TD Correction

Exercice 119

Posons $\forall k \in [\![0 ; n-1]\!]$,

$$\alpha_k = \begin{cases} 1 \text{ si } k=0 \\ 0 \text{ sinon} \end{cases} \quad ; \quad \beta_k = 0$$

et $\cdot \; 0_{\mathbb{C}} = \sum_{k=0}^{n-1} \beta_k \omega^k \in \mathbb{Z}[\omega]$

$\cdot \; 1_{\mathbb{C}} = \sum_{k=0}^{n-1} \alpha_k \omega^k \in \mathbb{Z}[\omega]$.

Soit $a, b \in \mathbb{Z}[\xi]$

$\exists (a_k)_{k \in [\![0;n-1]\!]}, (b_k)_{k \in [\![0;n-1]\!]} \in \mathbb{Z}^n$ tel que

$$a = \sum_{k=0}^{n-1} a_k \omega^k, \quad b = \sum_{k=0}^{n-1} b_k \omega^k$$

- $a - b = \sum_{k=0}^{n-1} a_k \omega^k - \sum_{k=0}^{n-1} b_k \omega^k = \sum_{k=0}^{n-1} \underbrace{(a_k - b_k)}_{\in \mathbb{Z}} \omega^k \in \mathbb{Z}[\xi]$

- $a \times b = \left(\sum_{i=0}^{n-1} a_i \omega^i\right)\left(\sum_{j=0}^{n-1} b_j \omega^j\right) = \sum_{(i,j) \in [\![0;n-1]\!]^2} a_i b_j \omega^{i+j}$

Il suffit de montrer que : $\forall (i,j) \in [\![0;n-1]\!]^2, \omega^{i+j} \in \mathbb{U}_n$.

Soit $(i,j) \in [\![0;n-1]\!]^2$

$\exists (q,r) \in \mathbb{N}^* \times [\![0;n-1]\!],\ i+j = qn+r$

donc $\omega^{i+j} = \underbrace{(\omega^n)^q}_{=1} \omega^r = \omega^r \in \mathbb{U}_n$.

- Il s'agit donc d'un sous-anneau de $(\mathbb{C},+,\times)$

Exercice 2 (TD)

Soit $x \in \mathbb{Z}$.

- $(*)$ $9x \equiv 6\ [24] \iff \bar{9}\bar{x} = \bar{6}$ (dans $\mathbb{Z}/24\mathbb{Z}$).

$24 = 3 \times 8$, avec $3 \wedge 8 = 1$. Par théorème des restes chinois,

$$f : \left| \begin{array}{ccc} \mathbb{Z}/24\mathbb{Z} & \longrightarrow & \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \\ \bar{x}^{[24]} & \longmapsto & (\bar{x}^{[3]}, \bar{x}^{[8]}) \end{array} \right.$$ isomorphismes d'anneaux.

- $(*) \iff f(\overline{9x}^{[24]}) = f(\bar{6}^{[24]})$

$$\iff \begin{cases} \bar{9}^{[3]}\bar{x}^{[3]} = \bar{6}^{[3]} \\ \bar{9}^{[8]}\bar{x}^{[8]} = \bar{6}^{[8]} \end{cases}$$

(On peut accélérer mais on détaille ici)

$\iff \bar{x}^{[8]} = \bar{6}^{[8]}$

$9x \equiv 6\ [24] \iff \bar{x}^{[8]} = \bar{6}^{[8]}$

$\iff x \in 6 + 8\mathbb{Z}$.

Exercice 3

Soit $n \in \mathbb{Z}$.

$(*)\ n^{13} \equiv n\ [42] \iff \bar{n}^{13} = \bar{n}$ (dans $\mathbb{Z}/_{42\mathbb{Z}}$)

$42 = 2 \times 3 \times 7$ et $2, 3, 7$ sont 2 à 2 premiers entre eux.
Par théorème des restes chinois,

$$\overline{n}^{[42]\,13} = \overline{n}^{[42]}$$

$$\iff \begin{cases} \left(\overline{n}^{[2]}\right)^{13} = \overline{n}^{[2]} & \text{tjrs vrai} \\ \left(\overline{n}^{[3]}\right)^{13} = \overline{n}^{[3]} & \text{tjrs vrai (on peut aussi procéder par exhaustion)} \\ \left(\overline{n}^{[7]}\right)^{13} = \overline{n}^{[7]} & \end{cases}$$

(Si p premier, $x^p \equiv x\ [p]$ tjrs vrai. Dans $\mathbb{Z}/_{p\mathbb{Z}}$: $\bar{x}^p = \bar{x}$)

Dans $\mathbb{Z}/_{3\mathbb{Z}}$: $\bar{n}^{13} = \bar{n}$
$\iff \bar{n} = \bar{n}$

$(*) \iff \bar{n}^{13} = \bar{n}$ dans $\mathbb{F}_7$
$\iff \bar{n}^{6 \cdot 7} - \bar{n} = \bar{0}$ ~~$\iff \bar{n}(\bar{n}^5 - \bar{1}) = \bar{0}$~~
tjrs vrai ~~$\iff \begin{cases} \bar{n} = \bar{0} \\ \text{ou} \\ \bar{n}^5 = \bar{1} \end{cases}$ $\mathbb{F}_7$ corps~~ ~~$\bar{n} \in \mathbb{F}_7^*$ groupe de card 6.~~
~~$\iff \bar{n} = \bar{1}$~~

$$\boxed{\text{D'où l'ensemble des } n \in \mathbb{Z} \text{ tq } n^{13} \equiv n\ [42] \text{ est } \mathbb{Z}}$$

