

## Série 9





**Exercice 1.** Soit  $A$  un anneau commutatif. Montrer que  $A[X]$  est principal  $\iff A$  est un corps.

**Exercice 2.** Soit  $A$  un anneau intègre et  $N : A \rightarrow \mathbb{N}$  une fonction vérifiant  $N(a) = 0 \iff a = 0$ . On suppose de plus que  $N$  est multiplicative c'est-à-dire  $N(xy) = N(x)N(y)$ .

- a) Montrer qu'il existe une fonction  $N' : Q(A) \rightarrow \mathbb{Q}_+$  telle que  $N'(a) = N(a)$  pour tout  $a \in A$ .  
 b) Montrer que  $A$  est euclidien  $\iff$  pour tout  $x \in Q(A)$  il existe  $c \in A$  tel que  $N'(x - c) < 1$ .


**Exercice 3. Entiers de Gauss**

Soit  $\mathbb{Z}[i]$  l'anneau des entiers de Gauss et  $N : \mathbb{Z}[i] \rightarrow \mathbb{N}$  la norme définie par  $N(a + ib) = a^2 + b^2$ .

-  a) Montrer que  $N(xy) = N(x)N(y)$  pour tout  $x, y \in \mathbb{Z}[i]$ . Montrer que  $N(x) = 1 \iff x \in \mathbb{Z}[i]^*$ .  
 b) Montrer que  $\mathbb{Z}[i]$  est euclidien par rapport à  $N$ . (utiliser 2b))  
 c) En déduire que  $\mathbb{Z}[i]$  est principal.  
 d) Montrer que  $\mathbb{Z}[X]/\langle X^2 + 1 \rangle \cong \mathbb{Z}[i]$ .  
 e) Soit  $p \in \mathbb{P}$  un premier. Montrer que  $\mathbb{Z}[i]/p\mathbb{Z}[i] \cong \mathbb{F}_p[X]/\langle X^2 + 1 \rangle$ .  
 f) Montrer que  $\mathbb{F}_p[X]/\langle X^2 + 1 \rangle$  est intègre si et seulement si l'équation  $x^2 = -1$  n'a pas de solution dans  $\mathbb{F}_p$ .

**Exercice 4. Les premiers de Gauss**

- a) Soit  $p \in \mathbb{P}$  un premier. Montrer que soit  $p$  est premier dans  $\mathbb{Z}[i]$ , soit  $p = N(\pi)$  pour un premier  $\pi$  de  $\mathbb{Z}[i]$ .  
 b) Soit  $\pi$  un premier de  $\mathbb{Z}[i]$ . Montrer que  $N(\pi)$  est un premier de  $\mathbb{Z}$  ou le carré d'un premier de  $\mathbb{Z}$ .  
 c) Soit  $p \in \mathbb{P}$ . Montrer que  $p \equiv 1 \pmod{4} \iff$  l'équation  $x^2 = -1$  admet une solution dans  $\mathbb{F}_p$ . (pour  $\Rightarrow$  utiliser le fait que  $\mathbb{F}_p^*$  est un groupe cyclique d'ordre  $p - 1$ ).  
 d) Soit  $p$  un premier avec  $p \equiv 3 \pmod{4}$ . Déduire de c) que si  $p \mid x^2 + y^2$  (avec  $x, y \in \mathbb{Z}$ ) alors  $p \mid x$  et  $p \mid y$ .  
 e) Soit  $p \in \mathbb{P}$ . Montrer que  $p$  est un premier de  $\mathbb{Z}[i]$  si et seulement si  $p \equiv 3 \pmod{4}$ . (Indication : utiliser 3e), 3f) et 4c)).  
 f) Soit  $p \in \mathbb{P}$ . Montrer que  $p \equiv 1 \pmod{4} \iff$  il existe des entiers  $a$  et  $b$  tel que  $p = a^2 + b^2$ . (Utiliser 4a) et 4e))

 **Exercice 5.** Montrer que l'équation  $x^2 + 5 = y^3$  n'a pas de solutions entières<sup>1</sup>.

<sup>1</sup>Raisonnement mod 4 puis réécrire l'équation sous la forme  $x^2 + 4 = (y - 1)(y^2 + y + 1)$ , puis utiliser 4 d).