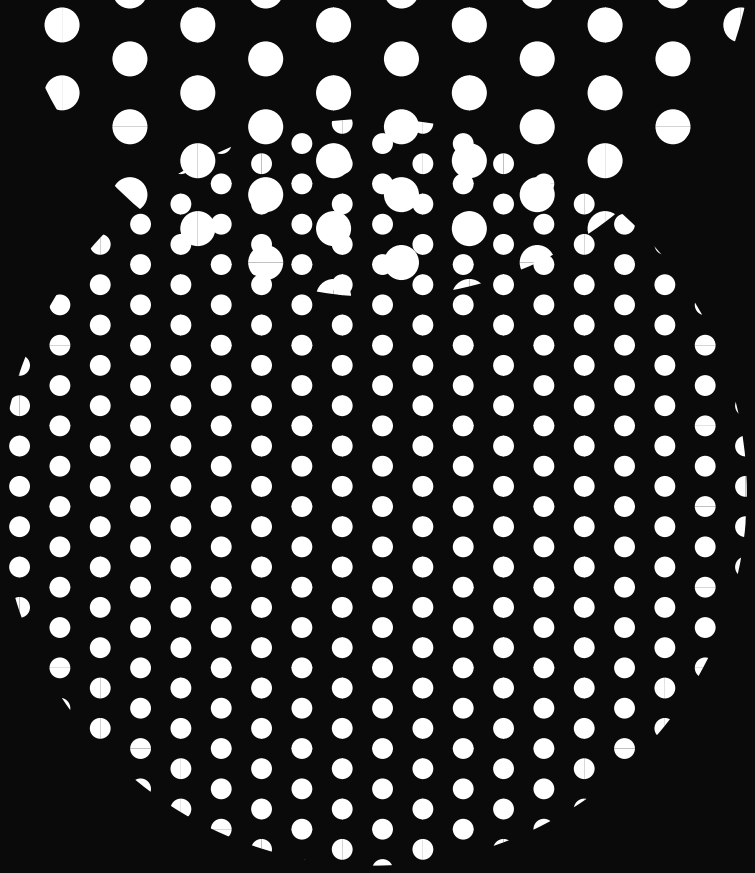

Exercice 1

a) $|(\mathbb{Z}/13\mathbb{Z})^\times| = \varphi(13) = 13-1 = 12$

$(\mathbb{Z}/13\mathbb{Z})^\times = \{\bar{1}, \dots, \overline{12}\}$

Si $x \in (\mathbb{Z}/13\mathbb{Z})^\times$, $o(x) \mid 12$ par Lagrange

donc $o(x) \in \{1, 2, 3, 4, 6, 12\}$

$\bar{2}^6 = \overline{64} = -1 \rightarrow o(2) \neq 6$
$\neq 3$
$\neq 2$
$\neq 1$
$\neq 4$ car $\bar{2}^4 = \overline{16} \neq 1$

donc $o(\bar{2}) = 12$ et $(\mathbb{Z}/13\mathbb{Z})^\times = \langle 2 \rangle$
donc $(\mathbb{Z}/13\mathbb{Z})^\times$ cyclique.

b) $(\mathbb{Z}/12\mathbb{Z})^\times$ $\varphi(12) = \varphi(4)\varphi(3)$
$= 2 \cdot (2-1)(3-1)$
$= 2 \cdot 2 = 4$

$(\mathbb{Z}/12\mathbb{Z})^\times = \{\bar{1}, \bar{5}, \bar{7}, \overline{11}\}$

$o(\bar{1}) = 1$
$\bar{5}^2 = \overline{25} = \bar{1}$ donc $o(\bar{5}) = 2$
$\bar{7}^2 = (-\bar{5})^2 = \bar{1}$ donc $o(\bar{7}) = 2$
$\overline{11}^2 = (-1)^2 = \bar{1}$ donc $o(\overline{11}) = 1$

Donc, il n'y a aucun élément d'ordre 4
d'où $(\mathbb{Z}/12\mathbb{Z})^\times$ n'est pas cyclique.

