Devoir à la maison n°4
CORRECTION

Exercice 1

1. En plusieurs temps...
   • On suppose que H_1H_2 est un groupe.
   Soit $z \in H_1H_2$, donc il existe $x \in H_1$ et $y \in H_2$ tel que $z = xy$.
   Or H_1H_2 est un groupe, donc $z^{-1} \in H_1H_2$.
   Donc il existe $(x', y') \in H_1 \times H_2$ tel que $z^{-1} = x'y'$.
   On a alors $z = (z^{-1})^{-1} = (x'y')^{-1} = (y')^{-1}(x')^{-1}$.
   Et comme H_1 et H_2 sont des groupes : $(y')^{-1} \in H_2$ et $(x')^{-1} \in H_1$.
   Et donc $z \in H_2H_1$. On a donc $H_1H_2 \subset H_2H_1$.
   Soit $z \in H_2H_1$.
   Il existe $x \in H_2$ et $y \in H_1$ tels que $z = xy$.
   $z^{-1} = y^{-1}x^{-1} \in H_1H_2$, donc $z \in H_1H_2$, car H_1H_2 est un groupe.
   Et donc $H_2H_1 \subset H_1H_2$.
   Par double inclusion, on a donc $H_1H_2 = H_2H_1$.
   • Réciproquement, supposons que $H_1H_2 = H_2H_1$.
   Montrons que H_1H_2 est un groupe, en montrant que c'est un sous-groupe de G.
   — $e = \underbrace{e}_{\in H_1}\underbrace{e}_{\in H_2} \in H_1H_2$.
   — Soit $z = xy \in H_1H_2$ avec $x \in H_1$ et $y \in H_2$.
   On a vu que $z^{-1} = y^{-1}x^{-1} \in H_2H_1 = H_1H_2$. Donc $z^{-1} \in H_1H_2$
   — Soient $z_1, z_2 \in H_1H_2$. Donc il existe $x_1, x_2 \in H_1$ et $y_1, y_2 \in H_2$ tels que $z_1 = x_1y_1$ et $z_2 = x_2y_2$.
   On a alors $z_1z_2 = x_1y_1x_2y_2$.
   Or $y_1x_2 \in H_2H_1 = H_1H_2$. Donc il existe $(x', y') \in H_1 \times H_2$ tel que $y_1x_2 = x'y'$.
   Donc $z_1z_2 = \underbrace{x_1x'}_{\in H_1}\underbrace{y'y_2}_{\in H_2} \in H_1H_2$
   Donc H_1H_2 est un sous-groupe de G.

$$\boxed{H_1H_2 \text{ est un sous-groupe de } G \text{ si et seulement si } H_1H_2 = H_2H_1}$$

2. On suppose que H_1 et H_2 sont finis et $H_1 \cap H_2 = \{e\}$ où e est le neutre de G.
   On note $\varphi : (H_1, H_2) \longrightarrow H_1H_2$, $(x, y) \longmapsto xy$.
   Par définition de H_1H_2, φ est surjective.
   Puis considérons (x, y) et $(x', y') \in (H_1, H_2)$ tels que $\varphi(x, y) = \varphi(x', y')$.
   Donc $xy = x'y'$ et ainsi $y(y')^{-1} = x^{-1}xy(y')^{-1} = x^{-1}x'y'(y')^{-1} = x^{-1}x'$.
   Or $y(y')^{-1} \in H_2$, $x^{-1}x' \in H_1$, donc $y(y')^{-1} = x^{-1}x' \in H_1 \cap H_2 = \{e\}$.
   Par conséquent, $y(y')^{-1} = e$ donc $y' = y$ et $x^{-1}x' = e$, donc $x = x'$.
   Ainsi φ est injective. Par conséquent, φ est bijective entre deux ensembles finis.

