Corrigé du TD n° 5

Relations d'ordre, bornes supérieures et bornes inférieures et Théorème de Lagrange

23 novembre 2020

Exercice 1. On considère la relation $\preccurlyeq$ sur $\mathbb{N}$ définie par $x \preccurlyeq y$ si par définition, il existe $n \in \mathbb{N}^*$ tel que $y = x^n$.

1. Montrer que $\preccurlyeq$ est une relation d'ordre. S'agit-il d'une relation d'ordre total ?
2. La partie $\{2, 3\}$ est-elle majorée ?

---

1. • **Réflexivité :** Soit $x \in \mathbb{N}$. On a $x = x^1$ et $1 \in \mathbb{N}^*$ donc $x \preccurlyeq x$.
   • **Antisymétrie :** Soit $(x, y) \in \mathbb{N}^{*2}$ tel que $x \preccurlyeq y$ et $y \preccurlyeq x$. Montrons que $x = y$.
   Comme $x \preccurlyeq y$, il existe $n \in \mathbb{N}^*$ tel que $y = x^n$. Comme $y \preccurlyeq x$, il existe $m \in \mathbb{N}^*$ tel que $x = y^m$. Donc
   $$x = y^m = (x^n)^m = x^{nm}.$$
   Si $x = 0$ alors, de l'égalité $y = x^n$, on en déduit que $y = 0$ et donc $x = y$.
   Supposons donc $x \neq 0$. Alors en divisant l'égalité $x = x^{nm}$ par x (car $x \neq 0$), on a $x^{nm-1} = 1$.
   On a alors $(nm - 1)\ln(x) = 0$. Donc soit $nm = 1$ et donc $n = m = 1$, donc $x = y$, soit $\ln(x) = 0$ et donc $x = 1$ et $y = x^n = 1 = x$.
   Donc, dans tous les cas, $x = y$.
   • **Transitivité :** Soit $(x, y, z) \in \mathbb{N}^3$ tel que $x \preccurlyeq y$ et $y \preccurlyeq z$. Alors il existe $n \in \mathbb{N}^*$ tel que $y = x^n$ et il existe $m \in \mathbb{N}^*$ tel que $z = y^m$. Donc $z = y^m = x^{nm}$ et $nm \in \mathbb{N}^*$ donc $x \preccurlyeq z$.

   De ces trois points, $\preccurlyeq$ est une relation d'ordre.
   Il ne s'agit pas d'un ordre total car par exemple, on ne peut pas comparer 2 et 3 : il n'existe pas d'élément $n \in \mathbb{N}^*$ tel que $2 = 3^n$ ou tel que $3 = 2^n$.
2. Supposons par l'absurde que $\{2, 3\}$ est majorée. Il existe donc $M \in \mathbb{N}$ tel que $2 \preccurlyeq M$ et $3 \preccurlyeq M$. Alors il existe $(n, m) \in \mathbb{N}^{*2}$ tel que $M = 2^n$ et $M = 3^m$. Donc M est à la fois pair et impair, ce qui est absurde. L'ensemble $\{2, 3\}$ n'est donc pas majoré.

Exercice 2. Soient A et B deux parties non vides majorées de $\mathbb{R}$.

1. Démontrer que si $A \subset B$ alors $\sup(A) \leq \sup(B)$.
2. Démontrer que $A \cup B$ possède une borne supérieure et que $\sup(A \cup B) = \max(\sup(A), \sup(B))$.
3. Démontrer que $\sup(A + B) = \sup(A) + \sup(B)$.
4. Démontrer que pour tout $\lambda > 0$, $\sup(\lambda A) = \lambda \sup(A)$.

A et B étant des parties non vides majorées de $\mathbb{R}$, elles admettent une borne supérieure. Donc $\sup(A)$ et $\sup(B)$ existent bien.

