

ID - Structures algébriques

Ex 2

Resoudre $9x \equiv 6 [24]$ avec $x \in \mathbb{Z}$

Soit $x \in \mathbb{Z}$

$$9x \equiv 6 [24] \iff 3x \equiv 2 [8]$$

$$\begin{array}{lcl} \overline{3} \times \overline{x} = \overline{2} & \iff & \overline{3} \overline{x} = \overline{2} \quad \text{dans } \mathbb{Z}/8\mathbb{Z} \\ \updownarrow & & \\ \iff & & \overline{x} = \overline{6} \quad \text{dans } \mathbb{Z}/8\mathbb{Z} \end{array}$$

Donc: $\text{Sol} = 6 + 8\mathbb{Z}$

Autre methode

$$9x \equiv 6 [24]$$

$$\iff \overline{3} \overline{x} = \overline{6} \quad \mathbb{Z}/24\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \quad \text{car } 3 \wedge 8 = 24$$

$$\iff \begin{array}{l} \text{Thm} \\ \text{chinois} \end{array} \left\{ \begin{array}{ll} \overline{3} \overline{x} = \overline{6} & \text{dans } \mathbb{Z}/3\mathbb{Z} \\ \overline{3} \overline{x} = \overline{6} & \text{dans } \mathbb{Z}/8\mathbb{Z} \end{array} \right.$$

$$\iff \overline{x} = \overline{6} \quad \text{dans } \mathbb{Z}/8\mathbb{Z}$$

$$\text{Sol} = 6 + 8\mathbb{Z}$$

Ex 4

37 premier donc $\mathbb{Z}_{137\mathbb{Z}}$ est un corps.

Soit $(x, y) \in (\mathbb{Z}_{137\mathbb{Z}})^2$

$$(S) \begin{cases} \overline{6}x + \overline{7}y = \overline{30} \\ \overline{3}x - \overline{7}y = \overline{0} \end{cases}$$

$$\Leftrightarrow \begin{cases} \overline{6}x + \overline{7}y = \overline{30} \\ \overline{6}x - \overline{14}y = \overline{0} \end{cases}$$

$$L_2 \leftarrow \overline{2}L_2$$

$\neq \overline{0}$

$$\Leftrightarrow \begin{cases} \overline{6}x + \overline{7}y \\ \overline{16}y = \overline{-30} \\ \overline{16} \neq \overline{0} \end{cases}$$

$$L_2 \leftarrow L_2 - L_1$$

$$\Leftrightarrow \begin{cases} \overline{6}x + \overline{7}y = \overline{30} \\ -\overline{3}y = \overline{1} \end{cases}$$

$$L_2 \leftarrow \overline{7}^{-1} L_2$$

$\neq \overline{0}$

$$\underline{1} = 37 \times 1 + 12 \times (-3)$$

$$\Leftrightarrow \begin{cases} \overline{6}x + \overline{7}y = \overline{30} \\ y = \overline{12} \end{cases}$$

$$L_2 \leftarrow \overline{12} L_2$$

$$\Leftrightarrow \begin{cases} \overline{6}x = \overline{30} - \overline{7}y \\ y = \overline{12} \end{cases}$$

$$\Leftrightarrow \begin{cases} \bar{c}_x = \bar{30} - \bar{89} = -\bar{59} \\ y = \bar{12} \end{cases} \Leftrightarrow \begin{cases} \bar{c}_x = \bar{20} \\ y = \bar{12} \end{cases}$$

$$\Leftrightarrow \begin{cases} \bar{x} = -\bar{120} \\ \bar{y} = \bar{12} \end{cases} \quad L_{\perp} \leftarrow \bar{\delta} L_{\perp}$$

$$\Leftrightarrow \begin{cases} \bar{x} = \bar{28} \\ y = \bar{12} \end{cases}$$

$$\text{Sol}(S) = \{ (\bar{28}, \bar{12}) \}$$

Ex.

Recherche d'un $x \in \mathbb{Z}$.

$$(S) \begin{cases} x \equiv -5 \pmod{7} \\ x \equiv -3 \pmod{11} \end{cases}$$

$$\underbrace{-3 \times 7}_{=a} + \underbrace{2 \times 11}_{=b} = 1$$

$$a \equiv \begin{cases} 0 \pmod{7} \\ 1 \pmod{11} \end{cases}, \quad b \equiv \begin{cases} 0 \pmod{11} \\ 1 \pmod{7} \end{cases}$$

$$\underline{3a + 5b} \equiv \begin{cases} 5 & [7] \\ 3 & [11] \end{cases}$$

$$\begin{aligned} &= -63 + 110 \\ &= 47 \end{aligned}$$

47 est solut° particulière

7 et 11 premiers entre eux. Le thm chinois line
que la solut° est unique mod 7×11

$$\text{Sol} = 47 + 77\mathbb{Z}$$

Ex:

