DS 3

Les calculatrices sont interdites.

Un exercice : racines cubiques rationnelles

1°) Soient $a \in \mathbb{N}$ et $b \in \mathbb{N}^*$. Établir que, si b^3 divise a^3, alors b divise a et $\dfrac{a^3}{b^3}$ est le cube d'un entier naturel.

2°) Soit $m \in \mathbb{N}$. Démontrer que $\sqrt[3]{m}$ est rationnel si et seulement si m est le cube d'un entier naturel.

Un problème sur les mots

Notations. Dans tout le problème, on fixe un ensemble A, appelé *alphabet*, dont les éléments sont appelés des *lettres*. Si $n \in \mathbb{N}$ avec $n \geq 2$ et si $a_1, \ldots, a_n \in A$, le n-uplet $(a_1, a_2, \ldots, a_n)$ est noté $a_1 a_2 \ldots a_n$: c'est le *mot* de longueur n dont les lettres sont $a_1, \ldots, a_n$.
On convient de l'existence du *mot vide*, noté ε, ne possédant aucune lettre ; sa longueur est 0. On pose $A^0 = \{\varepsilon\}$, $A^1 = A$ et $A^* = \bigcup_{n \in \mathbb{N}} A^n$: A^* est l'ensemble des mots écrits avec l'alphabet A. La longueur d'un mot u est notée $|u|$.
Si $u = a_1 \ldots a_p$ et $w = b_1 \ldots b_q$ sont deux mots, on dit que u est un *préfixe* de w lorsque $p \leq q$ et $a_i = b_i$ pour tout $i \in \{1, \ldots, p\}$; en particulier, ε est un préfixe de tout mot.
On dit que deux mots sont *p-comparables* lorsque l'un est un préfixe de l'autre.
Les parties **I** et **II** sont indépendantes.

Partie I : Ordre lexicographique

Si $(E, \leq_E)$ est un ensemble ordonné, on note $<_E$ la relation d'ordre strict associée : pour $x, y \in E$, $x <_E y$ signifie que $x \leq_E y$ et $x \neq y$. On rappelle que $<_E$ est transitive.
Dans toute cette partie, on fixe deux ensembles ordonnés $(A, \leq_A)$ et $(B, \leq_B)$. On définit une relation $\leq_{\text{lex}}$ sur $A \times B$ en posant, pour tous $(a, b), (a', b') \in A \times B$:

$$(a, b) \leq_{\text{lex}} (a', b') \quad \Longleftrightarrow \quad a <_A a' \text{ ou } (a = a' \text{ et } b \leq_B b').$$

On dit que $\leq_{\text{lex}}$ est l'*ordre lexicographique* sur $A \times B$.

1°) **1.a)** Montrer que $\leq_{\text{lex}}$ est une relation d'ordre sur $A \times B$.

1.b) Montrer que, si $\leq_A$ et $\leq_B$ sont des ordres totaux, alors $\leq_{\text{lex}}$ est un ordre total.

1.c) Dans cette sous-question uniquement, $A = B = \mathbb{N}^*$, muni de la relation de divisibilité. Donner deux éléments de $\mathbb{N}^* \times \mathbb{N}^*$ dont aucun n'est inférieur à l'autre pour $\leq_{\text{lex}}$.

2°) Ordre lexicographique sur A^n

Soit $n \in \mathbb{N}^*$. Pour tous mots $u = a_1 \dots a_n$ et $v = b_1 \dots b_n$ de A^n, on convient que $u \leq_n v$ si et seulement si $u = v$ ou il existe $k \in \{1, \dots, n\}$ tel que $a_i = b_i$ pour tout $i \in \{1, \dots, k-1\}$ et $a_k <_A b_k$.

2.a) On note φ_n l'application de A^{n+1} dans $A \times A^n$ définie par

$$\varphi_n(a_1 a_2 \dots a_{n+1}) = (a_1, a_2 \dots a_{n+1}),$$

et l'on note $\leq_{\text{lex}}$ l'ordre lexicographique sur $A \times A^n$ construit à partir de $\leq_A$ et de $\leq_n$, défini comme ci-dessus. Montrer que φ_n est bijective et que, pour tous $u, v \in A^{n+1}$,

$$u \leq_{n+1} v \quad \Longleftrightarrow \quad \varphi_n(u) \leq_{\text{lex}} \varphi_n(v).$$

2.b) En déduire que $\leq_n$ est une relation d'ordre sur A^n, totale lorsque $\leq_A$ est total.

3°) Ordre lexicographique sur A^*

Pour tous mots $u = a_1 \dots a_p$ et $v = b_1 \dots b_q$ de A^* et tout entier k, on écrit $u \prec_k v$ si et seulement si

- $1 \leq k \leq \min(p, q)$,
- pour tout $i \in \{1, \dots, k-1\}$, $a_i = b_i$,
- et $a_k <_A b_k$.

On pose $u \leq_* v$ lorsque u est un préfixe de v ou lorsqu'il existe un entier k tel que $u \prec_k v$.

3.a) Soient $u, v \in A^*$ et $k \in \mathbb{N}$ tels que $u \prec_k v$. Montrer que les mots u et v ne sont pas p-comparables.
Montrer que $\leq_*$ est une relation d'ordre sur A^*.

3.b) Montrer que, si $\leq_A$ est total, alors $\leq_*$ est total.

Il est clair (et on ne demande pas de le démontrer) que, pour tout $n \in \mathbb{N}^*$, la restriction de $\leq_*$ à A^n est égale à $\leq_n$.

4°) Ordres bien fondés

Un ordre $\leq_E$ sur un ensemble E est dit *bien fondé* lorsque toute partie non vide P de E possède un minimum.

