Exercice 2

① ⓐ Soit $(G,\times)$ un groupe commutatif de cardinal $n$.
Notons $g_1, \dots, g_n$ les $n$ éléments de $G$.
Soit $g \in G$. Alors il existe $i \in [\![1,n]\!]$ tq $g = g_i$.
Il s'agit de montrer que $g \times g \times \dots \times g = g^n = e_G$.
Etudions l'application $\varphi_k : G \to G$ où $k \in [\![1,n]\!]$.
$g \mapsto g_k \times g$

Soit $k \in [\![1,n]\!]$
En particulier, montrons que $\varphi_k$ est une bijection.

- Soit $(g,g') \in G^2$ tels que $\varphi(g) = \varphi(g')$
alors $g_k \times g = g_k \times g'$. or $g_k \in G$ et $(G,\times)$ est un groupe
donc $g_k$ est inversible pour $\times$ dans $G$ donc, si on note $g_k^{-1}$
l'inverse de $g_k$, on a :
$g_k \times g = g_k \times g' \Rightarrow g_k^{-1} \times g_k \times g = g_k^{-1} \times g_k \times g' \Rightarrow g = g'$
car $g_k^{-1} \times g_k = e_G$ et $e_G \times g = g$ et $e_G \times g' = g'$
donc $\varphi_k$ est injective

- Montrons que $\varphi_k$ est surjective
Soit $g \in G$. Montrons qu'il existe $g' \in G$ tq $g = \varphi_k(g')$
$g = g_k \times g_k^{-1} \times g = g_k \times (g_k^{-1} \times g)$ par associativité de $\times$
donc $g = \varphi_k(g_k^{-1} \times g)$. On a trouvé $g' = g_k^{-1} \times g \in G$
tel que $g = \varphi_k(g')$ car $(G,\times)$ est un groupe.

- Conclusion : $\varphi_k$ est bijective.

En particulier,
$\varphi_i$ est donc une permutation de $G = \{g_1, \dots, g_n\}$
On a donc $\prod_{j=1}^{n} g_j = \prod_{j=1}^{n} \varphi_i(g_j) = \prod_{j=1}^{n} g_i g_j = g_i^n \prod_{j=1}^{n} g_j$

or $\prod_{j=1}^{n} g_j = g_1 \times \dots \times g_n \in G$ et $(G,\times)$ est un groupe donc
$\prod_{j=1}^{n} g_j$ est inversible. On note $\left(\prod_{j=1}^{n} g_j\right)^{-1}$ son inverse.
On a donc $\left(\prod_{j=1}^{n} g_j\right)^{-1} \left(\prod_{j=1}^{n} g_j\right) = g_i^n \left(\prod_{j=1}^{n} g_j\right)^{-1} \left(\prod_{j=1}^{n} g_j\right)$ car $\times$ commutative dans $G$
Soit $e_G = g_i^n \times e_G$ c'àd $e_G = g_i^n$ c'àd $\boxed{e_G = g^n}$

1 b Soit $(G, \times)$ un sous-groupe de $(\mathbb{U}, \times)$.
On va montrer qu'il existe $n \in \mathbb{N}^*$ tq $G \subset \mathbb{U}_n$.
En tant que sous-groupe de $(\mathbb{U}, \times)$, $(G, \times)$ est un groupe commutatif car $(\mathbb{U}, \times)$ est un groupe commutatif.
On décide de plus de noter $m = \text{Card}(G)$ càd $m$ le nombre d'éléments de $G$.
Soit $g \in G$. D'après q1, $g^m = 1$
où 1 est le neutre pour $\times$ dans $\mathbb{U}$ donc dans $G$.
Donc $g$ est une racine mième de 1 donc $g \in \mathbb{U}_m$
On a mq $G \subset \mathbb{U}_m$
De plus $\text{Card}(G) = \text{Card}(\mathbb{U}_m)$ puisqu'il y a exactement $m$ racines mièmes de 1
Donc $G = \mathbb{U}_m$.

