exo 3

Si $p \in \mathbb{P}$ $\quad \forall x \in \mathbb{F}_p^* \quad x^{p-1} = 1$

$\mathbb{F}_p^*$: groupe de card $p-1$

$\forall x \in \mathbb{F}_p \quad x^p = x$

$42 = 2 \times 3 \times 7$ et, 2, 3 et 7 sont premiers entre eux

$$f \left| \begin{array}{ccc} \mathbb{Z}/42\mathbb{Z} & \longrightarrow & \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \\ \overline{x}^{[42]} & \longmapsto & (\overline{x}^{[2]}, \overline{x}^{[3]}, \overline{x}^{[7]}) \end{array} \right. \text{ est un isom d'anneaux}$$

Soit $x \in \mathbb{Z}$, $\quad x^{13} \equiv x \ [42] \iff \overline{x}^{13} = \overline{x}$ dans $\mathbb{Z}/42\mathbb{Z}$

$$\iff \begin{cases} \overline{x}^{13} = \overline{x} \text{ dans } \mathbb{Z}/2\mathbb{Z} \\ \overline{x}^{13} = \overline{x} \text{ dans } \mathbb{Z}/3\mathbb{Z} \\ \overline{x}^{13} = \overline{x} \text{ dans } \mathbb{Z}/7\mathbb{Z} \end{cases}$$

toujours vrai car :

- Dans $\mathbb{Z}/2\mathbb{Z}$: $\overline{x}^{13} = (\overline{x}^3)^4 \overline{x} = \overline{x}^4 \overline{x} = \overline{x}^3 \overline{x} \overline{x} = \overline{x}^3 = \overline{x}$
- Dans $\mathbb{Z}/7\mathbb{Z}$: $\overline{x}^{13} = \overline{x}^7 \overline{x}^6 = \overline{x}^7 = x$

$\text{Sol} = \mathbb{Z}$

exo

Il reste entre 100 et 300 soldats (x soldats)

On les range par 5, il en reste 1 ;

— 6 — 2 ;

— 7 — 3.

$$x \in \mathbb{Z}, \begin{cases} x \equiv 1 \ [5] \\ x \equiv 2 \ [6] \\ x \equiv 3 \ [7] \end{cases} \quad (S)$$

5, 6 et 7 sont 2 à 2 premiers entre eux $\quad (5 \cdot 6 \cdot 7 = 210)$

Ψ (du thm des restes chinois) est un morphisme d'anneau et S a une unique solution mod 210

a = 1, b = 2, c = 3

$x_0 = a6 \cdot 7 \cdot e + b5 \cdot 7 \cdot f + c5 \cdot 6g$

où $\left| \begin{array}{l} \overline{e} = \overline{6 \cdot 7}^{-1} \text{ dans } \mathbb{Z}/5\mathbb{Z} \\ \overline{f} = \overline{5 \cdot 7}^{-1} \text{ — 6 —} \\ \overline{g} = \overline{6 \cdot 5}^{-1} \text{ — 7 —} \end{array} \right.$

$$\exists (u_1, v_1), (u_2, v_2), (u_3, v_3) \in \mathbb{Z}^2 \ / \begin{cases} u_1 6 \cdot 7 + v_1 5 = 1 \\ u_2 5 \cdot 7 + v_2 6 = 1 \\ u_3 5 \cdot 6 + v_3 7 = 1 \end{cases} \xrightarrow{\mathbb{Z}/5\mathbb{Z}} \overline{e} = \overline{u_1}$$

$(\overline{e}, \overline{f}, \overline{g}) = (\overline{3}; \overline{-1}, \overline{4})$

Donc $x_0 = 126a - 35b + 120c$ puis $\text{Sol} = 126a - 35b + 120c + 210\mathbb{Z}$

exo 5

Mq $\langle G \setminus H \rangle = G$

$\exists x \in G \setminus H$

Soit $y \in G$, mq $y \in \langle G \setminus H \rangle$

Supposons par l'absurde que $x * y \in H$

alors $x = x * y * y^{-1} \in H$ ↯

Donc $x * y \in G \setminus H$

$y = \underbrace{x^{-1}}_{\in G \setminus H} * \underbrace{x * y}_{\in G \setminus H} \in \langle G \setminus H \rangle$ [Somme tordue] produit

$\subset \langle G \setminus H \rangle$

exo 8

1. • $0 \in \sqrt{I}$ car $0^2 = 0 \in I$ (idéal)

• Soit $(i,j) \in \sqrt{I}^2$, $\exists (n,m) \in \mathbb{N}^2 / i^n \in I$, $j^m \in I$

$$(i-j)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} i^k (-j)^{n+m-k} \quad \text{(binôme de Newton dans A commutatif)}$$

$$= \sum_{k=0}^{n} \binom{n+m}{k} i^k (-j)^{n+m-k} + \sum_{k=n+1}^{n+m} \binom{n+m}{k} i^k (-j)^{n+m-k}$$

Or : • $\forall k \in [\![0; n]\!]$, $n+m-k \geq m$

donc $\underbrace{\binom{n+m}{k} i^k (-j)^{n-k} (-1)^m}_{\in A} \underbrace{j^m}_{\in I} \in I$ (absorbance)

