Corrigé du DS 1.

MP* INP-HB / L. TINTINAGLIA

I 1 (0,5)

Posons

$$\Theta : \begin{cases} \mathbb{Z}[X] \longrightarrow \mathbb{Z}[i] \\ P \longmapsto P(i) \end{cases}$$

On vérifie que Θ est un morphisme d'anneaux : pour $P, Q \in \mathbb{Z}[X]$, $\Theta(PQ) = (PQ)(i) = P(i)Q(i) = \Theta(P)\Theta(Q)$ et $\Theta(1) = 1$.

Ainsi $\mathbb{Z}[i] = \mathrm{Im}(\Theta)$ est un sous-anneau de $\mathbb{C}$.

I.2 (2)

On a clairement $\{a+ib,\ (a,b) \in \mathbb{Z}^2\} \subseteq \mathbb{Z}[i]$.

Soit $P = X^2+1$. Soit $Q \in \mathbb{Z}[X]$ $(Q(i) \in \mathbb{Z}[i])$.

Par division euclidienne, $Q = \widetilde{Q}P + \widetilde{R}$, $\deg \widetilde{R} \leq 1$

$= \widetilde{Q}(X^2+1) + \widetilde{R}$

Comme P est unitaire, $\widetilde{Q}$ et $\widetilde{R}$ sont dans $\mathbb{Z}[X]$.

$\deg(\widetilde{R}) \leq 1$ donc on dispose de $(\alpha, \beta) \in \mathbb{Z}^2$,

$$\widetilde{R}(X) = \alpha X + \beta$$

d'où $Q(i) = \underbrace{\widetilde{Q}(i)P(i)}_{=0} + \widetilde{R}(i) = \alpha i + \beta$

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

I.3 (0,5)

Pour $z \in \mathbb{Z}[i]$, $N(z) = z\overline{z} = |z|^2 \in \mathbb{N}$.

I.4.a (1,5)

- Soit $z \in \mathbb{Z}[i]^*$. Alors $zz^{-1} = 1$ donc $N(zz^{-1}) = 1$

  soit $\underbrace{N(z)}_{\in \mathbb{N}} \underbrace{N(z^{-1})}_{\in \mathbb{N}} = 1$. Ainsi $\boxed{N(z) = |z|^2 = 1}$

- Réciproquement, si $N(z) = 1$, $z\overline{z} = 1$ et $\boxed{\overline{z} = z^{-1}}$

I.4.b (1,5)

Soit $z \in \mathbb{Z}[i]^*$. Alors $N(z) = 1$. Notons $z = a+ib$ avec $(a,b) \in \mathbb{Z}^2$. Ainsi $\underbrace{a^2}_{\text{entiers} \geq 0} + \underbrace{b^2}_{\text{entiers} \geq 0} = 1$ donc $\begin{cases} a^2 = 0 \text{ et } b^2 = 1 \\ \text{ou} \\ a^2 = 1 \text{ et } b^2 = 0 \end{cases}$

c'est-à-dire $\begin{cases} a = 0 \text{ et } b = \pm 1 \\ \text{ou} \\ a = \pm 1 \text{ et } b = 0 \end{cases}$ d'où $z \in \{\pm 1, \pm i\}$

Réciproquement, $N(\pm 1) = 1$ et $N(\pm i) = 1$ donc

$$\boxed{\mathbb{Z}[i]^* = \{\pm 1, \pm i\}}$$

I.5.a (3)

Si $z, t \in \mathbb{Z}[i] \setminus \{0\}$, on écrit dans $\mathbb{C}$:

$$\frac{z}{t} = x+iy \in \mathbb{C} \text{ et } q = a+ib \in \mathbb{Z}[i] \text{ avec}$$
$$|x-a| \leq \tfrac{1}{2} \text{ et } |y-b| \leq \tfrac{1}{2}$$

Par construction, $\left|\frac{z}{t} - q\right| = |(x-a) + i(y-b)|$

$$= \sqrt{|x-a|^2 + |y-b|^2}$$

$$\left|\frac{z}{t} - q\right| \leq \sqrt{\tfrac{1}{4} + \tfrac{1}{4}} = \frac{\sqrt{2}}{2}$$

Posons $r = z - qt \in \mathbb{Z}[i]$. Alors $|r| = |t| \left| \frac{z}{t} - q \right|$

$$|r| \leq \frac{\sqrt{2}}{2} |t| < |t|$$

Ainsi $z = tq + r$ avec $\begin{cases} N(r) < N(t) \\ (q, r) \in \mathbb{Z}[i]^2 \end{cases}$.

