{p-1}{2}}-1$, puisqu'ils forment un sous-groupe de cardinal $\frac{p-1}{2}$ de $\mathbb{F}_p^\times$;
- or le polynôme $X^{\frac{p-1}{2}}-1$ a au plus $\frac{p-1}{2}$ racines dans $\mathbb{F}_p$, puisque qu'il est de degré $\frac{p-1}{2}$ et $\mathbb{F}_p$ est un corps (donc est intègre), donc ses racines sont exactement les $\frac{p-1}{2}$ carrés contenus dans $\mathbb{F}_p$.

On a $(-1)^{\frac{p-1}{2}}\equiv 1\pmod p$ si et seulement si $p\equiv 1\pmod 4$, donc -1 est un carré dans $\mathbb{F}_p$ si seulement si $p\equiv 1\pmod 4$.

Si p est somme de deux carrés, alors $p\equiv 1\pmod 4$, d'après la question 2. Réciproquement, si $p\equiv 1\pmod 4$, alors -1 est un carré dans $\mathbb{F}_p$, donc (question 8) l'anneau $\mathbb{F}_p[X]/(X^2+1)$ n'est pas intègre, donc (question 7) $\mathbb{Z}[i]/(p)$ n'est pas intègre, donc (contraposition de la question 6) p est réductible dans $\mathbb{Z}[i]$, donc (question 5) p est somme de deux carrés.

On trouve donc que p est somme de deux carrés si et seulement si $p\equiv 1\pmod 4$.