Exercice 2

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

$(\mathbb{C}, +, *)$ anneau et corps

A ss-anneau ssi : 1) $(A,+)$ ss gpe
2) A stable par $*$

A ss-corps ssi : 1) A ss-anneau
2) $A^\times = A \setminus \{0\}$

a) Comme $\mathbb{Z} \subset \mathbb{C}$

donc $\forall\, a+bi \in \mathbb{Z}$ et $a'+b'i \in \mathbb{Z}[i]$

$a+bi \in \mathbb{C}$

$$a+bi - a'-b'i = \underbrace{(a-a')}_{a'' \in \mathbb{Z}} + \underbrace{(b-b')}_{b' \in \mathbb{Z}} i \quad \text{donc} \quad \in \mathbb{Z}[i]$$

Donc $\mathbb{Z}[i]$ est bien un ss-gpe

$$(a+bi)\times(a'+b'i) = aa' + ba'i + b'ai + bb'i^2$$
$$= \underbrace{aa' - bb'}_{a'' \in \mathbb{Z}} + \underbrace{(ba' + b'a)}_{b'' \in \mathbb{Z}} i \quad \text{donc} \quad \in \mathbb{Z}[i] \in \mathbb{C}$$

Donc un ss-anneau

Soit

et $2 \in \mathbb{Z} \subset \mathbb{Z}[i]$

pour 2 il n'y a pas d'inverse dans $\mathbb{Z}[i]$

donc $\mathbb{Z}[i]$ n'est pas un ss-corps.

Sol de prof :

a) 1) Soient $z, z' \in \mathbb{Z}[i] \subset \mathbb{C}$

$\exists\, a, a', b, b' \in \mathbb{Z}$ tq $z = a + bi$
$z' = a' + b'i$

on a : $z - z' = \underbrace{(a-a')}_{\in \mathbb{Z}} + i\underbrace{(b-b')}_{\in \mathbb{Z}}$ car $(\mathbb{Z}, +)$ un gpe

donc $\in \mathbb{Z}[i]$ donc un ss-gpe

2) $z \cdot z' = \underbrace{aa' - bb'}_{"a" \in \mathbb{Z}} + (\underbrace{ba' + b'a}_{"b" \in \mathbb{Z}})i \quad \in \mathbb{Z}[i]$ car $(\mathbb{Z}, +, \times)$ un anneau

donc $\mathbb{Z}[i]$ stable par multiplication.
Finalement, $\mathbb{Z}[i]$ est un ss-anneau de $\mathbb{C}$

$2 = 2 + 0i \in \mathbb{Z}[i]$ et $2^{-1} = \frac{1}{2} \notin \mathbb{Z}$ donc $2^{-1} \notin \mathbb{Z}[i]$
et $2^{-1} \in \mathbb{R}$

Ce qui conclut que $\mathbb{Z}[i]$ est (pas) un ss-corps.

b) Soit $z \in \mathbb{Z}[i]^\times$
donc $\exists\, a, b \in \mathbb{Z}$ tq $z = a + ib$
d'où $\bar{z} = a - ib \in \mathbb{Z}[i]^\times$

Donc $z\bar{z} \in \mathbb{Z}[i]^\times$
$\|$
$|z|^2 = a^2 + b^2$
$|z|^2 \in \mathbb{R}$ $z\bar{z} \in \mathbb{Z}^\times = \{-1, 1\}$

donc $|z|^2 = 1$
et $a^2 + b^2 = 1 \iff \begin{cases} a = \pm 1 \text{ et } b = 0 \\ \text{ou } a = 0 \text{ et } b = \pm 1 \end{cases}$

D'où $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$

Exercice 3

Anneau

A intègre $\Leftrightarrow (\forall a,b \in A,\ ab=0 \Rightarrow a=0 \text{ ou } b=0)$

$$(a,0) \times (0,a) = (0,0)$$
$$\neq (0,0) \qquad \neq (0,0)$$

Exercice 8

Soient $A = X^6+1 \in \mathbb{C}[X]$ $\quad$ $B = X^4+X^3+X-1 \in \mathbb{C}[X]$

$$\begin{array}{r|l}
X^6+1 & X^4+X^3+X-1 \\
\hline
X^6+X^5+X^3-X^2 & X^2-X+1 \\
\cline{1-1}
-X^5-X^3+X^2+1 & \\
-X^5-X^4-X^2+X & \\
\cline{1-1}
+2X^2 \quad X^4-X^3-X+1 & \\
X^4+X^3+X-1 & \\
\cline{1-1}
\underbrace{-2X^3+2X^2-2X+2}_{C} &
\end{array}$$

Donc $A = (X^2-X+1)B + C$

2) $\quad X^4+X^3+X-1 = -2(X^3-X^2+X-1)\left(-\frac{1}{2}X-1\right)$

$$\begin{array}{r|l}
X^4+X^3+X-1 & -2(X^3-X^2+X-1) \\
\hline
X^4-X^3+X^2-X & -\frac{1}{2}X-1 \\
\cline{1-1}
2X^3-X^2+2X-1 & \\
2X^3-2X^2+2X-2 & \\
\cline{1-1}
X^2+1 &
\end{array}$$

$$B = \left(-\tfrac{1}{2}X-1\right)C + (X^2+1)$$

$$
\begin{array}{l|l}
-2X^3+2X^2-2X+2 & X^2+1 \\
\hline
+2X^3+2X & -2X+2 \\
\hline
2X^2+2 & \\
-2X^2-2 & \\
\hline
0 &
\end{array}
$$