$$\boxed{\text{Card}(H_1H_2) = \text{Card}(H_1) \times \text{Card}(H_2)}$$

3. Montrer que le cardinal (=ordre) de tout sous groupe H du groupe G fini divise l'ordre de G.
   C'est très classique. Il faut **savoir faire** cela.
   On note $\mathcal{R}$ la relation définie par $a\mathcal{R}b \Leftrightarrow ab^{-1} \in H$.
   • $\forall\ a \in G$, $aa^{-1} = e \in H$,
   donc $\mathcal{R}$ est réflexive.
   • $\forall\ a, b \in G$, tels que $ab^{-1} \in H$, alors $ba^{-1} = (ab^{-1})^{-1} \in H$ car H est un groupe,
   donc $\mathcal{R}$ est symétrique.
   • $\forall\ a, b, c \in G$, tels que $ab^{-1} \in H$, $bc^{-1} \in H$, par stabilité : $ab^{-1}bc^{-1} = ac^{-1} \in H$,
   donc $\mathcal{R}$ est transitive.
   $\mathcal{R}$ est une relation d'équivalence. Or toute classe d'équivalence a le même cardinal : celui de H,
   en effet, la classe de a (quelconque de G) est $\{b \in G \mid ba^{-1} \in H\} = \{ar, r \in H\}$ noté aH.
   Si N est le nombre de classe d'équivalence, on a donc $\text{ordre}(G) = N \times \text{ordre}(H)$.

$$\boxed{\text{ordre}(H) | \text{ordre}(G)}$$

4. Soit H un groupe d'ordre p premier.
Soit $a \in H$ et $A = \{a^k, k \in \mathbb{Z}\}$.
Par stabilité de H par produit (c'est un groupe) : $A \subset H$.
Et pour tout $a_1, a_2 \in A$, il existe $k_1, k_2 \in \mathbb{Z}$ tels que $a_1 = a^{k_1}$, $a_2 = a^{k_2}$.
Ainsi $a_1 a_2^{-1} = a^{k_1 - k_2} \in A$.
Ainsi, d'après la seconde caractéristique, A est un sous-groupe de H.
Et donc, d'après la question précédente : ordre$(A)|$ordre$(H) = p$.
Or les seuls diviseurs de p sont 1 et p. donc ordre$(A) \in \{1, p\}$.
Puis ordre$(A) = 1$ si et seulement si $a^1 = e$
Donc pour tout $a \neq e \in H$, $A = H$, c'est-à-dire : pour tout $x \in H$, $\exists\ k \in \mathbb{Z}$ tel que $x = a^k$.
Puis, H étant fini (d'ordre p), A l'est également nécessairement.
Donc $\{k \in \mathbb{N} \mid \exists\ i \in [\![0, k-1]\!] \text{ tel que } a^k = a^i\}$ est non vide, inclus dans N.
Il admet donc un plus petit élément : noté r.
Il existe $i \in [\![0, r-1]\!]$ tel que $a^r = a^i$, donc $a^{r-1} = a^{i-1}$ (en multipliant par a^{-1}).
Or $r - 1 \notin \{k \in \mathbb{N} \mid \exists\ i \in [\![0, k-1]\!] \text{ tel que } a^k = a^i\}$, sinon on aurait une contradiction.
Par conséquent, $i - 1 \notin [\![0, r-1]\!]$ et donc $i = 0$. Ainsi $a^r = e$ et $A = \{a^k, k \in [\![0, r-1]\!]\}$.
Donc ordre$(A) = r|p$ et donc $r = p$.

$$\boxed{\forall\ a \in H : \forall\ x \in H, \exists\ k \in [\![0, p-1]\!] \text{ tel que } x = a^k.}$$

5. On suppose que G est abélien, H_1 et H_2 d'ordres finis p et q (avec $p \wedge q = 1$).
Comme G est abélien, les éléments de G commutent et donc $H_1 H_2 = H_2 H_1$ nécessairement.
Ainsi $H_1 H_2$ est un sous-groupe de G. Puis H_1 est d'ordre p, premier donc il existe $a \in H_1$ tel que $H_1 = \{a^k, k \in [\![0, p-1]\!]\}$.
et de même, H_2 est d'ordre q, premier donc il existe $b \in H_2$ tel que $H_2 = \{b^k, k \in [\![0, q-1]\!]\}$.
Nécessairement (par stabilité de la loi), $\{(ab)^r, r \in \mathbb{Z}\}$ est un sous-groupe de $H_1 H_2$.
Réciproquement, si $xy \in H_1 H_2$, $\exists\ k, s \in [\![0, p-1]\!] \times [\![0, q-1]\!]$ tel que $x = a^k$ et $y = b^s$.
On sait que $p \wedge q = 1$, donc il existe $u, v \in \mathbb{Z}$ tel que $up + vq = 1$.
Considérons $r = kvq + sup$.
Alors $r = k(1-up) + sup = k + (su - ku)p \equiv k[p]$ et $r = kvq + s(1-vq) = s + (kv - sv)q \equiv s[q]$.
Donc comme G est abélien

$$(ab)^r = a^r b^r = a^{k+(su-ku)p} b^{s+(kv-sv)q} = a^k (a^p)^{su-ku} b^s (b^q)^{kv-sv} = a^k b^s = xy$$

