GOOD
OOD

Feuille 3

Exercice 1

associativité
neutre
inverse

$(\mathbb{R}, +)$

$\forall a, b, c \in \mathbb{R}, \quad (a+b)+c = a+(b+c)$
$0 \in \mathbb{R}$ est un élément neutre
car $\forall x \in \mathbb{R}, \; x+0 = x = 0+x$

$\forall x \in \mathbb{R} \quad x+(-x) = 0 = (-x)+x \Rightarrow$ toute $x \in \mathbb{R}$
admet l'inverse donc $(\mathbb{R}, +)$ est bien un groupe.

$(\mathbb{R}, \times)$ n'est pas un groupe
car il n'existe pas d'inverse pour le 0

$(\mathbb{C}, +)$
Idem avec $(\mathbb{R}, +)$

$(\mathbb{C}^\times, \times)$
$\forall a, b, c \in \mathbb{C}^\times, \quad (a \cdot b) \cdot c = a(b \cdot c)$
$\forall x \in \mathbb{C}^\times \quad x \cdot 1 = x = 1 \cdot x$
$\forall x \in \mathbb{C}^\times \; \exists x' \in \mathbb{C}^\times$ tq $x \cdot x' = 1 = x' \cdot x$

Donc $(\mathbb{C}^\times, \times)$ est bien un groupe

Exercice 3

Or G est un groupe donc $\exists g^{-1} \in G$ tq $gg^{-1} = e_G = g^{-1}g$

$g^{-1}(gh = e_G) \iff g^{-1}gh = g^{-1}e_G$
$\iff \underline{h = g^{-1}}$

Exercice 4

Soit G un groupe et $\forall g \in G \quad g^2 = e_G$

Commutatif: $\forall a, b \in G \quad a * b = b * a$

Soit $h \in G$

On a $g^2 = e_G$

$(g^2 \cdot h = h)g$

$g^2 hg = hg$

$(gh)(gh) = e_G$

$ggghhh = gh$

$hg = gh$

Donc bien commutatif

Exercice 6

$e^{x+y} = e^x e^y$

$e : (\mathbb{R}, +) \longrightarrow (\mathbb{R}_1^*, \times)$

$\ln : (\mathbb{R}_+^*, \times) \longrightarrow (\mathbb{R}, +)$

$\sqrt{\cdot} : (\mathbb{R}_+^*, \times) \longrightarrow (\mathbb{R}_+^*, \times)$

$\sqrt[3]{\cdot} : (\mathbb{R}^*, \times) \longrightarrow (\mathbb{R}^*, \times)$

$\det : (GL(\mathbb{C}), \times) \longrightarrow (\mathbb{C}^*, \times)$

$x \mapsto x^n : (\mathbb{R}^*, \times) \longrightarrow (\mathbb{R}^*, \times)$ $\quad |zz'| = \sqrt{zz'\overline{zz'}}$

$n \mapsto x^n : (\mathbb{Z}, +) \longrightarrow (\mathbb{Z}^*, \times)$

$z \mapsto |z| :$

$z \mapsto \overline{z} : (\mathbb{C}, +) \longrightarrow (\mathbb{C}, +)$

$\overline{a+bi} + \overline{c+di} = a - bi + c - di = (a+c) + (-b-d)i$

$\overline{a+bi+c+di} = a + c + (-b-d)i$

Exercice 7

$(\mathbb{Q}, +) \longrightarrow (\mathbb{Q}_+^*, \cdot)$

$$f(x+y) = f(x)\, f(y)$$
$$\overset{\shortparallel}{y} = 2 \cdot x$$
$$f(q+h) = f(q)\, f(h)$$

