TD 12 cor

ex 1 : Rq : $\forall a \in G,\ a^2 = 1 \iff a \cdot a = 1 \iff a$ est inversible d'inverse a^{-1}

Mq . est commutative . On sait que $(G, \cdot)$ est un groupe
Soient x et y 2 éléments de G. $x \cdot y$ est un élément de G car . est une LCI et :

$$x \cdot y = (x \cdot y)^{-1} = y^{-1} \cdot x^{-1} = y \cdot x$$

(d'après Rq)

Donc . commutative dans G

ex 2 : Soient a et b 2 éléments de G. On sait que $(G, \cdot)$ est un groupe

$(ab)^2 = a^2 \cdot b^2$ donc $(ab)(ab) = a^2 b^2$

donc $a(ba)b = a(ab)b$ ← . assoc car $(G, \cdot)$ groupe

Puisque $(G, \cdot)$ est un groupe, a et b sont inversibles

donc $a^{-1}(a(ba)b) = a^{-1}a(ab)b$

donc $(a^{-1}a).(ba).b = (a^{-1}a).(ab)b$

donc $(ba).b = (ab).b$

donc $(ba)b.b^{-1} = (ab).bb^{-1}$

donc $(ba)(bb^{-1}) = (ab)(bb^{-1})$

donc $ba = ab$.

Donc . est commutative dans G

TD 12 corr ex 6 Soit e l'élément neutre de G

① . $A \cap B \neq \emptyset$ car $e \in A$ et $e \in B$

. $\forall x, x' \in A \cap B$, $x * x'^{-1} \in A$ car $(A, *)$ ss-gpe de $(G, *)$ et $A \cap B \subset A$

$\forall x, x' \in A \cap B$, $x * x'^{-1} \in B$ car $(B, *)$ ss-gpe de $(G, *)$ et $A \cap B \subset B$.

Donc $x * x'^{-1} \in A \cap B$

Concl : $(A \cap B, *)$ est un sous-gpe de $(G, *)$

② $\subseteq$ évident

$\Rightarrow$ par contraposée

Supposons non $(A \subset B$ ou $B \subset A)$ vrai

alors il existe $x \in A \setminus B$ et il existe $x' \in B \setminus A$.

Comme $A \setminus B \subset A \cup B$, $x \in A \cup B$ et comme $B - A \subset A \cup B$, $x' \in A \cup B$

Soit $y = x * x'$

- si $y \in A$ alors $x' = x^{-1} * y \in A$ or $x' \in B - A$ contradiction donc $y \notin A$
- si $y \in B$ alors $x = y * x'^{-1} \in B$ or $x \in A \setminus B$ contradiction donc $y \notin B$

Comme $y \notin A$ et $y \notin B$, $y \notin A \cup B$ - or $x \in A \cup B$ et $x' \in A \cup B$

donc $*$ n'est pas une LCI dans $A \cup B$

donc $A \cup B$ n'est pas un groupe.

Concl : $A \cup B$ est un groupe $\Rightarrow (A \subset B$ ou $B \subset A)$

TD 12 ex 7 : voir ex 13-7 du livre jaune

Ex 8 TD12

① Voir au tableau de papa

② Soit $(z,z') \in \mathbb{Z}[i]^2$

$N(zz') = (zz')(\overline{z}\,\overline{z'}) = zz'\overline{z}\,\overline{z'} = z\overline{z}\,z'\overline{z'} = (z\overline{z})(z'\overline{z'})$

(conjugué d'un produit ; × commutative dans $\mathbb{Z}$; × associative dans $\mathbb{Z}$)

$= N(z) \times N(z')$

③ Soit $z \in \mathbb{Z}[i]$

z est inversible dans $\mathbb{Z}[i]$ ssi $\exists z' \in \mathbb{Z}[i]$ tq $zz' = z'z = 1$ (neutre pour ×)

Supposons que z' est inversible dans $\mathbb{Z}[i]$

alors $\exists z' \in \mathbb{Z}[i]$ tq $zz' = 1$ donc $N(zz') = N(1)$

donc $N(z)N(z') = 1\overline{1} = 1$

donc $N(z)$ est inversible dans $\mathbb{Z}$

donc $N(z) = \pm 1$

or $N(z) \geqslant 0$ donc $N(z) = 1$

or $z = a + ib$ avec $(a,b) \in \mathbb{Z}^2$

donc $N(z) = 1 \Rightarrow a^2 + b^2 = 1$

donc $a^2 = 1$ et $b^2 = 0$ ou $a = 0$ et $b^2 = 1$

donc $(a = \pm 1$ et $b = 0)$ ou $(a = 0$ et $b = \pm 1)$

donc $z = 1$ ou -1 ou i ou $-i$

Réciproquement, si $z = 1$ alors z est inversible dans $\mathbb{Z}[i]$ d'inverse 1

Si $z = -1$ ——— -1

Si $z = i$ ——— $-i$

Si $z = -i$ ——— i

puisque $1 \times 1 = 1$, $-1 \times (-1) = 1$, $i \times (-i) = 1$ et $(-i) \times i = 1$ et × commutative dans $\mathbb{Z}$.

Concl : les éléments inversibles de $\mathbb{Z}[i]$ sont : $1, -1, i$ et $-i$.

④ $(\mathbb{Z}[i], +, \times)$ est un sous-anneau de $(\mathbb{C}, +, \times)$

car $\mathbb{Z}[i] \subset \mathbb{C}$ par définition (car $\mathbb{Z} \subset \mathbb{R}$)

- $1 = 1 + i \times 0$ donc $1 \in \mathbb{Z}[i]$
- $\forall z \in \mathbb{Z}[i]\ \forall z' \in \mathbb{Z}[i]$, $z - z' \in \mathbb{Z}[i]$ et $z \times z' \in \mathbb{Z}[i]$

en effet $\exists (a,b,a',b') \in \mathbb{Z}^4$ tq $z = a + ib$ et $z' = a' + ib'$

et $z - z' = (a - a') + i(b - b') \in \mathbb{Z}[i]$ car $a - a' \in \mathbb{Z}$ et $b - b' \in \mathbb{Z}$

et $z \times z' = (a + ib)(a' + ib') = (aa' - bb') + i(ab' + ba') \in \mathbb{Z}[i]$

car $aa' - bb' \in \mathbb{Z}$ et $ab' + ba' \in \mathbb{Z}$

Et comme $(\mathbb{C}, +, \times)$ est un anneau commutatif, $(\mathbb{Z}[i], +, \times)$ aussi

TD16 cor

ex 9 bis

On sait que ab est inversible donc $\exists c \in A \mid c(ab) = (ab)c = 1_A = 1$

Examinons $ba\,(bca - 1)$

$ba\,(bca-1) = babca - ba = b(abc)a - ba = b.1a - ba = ba - ba = 0_A$

or ba n'est pas un diviseur de 0 donc $bca - 1 = 0$ donc $bca = 1$

D'une part, $b.(ca) = 1$ puisque $bca = 1$ et par ailleurs $(a).b = 1$
puisque $c(ab) = 1$
donc b est inversible d'inverse ca

D'autre part, $(bc).a = 1$ puisque $bca = 1$ et par ailleurs $a(bc) = 1$
puisque $(ab)c = 1$
donc a est inversible d'inverse bc.