Chapitre 12

TD

Hugo Salou MP2I

Dernière mise à jour le 1er février 2022

Table des matières

I Exercice 3 1

II Exercice 2 1

III Exercice 6 2

IV Exercice 7 2

V Exercice 12 3

VI Exercice 19 3

VII Exercice 20 4

VIII Exercice 10 5

IX Exercice 15 6

Première partie

Exercice 3

Soit $f : \mathbb{C}_* \to \mathbb{R}_*$ un isomorphisme.
$i^2 = -1$ donc $f(i^2) = f(-1)$ donc $f(i)^2 = f(-1)$
$(-1)^2 = 1$ donc $f\left((-1)^2\right) = f(1) = 1$ donc $f(-1)^2 = 1$ donc $f(-1) = \pm 1$
Or, $f(-1) = 1 \iff f(-1) = f(1) \iff -1 = 1$: une contradiction
Donc, $\underbrace{f(i)^2}_{>0} = -1$ une contradiction aussi

Deuxième partie

Exercice 2

1. "$i \implies ii$"

$$\begin{aligned}\forall a, b \in G, (ab)^2 &= abab \\ &= aabb \\ &= a^2b^2\end{aligned}$$

   "$ii \implies i$"

$$\begin{aligned}\forall (a,b) \in G^2, abab &= a^2b^2 \\ &\text{donc } bab = ab^2 \\ &\text{donc } ba = ab\end{aligned}$$

   ' $\implies iii$"

$$\forall a, b \in G, (a,b)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1}$$

   "$iii \implies i$"

$$\forall a, b \in G, ab = \left(b^{-1}a^{-1}\right)^{-1} = \left(b^{-1}\right)^{-1} = ba$$

2. Soit $a, b \in G$

   — $(a,b)^2 = e$
   — $a^2b^2 = e \cdot e = e$
   Donc, $(a,b)^2 = a^2b^2$ donc G est abélien

Troisième partie

Exercice 6

$$\begin{aligned}&\langle 1 \rangle = \mathbb{Z} \text{ à prouver avec } \mathbb{Z} \subset \langle 1 \rangle \subset \mathbb{Z} \\ &\langle 2 \rangle = 2\mathbb{Z}\end{aligned}$$

Quatrième partie

Exercice 7

Soit $f : (\mathbb{Q}, +) \to (\mathbb{Q}_*, \times)$ un isomorphisme.

On pose

$$\begin{cases} a = f^{-1}(2) \in \mathbb{Q} \\ b = \dfrac{a}{2} \in \mathbb{Q} \end{cases}$$

Domme $a = 2b$, on a $2 = f(a) = f(b+b) = f(b) \times f(b) = f(b)^2$
Donc, $f(b) = \pm\sqrt{2}$. Or, $f(b) \in \mathbb{Q}_*$. $\lightning$