~~$\iff \bar{n} = \bar{0}$ ou $\bar{n} = \bar{1}$ dans $\mathbb{Z}/_{7\mathbb{Z}}$~~

~~L'ensemble des $x \in \mathbb{Z}$ tq $n^{13} \equiv n\ [42]$ est~~

$$\boxed{\cancel{7\mathbb{Z} \sqcup (1 + 7\mathbb{Z})}}$$

Exercice 163 $\quad x \in \mathbb{Z}$

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

5, 6 et 7 sont 2 à 2 premiers entre eux, donc le théorème des restes chinois s'applique : (S) a une unique solution mod 210

$42 \times 3 + 5 \times (-25) = 1$

$35 \times (-1) + 6 \times 6 = 1$

$7 \times 13 + 30 \times (-3) = 1$

$30 = 7 \times 4 + 2 \qquad 7 = 3 \times 2 + 1$

donc $1 = 7 - 3 \times 2 = 7 - 3 \times (30 - 7 \times 4)$

$= 13 \times 7 - 3 \times 30$

D'après le théorème des restes chinois,

$x = 1 \times (1 - (-25) \times 5) + 2 \times (1 - 6 \times 6) + 3 \times (1 - 7 \times 13)$

$= 126 - 70 - 270 = -214$ est solution particulière de (S)

$\overline{x} = \overline{206}$ (dans $\mathbb{Z}/210\mathbb{Z}$)

Donc $Sol(S) = 206 + 210\mathbb{Z}$

Exercice 8

1) • $0_A \in \sqrt{I}$ car $0_A^1 = 0_A \in I$

• Soient $a, b \in \sqrt{I}$. Il existe $n, m \in \mathbb{N}$, $a^n \in I$ et $b^m \in I$.

Mq $(a-b) \in I$.

$$(a-b)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} a^k b^{n+m-k} \quad (A \text{ est commutatif})$$

Soit $k \in [\![0 ; n+m]\!]$.

• 1er cas : si $k \geq n$

Alors $a^k = a^n \times a^{k-n}$ avec $k-n \geq 0$ $\in I$ (I absorbant)

Donc $\binom{m+n}{k} a^k b^{m+n-k} \in I$ (I absorbant)

- 2ᵉ cas : si $k \leq n$.

Alors $-k \geq -n$, donc $n+m-k \geq m$
D'où $b^k = b^m \times b^{m-k} \in I$ (I absorbant)
De m̂, $\binom{m+n}{k} a^k b^{m+n-k} \in I$.

- Caractère absorbant, soit $(a,b) \in \sqrt{I} \times A$.

Alors $\exists n \in \mathbb{N}, a^n \in I$.
Donc $(ba)^n = b^n a^n$ (A commutatif)
$\in I$ (I absorbant)

2) $107800 = 2^3 \times 5^2 \times 7^2 \times 11$

$$\sqrt{107800\mathbb{Z}} = \{a \in \mathbb{Z} \mid \exists n \in \mathbb{N}, \underbrace{a^n \in 107800\mathbb{Z}}_{107800 \mid a^n}\}$$

$$= \{a \in \mathbb{Z} \mid \exists n \in \mathbb{N}, 107800 \mid a^n\}.$$

Conjecture : $\sqrt{107800\mathbb{Z}} = \underbrace{2 \times 5 \times 11 \times 7}_{770}\mathbb{Z}$

Procédons par double-inclusion.

$\boxed{\subset}$ Soit $x \in \sqrt{107800\mathbb{Z}}$

Il existe $n \in \mathbb{N}$, $2^3 \times 5^2 \times 7^2 \times 11 \mid x^n$
donc $v_2(x^n) \geq 3$, donc $n v_2(x) \geq 3$, donc $v_2(x) \geq \frac{3}{n} > 0$
donc $2 \mid x$

De m̂, $5 \mid x$, $7 \mid x$, $11 \mid x$.
Donc $2 \times 5 \times 7 \times 11 \mid x$ car ils sont premiers
Donc $x \in 770\mathbb{Z}$.

$\boxed{\supset}$ Soit $x \in 770\mathbb{Z}$.
$2 \times 5 \times 7 \times 11 \mid x$.

En particulier, $107800 \mid x^3$, donc $x \in \sqrt{107800\mathbb{Z}}$

Finalement, $\sqrt{107800\mathbb{Z}} = 770\mathbb{Z}$.

Exercice 11

Reformulation : Mq $f \left| \begin{array}{l} G \longrightarrow G \\ x \longmapsto x^m \end{array} \right.$ est bijective. (⚠ pas morphisme, G pas abélien)

Comme G est fini, montrons que f est injectif.
Soit $(x,y) \in G \times G$, tq $x^m = y^m$
Il existe $(u,v) \in \mathbb{Z}$ tel que $um + vn = 1$
$x^{mu} = y^{mu} \Rightarrow x^{1-nv} = y^{1-nv} \Rightarrow x\underbrace{(x^n)}_{e}{}^{-v} = y\underbrace{(y^n)}_{e}{}^{-v}$
$\Rightarrow x = y$.