$\mathbb{Z}[i]$ est donc euclidien.

I.5.b ②

▵ Soit I un idéal de $\mathbb{Z}[i]$, $I \neq \{0\}$. Considérons

$$\begin{cases} \mathcal{S} = \{ P \in \mathbb{Z}[X] \mid P(i) \in I \} \\ \mathcal{D} = \{ \deg(P), \ P \in \mathcal{S} \} \end{cases}$$

. $\mathcal{S} \neq \emptyset$ et donc

$\mathcal{D} \neq \emptyset$. De plus $\mathcal{D}$ est une partie de $\mathbb{N}$, elle admet donc un minimum d_0. Soit $A_0 \in \mathcal{S}$, $\deg A_0 = d_0$.

Écrivons la division euclidienne de $P \in I$ par A_0 :

$$P = QA_0 + R, \quad \deg R < d_0$$

Mais $R = P - QA_0 \in I$ et $\deg R < d_0$ donc $R = 0$.

Ainsi $P = QA_0$ et $A_0 \mid P$. Ainsi $I \subseteq (A_0)$.

▵ Réciproquement $(A_0) \subseteq I$ donc I est principal

I.6 (1,5)

▵ π est irréductible donc soit $\pi \mid \alpha_1$, soit $\pi \wedge \alpha_1 = 1$

Si $\pi \mid \alpha_1$, on a terminé.

▵ Sinon, $\pi \wedge \alpha_1 = 1$ et par le lemme de Gauss,

$\pi \mid \alpha_2 \cdots \alpha_n$.

◁ Ainsi de suite, on trouve $\boxed{k \in [\![1,n]\!],\ \pi \mid \alpha_k}$.

II.1 (1,5)

On écrit, comme $\varphi|^{\mathrm{Im}\varphi}$ est surjectif : $G = \bigsqcup_{y \in \mathrm{Im}\varphi} \varphi^{-1}(\{y\})$.

Or soit x_0 tel que $\varphi(x_0) = y$. Alors $\varphi^{-1}\{y\} = x_0 \ker\varphi$.

Ainsi $|G| = \sum_{y \in \mathrm{Im}\varphi} |x_0 \ker\varphi| \boxed{= |\ker\varphi| \cdot |\mathrm{Im}\varphi|.}$

II.2 (2)

On considère le morphisme de groupes $\varphi : \begin{cases} \mathbb{F}_p^{\times} \longrightarrow \mathbb{F}_p^{\times} \\ x \longmapsto x^2 \end{cases}$

On a bien $\forall (x,y) \in (\mathbb{F}_p^{\times})^2$, $\varphi(xy) = (xy)^2 = x^2y^2$ par commutativité et $\varphi(xy) = \varphi(x)\varphi(y)$.

◁ On remarque que $\ker(\varphi) = \{y \in \mathbb{F}_p^{\times},\ y^2 = 1\}$

$= \{y \in \mathbb{F}_p^{\times},\ (y+1)(y-1) = 0\}$

$\ker(\varphi) = \{-1 ; 1\}$ par intégrité

◁ Ainsi $|\mathrm{Im}\varphi| = \dfrac{|\mathbb{F}_p^{\times}|}{|\ker\varphi|} = \dfrac{p-1}{2}$.

◁ Donc $|\{x \in \mathbb{F}_p,\ \exists y \in \mathbb{F}_p,\ x = y^2\}| = |\{x \in \mathbb{F}_p^{\times},\ \exists y \in \mathbb{F}_p^{\times},\ x = y^2\}| + 1$

$\boxed{= \dfrac{p+1}{2}.}$

II.3.a ②

Supposons qu'il existe $x \in \mathbb{F}_p$, $x^2 = -1$ dans $\mathbb{F}_p$, avec $p \neq 2$.