Cinquième partie

Exercice 12

$G \cap \mathbb{R}_*^+ \neq \varnothing$ minoré par 0 donc a existe

1. $a = \min(G \cap \mathbb{R}_*^+)$. On adapte l'exercice 5. Soit $g \in G$
   On pose $q = \left\lfloor \dfrac{g}{a} \right\rfloor \in \mathbb{Z}$ et $r = g - qa \in G$
   Or, $q \leqslant \dfrac{g}{a}$ donc $aq \leqslant g$ donc $r \geqslant 0$
   $\dfrac{g}{a} < q + 1$ donc $g < aq + a$ donc $r < a$
   Si $r > 0$, alors $\begin{cases} r \in G \cap \mathbb{R}_*^+ \\ r < a \leqslant r : \text{une contradiction } \lightning \end{cases}$
   Donc $r = 0$ donc $g = aq$ avec $q \in \mathbb{Z}$ donc $g \in a\mathbb{Z}$
   Donc, $G \subset a\mathbb{Z}$
   $a \in G$ donc $a\mathbb{Z} \subset G$
   Donc $G = a\mathbb{Z}$
2. Soit $g \in G \cap \mathbb{R}_*^+$. Comme $a \notin \left(G \cap \mathbb{R}_*^+\right)$, $g \neq a$
   Or, $g \geqslant a$ donc $g > a$ donc g ne minore pas $G \cap \mathbb{R}_*^+$ donc il existe $g_1 \in G \cap \mathbb{R}_*^+$ tel que $g_1 < g$
   De cette façon, on fabrique une suite (g_n) strictement décroissante minorée par a. Donc (g_n) converge. On pose $\ell = \lim\limits_{n\to+\infty} g_n$
   Donc $\underbrace{g_{n+1} - g_n}_{\in G} \xrightarrow[n\to+\infty]{} \ell - \ell = 0$
   On vient de trouver une suite $(g_{n+1} - g_n)_{n\in\mathbb{N}_*}$ de G qui converge vers 0.
   Donc $a = 0$
   Soit $I =]a, b[$ et $g \in G$ tel que $0 < g < b - a$
   On pose $n = \left\lfloor \dfrac{a}{g} \right\rfloor$. On a donc

   $$n \leqslant \frac{a}{g} < n + 1$$

   donc $ng \leqslant a < g(n+1)$.
   Or,

   $$g(n+1) = ng + g \leqslant a + g < a + b - a < b$$

   donc $(n+1) \in]a, b[\cap G$

Sixième partie

Exercice 19

Soit $a \in A \setminus \{0\}$

$$\begin{aligned} f : A &\longrightarrow A \\ x &\longmapsto ax \end{aligned}$$

$1 \in \mathrm{Im}(f)$?

— Soient $x, y \in A$

$$f(x+y) = a(x+y)ax + ay = f(x) + f(y)$$

donc f est un endomorphisme de $(A, +)$

— Soit $x \in A$

$$\begin{aligned} x \in \mathrm{Ker}(f) &\iff f(x) = 0 \\ &\iff ax = 0 \\ &\iff a = 0 \text{ ou } x = 0 \\ &\iff x = 0 \end{aligned}$$

$\mathrm{Ker}(f) = \{0\}$ donc f est injective.
Comme A est <u>fini</u>, f est bijective donc $\mathrm{Im} = A \ni 1$

Septième partie

Exercice 20

<u>Analyse :</u> Soit $\mathbb{K} = (\{0, 1, a, b\}, +, \times)$ un corps à 4 éléments.

$+$	0	1	a	b
0	0	1	a	b
1	1	$b \backslash 0$	$0 \backslash b$	$a \backslash a$
a	a	$0 \backslash b$	$b \backslash 1$	$1 \backslash$
b	b	$a \backslash a$	$1 \backslash$	$0 \backslash$

$\times$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

$$\begin{aligned} a^2 &= b \neq 1 \\ b^2 &= a \neq 1 \\ \implies & -1 \notin \{0, a, b\} \\ \implies & -1 = 1 \\ \implies & 1 + 1 = 0 \end{aligned}$$

$$\begin{aligned} a + a &= a(1+1) \\ &= a \times 0 \\ &= 0 \end{aligned}$$

Donc, $\mathbb{K} = \left\{0, 1, a, a^{-1}\right\}$: le sous-corps engendré par a

$+$	0	1	a	a^{-1}
0	0	1	a	a^{-1}
1	1	0	a^{-1}	a
a	a	a^{-1}	0	1
a^{-1}	a^{-1}	a	1	0

$\times$	0	1	a	a^{-1}
0	0	0	0	0
1	0	1	a	a^{-1}
a	0	a	a^{-1}	1
a^{-1}	0	a^{-1}	1	a

Synthèse : Il faut vérifier que

— $+$ est associative

— $\times$ est associative

— la distributivité

Huitième partie

Exercice 10

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

— $\mathbb{Z}[i] \subset \mathbb{C}$

— Soient $u, v \in \mathbb{Z}[i]$. On pose $u = a + ib$ et $v = c + id$ avec $(a,b,c,d) \in \mathbb{Z}^4$.