2 Soit $(m, n) \in \mathbb{N}^{*2}$. Raisonnons par double inclusion

a $\Rightarrow$ Supposons que $\mathbb{U}_m \subset \mathbb{U}_n$ et mq $m \mid n$.
Comme $\mathbb{U}_m \subset \mathbb{U}_n$, tous les éléments de $\mathbb{U}_m$ appartiennent à $\mathbb{U}_n$, en particulier par exemple $e^{\frac{2i\pi}{m}}$.
Ainsi comme $e^{\frac{2i\pi}{m}} \in \mathbb{U}_m$, $e^{\frac{2i\pi}{m}} \in \mathbb{U}_n$ et donc $\left(e^{\frac{2i\pi}{m}}\right)^n = 1$
Donc $e^{\frac{2i\pi n}{m}} = 1$ par la formule de Moivre donc $\frac{2\pi n}{m} = 0 [2\pi]$
Donc il existe $k \in \mathbb{Z}$ tq $\frac{2\pi n}{m} = 2k\pi$ càd $\frac{n}{m} = k$ ou encore $n = km$.
Ainsi $\underline{m \mid n}$

$\Leftarrow$ Supposons que $m \mid n$. Il existe donc $q \in \mathbb{N}$ tq $n = mq$
Soit $z \in \mathbb{U}_m$ alors $z^m = 1$.
$z^n = z^{mq} = (z^m)^q = 1^q = 1$ donc $z \in \mathbb{U}_n$. Donc $\underline{\mathbb{U}_m \subset \mathbb{U}_n}$

b On raisonne par double inclusion

- Soit $d = m \wedge n$.
$d \mid m$ donc $\mathbb{U}_d \subset \mathbb{U}_m$ d'après 2 a
$d \mid n$ donc $\mathbb{U}_d \subset \mathbb{U}_n$ d'après 2 a
$\Big\}$ donc $\underline{\mathbb{U}_d \subset \mathbb{U}_m \cap \mathbb{U}_n}$
- Soit $z \in \mathbb{U}_m \cap \mathbb{U}_n$ alors $z \in \mathbb{U}_m$ et $z \in \mathbb{U}_n$, càd $z^m = 1$ et $z^n = 1$.

Par la relation de Bézout on a :
il existe $(u,v)\in\mathbb{Z}^2$ tq $mu+nv=d$

Donc $z^d = z^{mu+nv} = (z^m)^u \times (z^n)^v = 1^u \times 1^v = 1\times 1 = 1$

donc $z\in\mathbb{U}_d$ donc $\underline{\mathbb{U}_m\cap\mathbb{U}_n\subset\mathbb{U}_d}$.

(c) Mq le sous-groupe engendré par $\mathbb{U}_m\cup\mathbb{U}_n$ est $\mathbb{U}_{m\vee n}$, c'est-à-dire que c'est le plus petit sous groupe de $\mathbb{U}$ contenant $\mathbb{U}_m\cup\mathbb{U}_n$. On doit montrer 3 points:

(i) - mq $\mathbb{U}_{m\vee n}$ est un sous-groupe de $\mathbb{U}$
(ii) - mq $\mathbb{U}_{m\vee n}$ contient $\mathbb{U}_m\cup\mathbb{U}_n$
(iii) - mq si $H$ est un sous-groupe de $\mathbb{U}$ qui contient $\mathbb{U}_m\cup\mathbb{U}_n$ alors $H$ contient $\mathbb{U}_{m\vee n}$

(i) - $\underline{\text{Soit } M = m\vee n}$

- $1\in\mathbb{U}_M$ car $1^M=1$
- $\mathbb{U}_M\subset\mathbb{U}$ car si $z\in\mathbb{U}_M$ alors $z^M=1$ donc $|z^M|=1$ donc $|z|^M=1$ donc $|z|=1$ et $z\in\mathbb{U}$
- Soit $(z,z')\in\mathbb{U}_M^2$ alors $z^M=1$, $z'^M=1$