Ainsi $H_1 H_2 \subset \{(ab)^r, r \in \mathbb{Z}\}$.
Par double inclusion $H_1 H_2 = \{(ab)^r, r \in \mathbb{Z}\}$.
Enfin, comme en question précédente, on montre que $\{(ab)^r, r \in \mathbb{Z}\} = \{(ab)^r, r \in [\![0, pq-1]\!]\}$.

$$\boxed{H_1 H_2 \text{ est un sous-groupe cyclique de } G.}$$

Remarques !
Dans cette dernière question, on exploite le lemme des restes (sans le savoir).
La question est : trouver $r \in \mathbb{Z}$ tel que $\begin{cases} r & \equiv k[p] \\ r & \equiv s[q] \end{cases}$
On a, en effet, $a^r = a^{k+mp} = a^k (a^p)^m = a^k 1^m = a^k = x$ et $b^r = \cdots = b^s = y$.
Mais ce système de congruence étant linéaire, on préfère résoudre les deux systèmes :
$\begin{cases} r_p & \equiv 1[p] \\ r_p & \equiv 0[q] \end{cases}$ *et* $\begin{cases} r_q & \equiv 0[p] \\ r_q & \equiv 1[q] \end{cases}$
on aura alors $r = kr_p + sr_q$.
Or puisque $up + vq = 1$, on a des solutions simples : $r_p = 1 - up = vq$ et $r_q = 1 - vq = up$.

Exercice 2

1. Par addition de fonctions de référence, f est dérivable sur $\mathbb{R}$. Et pour tout $x \in \mathbb{R}$, $f'(x) = e^x - 1$.
Donc f est strictement croissante sur $\mathbb{R}_+$.
f étant continue, elle établit donc une bijection de $\mathbb{R}_+$ sur $I = [f(0), \lim_{+\infty} f[= [1, +\infty[$.

$$\boxed{f \text{ établit une bijection de } \mathbb{R}_+ \text{ sur } I = [1, +\infty[.}$$

2. $\mathbb{N}^* \subset I$, donc pour tout $n \in \mathbb{N}^*$, n a un unique antécédent par f.

$$\boxed{\text{Pour tout } n \in \mathbb{N}^*, \text{ l'équation : } f(x) = n, \text{ a une solution notée } u_n.}$$

3.

$$\boxed{f(0) = 1, \text{ donc } u_1 = 0}$$

4. Soit $n \in \mathbb{N}^*$. $f(u_n) = n < n+1 = f(u_{n+1})$. Or f est croissante donc $u_n < u_{n+1}$.

$$\boxed{u_n \text{ est croissante.}}$$

5. Soit $n \in \mathbb{N}^*$. $f(\ln n) = e^{\ln n} - \ln n = n - \ln n < n = f(u_n)$. Par croissance de f :

$$\boxed{\text{Pour tout } n \in \mathbb{N},\ u_n \geqslant \ln n.}$$

Et comme $\lim \ln n = +\infty$, (u_n) diverge vers $+\infty$ par minoration.

$$\boxed{\lim(u_n) = +\infty}$$

6. Soit $n \in \mathbb{N}^*$, $n = f(u_n) = e^{u_n} - u_n$. En divisant par n : $\dfrac{e^{u_n}}{n} = 1 + \frac{u_n}{n}$.
Or $f(2\ln n) = e^{2\ln n} - 2\ln n = n^2 - 2\ln(n) > n = f(u_n)$ dès que $n \geqslant 2$, donc $\ln n < u_n < 2\ln n$.
Ainsi $\frac{u_n}{n} \to 0$, par encadrement et donc $\dfrac{e^{u_n}}{n} \to 1$.