Donc $(-1)^{\frac{p-1}{2}} = (x^2)^{\frac{p-1}{2}} = x^{p-1} = 1$ par le petit théorème de Fermat. Ainsi $\frac{p-1}{2} \equiv 0\ [2]$ et $p \equiv 1\ [4]$.

II.3.b ②

- Si $p = 2$, $-1 = 1$ dans $\mathbb{F}_2$ donc (-1) est un carré
- Si $p \equiv 1\ [4]$, $(-1)^{\frac{p-1}{2}} = 1$ donc (-1) est racine du polynôme $X^{\frac{p-1}{2}} - 1$.

Or $\underbrace{\mathrm{Im}\,\varphi}_{\text{cardinal } \frac{p-1}{2}} \subseteq \underbrace{\mathrm{Rac}\,(X^{\frac{p-1}{2}} - 1)}_{\text{cardinal } \leq \frac{p-1}{2}}$ donc il y a égalité.

Ainsi $(-1) \in \mathrm{Rac}\,(X^{\frac{p-1}{2}} - 1) \subseteq \mathrm{Im}\,\varphi$ et $\underline{(-1) \text{ est un carré dans } \mathbb{F}_p}$:

III.A.1 ②

Supposons $p \in \Sigma_2$. Alors $p = a^2 + b^2$, $(a,b) \in \mathbb{N}^2$.

$$p = \underbrace{(a-ib)}_{\in \mathbb{Z}[i]} \underbrace{(a+ib)}_{\in \mathbb{Z}[i]}$$

avec $a \pm ib$ qui ne sont pas inversibles (sinon p serait inversible dans $\mathbb{Z}[i]$, donc dans $\mathbb{Z}$, donc $p = \pm 1$ ce qui est exclu)

III.A.2a (0,5)

p est réductible dans $\mathbb{Z}[i]$. Alors il existe $(a,b) \in \mathbb{Z}[i]^2$ non-inversibles, $p = ab$.

Alors $\boxed{N(p) = N(ab) = N(a)N(b)}$

III.A.2b (1,5)

On a $N(p) = p^2$ donc $\underbrace{N(a)}_{\in \mathbb{N}} \underbrace{N(b)}_{\in \mathbb{N}} = p^2$.

On ne peut avoir $N(a) = 1$ ou $N(b) = 1$ car a et b ne sont pas inversibles (voir I.4a). Ainsi comme

$\begin{cases} N(a) \mid p^2 \\ N(b) \mid p^2 \end{cases}$, on a $\boxed{N(a) = N(b) = p}$.

III.A.2c (1)

En écrivant $a = x + iy$ avec $(x,y) \in \mathbb{Z}^2$,

$p = N(a) = x^2 + y^2$ donc $\boxed{p \in \Sigma_2}$.

III.A.3a (1)

$x \equiv \ldots [4]$	0	1	2	3
$x^2 \equiv \ldots [4]$	0	1	1	1

donc si $(a,b) \in \mathbb{Z}^2$,

- Soit $a \equiv 0\,[4]$ et $b \equiv 0\,[4]$, $a^2 + b^2 \equiv 0\,[4]$
- Si $a \equiv 1\,[4]$, $a^2 + b^2 \equiv 1\,[4]$ ou $\equiv 2\,[4]$
- De même si $b \equiv 1\,[4]$

Donc : $\forall (a,b) \in \mathbb{Z}^2$, $\boxed{a^2 + b^2 \not\equiv 3\,[4]}$

III.A.3b ①

Supposons $p = a^2+b^2$, $(a,b) \in \mathbb{Z}^2$, $p \neq 2$.

Alors $p \not\equiv 3 \ [4]$. Mais $p \in \mathbb{P} \setminus \{2\}$ donc p est impair.

Ainsi $p \equiv 1 \ [4]$.