Donc $C = (-2X+2)(X^2+1)$

Finalement $\text{pgcd}(A,B) = \text{pgcd}(B,C) = \text{pgcd}(C, X^2+1) = X^2+1 = D$

c)

$$\overbrace{X^2+C}^{D} = B + \left(\tfrac{1}{2}X+1\right)C$$

$$= B + \left(\tfrac{1}{2}X+1\right)\left(A-(X^2-X+1)B\right)$$

$$= B\left[1-\left(\tfrac{1}{2}X^3-\tfrac{1}{2}X^2+\tfrac{1}{2}X+X^2-X+1\right)\right] + \left(\tfrac{1}{2}X+1\right)A$$

$$= B\left(-\tfrac{1}{2}X^3-\tfrac{1}{2}X^2+\tfrac{1}{2}X\right) + \left(\tfrac{1}{2}X+1\right)A$$

$$D = B\cdot\overbrace{\left(-\tfrac{1}{2}(X^3+X^2-X)\right)}^{=V_0} + \overbrace{\left(\tfrac{1}{2}X+1\right)}^{U_0}A$$

$$D = AU+BV$$

$$\iff 0 = A(U-U_0)+B(V-V_0)$$

$$\iff \tilde{A}\underbrace{(U-U_0)}_{\tilde{U}} + \tilde{B}\underbrace{(V-V_0)}_{\tilde{V}}$$

avec $\tilde{A} = \frac{A}{D}$ $\tilde{B} = \frac{B}{D}$

donc $\begin{cases} \tilde{U} = \tilde{B}P \\ \tilde{V} = -\tilde{A}P \end{cases}$ $P \in \mathbb{R}[X]$

D'où $S = \left\{ (U,V) \text{ avec } \begin{cases} U = \tilde{B}P + U_0 \\ V = \tilde{B}P + V_0 \end{cases} \right\}$

où $P \in \mathbb{R}[X]$

où $A = X^4 - X^2 + 1$
$B = X^2 + X - 1$

Exercice 4

Anneau commutatif

I idéal de $A \Leftrightarrow$ (1) $(I, +)$ ss-gpe
(2) $\forall a \in A, \forall b \in I$
$ab \in I$

$N = \{a \in A \,/\, \exists n \geq 1 \text{ tq } a^n = 0\}$

a) $N \subset A$

2) Soient $a \in A$ et $b \in N$

$\exists n \geq 1$ tq $b^n = 0$

d'où $(ab)^n = a^n b^n = a^n \cdot 0 = 0$
($ab \in A$)

donc $ab \in N$

1) Soient $a, b \in N$

donc $\exists n, m \geq 1$ tq $a^n = 0$ et $b^m = 0$

$(a-b)^l = 0$ pour $l \geq 1$

Soit $l \geq 1$ on a $(a-b)^l = \sum_{k=0}^{l} \binom{l}{k} a^k (-b)^{l-k}$

Il suffit que : $a^k = 0$ ou $b^{l-k} = 0$ pour $0 \leq k \leq l$

On pose $l = n + m$

si $k \geq n$: $a^k = 0$ ok :

$0 \leq k \leq m$ donc $l - k > m$ d'où $b^{l-k} = 0$ ok !

d'où $(a-b)^l = 0$ avec $l \geq 1$

Donc $a - b \in N$

Finalement N idéal de A

B) Soit $a \in N$ donc $\exists n \geq 1 \quad a^n = 0$

$(1-a)^{-1}$

$-1 = a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + \dots + 1)$

donc $\quad 1 = (1-a)(a^{n-1} + a^{n-2} + \dots + 1)$

D'où $1 - a \in A^\times$

On pose $\tilde{n} = 2n+1 \geq 1$

$1 = 1 + a^{\tilde{n}} = 1 - (-a)^{\tilde{n}}$

$= (1+a)(a^{\tilde{n}-1} - a^{\tilde{n}-2} + \dots + 1)$

D'où $1 + a \in A^\times$

C) Soit $a \in A^\times$ et $b \in N$

$\in N$ car Jideal

on a : $a + b = a\underbrace{(1 + \overbrace{a^{-1}b}^{\in N})}_{\text{inversible}} \in A^\times$