$z\times z'^{-1} = \dfrac{z}{z'}$ et $(zz'^{-1})^M = \left(\dfrac{z}{z'}\right)^M = \dfrac{z^M}{z'^M} = \dfrac{1}{1} = 1$

donc $zz'^{-1}\in\mathbb{U}_M$

Concl: $(\mathbb{U}_M,\times)$ est un sous-groupe de $(\mathbb{U},\times)$

(ii) - $m\mid M$ et $n\mid M$ donc par q(2)(a) $\mathbb{U}_m\subset\mathbb{U}_M$ et $\mathbb{U}_n\subset\mathbb{U}_M$
donc $\mathbb{U}_m\cup\mathbb{U}_n\subset\mathbb{U}_M$.

(iii) - Soit $H$ un sous-groupe de $\mathbb{U}$ qui contient $\mathbb{U}_m\cup\mathbb{U}_n$
Mq $\mathbb{U}_M\subset H$.

Soit $z\in\mathbb{U}_M$ - Mq $z\in H$

Introduisons $\underline{d=m\wedge n}$

Il existe $m'\in\mathbb{N}$ et $n'\in\mathbb{N}$ tq $m=dm'$ et $n=dn'$ et $m'\wedge n'=1$

Comme $m'\wedge n'=1$, par le théorème de Bézout, $\underline{\text{il existe}}$
$\underline{(u,v)\in\mathbb{Z}^2 \text{ tq } um'+vn'=1}$. Par ailleurs $Md = mn = m'dn'd$ donc $\underline{M=m'n'd}$

On a alors d'une part $z^{mn'} = z^{m'dn'} = z^M = 1$
d'autre part $z^{m'n} = z^{m'n'd} = z^M = 1$

Comme $z^{mn'} = (z^{n'})^m = 1$ on a que $z^{n'} \in \mathbb{U}_m$ or $\mathbb{U}_m \subset H$

Comme $z^{nm'} = (z^{m'})^n = 1$ on a aussi que $z^{m'} \in \mathbb{U}_n$ or $\mathbb{U}_n \subset H$

Donc $z^{n'} \in H$, $z^{m'} \in H$ et $(H, \times)$ est un sous-groupe de $(\mathbb{U}, \times)$

donc $(z^{n'})^u \in H$ et $(z^{m'})^v \in H$ et $(z^{n'})^u \times (z^{m'})^v \in H$

or $(z^{n'})^u \times (z^{m'})^v = z^{n'u} \times z^{m'v} = z^{n'u + m'v} = z^1 = z$

Donc $\underline{z \in H}$ Youpi !

③ Soit $p \in \mathcal{P}$ et $G_p = \bigcup_{n \in \mathbb{N}} \mathbb{U}_{p^n}$

ⓐ • $G_p \subset \mathbb{U}$. En effet si $z \in G_p$ alors il existe $k \in \mathbb{N}$ tq $z \in \mathbb{U}_{p^k}$ donc $z$ est une racine $p^k$ième de l'unité donc son module vaut 1 et $z \in \mathbb{U}$

• $1 \in G_p$ car $\forall n \in \mathbb{N}$ 1 est une racine $p^n$ de l'unité ($1^{p^n} = 1$).

• $\underline{\text{Soit } g \in G_p \text{ et } h \in G_p \text{ Mq } g h^{-1} \in G_p.}$

$g \in G_p$ donc il existe $k \in \mathbb{N}$ tq $g^{p^k} = 1$

$h \in G_p$ donc il existe $l \in \mathbb{N}$ tq $h^{p^l} = 1$.