Resoudre l'inconnue $x \in \mathbb{Z}$:

$$\begin{cases} x \equiv 1 & [7] \\ x \equiv 2 & [9] \\ x \equiv 3 & [13] \end{cases}$$

$$\bullet (-50) \times 7 + \boxed{3 \times (9 \times 13)} \stackrel{=9}{=} 1$$

$$\bullet (-10) \times 9 + \boxed{1 \times (7 \times 13)} \stackrel{=6}{=} 1$$

$$\bullet (-29) \times 13 + \boxed{6 \times (7 \times 9)} \stackrel{=63}{=} 1$$

$$a \equiv \begin{cases} 1 & [7] \\ 0 & [9] \\ 0 & [13] \end{cases}, \quad b \equiv \begin{cases} 0 & [7] \\ 1 & [9] \\ 0 & [13] \end{cases}$$

$$c \equiv \begin{cases} 0 & [7] \\ 0 & [9] \\ 1 & [13] \end{cases}$$

$$a + 2b + 3c \equiv \begin{cases} 4 & [7] \\ 2 & [9] \\ 3 & [13] \end{cases}$$

$$a + 2b + 3c = 351 + 2 \times 91 + 3 \times 378$$

$$= 351 + 182 + 1134$$

$$= 1667$$

7, 9, 13 sont 2 à 2 premiers entre eux

Thm chinois: le système a une unique solution
mod $7 \times 9 \times 13 = 819$

$$\text{Sol} = 1667 + 819\mathbb{Z} = 29 + 819\mathbb{Z}$$

$$= 2 \times 819 + 29$$

Ex 11:

- G grp fini de card n .
- $a \in G$
- $m \in \mathbb{Z}$ tel que $na^m = 1$

$$\forall a \in G \exists ! x \in G \quad x^m = a$$

$$\Leftrightarrow \begin{array}{c|c} & G \longrightarrow G \\ & x \longmapsto x^m \end{array} \quad \text{bij.}$$

$$\Rightarrow \text{f. inj. car } G \text{ est fini}$$

Soit $x, y \in G$ tel que $f(x) = f(y)$.

Montrons que $x = y$.

Q1a: $x^m = y^m$.

Par Bézout: $\exists u, v \in \mathbb{Z}$ tel que $nu + mv = 1$

Alors: $x^{mv} = y^{mv}$

$$x^{1-nu} = y^{1-nu}$$

$$x \underbrace{(x^n)^{-u}}_{\in G} = y \underbrace{(y^n)^{-u}}_{\in G}$$

Donc $x = y$

Ex 13: $\mathbb{Z}[i] = \{a + ib : (a, b) \in \mathbb{Z}^2\}$

$$\begin{array}{ccc} N & | & \mathbb{Z}[i] \longrightarrow \mathbb{R}_+ \\ & & z \longmapsto z \times \bar{z} \end{array}$$

Q1) Claire que $\mathbb{Z}[i]$ ss-anneau de $\mathbb{C}$

Q2) $\mathbb{Z}[i] \subset \mathbb{C}$ donc $\forall x \in \mathbb{Z}[i]$

$\exists ! (a, b) \in \mathbb{Z}^2$ tel que $x = a + ib$

Soit $x \in \mathbb{Z}[i] \setminus \{0\}$ et $a, b \in \mathbb{Z}$ tel que
 $x = a + ib$

Montrons que x est inversible $\Leftrightarrow N(x) = 1$

$\Leftarrow$ Supposons que $N(x) = 1$.

$$\frac{1}{x} = \frac{1}{a+ib} = \frac{a}{a^2+b^2} - \frac{ib}{a^2+b^2} = \frac{a}{1} - \frac{ib}{1} \in \mathbb{Z}[i]$$

$\Rightarrow$ Supposons x est inversible.

$$\exists y \in \mathbb{Z}[i] \quad xy = 1$$

Donc $|x|^2 |y|^2 = 1$
 $\Rightarrow N(x) = N(y)$

$$N(x), N(y) \in \mathbb{N} \quad \text{donc} \quad N(x) = 1$$

Q3) Raisonnons par analyse-synthèse

(A) Soit $x \in U(\mathbb{Z}[i])$, $a, b \in \mathbb{Z}$ tel que $x = a+ib$

Alors $a^2 + b^2 = 1$

D'où 4 choix: $x = 1$ ou $x = -1$
ou $x = i$ ou $x = -i$

(S) Les q conviennent

$$U(\mathbb{Z}[i]) = \mathcal{U}_4 \subseteq \mathbb{Z}/4\mathbb{Z}$$

Q4) $x \in \mathbb{Z}[i]$ inversé si

$$\begin{cases} \cdot x \text{ est inv} \\ \cdot \forall y, z \in \mathbb{Z}[i] \quad x = yz \Rightarrow y \text{ unité ou } z \text{ unité} \end{cases}$$

$$2 = \underbrace{(1-i)}_{\text{non inv}} \underbrace{(1+i)}_{\text{non inv}}$$

Q5) Soit $z \in \mathbb{Z}[i]$; $w \in \mathbb{Z}[i] \setminus \{0\}$

① $\frac{z}{w} \in \mathbb{C} \quad \frac{z}{w} = x + iy \quad \text{ou } x, y \in \mathbb{R}$

On pose $a, b \in \mathbb{Z} \subset \mathbb{R}$ tel que

$$|x - a| \leq \frac{1}{2}; \quad |y - b| \leq \frac{1}{2}$$

On pose alors $q = a + ib \in \mathbb{Z}[i]$

$$\text{et } r = z - qw \in \mathbb{Z}[i]$$

② Placements; $z = qw + r$

On vérifie $N(r) \leq N(w)$

$$r = z - qw = w \left(\frac{z}{w} - q \right) = w \left((x-a) + i(y-b) \right)$$

$$\text{Donc } N(r) \leq |r|^2 = |w|^2 \left| (x-a) + i(y-b) \right|^2$$

$$\leq N(w) \times \left(\frac{1}{4} + \frac{1}{4} \right) = \frac{N(w)}{2} \\ \leq N(w)$$

On note:

Centre-exemple $z = 3+3i$; $w = 2$;

$$q_1 = 1+i; r_1 = 1+i$$

$$q_2 = 2+2i; r_2 = -1-i$$

$$z = q_1 w + r_1 = q_2 w + r_2$$

mais: $q_1 \neq q_2$ et $r_1 \neq r_2$