1. Supposons $A \subset B$. Pour tout $a \in A$, on a $a \in B$, donc $\sup(B)$ étant un majorant de B, $a \leq \sup(B)$. Ainsi, $\sup(B)$ majore A. La borne supérieure étant le plus petit des majorants, on en déduit que $\sup(A) \leq \sup(B)$.
2. • Soit $x \in A \cup B$.
   1^{er} cas : $x \in A$. Alors $x \leq \sup(A) \leq \max(\sup(A), \sup(B))$.
   2nd cas : $x \in B$. Alors $x \leq \sup(B) \leq \max(\sup(A), \sup(B))$.
   Dans tous les cas, $x \leq \max(\sup(A), \sup(B))$.
   x étant un élément quelconque de $A \cup B$, $\max(\sup(A), \sup(B))$ majore $A \cup B$.
   A étant non vide, $A \cup B$ l'est aussi. Donc $A \cup B$, partie non vide majorée de $\mathbb{R}$, admet une borne supérieure.
   La borne supérieure étant le plus petit des majorants, $\sup(A \cup B) \leq \max(\sup(A), \sup(B))$.
   • Comme $A \subset A \cup B$, d'après la question 1, $\sup(A) \leq \sup(A \cup B)$. De même, $B \subset A \cup B$ donc $\sup(B) \leq \sup(A \cup B)$. Donc $\max(\sup(A), \sup(B)) \leq \sup(A \cup B)$.

   Finalement, $\sup(A \cup B) = \max(\sup(A), \sup(B))$.

3. • Soit $x \in A+B$. Alors il existe $a \in A$ et $b \in B$ tel que $x = a+b$.
Or $a \leq \sup(A)$ et $b \leq \sup(B)$. Donc $x \leq \sup(A)+\sup(B)$.
x étant un élément quelconque de $A+B$, $\sup(A)+\sup(B)$ majore $A+B$. La borne supérieure étant le plus petit des majorants, $\sup(A+B) \leq \sup(A)+\sup(B)$.
• Soit $(a,b) \in A \times B$.
Comme $a+b \in A+B$, on a $a+b \leq \sup(A+B)$.
Donc $a \leq \sup(A+B)-b$.
a étant un élément quelconque de A, $\sup(A+B)-b$ majore A. La borne supérieure étant le plus petit des majorants, $\sup(A) \leq \sup(A+B)-b$.
On en déduit que $b \leq \sup(A+B)-\sup(A)$.
b étant un élément quelconque de B, $\sup(A+B)-\sup(A)$ majore b. La borne supérieure étant le plus petit des majorants, $\sup(B) \leq \sup(A+B)-\sup(A)$.
Donc $\sup(A)+\sup(B) \leq \sup(A+B)$.

Finalement $\sup(A+B) = \sup(A)+\sup(B)$.

4. Soit $\lambda \geq 0$.
• Soit $x \in \lambda A$. Alors il existe $a \in A$ tel que $x = \lambda a$.
Comme $a \in A$, $a \leq \sup(A)$. On a donc $x = \lambda a \leq \lambda \sup(A)$.
x étant un élément quelconque de λA, $\lambda \sup(A)$ majore λA. La borne supérieure étant le plus petit des majorants,
$$\sup(\lambda A) \leq \lambda \sup(A). \quad (*)$$
• Si $\lambda = 0$ alors $\lambda A = \{0\}$ et $\sup(\lambda A) = \lambda \sup(A) = 0$.
Supposons donc $\lambda > 0$.
Posons $\lambda' = \dfrac{1}{\lambda}$ et $A' = \lambda A$. D'après la relation $(*)$ appliquée à λ' et A', on a $\sup(\lambda' A') \leq \lambda' \sup(A')$, soit encore $\sup(\dfrac{1}{\lambda}\lambda A) \leq \dfrac{1}{\lambda}\sup(\lambda A)$. Donc $\sup(A) \leq \dfrac{1}{\lambda}\sup(\lambda A)$.
Ainsi, comme $\lambda > 0$, $\lambda \sup(A) \leq \sup(\lambda A)$.

