UNIVERSITÉ DE BORDEAUX
M1, Théorie des Nombres
2020-2021

Feuille 1. Les entiers de Gauss

Exercice 1. Les entiers du corps $\mathbf{Q}[i]$. Soit

$$\mathbf{Q}[i] = \{a + bi \mid a, b \in \mathbf{Q}\}$$

le corps engendré sur $\mathbf{Q}$ par l'élément $i = \sqrt{-1}$.

1) Montrer que $[\mathbf{Q}[i] : \mathbf{Q}] = 2$ et donner une base simple de $\mathbf{Q}[i]$ sur $\mathbf{Q}$.

On note $\mathrm{N} := \mathrm{N}_{\mathbf{Q}[i]/\mathbf{Q}}$ et $\mathrm{Tr} := \mathrm{Tr}_{\mathbf{Q}[i]/\mathbf{Q}}$ les applications norme et trace respectivement.

2) Soit $\alpha = a + bi \in \mathbf{Q}[i]$, $a, b \in \mathbf{Q}$. Expliciter $\mathrm{N}(\alpha)$ et $\mathrm{Tr}(\alpha)$ en fonction de a et b. Donner le polynôme minimal de α.
3) Montrer que α est un élément entier sur $\mathbf{Z}$ si et seulement si $\mathrm{Tr}(\alpha)$ et $\mathrm{N}(\alpha) \in \mathbf{Z}$.
4) Montrer que α est un élément entier sur $\mathbf{Z}$ si et seulement si $a, b \in \mathbf{Z}$.

On définit l'anneau des entiers de Gauss comme étant l'ensemble

$$\mathbf{Z}[i] = \{a + bi \mid a, b \in \mathbf{Z}\}$$

muni de l'addition et la multiplication usuelles.

Exercice 2. L'anneau $\mathbf{Z}[i]$: premières propriétés.
1) Déterminer le groupe des éléments inversibles (groupe des unités) de $\mathbf{Z}[i]$. (Indication : utiliser la multiplicativité de la norme).
2) Montrer que pour tout $z \in \mathbf{C}$ il existe $q \in \mathbf{Z}[i]$ tel que $N(z - q) \leqslant \frac{1}{2}$.
3) Montrer que $\mathbf{Z}[i]$ est un anneau euclidien. En dédure qu'il est principal.

Exercice 3. Éléments irréductibles I.
1) On dit qu'un entier $n \geqslant 1$ est somme de deux carrés s'il existe deux entiers $a, b \in \mathbf{Z}$ tels que $n = a^2 + b^2$. Montrer que si m et n sont sommes de deux carrés, alors le produit mn l'est. (Indication: utiliser l'application norme).
2) Soit $\pi = a+bi$ un élément irréductible. Montrer que $\bar{\pi} = a-bi$ est irréductible. Soient $a, b \neq 0$. Montrer que π et $\bar{\pi}$ sont associés si et seulement si $|a| = |b| = 1$. (Rappelons que deux éléments α et β sont associés si et seulement s'il existe un élément inversible u tel que $\alpha = \beta u$).
3) Soit $\pi \in \mathbf{Z}[i]$. Montrer que si $N(\pi)$ est un nombre premier, alors π est irréductible.
4) Décomposer 2 en produit d'élements irréductibles dans $\mathbf{Z}[i]$.
5) Soit $\pi = a + bi$ avec $a, b \neq 0$. Montrer que π est irréductible si et seulement si $N(\pi)$ est un nombre premier.
6) Soit $p \geqslant 2$ un nombre premier. Montrer que p est somme de deux carrés si et seulement si p n'est pas irréductible dans $\mathbf{Z}[i]$.
7) Soit p un nombre premier. Montrer que p est réductible dans $\mathbf{Z}[i]$ si et seulement si p est somme de deux carrés.
8) Montrer que si $p \equiv 3 \pmod 4$, alors p est irréductible dans $\mathbf{Z}[i]$.

Tournez la page s.v.p.

Exercice 4. La congruence $x^2 \equiv -1 \pmod p$. Soit p un nombre premier $\neq 2$.

1) Soit $x \in \mathbf{Z}$. Décomposer x^2+1 en produit de deux facteurs dans $\mathbf{Z}[i]$.

2) Montrer que si la congruence $x^2 \equiv -1 \pmod p$ admet une solution dans $\mathbf{Z}$, alors p est réductible dans $\mathbf{Z}[i]$. En déduire que si la congruence $x^2 \equiv -1 \pmod p$, alors $p \equiv 1 \pmod 4$.

3) Montrer que réciproquement, si $p \equiv 1 \pmod 4$, alors $x^2 \equiv -1 \pmod p$ admet une solution dans $\mathbf{Z}$. Indication: le groupe multiplicatif $(\mathbf{Z}/p\mathbf{Z})^*$ est cyclique (pourquoi ?).

Exercice 5. Éléments irréductibles II.

1) Montrer que si $p \equiv 1 \pmod 4$, alors p est réductible dans $\mathbf{Z}[i]$.

2) Donner la liste d'éléments irréductibles de $\mathbf{Z}[i]$.