III.A.4a ②

On a $p \equiv 1 \ [4]$. Alors (-1) est un carré modulo p par la partie II.

Ainsi $\exists x \in \mathbb{Z}, \ x^2 \equiv -1 \ [p]$

$\Leftrightarrow$ $\boxed{\exists x \in \mathbb{Z}, \ p \mid x^2+1}$.

III.A.4b ①

Par la question précédente, $p \mid x^2+1 = (x-i)(x+i)$ dans $\mathbb{Z}[i]$.

Or p est irréductible dans $\mathbb{Z}[i]$ par hypothèse.

Comme $(x-i)$ et $(x+i)$ sont premiers entre eux, par I.6, $\boxed{p \mid x+i \text{ ou } p \mid x-i}$

III.A.4c (2,5)

Sans perte de généralité, $p \mid x+i$. Alors il existe $(m,n) \in \mathbb{Z}^2$, $p(m+in) = x+i$ donc $\begin{cases} pm = x \\ pn = 1 \end{cases}$

Si $p \mid x-i$, on obtient $pn = -1$. Dans tous les cas, $pn = \pm 1$ ce qui est impossible.

Ainsi, p est réductible dans $\mathbb{Z}[i]$. On a bien démontré le **lemme III.A.1**.

III.B.1 ③

- Soient $(x, y) \in \Sigma_2^2$. $\begin{cases} x = a^2+b^2 \\ y = c^2+d^2 \end{cases}$, $(a,b,c,d) \in \mathbb{Z}^4$.

$$\begin{aligned} xy &= (a^2+b^2)(c^2+d^2) \\ &= (a+ib)(c-id)(a-ib)(c+id) \\ &= (ac+i(b-d)+bd)(ac+i(-b+d)+bd) \\ &= (ac+bd+i(b-d))(ac+bd-i(b-d)) \end{aligned}$$

$$xy = \underbrace{(ac+bd)}_{\in\mathbb{Z}}{}^2 + \underbrace{(b-d)}_{\in\mathbb{Z}}{}^2 \in \Sigma_2$$

donc **Σ_2 est stable par multiplication**.

- Soit $n \in \mathbb{N}^*$, tel que pour tout premier $p \equiv 3\,[4]$, $v_p(n)$ est paire. Alors :

$$n = 2^{v_2(n)} \prod_{\substack{p\in\mathbb{P} \\ p\equiv 1\,[4]}} p^{v_p(n)} \prod_{\substack{p\in\mathbb{P} \\ p\equiv 3\,[4]}} p^{v_p(n)}$$

- $2 \in \Sigma_2$ donc $2^{v_2(n)} \in \Sigma_2$
- si $p \in \mathbb{P}$, $p \equiv 1\,[4]$, par le lemme III.A.1, $p \in \Sigma_2$ donc $p^{v_p(n)} \in \Sigma_2$ puis $\prod_{p\equiv 1\,[4]} p^{v_p(n)} \in \Sigma_2$.
- pour $p \in \mathbb{P}$, $p \equiv 3\,[4]$, $\prod_{\substack{p\in\mathbb{P} \\ p\equiv 3\,[4]}} p^{v_p(n)} = m^2$, $m \in \mathbb{Z}$

Ainsi $n = m^2(\underbrace{a^2+b^2}) \text{ avec } (m,a,b) \in \mathbb{Z}^2$

$$= 2^{v_2(n)} \prod_{p \equiv [4]} p^{v_p(n)} \in \Sigma_2$$

donc $n = (ma)^2 + (mb)^2 \in \Sigma_2$. D'où la réciproque souhaitée.

III.B.2 ②

On peut supposer $v_p(n) \geq 1$, ie $p|n$, le cas échéant le résultat est évident.

On a $n = a^2+b^2 = (a+ib)(a-ib)$. Ainsi $p \mid (a+ib)(a-ib)$ et donc comme $(a+ib) \wedge (a-ib) = 1$, $p \mid a+ib$ ou $p \mid a-ib$

Mais $p \in \mathbb{Z}$ donc $\underline{p|a \text{ et } p|b}$.