Exercice 8

$(G, \cdot)$ gpe $\quad A, B$ ss-gpes de $(G, \cdot)$

Supposons que A est ss-gpe de $(G, \cdot)$

donc $AB = \{ a \cdot b : a \in A,\ b \in B \}$

$$a \cdot b\, (a' \cdot b')^{-1} \in AB$$
$$= a \cdot b\, \underbrace{(b'^{-1} a'^{-1})}_{\in AB} \in AB$$

mais $\underset{\overset{\shortparallel}{b''}}{b'^{-1}} \in B$ et $\underset{\overset{\shortparallel}{a''}}{a'^{-1}} \in A$

donc $b'' a'' \in AB$

$\forall\, b'' \in B$, $a'' \in A$ $\quad b'' a'' \in AB \quad$ donc $AB = BA$

Supposons que $AB = BA$

Donc $a \cdot b \in AB$

$b' \cdot a' \in BA$

$$(a \cdot b) \cdot (b' \cdot a')^{-1} = (a \cdot b)(\underset{\in A}{a'^{-1}} \cdot \underset{\in B}{b'^{-1}})$$

donc $\underset{\overset{\shortparallel}{a''}}{a'^{-1}} \cdot \underset{\overset{\shortparallel}{b''}}{b'^{-1}} \in AB$

$$= a \cdot \underbrace{b \cdot a''}_{\in BA = AB} \cdot b'' \quad \exists\, a''' \cdot b''' = b \cdot a'' \in AB$$

$$= \underbrace{a \cdot a'''}_{\in A} \cdot \underbrace{b''' \cdot b''}_{\in B} \in AB$$

donc est un ss-gpe

Exercice 10

A ss-gpe de G
B ss-gpe de G

$A \cap B$ ss-gpe de A et de B

par le théorème de Lagrange $|A \cap B| \mid |A|$
et $|A \cap B| \mid |B|$

Comme $|A| \wedge |B| = 1 \Rightarrow |A \cap B| = 1 \Rightarrow A \cap B = \{1_G\}$

Exercice 16

Soit un groupe $\mathbb{Z}/n\mathbb{Z}$ avec $|\mathbb{Z}/n\mathbb{Z}| = n$

Soit $\bar{a}$

On sait que $\bar{1}$ est un générateur de $\mathbb{Z}/n\mathbb{Z}$
donc $o(\bar{1}) = n$

$\bar{a} = a \cdot \bar{1} = \bar{1}^a$

D'après le théorème du cours $o(\bar{1}^a) = \dfrac{o(\bar{1})}{pgcd(a, o(\bar{1}))}$

$= \dfrac{n}{pgcd(a,n)}$

b) Pour que $\bar{a}$ soit un générateur de $\mathbb{Z}/n\mathbb{Z}$
il faut que $o(\bar{a}) = o(\bar{1}^a) = n$

$n = \dfrac{n}{pgcd(a,n)} \Rightarrow pgcd(a,n) = 1$

c) D'après (b) les générateurs de $\mathbb{Z}/12\mathbb{Z}$ sont
tels a tels que $pgcd(a,12) = 1$
$\Rightarrow a = 1,\ a = 5,\ a = 7,\ a = 11$

$\varphi(12) = \varphi(2^2)\varphi(3) = (2^2 - 2)(3 - 1) = 2 \cdot 2 = 4$

$o(\bar{3}) = \dfrac{12}{3 \wedge 12} = \dfrac{12}{3} = 4$

$o(\bar{5}) = 12$

$o(\bar{6}) = \dfrac{12}{6 \wedge 12} = \dfrac{12}{6} = 2$

$o(\bar{9}) = \dfrac{12}{9 \wedge 12} = \dfrac{12}{3} = 4$

d) $\{\bar{0}\}$ $\{\bar{0}, \bar{6}\}$, $\{\bar{0}, \bar{4}, \bar{8}\}$, $\{\bar{0}, \bar{3}, \bar{6}, \bar{9}\}$

$\{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \overline{10}\}$, $\mathbb{Z}/n\mathbb{Z}$

<u>Exercice 9</u>

$(\mathbb{C}^\times, \times)$ $z^4 - 1 = 0$

$\Leftrightarrow (z^2-1)(z^2+1) = 0$

$\Leftrightarrow (z-1)(z+1)(z-i)(z+i) = 0$

$\Leftrightarrow z \in \{-1, 1, -i, i\}$

$(\mathbb{R}^\times, \times)$ $x^4 - 1 = 0$

$(x^2-1)(x^2+1) = 0$

$\Rightarrow (x-1)(x+1) = 0$

$\Rightarrow x \in \{-1, 1\}$

Supposons par l'absurde que $\varphi : \mathbb{C}^\times \longrightarrow \mathbb{R}^\times$ est isomorphe