$$\boxed{\exp(u_n) \sim n}$$

7. Soit $n \in \mathbb{N}$, $e^{v_n} = e^{u_n - \ln n} = \dfrac{e^{u_n}}{n} \to 1$. Donc, en composant par $t \mapsto \ln t$, continue en 1,

$$\boxed{v_n \to \ln 1 = 0}$$

8. Soit $n \in \mathbb{N}$

$$n = f(u_n) = e^{u_n} - u_n = e^{v_n + \ln n} - u_n = ne^{v_n} - u_n \Rightarrow u_n = n(e^{v_n} - 1)$$

On sait que $\frac{e^x - 1}{x} \underset{x \to 0}{\longrightarrow} 1$. Donc $\dfrac{u_n}{v_n} = n\dfrac{e^{v_n} - 1}{v_n} \sim n$, donc $v_n \sim \dfrac{u_n}{n}$.
Enfin, comme $v_n \to 0$, $u_n \sim \ln n$ et donc

$$\boxed{v_n \sim \frac{\ln n}{n}}$$

9. On a donc

$$\boxed{u_n = \ln n + v_n = \ln n + \frac{\ln n}{n} + o\left(\frac{\ln n}{n}\right)}$$

Problème

1. On considère une suite (u_n) bornée, quelconque.
   (a) Pour tout $n \in \mathbb{N}$, l'ensemble U_n est bornée, inclus dans $\mathbb{R}$, donc admet une borne supérieure et inférieure, d'après les propriétés de $\mathbb{R}$.

$$\boxed{\text{Les suite } (m_n) \text{ et } (M_n) \text{ sont bien définies.}}$$

   (b) (u_n) est bornée : $\exists\ a, b \in \mathbb{R}$ tel que $\forall\ k \in \mathbb{N}$, $a \leqslant u_k \leqslant b$.
   Donc pour tout $n \in \mathbb{N}$: $\forall\ k \geqslant n$, $a \leqslant u_k \leqslant b$ Ainsi a (respectivement b) est un minorant de l'ensemble U_n.
   $m_n = \inf\{u_k, k \geqslant n\}$ est le plus grand des minorants de cet ensemble : $a \leqslant m_n$ Ainsi b est un majorant de l'ensemble U_n.
   $M_n = \sup\{u_k, k \geqslant n\}$ est le plus grand des minorants de cet ensemble : $M_n \leqslant b$ Enfin, pour tout $n \in \mathbb{N}$: $m_n \leqslant u_n \leqslant M_n$.
   Donc pour tout $n \in \mathbb{N}$: $a \leqslant m_n \leqslant M_n \leqslant b$.

$$\boxed{(m_n) \text{ et } (M_n) \text{ sont bornées.}}$$

   (c) Soit $n \in \mathbb{N}$, $U_n = U_{n+1} \cup \{u_n\}$.
   Si a est un minorant de U_n, alors $\forall\ k \geqslant n+1$, $a \leqslant u_k$ et donc a est minorant de U_{k+1}.
   Ainsi, m_n, le plus grand des minorants de U_n est un minorant de U_{n+1},
   il est plus petit que le plus grand des minorants de U_{n+1}. Donc $m_n \leqslant m_{n+1}$.
   Si b est un majorant de U_n, alors $\forall\ k \geqslant n+1$, $b \geqslant u_k$ et donc b est majorant de U_{k+1}.
   Ainsi, M_n, le plus petit des majorants de U_n est un majorant de U_{n+1},
   il est plus grand que le plus petit des majorants de U_{n+1}. Donc $M_n \geqslant M_{n+1}$.

$$\boxed{(m_n) \text{ est croissante et } (M_n) \text{ décroissante. Elles sont bornées donc convergentes.}}$$

2. Quelques exemples.

(a) Pour tout $n \in \mathbb{N}$, $U_n = \{-1, 1\}$, donc $m_n = -1$ et $M_n = 1$.

$$\boxed{\text{Ce sont des suites constantes : } \liminf u_n = -1 \text{ et } \limsup u_n = 1}$$

(b) Dans ce cas u_n est décroissante de limite nulle. Donc pour tout $n \in \mathbb{N}$, $m_n = 0$ et $M_n = \frac{1}{n+1}$.