Finalement, $\sup(\lambda A) = \lambda \sup(A)$.

Exercice 3. Déterminer les bornes supérieure et inférieure des parties suivantes, après avoir justifié leur existence. Ces parties admettent-elles un maximum ou un minimum ?

1. $A = \left\{(-1)^n + \dfrac{1}{n+1} \mid n \in \mathbb{N}\right\}$.
2. $B = \left\{\dfrac{1}{n} - \dfrac{1}{p} \mid (n,p) \in (\mathbb{N}^*)^2\right\}$.

---

1. • A est non vide et pour tout $n \in \mathbb{N}^*$, comme $\dfrac{1}{n+1} > 0$, $-1 < (-1)^n + \dfrac{1}{n+1}$, donc A est minoré par -1. Donc A admet une borne inférieure.
1. -1 minore A.
2. Posons, pour tout $p \in \mathbb{N}$, $u_p = (-1)^{2p+1} + \dfrac{1}{2p+2}$. Alors, pour tout $p \in \mathbb{N}$, $u_p \in A$ (avec $n = 2p+1 \in \mathbb{N}$) et $u_p = -1 + \dfrac{1}{2p+2}$ tend vers -1 lorsque p tend vers $+\infty$.
Donc d'après la caractérisation séquentielle de la borne inférieure, $\inf(A) = -1$.
A n'admet pas de minimum car sinon, d'après le cours, ce serait $\inf(A) = -1$. Or pour tout $n \in \mathbb{N}^*$, $(-1)^n + \dfrac{1}{n+1} > -1$ donc $-1 \notin A$.
• A est non vide et pour tout $n \in \mathbb{N}^*$, $(-1)^n + \dfrac{1}{n+1} \leq 1+1 = 2$. Donc A admet une borne supérieure.
1. 2 majore A.
2. On a $(-1)^0 + \dfrac{1}{0+1} = 2$ et $(-1)^0 + \dfrac{1}{0+1} \in A$, donc $2 \in A$.
On en déduit que $2 = \max(A)$ et donc $2 = \sup(A) = \max(2)$.

2. • B est non vide et pour tout $(n,p) \in (\mathbb{N}^*)^2$, $\dfrac{1}{n} - \dfrac{1}{p} < \dfrac{1}{n} \leq 1$ car $p > 0$ et $n \geq 1$. Donc B est une partie non vide et majorée de $\mathbb{R}$, elle admet donc une borne supérieure.
1. 1 majore B.
2. Posons, pour tout $p \in \mathbb{N}^*$, $u_p = \dfrac{1}{1} - \dfrac{1}{p}$. Alors, pour tout $p \in \mathbb{N}^*$, $u_p \in B$ (avec $n = 1$) et $u_p = 1 - \dfrac{1}{p}$ tend vers 1 lorsque p tend vers $+\infty$.
Donc, d'après la caractérisation séquentielle de la borne supérieure, $\sup(B) = 1$.

B n'a pas de maximum car sinon ce serait $\sup(B) = 1$ et donc $1 \in B$. Or pour tout $(n,p) \in (\mathbb{N}^*)^2$, $\frac{1}{n} - \frac{1}{p} < 1$ donc $1 \notin B$.

• B est non vide et pour tout $(n,p) \in (\mathbb{N}^*)^2$, $\frac{1}{n} - \frac{1}{p} > -\frac{1}{p} \geq -1$ car $n > 0$ et $p \geq 1$. Donc B est une partie non vide et minorée de $\mathbb{R}$, elle admet donc une borne inférieure.

1. -1 minore B.

2. Posons, pour tout $n \in \mathbb{N}^*$, $v_n = \frac{1}{n} - \frac{1}{1}$. Alors, pour tout $n \in \mathbb{N}^*$, $v_n \in B$ (avec $p = 1$) et $v_n = \frac{1}{n} - 1$ tend vers -1 lorsque n tend vers $+\infty$.