Alors $\varphi(1) = 1 \Rightarrow \varphi(-1) \neq 1$

$\Rightarrow \varphi(-1) = -1$

Donc $\varphi(i) \neq -1$ et $\varphi(i) \neq 1$

mais $\varphi(i^4) = \varphi(i)^4 = \varphi(1) = 1 \Rightarrow \varphi(i) = 1$ ou $\varphi(i) = -1$

ce qui est absurde

Donc $\mathbb{C}^\times$ et $\mathbb{R}^\times$ ne sont pas isomorphes

Exercice 20

Si le G était de cardinal infini, G aurait le nombre de sous-groupes infini, ce qui n'est pas le cas (il n'y a que 2).

Donc G est finie.

Comme G a seulement 2 sous-groupes alors tout élément sauf l'élément neutre engendre G car sinon : supposons qu'il existe $g \in G \neq 1_G$ qui n'engendre pas G, par contre il engendre un autre groupe car G finie et $\langle g \rangle \subset G$ et $\langle g \rangle \neq \{1_G\}$ car $g \neq 1_G$
Absurde, car G admet seulement 2 sous-groupes.
Donc $\exists g \in G \neq 1_G$ tq $\langle g \rangle = G$ donc G est cyclique.

Soit $n = |G| \geq 2$

Supposons par l'absurde que n n'est pas premier. Alors $\exists d$ tq $d \mid n$ et $d \neq 1, n$

Alors, notons $n' = \frac{n}{d}$

Soit $g \in G$ $\langle g^d \rangle$ groupe cyclique

$|\langle g^d \rangle| = n' = \frac{n}{d} < n$
générateur de G ce qui est impossible car $|G| = n$, d'où n est premier.

Exercice 13

$\mathcal{U}_n = \{z \in \mathbb{C} : z^n = 1\}$

Le polynome $z^n - 1 = 0$ est de degré n
donc a exactement n racines,
d'où $\#\mathcal{U}_n = n$

On note $z_k = e^{\frac{2ik}{n}}$

On veut trouver tous les z_k tq $\langle z_k \rangle = \mathcal{U}_n$
i.e $o(z_k) = n$

$o(z_k) = n$ si $\min\{m \in \mathbb{Z} : z_k^m = 1\} = n$ i.e $m = n$
$\min\{m \in \mathbb{Z} : e^{\frac{2ik}{n} \cdot m} = 1\} = n$

C'est le cas ssi $k \wedge n = 1$

Alors $\langle z_k \rangle = \mathcal{U}_n$ $\forall k \in \mathbb{Z}$ tq $k \wedge n = 1$

Exercice 14

Soient $n, m \in \mathbb{N}^*$ $\mathcal{U}_n = \{z \in \mathbb{C} : z^n = 1\}$

a) $\mathcal{U}_n = \{z \in \mathbb{C} : z^n = 1\} = \{e^{\frac{2ik}{n}} : 1 \leq k \leq n\}$

$\mathcal{U}_m = \{z \in \mathbb{C} : z^m = 1\} = \{e^{\frac{2ik}{m}} : 1 \leq k \leq m\}$

Supposons que $n \leq m$:

Soit $z \in \mathcal{U}_n \cap \mathcal{U}_m$ alors $z^n = z^m = 1$
$\Rightarrow (z^d)^{n'} = (z^d)^{m'} = 1$
$\Rightarrow z^d = 1$

Donc $z \in \mathcal{U}_d$
Donc $\mathcal{U}_d \cap \mathcal{U}_m \subset \mathcal{U}_d$

Soit $z \in \mathcal{U}_d \Rightarrow z^d = 1$ donc $z^n = z^{dn'} = 1$
et $z^m = z^{dm'} = 1$