III.B.3 ①

Comme $p|a$ et $p|b$, $\underline{p^2 | a^2+b^2 = n}$.

III.B.4 (2,5)

$p^2|n$ donc $\frac{n}{p^2} \in \mathbb{N}$. On va appliquer l'hypothèse de récurrence à n/p^2. En effet $\frac{n}{p^2} = \underbrace{\left(\frac{a}{p}\right)^2}_{\in \mathbb{N}} + \underbrace{\left(\frac{b}{p}\right)^2}_{\in \mathbb{N}} \in \Sigma_2$

et $v_p\left(\frac{n}{p^2}\right) = v_p(n) - 2 \leq k$. Donc $v_p\left(\frac{n}{p^2}\right)$ est pair et ainsi $v_p(n) = v_p\left(\frac{n}{p^2}\right) + 2$ est pair.

Donc $\underline{\mathcal{P}_{k+1} \text{ est vraie}}$ On conclut par récurrence

III.C.1 ②

avec $a_1 \not\equiv a_2 \ [p]$

◁ Soit $a_1 \in [\![0, \frac{p-1}{2}]\!]$, $a_2 \in [\![0, \frac{p-1}{2}]\!]$. Si par l'absurde $a_1^2 \equiv a_2^2 \ [p]$, $(a_1+a_2)(a_1-a_2) \equiv 0 \ [p]$. Par intégrité dans $\mathbb{F}_p$, comme $a_1 \not\equiv a_2 \ [p]$, $a_1+a_2 \equiv 0 \ [p]$ soit $\underbrace{a_1}_{\in [\![0, \frac{p-1}{2}]\!]} \equiv -a_2 \equiv \underbrace{p-a_2}_{\in [\![\frac{p+1}{2}; p]\!]} \ [p]$ ce qui est impossible

donc : $\forall (a_1, a_2) \in [\![0, \frac{p-1}{2}]\!]^2$, $a_1^2 \not\equiv a_2^2 \ [p]$

◁ De même pour les $(-b^2-1)_{b \in [\![0, \frac{p-1}{2}]\!]}$.

III.C.2 ②

Par principe des tiroirs, par III.C.1, on dispose de $(a,b) \in [\![0, \frac{p-1}{2}]\!]^2$, $a^2 \equiv -b^2-1 \ [p]$. Ainsi

$$\boxed{p \mid 1+a^2+b^2}$$

III.C.3 ②

Remarquons tout d'abord que $\mathcal{M} = \{n \in \mathbb{N}^* \mid np \in \Sigma_4\}$ est non-vide. D'après la question précédente, $p \mid 1+a^2+b^2$ donc il existe $n \in [\![1, p-1]\!]$,

$$np = a^2+b^2+1^2+0^2$$

donc $n \in \mathcal{M}$. D'où l'existence de m. De plus $n < p$ et $m \leq n$ donc $\boxed{m < p}$

III.C.4 ②

On considère pour chaque x_i, $i \in [\![1,4]\!]$ l'entier $y_i \in [\![\frac{-m+1}{2}; \frac{m}{2}]\!]$ qui lui est congru modulo m.

Alors pour un entier $r \in [\![0, m]\!]$, $\boxed{mr = y_1^2 + y_2^2 + y_3^2 + y_4^2}$.

De plus $r < m$ car sinon $m^2 \mid mp = \sum_{i=1}^{4} x_i^2$ donc $m \mid p$ avec $1 < m < p$ et $p \in \mathbb{P}$: impossible.

Donc $\boxed{r \in [\![0, m-1]\!]}$.

III.C.5 ②

C'est un calcul (plus ou moins laborieux) qu'il faut poser.