Posons $i = \max(k, l)$

alors si $k \leq l$, $i = l$ et $\begin{cases} g^{p^i} = g^{p^k \times p^{i-k}} = (g^{p^k})^{p^{i-k}} = 1^{p^{i-k}} = 1 \\ h^{p^i} = h^{p^l} = 1 \end{cases}$

si $l \leq k$, $i = k$ et $\begin{cases} g^{p^i} = g^{p^k} = 1 \\ h^{p^i} = h^{p^k} = h^{p^l p^{k-l}} = (h^{p^l})^{p^{k-l}} = 1^{p^{k-l}} = 1 \end{cases}$

dans les 2 cas, $g \in \mathbb{U}_{p^i}$ et $h \in \mathbb{U}_{p^i}$

Comme $(\mathbb{U}_{p^i}, \times)$ est un groupe, $gh^{-1} \in \mathbb{U}_{p^i}$

or $\mathbb{U}_{p^i} \subset \bigcup_{n \in \mathbb{N}} \mathbb{U}_{p^n}$ donc $\underline{gh^{-1} \in G_p}$

Concl : $\underline{(G_p, \times) \text{ est un sous-groupe de } (\mathbb{U}, \times)}$

ⓑ • Montrons que $G_p$ est infini

Soit $n \in \mathbb{N}$. $G_p$ contient $\mathbb{U}_{p^n}$ donc $G_p$ a au moins $p^n$ éléments

Ceci est vrai pour tout entier naturel $n$

$\underline{\text{Donc } G_p \text{ est infini}}$

- Soit $H$ un sous-groupe propre de $G_p$.
  Il existe donc un élément $w$ tel que $w \in G_p$ et $w \notin H$
  Il existe donc $n_0 \in \mathbb{N}$ tq $w \in \mathbb{U}_{p^{n_0}}$ et $w \notin H$.
  On a donc $w^{p^{n_0}} = 1$

  Soit $h \in H$
  Soit $n_1$ le plus petit entier $n$ tel que $h^{p^n} = 1$.

(X) On a donc $\mathbb{U}_{p^{n_1}} \subset H$.

or $w \notin H$ donc $\mathbb{U}_{p^{n_0}} \not\subset \mathbb{U}_{p^{n_1}}$ (car sinon $\mathbb{U}_{p^{n_0}} \subset \mathbb{U}_{p^{n_1}} \subset H$ et $w \in H$)
donc d'après 2a $p^{n_0} \nmid p^{n_1}$
donc $n_0 > n_1$ donc $n_0 - 1 \geq n_1$ et $h^{p^{n_0-1}} = h^{p^{n_1} \times p^{n_0-1-n_1}}$
$= \left(h^{p^{n_1}}\right)^{n_0-1-n_1}$
$= 1^{n_0-1-n_1}$
$= 1$

donc $h \in \mathbb{U}_{p^{n_0-1}}$

donc $H \subset \mathbb{U}_{p^{n_0-1}}$

donc <u>$H$ est un ensemble fini.</u>

## Exercice 3

1) $f$ est continue sur le segment $[0,a]$ donc d'après le théorème de Heine, elle est uniformément continue sur $[0,a]$

2) Soit $\varepsilon>0$. On cherche $\eta>0$ tq $\forall (x,y)\in\mathbb{R}^+ \quad |x-y|<\eta \Rightarrow |\sqrt{x}-\sqrt{y}|\leq\varepsilon$

Soit $(x,y)\in\mathbb{R}^+_*$

$$|\sqrt{x}-\sqrt{y}| = |\sqrt{x}-\sqrt{y}|\frac{(\sqrt{x}+\sqrt{y})}{\sqrt{x}+\sqrt{y}} = \frac{|(\sqrt{x}-\sqrt{y})(\sqrt{x}+\sqrt{y})|}{\sqrt{x}+\sqrt{y}} = \frac{|x-y|}{\sqrt{x}+\sqrt{y}}$$

or $\lim\limits_{x\to+\infty}\frac{1}{\sqrt{x}}=0$

donc $\exists a>0$ tq $\forall x\in\mathbb{R}, \quad x\geq a\Rightarrow \frac{1}{\sqrt{x}}\leq 2 \Rightarrow \sqrt{x}\geq\frac{1}{2}$