Donc $z \in \mathcal{U}_n \cap \mathcal{U}_m \Rightarrow \mathcal{U}_d \subset \mathcal{U}_n \cap \mathcal{U}_m$
Donc $\mathcal{U}_d = \mathcal{U}_n \cap \mathcal{U}_m$

b) Soit $f : \mathbb{U}_m \longrightarrow \mathbb{U}_n$

$f(e^{\frac{2\pi i}{m}}) = e^{\frac{2\pi i}{n}}$

$f(e^{\frac{2\pi i}{m}\cdot m}) = f(e^{2\pi i}) = f(1) = 1 = f(e^{\frac{2\pi i}{m}})^m = e^{\frac{2\pi i}{n}\cdot m}$

Soit $f(e^{\frac{2\pi i}{m}}) = e^{\frac{2\pi i k}{n}}$

donc $e^{\frac{2\pi i k}{n} m} = 1$

i.e. $km \equiv 0 \mod n$

Donc $n \mid km \Rightarrow \exists q$ tq $nq = km \Rightarrow k = \frac{n}{m} q$

$\Rightarrow k = \frac{n}{pgcd(n,m)} \cdot q$ avec $0 \leq q \leq n-1$

Donc il y a n tels k possibles.

Donc il y a n morphismes.

c) $\mathbb{U}_m \times \mathbb{U}_n \cong \mathbb{U}_{mn} \iff m \wedge n = 1 = d$

$f((e^{\frac{2\pi i}{m}}, e^{\frac{2\pi i}{n}})) = e^{\frac{2\pi i}{mn}}$

$f((e^{\frac{2\pi i}{m}}, e^{\frac{2\pi i}{n}})^{mn}) = 1 = f((1,1))$ où m

Supposons par l'absurde que $d := m \wedge n \neq 1$

$\begin{cases} n = dn'^3 \\ m = dm'^3 \end{cases}$

$f((e^{\frac{2\pi i}{m}}, e^{\frac{2\pi i}{n}})^{mn}) = 1 = f((1,1))$ où $mn = d^2 n' m'$

$f((e^{\frac{2\pi i}{m}}, e^{\frac{2\pi i}{n}})^{dm'n'}) = 1 = f(1,1)$

$\Rightarrow \overset{=ppcm(m,n)}{|\mathbb{U}_m \times \mathbb{U}_n|} = dm'n' \neq |\mathbb{U}_{mn}| = d^2 m'n'$

L'absurde

donc $\mathbb{U}_n \times \mathbb{U}_m \cong \mathbb{U}_{mn} \Rightarrow m \wedge n = 1$

Supposons que $m \wedge n = 1$

$$f\left(\left(e^{\frac{2\pi i}{m}}, e^{\frac{2\pi i}{n}}\right)^{mn}\right) = 1 = f((1,1))$$

$$f\left(\left(e^{\frac{2\pi i}{m}k}, e^{\frac{2\pi i}{n}k'}\right)\right) = \left(e^{\frac{2\pi i}{mn}}\right)^{z_1} \cdot f\left(\left(e^{\frac{2\pi i}{m}l}, e^{\frac{2\pi i}{n}l_1}\right)\right) = \left(e^{\frac{2\pi i}{mn}}\right)^{z_2}$$

$$f\left(\left(e^{\frac{2\pi i}{m}k}, e^{\frac{2\pi i}{n}k'}\right)\right) \cdot f\left(\left(e^{\frac{2\pi i}{m}l}, e^{\frac{2\pi i}{n}l_1}\right)\right) = \left(e^{\frac{2\pi i}{mn}}\right)^{z_1} \cdot \left(e^{\frac{2\pi i}{mn}}\right)^{z_2}$$

$$= \left(e^{\frac{2\pi i}{mn}}\right)^{z_1+z_2}$$

f un morphisme

$$|U_m \times U_n| = \text{ppcm}(m,n) = mn$$

$$\parallel$$

$$|U_{mn}| = mn$$

Donc f bijective donc $m \wedge n = 1$

$$\Rightarrow U_n \times U_m \cong U_{mn}$$