• $\forall k \in [\![n+1; n+m]\!]$, $i^k \in I$ $(k \geq n)$

donc $\binom{n+m}{k} i^k (-j)^{n+m-k} \in I$

Conclusion $(i-j)^{n+m} \in I$ (somme)

donc $i - j \in \sqrt{I}$

• Soit $(a,x) \in A \times \sqrt{I}$

$\exists n \in \mathbb{N} / x^n \in I$

Or I est un idéal : $a^n x^n \in I$

Or A est commutatif donc $a^n x^n = (ax)^n$

Donc $ax \in \sqrt{I}$

2. $107800 = 2^2 \cdot 5^2 \cdot 1078 = 2^3 \cdot 5^2 \cdot 11 \cdot 49 = 2^3 \cdot 5^2 \cdot 7^2 \cdot 11$

Mq $\sqrt{107800\,\mathbb{Z}} = 770\,\mathbb{Z}$ $(2 \cdot 5 \cdot 7 \cdot 11\,\mathbb{Z})$

⇒ $x \in 770\,\mathbb{Z}$

$\exists k \in \mathbb{Z} / x = 2 \cdot 5 \cdot 7 \cdot 11 k$ donc $x^3 = k^3 \overbrace{2^3 \cdot 5^2 \cdot 7^2 \cdot 11}^{107800} \times 5 \cdot 7 \cdot 11^2$

donc $x^3 \in 107800\,\mathbb{Z}$

$\subset$ Soit $x \in \sqrt{1078800\mathbb{Z}}$

$\exists (k,v) \in \mathbb{N}^* \times \mathbb{Z} \;/\; x^k = (2^3 \cdot 5^2 \cdot 7^2 \cdot 11)v$

$v_2(x) \geq 3/k > 0$

$v_5(x) \geq 2/k > 0$

$v_7(x) \geq 2/k > 0$

$v_{11}(x) \geq 1/k > 0$

Or $v_\uparrow : \mathbb{Z} \to \mathbb{N}$ donc

$v_2(x), v_5(x), v_7(x), v_{11}(x) \geq 1$

Donc $x \in 770\mathbb{Z}$ $(\exists a \in \mathbb{Z}^* / x = 2 \cdot 5 \cdot 7 \cdot 11 a)$

exo 11

Rq $f \left| \begin{array}{l} G \to G \\ x \mapsto x^m \end{array} \right.$ est bijective

Il suffit de mq elle est injective car $|G| < +\infty$

Soit $x, y \in G$ tq $x^m = y^m$

$\exists (u,v) \in \mathbb{Z}^2 / um + vm = 1$

$x^{vm} = y^{vm}$ donc $x^{1-um} = y^{1-um}$

ie $x(x^{-u})^m = y(y^{-u})^m$

$= 1_G$ car $\mathrm{ord}(x^{-u}) \mid m$

Donc $x = y$

exo

K corps commutatif fini $\Longrightarrow \exists p \in \mathbb{P}, \exists r \geq 1, |K| = p^r$

Soit K un tel corps et $f : \left| \begin{array}{l} \mathbb{Z} \to K \\ n \mapsto n1_K \end{array} \right.$ un morphisme d'anneaux $\begin{pmatrix} f(0) = 0 \\ f(1) = 1 \end{pmatrix}$

$\mathrm{Ker}(f) = a\mathbb{Z}$ où $a \in \mathbb{N}^*_{\geq 2}$ (sg de $\mathbb{Z}$)

Supposons $a \notin \mathbb{P}$: $\exists 2 \leq q_1, q_2 \leq a-1$, $a = q_1 q_2$

alors $0 = f(q_1 q_2) = f(q_1) f(q_2) \in K$ intègre

donc $f(q_1) = 0$ ou $f(q_2) = 0$

donc $q_1 \in a\mathbb{Z}$ ou $q_2 \in a\mathbb{Z}$ ↯

Donc $a \in \mathbb{P}$

Soit $\overline{f} : \left| \begin{array}{l} \mathbb{Z}/p\mathbb{Z} \to K \\ \overline{n} \mapsto n1_K \end{array} \right.$; $\overline{n_1} = \overline{n_2} \Longrightarrow n_1 - n_2 \in p\mathbb{Z}$

$\Longrightarrow f(n_1) - f(n_2) = 0$

Sur K on a + et $\cdot : \left| \begin{array}{l} \mathbb{Z}/p\mathbb{Z} \times K \to K \\ (\overline{n}, x) \mapsto \overline{f}(\overline{n}).x \end{array} \right.$

$\overline{f}(\overline{n}).x = n.1_K$

$(K, +, \cdot)$ est un $\mathbb{F}_p$-ev

K est une famille génératrice finie de ce $\mathbb{F}_p$-ev
On en extrait une base $e_1, \dots, e_r$

On pose $\begin{cases} \mathbb{F}_p^r \longrightarrow K \\ (\lambda_1, \dots, \lambda_r) \longmapsto \sum_{i=1}^{r} \lambda_i e_i \end{cases}$ isom de $\mathbb{F}_p$-ev

$|\underbrace{\mathbb{F}_p^r}_{p^r}| = |K|$