Donc, d'après la caractérisation séquentielle de la borne inférieure, $\inf(B) = -1$.

B n'a pas de minimum car sinon ce serait $\inf(B) = -1$ et donc $-1 \in B$. Or pour tout $(n,p) \in (\mathbb{N}^*)^2$, $\frac{1}{n} - \frac{1}{p} > -1$ donc $-1 \notin B$.

Exercice 4. Soient $(E, \preccurlyeq_E)$ et $(F, \preccurlyeq_F)$ deux ensembles ordonnés et A une partie non vide de E. Soit f une application croissante de E dans F, c'est-à-dire, telle que pour tout $(x,y) \in E^2$, si $x \preccurlyeq_E y$ alors $f(x) \preccurlyeq_F f(y)$.

1. Montrer que si $\max(A)$ existe, alors $\max(f(A))$ existe et est égal à $f(\max A)$.
2. Est-ce encore vrai si on remplace les max par des sup ?

---

1. Supposons que $\max(A)$ existe. Il existe donc $a_0 \in A$ tel que $a_0 = \max(A)$ et a_0 majore A.
   Pour tout $a \in A$, on a donc $a \preccurlyeq_E a_0$. f étant croissante, pour tout $a \in A$, $f(a) \preccurlyeq_F f(a_0)$.
   Donc, a étant un élément quelconque de A, $f(a_0)$ majore $f(A)$, et comme $a_0 \in A$, $f(a_0) \in f(A)$.
   D'après la définition du maximum, $f(A)$ admet donc un maximum, égal à $f(a_0)$. Or $a_0 = \max(A)$.
   Donc $\max(f(A)) = f(a_0) = f(\max(A))$.
   D'où le résultat.
2. Le résultat n'est plus vrai si on remplace max par sup. Prenons $(E, \preccurlyeq_E) = (F, \preccurlyeq_F) = (\mathbb{R}, \leq)$ et considérons la fonction E partie entière. Alors E est une application croissante de $\mathbb{R}$ dans $\mathbb{R}$. Soit $A = [0, 1[$. On a $\sup(A) = 1$ et $E(\sup(A)) = E(1) = 1$. De plus, $E(A) = \{0\}$ car E est nulle sur A et donc $\sup(E(A)) = \sup(\{0\}) = 0$.
   Donc $\sup(E(A)) \neq E(\sup(A))$.
   Remarquons qu'ici, A n'admet pas de maximum.

Exercice 5. Soient A et B deux parties non vides de $\mathbb{R}$ vérifiant les deux propriétés suivantes :

1. Pour tout $a \in A$ et tout $b \in B$, $a \leq b$,
2. Pour tout $\varepsilon > 0$, il existe $a_0 \in A$ et $b_0 \in B$ tel que $b - a < \varepsilon$.

Montrer que $\sup(A) = \inf(B)$.

• Soit $b_0 \in B$. D'après 1., pour tout $a \in A$, $a \leq b_0$ donc b_0 majore A. A est donc une partie non vide majorée de $\mathbb{R}$, elle admet donc une borne supérieure $\sup(A)$.

Soit $a_0 \in A$. D'après 1., pour tout $b \in B$, $a_0 \leq b$ donc a_0 minore B. B est donc une partie non vide majorée de $\mathbb{R}$, elle admet donc une borne inférieure $\inf(B)$.

• Commençons par montrer que $\sup(A) \leq \inf(B)$.

Soit $b \in B$. D'après 1., pour tout $a \in A$, $a \leq b$. Donc b majore A (*on retrouve que A admet une borne supérieure*) et la borne supérieure étant le plus petit des majorants, $\sup(A) \leq b$.

De cette inégalité, b étant un élément quelconque de B, on en déduit que $\sup(A)$ minore B (*On retrouve que B admet une borne inférieure*). La borne inférieure étant le plus grand des minorants, $\sup(A) \leq \inf(B)$.