$$\boxed{\liminf u_n = 0 = \limsup u_n}$$

(c) Soit $\epsilon > 0$, il existe $N \in \mathbb{N}$ tel que $\forall\ n \in \mathbb{N}$, $|u_n - \ell| \geqslant \epsilon$,
Donc $\forall\ n \geqslant N$, $U_n \subset [\ell - \epsilon; \ell + \epsilon]$ et donc $\ell - \epsilon \leqslant m_n \leqslant M_n \leqslant \ell + \epsilon$.
Donc $\forall\ n \geqslant N$, $|m_n - \ell| \leqslant \epsilon$ et $|M_n - \ell| \leqslant \epsilon$.

$$\boxed{\text{Donc } \liminf u_n = \limsup u_n = \ell}$$

3. Une suite particulière.
On note $\mathcal{D}_+(n)$, l'ensemble des diviseurs positifs de n.

(a) $\mathcal{D}_+(2) = \{1, 2\}$, $\mathcal{D}_+(3) = \{1, 3\}$ et $\mathcal{D}_+(15) = \{1, 3, 5, 15\}$

$$\boxed{d_2 = 2, \quad d_3 = 2 \quad d_{15} = 4}$$

(b) Pour tout nombre entier n, $d_n \geqslant 2$. Donc $m(d_n) \geqslant 2$.
Pour tout nombre premier p, $\mathcal{D}_+(p) = \{1, p\}$.
Soit $n \in \mathbb{N}$, on sait qu'il existe une infinité de nombres premiers donc il existe $p > n$, premier.
Ainsi $m(d_n) \leqslant 2$.

$$\boxed{\liminf d_n = 2 \text{ car } m(d_n) \text{ est constante égale à } 2}$$

(c) Si $n = 2^m$, alors $\mathcal{D}(n) = \{1, 2, 4, 8, \dots 2^m\}$ et donc $d_n = m + 1$.

$$\boxed{\text{Avec (par exemple) } \varphi : m \mapsto 2^m, \text{ strictement croissante , } d_{\varphi(m)} = (m+1) \text{ est strictement croissante.}}$$

4. Regardons le résultat moyen (Cesaro). On note $D_n = \dfrac{1}{n}\displaystyle\sum_{k=1}^{n} d_k$.

(a) On note H_k, l'hyperbole d'équation $yx = k$ (branche positive : $x, y > 0$).
On note $H_n^{\mathbb{N}}$, l'ensemble des points à coordonnées entières sur H_n.
$M(a, b) \in H_n \iff ab = n$. Donc $\Phi : \mathcal{D}_+(n) \to H_n^{\mathbb{N}}$, $a \mapsto (a, \frac{n}{a})$ est une bijection.

$$\boxed{\text{L'égalité des cardinaux signifie : } d_n \text{ est le nombre de points à coordonnées entières sur } H_n.}$$

(b) Comme les ensembles $H_k^{\mathbb{N}}$ sont disjoints (les hyperboles ne se coupent pas) :

$$nD_n = \sum_{k=1}^{n} d_k = \sum_{k=1}^{n} \text{Card}(H_k^{\mathbb{N}}) = \text{Card}\left(\bigcup_{k=1}^{n} H_k^{\mathbb{N}}\right)$$

$$\boxed{nD_n \text{ est le nombre de points entiers compris entre } H_n \text{ et les demi-axes } y = 0 (x > 0) \text{ et } x = 0 (y > 0).}$$

(c) (k, r) est situé sous l'hyperbole H_n signifie que $kr < n$, donc $r < \frac{n}{k}$.

$$\boxed{\text{Il y a donc } \left\lfloor \tfrac{n}{k} \right\rfloor \text{ points avec } k \text{ comme abscisses, dans la surface considérée}}$$

On somme toutes les abscisses possibles donc k évoluant de 1 à n.

$$\boxed{nD_n = \sum_{k=1}^{n} \left\lfloor \frac{n}{k} \right\rfloor \Longrightarrow D_n = \frac{1}{n}\sum_{k=1}^{n} \left\lfloor \frac{n}{k} \right\rfloor}$$

(d) On sait que pour tout $k \in \mathbb{N}_n$, $\frac{n}{k} - 1 \leqslant \lfloor \frac{n}{k} \rfloor \leqslant \frac{n}{k}$.
En sommant, puis divisant par n :

$$\sum_{k=1}^{n} \left(\frac{n}{k} - 1\right) = nH_n - n \leqslant nD_n \leqslant \sum_{k=1}^{n} \frac{n}{k} = nH_n$$

.

$$\boxed{D_n \sim \ln n \Rightarrow D_n = \ln n + O(1).}$$