ENTIERS DE GAUSS

1. On montre que c'est un sous-anneau de $(\mathbb{C},+,\times)$.

- $\mathbb{Z}[i]\subset\mathbb{C}$
- $1=1+0\cdot\mathrm{i}\in\mathbb{Z}[i]\neq\varnothing$
- Si $a,b,a',b'\in\mathbb{Z}$,

$$(a+\mathrm{i}b)-(a'+\mathrm{i}b')=(a-a')+\mathrm{i}(b-b')\in\mathbb{Z}[i]$$
$$(a+\mathrm{i}b)\cdot(a'+\mathrm{i}b')=(ab'-bb'')+\mathrm{i}(ab'+ba')\in\mathbb{Z}[i]$$

Donc $(\mathbb{Z}[i],+,\times)$ est un anneau.

---

2. Si $z\in\mathbb{Z}[i]$, $a,b\in\mathbb{Z}$ tel que $z=a+\mathrm{i}b$ est inversible, on a $z'\in\mathbb{Z}[i]$ tel que $zz'=1$.
Alors $N(1)=1=N(zz')=\left|zz'\right|^2=|z|^2\left|z'\right|^2=\underbrace{N(z)}_{\in\mathbb{N}}\underbrace{N(z')}_{\in\mathbb{N}}$ donc $N(z)=1=\underbrace{a^2}_{\in\mathbb{N}}+\underbrace{b^2}_{\in\mathbb{N}}$ et $\{a^2,b^2\}=\{0,1\}$ et donc $z\in\{-1,1,\mathrm{i},-\mathrm{i}\}$.
Réciproquement, $-1,1,\mathrm{i},-\mathrm{i}$ sont bien inversibles dans $\mathbb{Z}[i]$.

Donc $U_{\mathbb{Z}[i]}=\mathbb{U}_4=\{-1,1,\mathrm{i},-\mathrm{i}\}$.

---

3. Il suffit d'écrire (par exemple) $2=(1+\mathrm{i})(1-\mathrm{i})$ avec $1\pm\mathrm{i}\notin U_{\mathbb{Z}[i]}$ donc 2 n'est pas irréductible.

4.a) On a $\varphi(\mathrm{i})^2=\varphi\left(\mathrm{i}^2\right)=\varphi(-1)=-\varphi(1)=-1$. Donc $\varphi(i)\in\{-\mathrm{i},\mathrm{i}\}$.

4.b) On a par récurrence que pour tout $n\in\mathbb{N}$, $\varphi(n)=n$ (car $\varphi(0)=0$ et si pour un $n\in\mathbb{N}$, $\varphi(n)=n$, alors $\varphi(n+1)=\varphi(n)+1=n+1$).
Puis pour tout $n\in\mathbb{N}$, $\varphi(-n)=-\varphi(n)=-n$ donc pour tout $k\in\mathbb{Z}$, $\varphi(k)=k$.
En suite, si $a,b\in\mathbb{Z}$, $\varphi(a+\mathrm{i}b)=\varphi(a)+\varphi(\mathrm{i})\varphi(b)=a+\varphi(i)b$.

Donc si $\varphi(\mathrm{i})=\mathrm{i}$, $\varphi=\mathrm{id}_{\mathbb{Z}[i]}$ et si $\varphi(\mathrm{i})=-\mathrm{i}$, $\varphi:z\mapsto\overline{z}$.

Réciproquement, ces deux applications sont bien des morphismes d'anneau.

---

5. $\mathbb{Q}[i]$ est un sous-corps de $(\mathbb{C},+,\times)$.

- $\mathbb{Q}[i]\subset\mathbb{C}$
- $1=1+0\cdot\mathrm{i}\in\mathbb{Q}[i]\neq\varnothing$
- Si $a,b,a',b'\in\mathbb{Q}$,

$$(a+\mathrm{i}b)-(a'+\mathrm{i}b')=(a-a')+\mathrm{i}(b-b')\in\mathbb{Q}[i]$$

et si $a'+\mathrm{i}b'\neq0$,

$$\frac{a+\mathrm{i}b}{a'+\mathrm{i}b'}=\frac{(a+\mathrm{i}b)(a'-\mathrm{i}b')}{a'^2+b'^2}=\frac{aa'+bb'}{a'^2+b'^2}+\mathrm{i}\frac{ba'-ab'}{a'^2+b'^2}\in\mathbb{Q}[i]$$

Donc $(\mathbb{Q}[i],+,\times)$ est un corps.

---

6. Comme dans la question 4, on démontre que si φ est un endomorphisme de $\mathbb{Q}[\mathrm{i}]$, $\varphi(\mathrm{i})\in\{\pm\mathrm{i}\}$ et pour tout $k\in\mathbb{Z}$, $\varphi(k)=k$.
Puis, si $r=\dfrac{p}{q}\in\mathbb{Q}$ avec $p\in\mathbb{Z}$ et $q\in\mathbb{N}^*$, alors $\varphi(r)=\varphi\left(\frac{p}{q}\right)=\dfrac{\varphi(p)}{\varphi(q)}=\dfrac{p}{q}=r$. Donc pour tout $a,b\in\mathbb{Q}$, $\varphi(a+\mathrm{i}b)=a+\varphi(\mathrm{i})b$.

Donc les morphismes de corps de $\mathbb{Q}[i]$ sont $z\mapsto z$ et $z\mapsto\overline{z}$.

Fin