• Utilisons la caractérisation en ε de la borne supérieure. Posons $M = \inf(B)$.

1. On a vu que M majore A.

2. Soit $\varepsilon > 0$. Montrons qu'il existe $a_0 \in A$ tel que $M - \varepsilon < a_0 \leq M$.

D'après 2., il existe $a_0 \in A$ et $b_0 \in B$ tel que $b_0 - a_0 < \varepsilon$. On a donc $b_0 - \varepsilon < a_0$. Or $\inf(B)$ minore B donc $\inf(B) \leq b_0$. Donc $M - \varepsilon = \inf(B) - \varepsilon \leq b_0 - \varepsilon < a_0$. M étant un majorant de A, on a aussi $a_0 \leq M$.

Donc $M - \varepsilon < a_0 \leq M$.

D'après la caractérisation de la borne supérieure, on a donc $\sup(A) = M = \inf(B)$.

Exercice 6. Soit G un groupe d'ordre 8.

1. Soit $a \in G$, quelles valeurs peut prendre $\gamma(a)$ l'ordre de a ?
2. S'il existe $a \in G$, tel que $\gamma(a) = 8$, que dire de G ?
   On supppose désormais qu'il n'existe pas d'élements d'ordre 8.
3. Si pour tout $a \in G$, $\gamma(a) = 2$, montrer que G est commutatif et en déduire que G isomorphe à $(\mathbb{Z}/2\mathbb{Z})^3$.
4. On suppose qu'il existe $a \in G$ d'ordre 4.
   (a) Montrer qu'il existe $b \in G\backslash < a >$ d'ordre 2.
   (b) En déduire que si G est commutatif, $\varphi : \mathbb{Z}/4\mathbb{Z} \times 2\mathbb{Z} \to G$, $(\bar{p}, \dot{q}) \mapsto a^p b^q$ est un isomorphisme de groupes.

L'exercice ci-dessous montre qu'il existe des groupes d'ordre 8 non abélien avec H isomorphe à $\mathbb{Z}/2\mathbb{Z}$.

---

1. Le théorème de Lagrange nous dit que l'ordre d'un élément divise l'ordre du groupe, donc $\gamma(a)$ vaut 2, 4 ou 8.
2. S'il existe $a \in G$, avec $\gamma(a) = 8$, alors par définition de l'ordre d'un élément $G =< a >$ et G est isomorphe à $\mathbb{Z}/8\mathbb{Z}$.
3. Si pour tout $a \in G$, $a^2 = e$, alors pour tout a et $b \in G$, $(ab)^2 = abab = e$. On multiplie l'inégalité à gauche par a et à droite par b, et on obtient $ba = ab$. Le groupe est bien commutatif.
   De plus, si $a \in G \setminus \{e\}$, $< a >=< e, a >$ et si $b \in G\backslash < a >$, alors $ab \neq a, b, e$ car a et $b \neq e$ et $a \neq b$. Donc $< a, b >= \{e, a, b, ab\}$ a exactement 4 éléments. Si $c \in G\backslash < a, b >$, alors $< a, b, c >$ contient $\{e, a, b, c, ab, ac, bc, abc\}$. On vérfie facilement que ces éléments sont 2 à 2 distincts, donc $< a, bc >= G$.
   Soit l'application $\varphi : \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to G$, telle que $\varphi(\bar{p}, \bar{q}, \bar{s}) = a^p b^q c^s$ est bien définie car si $\bar{p} = \bar{p}'$, $\bar{q} = \bar{q}'$ et $\bar{s} = \bar{s}'$, alors $p - p'$, $q - q'$, $s - s'$ sont pairs et donc $a^{p-p'} = 1$, $b^{q-q'} = 1$ et $c^{s-s'} = 1$, ce qui donne $a^p = a^{p'}$, $b^q = b^{q'}$ et $c^q = c^{q'}$. Comme G est abélien, φ est un morphisme et il est bijectif, c'est un isomorphisme.
4. (a) Soit $a \in G$ d'ordre 4, alors il existe $b \in G\backslash < a >$ car $| < a > | = 4 < |G| = 8$. On a vu que $\gamma(b) = 4$ ou 2. Si $\gamma(b) = 4$, alors $\gamma(b^2) = 2$. Si $b^2 \in< a >$, alors $b^2 = a^2$ car a^2 est le seul élément d'ordre 2, mais alors $\gamma(ab) = 2$ car $(ab)^2 = a^2b^2 = a^2b^2 = a^4 = 1$. Et si $ab = a^k$, alors $b = a^{k-1}$, ce qui contredit $b \notin< a >$.
   En conclusion soit b est d'ordre 2, soit b^2 est d'ordre 2 et $b^2 \in G\backslash < a >$, soit $b^2 \in< a >$, mais alors $ab \notin< a >$ est d'ordre 2.
   (b) Si G est abélien, on vérifie comme précédemment que l'application ne dépend pas des représentants p et q des classes d'équivalences $\bar{p}$ modulo 4 et $\dot{q}$ modulo 2. De plus, l'image de ce morphisme est un sous-groupe qui contient au moins 5 éléments : ceux de $< a >$ et b. Comme G a 8 éléments, la seule possibilité est 8 d'après le théorème de Lagrange. Donc φ est surjective. Et comme les deux ensembles ont le même nombre éléments, on en déduit que φ est injective.