◁ Soit $\varepsilon \in \{-1, 1\}$,

$$(ap+bq+cr+ds)^2 + (aq-bp-\varepsilon cs+\varepsilon dr)^2 + (ar+\varepsilon bs-cp-\varepsilon dq)^2 + (as-\varepsilon br+\varepsilon cq-dp)^2$$

$$= a^2p^2 + \cancel{2abpq} + \cancel{2acpr} + \cancel{2adps} + b^2q^2 + \cancel{2bcqr} + \cancel{2bdqs} + c^2r^2 + \cancel{2cdrs} + d^2s^2$$
$$+ c^2s^2 - \cancel{2cdrs} + d^2r^2 - \cancel{2acqs\varepsilon} + \cancel{2adqr\varepsilon} + \cancel{2bcps\varepsilon} - \cancel{2bdpr\varepsilon} + a^2q^2 - \cancel{2abpq} + b^2p^2$$
$$+ b^2s^2 - \cancel{2bdqs} + d^2q^2 - \cancel{2adqr\varepsilon} - \cancel{2bcps\varepsilon} + \cancel{2cdpq\varepsilon} + a^2r^2 - \cancel{2acpr} + c^2p^2$$
$$+ b^2r^2 - \cancel{2bcqr} + c^2q^2 + \cancel{2acqs\varepsilon} + \cancel{2bdpr\varepsilon} - \cancel{2cdpq\varepsilon} + a^2s^2 - \cancel{2adps} + d^2p^2$$

$$= a^2p^2 + a^2q^2 + a^2r^2 + a^2s^2$$
$$+ b^2p^2 + b^2q^2 + b^2r^2 + b^2s^2$$
$$+ c^2p^2 + c^2q^2 + c^2r^2 + c^2s^2$$
$$+ d^2p^2 + d^2q^2 + d^2r^2 + d^2s^2$$

$= (a^2+b^2+c^2+d^2)(p^2+q^2+r^2+s^2)$.

Voilà les identités.

◁ Il existe évidemment une astuce avec les quaternions.

III.C.6 (3)

◁ L'identité des quatre carrés d'Euler montre en fait que Σ_4 est stable par multiplication.

Ainsi on dispose de $(z_1,\dots,z_4)\in\mathbb{Z}^4$, $\underbrace{(mp)}_{\in\Sigma_4}\underbrace{(mr)}_{\in\Sigma_4} = \sum_{i=1}^{4} z_i^2$

◁ Plus précisément,

$$\begin{cases} z_1 = x_1y_1+x_2y_2+x_3y_3+x_4y_4 \equiv x_1^2+x_2^2+x_3^2+x_4^2 \equiv mp \equiv 0 \ [m] \\ z_2 = x_1y_2-x_2y_1+x_3y_4-x_4y_3 \equiv x_1x_2-x_2x_1+x_3x_4-x_4x_3 \equiv 0 \\ z_3 = x_1y_3-x_2y_4-x_3y_1+x_4y_2 \equiv x_1x_3-x_2x_4-x_3x_1+x_4x_2 \equiv 0 \ [m] \\ z_4 = x_1y_4+x_2y_3-x_3y_2-x_4y_1 \equiv x_1x_4+x_2x_3-x_3x_2-x_4x_1 \equiv 0 \ [m] \end{cases}$$

Donc pour $k\in[\![1,4]\!]$, $m \mid z_k$.

III.C.7 (1,5)

Par $\omega_i = \frac{z_i}{m} \in \mathbb{Z}$ $(i\in[\![1,4]\!])$, $rp = \omega_1^2+\omega_2^2+\omega_3^2+\omega_4^2$ avec $r<m$: cela contredit la minimalité de m. Donc $m=1$, c'est-à-dire que $\boxed{p\in\Sigma_4}$. C'est le Lemme III.C2.

III.C.8 (1,5)

On écrit $n = 2^{v_2(n)} \prod_{\substack{p\in\mathbb{P}\\ \text{impair}}} p^{v_p(n)}$. $2\in\Sigma_4$ car $2=1^2+1^2+0^2+0^2$ et pour $p\in\mathbb{P}$ impair, $p\in\Sigma_4$. Par stabilité par multiplication, $n\in\Sigma_4$. Donc $\boxed{\Sigma_4=\mathbb{N}}$. C'est le théorème des 4 carrés.

HORS-BARÈME : http://vonbuhren.free.fr/Agregation/Developpements/deux.htm deux carrés.pdf