$$\begin{aligned} u + v &= \underbrace{(a+c)}_{\in\mathbb{Z}} + i\underbrace{(b+d)}_{\in\mathbb{Z}} \in \mathbb{Z}[i] \\ uv &= \underbrace{(ac - bd)}_{\in\mathbb{Z}} + i\underbrace{(ad + bc)}_{\in\mathbb{Z}} \in \mathbb{Z}[i] \end{aligned}$$

$$-u = -a - ib \in \mathbb{Z}[i]$$
$$0 = 0 + i \times 0 \in \mathbb{Z}[i]1 \qquad = 1 + i \times 0 \in \mathbb{Z}[i]$$

— Soit $u \in \mathbb{Z}[i]^\times$. On sait qu'il existe $v \in \mathbb{Z}[i]$ tel que $uv = 1$.
Donc, $|u|^2 |v|^2 = |uv|^2 = 1^2 = 1$
Comme $u \in \mathbb{Z}[i]$, $|u|^2 = \mathfrak{Re}(u)^2 + \mathfrak{Im}(u)^2 \in \mathbb{N}$
De même, $|v|^2 \in \mathbb{N}$
Donc, $|u|^2 = 1$.
On pose $u = a + ib, (a, b) \in \mathbb{Z}^2$. On a $a^2 + b^2 = 1$
donc $\begin{cases} 0 \leqslant a^2 \leqslant 1 \\ 0 \leqslant b^2 \leqslant 1 \end{cases}$
Donc, $\begin{cases} a^2 \in \{0, 1\} \\ b^2 \in \{0, 1\} \\ a^2 + b^2 = 1 \end{cases}$
Donc, $u \in \{\pm i, \pm 1\}$

—

$$\begin{aligned} 1^{-1} &= 1 \in \mathbb{Z}[i] \\ (-1)^{-1} &= -1 \in \mathbb{Z}[i] \\ i^{-1} &= -i \in \mathbb{Z}[i] \\ (-i)^{-1} &= i \in \mathbb{Z}[i] \end{aligned}$$

Autre méthode $u \in \mathbb{Z}[i] \setminus \{0\}$. $u = a + ib$ avec $a, b \in \mathbb{Z}$.

$$\begin{aligned} \frac{1}{u} \in \mathbb{Z}[i] &\iff \frac{1}{a+ib} \in \mathbb{Z}[i] \\ &\iff \frac{a-ib}{a^2-b^2} \in \mathbb{Z}[i] \\ &\iff \begin{cases} \dfrac{a}{a^2+b^2} \in \mathbb{Z} \\ \dfrac{-b}{a^2+b^2} \in \mathbb{Z} \end{cases} \qquad \iff \begin{cases} a^2+b^2 \mid a \\ a^2+b^2 \mid b \end{cases} \\ &\implies \begin{cases} a^2+b^2 \leqslant |a| \\ a^2+b^2 \leqslant |b| \end{cases} \qquad \implies \begin{cases} a \in \{0, 1, -1\} \\ b \in \{0, 1, -1\} \\ a^2+b^2 = 1 \end{cases} \end{aligned}$$

Neuvième partie

Exercice 15

$f : \mathbb{C} \longrightarrow \mathbb{C}$ morphisme d'anneaux
$f_{\mathbb{R}} = \mathrm{id}_{\mathbb{R}}$

Soit $z \in \mathbb{C}$. On pose $z = a + ib$, $(a, b) \in \mathbb{R}^2$

$$\begin{aligned} f(z) &= f(a+ib) \\ &= f(a) + f(ib) \\ &= a + f(i)f(b) \\ &= a + bf(i) \end{aligned}$$

$i^2 = -1$ donc $f\left(i^2\right) = f(-1) = -1$ donc $f(i)^2 = -1$ donc $f(i) \in \{i, -i\}$
Donc $f \in \{\mathrm{id}_{\mathbb{C}}, z \mapsto \overline{z}\}$