4.a) On suppose que $\leq_E$ est un ordre bien fondé sur l'ensemble E.
Montrer que $\leq_E$ est un ordre total.

4.b) On suppose que $\leq_A$ et $\leq_B$ sont bien fondés.
Montrer que $\leq_{\text{lex}}$ est bien fondé sur $A \times B$.

4.c) On suppose que $\leq_A$ est bien fondé.
Montrer que $\leq_n$ est bien fondé pour tout $n \in \mathbb{N}^*$.

4.d) Lorsque $\leq_A$ est bien fondé, l'ordre $\leq_*$ sur A^* est-il bien fondé ?

5°) Bornes supérieures
Dans cette question, $A = [0, 1]$ et B est un intervalle de $\mathbb{R}$, tous deux munis de l'ordre usuel.

5.a) Lorsque $B = [0, 1]$, est-ce que toute partie non vide de $A \times B$ possède une borne supérieure pour $\leq_{\text{lex}}$?

5.b) Lorsque $B =]0, 1]$, est-ce que toute partie non vide de $A \times B$ possède une borne supérieure pour $\leq_{\text{lex}}$?

Partie II : Un groupe de mots

Si $u = a_1 \dots a_p$ et $v = b_1 \dots b_q$ sont deux mots de A^*, on appelle *concaténation* de u et v le mot $uv = a_1 \dots a_p b_1 \dots b_q$, de longueur $p + q$. En particulier, $u\varepsilon = \varepsilon u = u$.
Pour tout $n \in \mathbb{N}$, on note u^n le mot $uu \dots u$ obtenu en concaténant n copies de u. En particulier, $u^0 = \varepsilon$.

6°) 6.a) Montrer que la concaténation est une loi interne sur A^*, associative et possédant un élément neutre. Est-elle commutative ?

6.b) On suppose que $A \neq \emptyset$. $(A^*, \cdot)$ est-il un groupe ?

Lorsque $u, w \in A^*$, il est clair que u est un préfixe de w si et seulement s'il existe $v \in A^*$ tel que $w = uv$. On ne demande pas de le démontrer, pas plus que le résultat suivant : pour tous $u, v, v' \in A^*$, si $uv = uv'$, alors $v = v'$.

Pour tous $u, v \in A^*$, on écrit $u \longrightarrow v$ lorsqu'il existe $x, y \in A^*$ et $a \in A$ tels que $u = xaay$ et $v = xy$: le mot v s'obtient en effaçant dans u deux lettres identiques consécutives.
On écrit $u \, R \, v$ lorsqu'il existe $n \in \mathbb{N}$ et des mots $w_0, w_1, \dots, w_n$ tels que $w_0 = u$, $w_n = v$ et, pour tout $j \in \{0, \dots, n-1\}$, $w_j \longrightarrow w_{j+1}$ ou $w_{j+1} \longrightarrow w_j$.

7°) 7.a) On suppose que A contient deux lettres distinctes a et b.
Vérifier que $baabbbab \, R \, abaa$.

7.b) Montrer que R est une relation d'équivalence sur A^*.

7.c) Soient $u, u', v \in A^*$ tels que $u \, R \, u'$. Montrer que $uv \, R \, u'v$ et $vu \, R \, vu'$.
En déduire que, pour tous $u, u', v, v' \in A^*$, si $u \, R \, u'$ et $v \, R \, v'$, alors $uv \, R \, u'v'$.

On note $G = A^*/R$ l'ensemble des classes d'équivalence pour R, et pour tout $u \in A^*$, on note $\overline{u}$ la classe d'équivalence du mot u.

8°) 8.a) Montrer que l'on définit une loi interne sur G en posant $\overline{u} \cdot \overline{v} = \overline{uv}$ pour tous $u, v \in A^*$.

8.b) Montrer que $(G, \cdot)$ est un groupe.

Un mot $w \in A^*$ est dit *réduit* lorsqu'il n'existe pas de $x, y \in A^*$ et de $a \in A$ tels que $w = xaay$.

9°) Soit $w \in A^*$. On suppose que w est réduit.
Montrer que tout préfixe de w est réduit.

Lorsque $a \in A$, on note T_a l'application de A^* dans A^* définie par : pour tout $w \in A^*$, s'il existe $w' \in A^*$ tel que $w = w'a$, alors $T_a(w) = w'$, et sinon, alors $T_a(w) = wa$. Ainsi, T_a efface la dernière lettre de w si c'est un a, et ajoute un a à la fin de w sinon.

10°) Montrer qu'il existe une unique application ρ de A^* dans A^* vérifiant : $\rho(\varepsilon) = \varepsilon$ et, pour tous $u \in A^*$ et $a \in A$, $\rho(ua) = T_a(\rho(u))$.

11°) Soient $a \in A$ et w un mot réduit.
Montrer que $T_a(w)$ est réduit et que $T_a(T_a(w)) = w$.

12°) Montrer que, pour tout $u \in A^*$, $\rho(u)$ est réduit.
Montrer que, pour tout $u \in A^*$, si u est un mot réduit, alors $\rho(u) = u$.

13°) Pour tout $u \in A^*$, montrer que $u \, R \, \rho(u)$.

14°) Montrer que, pour tous $u, v \in A^*$, $\rho(uv) = \rho(\rho(u)v)$.

15°) En déduire que, pour tous $u, v \in A^*$, $u \, R \, v$ si et seulement si $\rho(u) = \rho(v)$.

16°) Montrer que chaque classe d'équivalence pour R contient un unique mot réduit.
Lorsque A contient au moins deux lettres distinctes, montrer que le groupe G n'est pas commutatif.