Ainsi, si $x\geq a$ et $y\geq a$, $\sqrt{x}+\sqrt{y}\geq\frac{1}{2}+\frac{1}{2}=1$ donc $\frac{1}{\sqrt{x}+\sqrt{y}}\leq 1$

et donc si $x\geq a$ et $y\geq a$, $|\sqrt{x}-\sqrt{y}| = \frac{|x-y|}{\sqrt{x}+\sqrt{y}}\leq|x-y|$

Par ailleurs, on sait que $f$ est uniformément continue sur $[0,a]$

donc $\exists \eta_1>0$ tq $\forall (x,y)\in[0,a], \quad |x-y|<\eta_1\Rightarrow|\sqrt{x}-\sqrt{y}|\leq\frac{\varepsilon}{2}$

On pose alors $\eta=\min(\eta_1,\frac{\varepsilon}{2})$.

En effet si $|x-y|<\eta$,

3 cas possibles
- alors $|\sqrt{x}-\sqrt{y}|\leq|x-y|<\eta\leq\frac{\varepsilon}{2}<\varepsilon$ si $(x,y)\in[a,+\infty[$
- alors $|\sqrt{x}-\sqrt{y}|\leq\frac{\varepsilon}{2}<\varepsilon$ si $(x,y)\in[0,a]$
- alors $|\sqrt{x}-\sqrt{y}|\underset{IT}{\leq}|\sqrt{x}-\sqrt{a}|+|\sqrt{a}-\sqrt{y}|\leq\frac{\varepsilon}{2}+\frac{\varepsilon}{2}\leq\varepsilon$ si $x\leq a\leq y$

(idem si $y\leq a\leq x$, rôles symétriques de $x$ et de $y$).

Donc $f$ est uniformément continue sur $[0,+\infty[$.

2) Autre méthode

on montre que $\forall(x,y)\in\mathbb{R}^{+2}, |\sqrt{y}-\sqrt{x}|\leq\sqrt{|y-x|}$ $(*)$

Soit $\varepsilon>0$ On pose $\eta=\varepsilon^2$.

Soient $(x,x')\in\mathbb{R}_+^2$, si $|x-x'|<\eta$ alors $|\sqrt{x'}-\sqrt{x}|\leq\sqrt{|x'-x|}<\sqrt{\eta}=\varepsilon\leq\varepsilon$

Donc $x\mapsto\sqrt{x}$ est uniformément continue sur $[0,+\infty[$

$(*)$ en 2 temps:
- si $y\geq x$, $\sqrt{y}\leq\sqrt{y-x}+\sqrt{x}$ donc $|\sqrt{y}-\sqrt{x}|=\sqrt{y}-\sqrt{x}\leq\sqrt{y-x}=\sqrt{|y-x|}$
- si $x>y$, $|\sqrt{y}-\sqrt{x}|=\sqrt{x}-\sqrt{y}\leq\sqrt{|x-y|}=\sqrt{|y-x|}$.

3) Raisonnons par l'absurde en supposant qu'il existe $K\in\mathbb{R}_+^*$ tq $f$ est K lipschitzienne sur $\mathbb{R}^+$.

Alors $\forall(x,y)\in\mathbb{R}^{+2}$, $|\sqrt{x}-\sqrt{y}|\leq K|x-y|$. En particulier $\binom{x>0}{y=0}$ :

$\forall x\in\mathbb{R}_+^*$ $|\sqrt{x}|=\sqrt{x}\leq K|x|$ càd $\forall x>0$ $\frac{\sqrt{x}}{x}\leq K$ càd $\forall x>0$ $\frac{1}{\sqrt{x}}\leq K$

Or si $x\to0^+$, $\frac{1}{\sqrt{x}}\to+\infty$ Absurde ! Donc $f$ n'est pas lipschitzienne sur $\mathbb{R}^+$

4) La fonction réciproque d'une fonction uniformément continue sur $\mathbb{R}^+$ n'est pas nécessairement uniformément continue. En effet on a mq $x\mapsto x^2$ n'est pas uniformément continue sur $\mathbb{R}^+$ alors que $x\mapsto\sqrt{x}$ est uniformément continue sur $\mathbb{R}^+$.