Exercice 7. Le groupe $\mathfrak{Q}$ des quaternions (\四元群\) est le groupe engendré par deux éléments distincts i et j dont on note l'élément neutre e (différent de i et j) et qui vérifie en posant $k = ij$ et $m = i^2 \neq e$

$$i^4 = j^4 = e, \ i^2 = j^2 = m, \ k = ij = mji.$$

On a par exemple $k^2 = mjiij = mj^4 = m$.

1. Montrer que $\mathfrak{Q} = \{e, m, i, i^3, j, j^3, k, k^3\}$ est stable par multiplication : on écrira le tableau de multiplication des éléments de $\mathfrak{Q}$

$\circ$	e	m	i	i^3	j	j^3	k	k^3
e	e	m	i	i^3	j	j^3	k	k^3
m	m							
i	i							
i^3	i^3							
j	j							
j^3	j^3							
k	k							
k^3	k^3							

.

2. Vérifier que $\mathfrak{Q}$ est un groupe (on admettra que la loi est associative !).
3. Combien a-t-il d'éléments ?

4. Est-il commutatif ?

---

1. On trouve

$\circ$	e	m	i	i^3	j	j^3	k	k^3
e	e	m	i	i^3	j	j^3	k	k^3
m	m	e	i^3	i	j^3	j	k^3	k
i	i	i^3	m	e	k	k^3	j^3	j
i^3	i^3	i	e	m	k^3	k	j	j^3
j	j	j^3	k^3	k	m	e	i	i^3
j^3	j^3	j	k	k^3	e	m	i^3	i
k	k	k^3	j	j^3	i^3	i	m	e
k^3	k^3	k	j^3	j	i	i^3	e	m

.

   La loi est bien stable dans $\mathfrak{Q}$.

2. Tout élément est inversible. Il reste encore à montrer que la loi est associative. Vous pouvez le faire si vous le souhaitez !
3. Comme $\mathfrak{Q}$ est un groupe, $i \neq j$ et $m \neq e$, alors $i \neq i^3$ car sinon, $i^2 = m = e$. $k = ij \neq i$ car sinon $j = e$. $i \neq j^3 = mj = i^2j$, car sinon $m = ij = e$. On vérifie ainsi que les éléments sont deux à deux distincts. Le groupe des quaternions a 8 éléments.
4. Le groupe n'est pas abélien car $ij = ji = mji$ implique $m = e$.