DS 3 : un corrigé

Barème

Le barème comporte 70 points :

- **Exercice (4 points)** : 2,2.
- **Partie 1 (34 points)** : 2+1+1,3+2,1+4+1,1+2+3+2,6+5.
- **Partie 2 (32 points)** : 1+2,1+2+2,1+2,1,3,3,3,2,3,4,2.

Un exercice : racines cubiques rationnelles

1°) ◇ Si $a = 0$, alors b divise a et $\dfrac{a^3}{b^3} = 0 = 0^3$ est un cube parfait.

◇ Supposons que $a \neq 0$ et que b^3 divise a^3. Pour tout nombre premier p, on a alors $v_p(a^3) \geq v_p(b^3)$, c'est-à-dire $3v_p(a) \geq 3v_p(b)$, ou encore $v_p(a) \geq v_p(b)$. D'après la caractérisation de la divisibilité par les valuations p-adiques, b divise a.

Dès lors, $\dfrac{a}{b} \in \mathbb{N}$, donc $\dfrac{a^3}{b^3} = \left(\dfrac{a}{b}\right)^3$ est un cube parfait.

En conclusion, $\boxed{\text{si } b^3 \text{ divise } a^3, \text{ alors } b \text{ divise } a \text{ et } \dfrac{a^3}{b^3} \text{ est un cube parfait}}$.

2°) ◇ Si m est un cube parfait, il existe $k \in \mathbb{N}$ tel que $m = k^3$. Alors $\sqrt[3]{m} = k$ est un entier, donc, a fortiori, un rationnel.

◇ Réciproquement, supposons que $\sqrt[3]{m}$ soit rationnel. Comme $\sqrt[3]{m} \geq 0$, il existe $a \in \mathbb{N}$ et $b \in \mathbb{N}^*$ tels que $\sqrt[3]{m} = \dfrac{a}{b}$. En élevant au cube, il vient $mb^3 = a^3$, ce qui montre que b^3 divise a^3. D'après la question précédente, $m = \dfrac{a^3}{b^3}$ est un cube parfait.

En conclusion, $\boxed{\sqrt[3]{m} \in \mathbb{Q} \text{ si, et seulement si, } m \text{ est un cube parfait}}$.

Un problème sur les mots

Partie I : Ordre lexicographique

1°) 1.a) ◇ *Réflexivité.* Soit $(a, b) \in A \times B$. On a $a = a$ et $b \leq_B b$, donc $(a, b) \leq_{\text{lex}} (a, b)$.

◇ *Antisymétrie.* Soient $(a, b), (a', b') \in A \times B$ tels que $(a, b) \leq_{\text{lex}} (a', b')$ et

$(a',b') \leq_{\text{lex}} (a,b)$. Dans les deux cas de la définition, $a \leq_A a'$; de même, $a' \leq_A a$, donc $a = a'$ par antisymétrie de $\leq_A$. Alors $\neg(a <_A a')$ et $\neg(a' <_A a)$, donc $b \leq_B b'$ et $b' \leq_B b$, puis $b = b'$. Ainsi $(a,b) = (a',b')$.
$\diamond$ *Transitivité.* Soient $(a,b),(a',b'),(a'',b'') \in A \times B$ tels que $(a,b) \leq_{\text{lex}} (a',b')$ et $(a',b') \leq_{\text{lex}} (a'',b'')$.
Si $a = a' = a''$, alors $b \leq_B b' \leq_B b''$, donc $(a,b) \leq_{\text{lex}} (a'',b'')$. Sinon, on a $a \leq_A a' \leq_A a''$, donc $a \leq_A a''$, et $a \neq a''$: en effet, si $a = a''$, alors $a \leq_A a' \leq_A a$, donc $a = a' = a''$ par antisymétrie, ce qui est exclu. Ainsi $a <_A a''$, donc $(a,b) \leq_{\text{lex}} (a'',b'')$.
Par conséquent, $\boxed{\leq_{\text{lex}} \text{ est une relation d'ordre sur } A \times B}$.

1.b) Supposons que $\leq_A$ et $\leq_B$ sont des ordres totaux.
Soient $(a,b),(a',b') \in A \times B$. Si $a \neq a'$, comme $\leq_A$ est total, $a <_A a'$ ou $a' <_A a$, donc $(a,b) \leq_{\text{lex}} (a',b')$ ou $(a',b') \leq_{\text{lex}} (a,b)$. Si $a = a'$, comme $\leq_B$ est total, $b \leq_B b'$ ou $b' \leq_B b$, d'où la même conclusion. Ainsi, $\boxed{\leq_{\text{lex}} \text{ est total}}$.

1.c) 2 ne divise pas 3 et 3 ne divise pas 2, donc ni $2 < 3$, ni $3 < 2$, ni $2 = 3$ au sens de la divisibilité : $\boxed{(2,1) \text{ et } (3,1) \text{ ne sont pas comparables pour } \leq_{\text{lex}}}$.

2°) 2.a) $\diamond$ Notons Ψ_n l'application de $A \times A^n$ dans A^{n+1} définie par : pour tout $a_1,\ldots,a_{n+1} \in A$, $\Psi_n(a_1,a_2\ldots a_{n+1}) = a_1a_2\ldots a_{n+1}$. Il est clair que $\varphi_n \circ \Psi_n = Id_{A\times A^n}$ et $\Psi_n \circ \varphi_n = Id_{A^{n+1}}$, donc φ_n est une bijection, dont Ψ_n est la bijection réciproque.
$\diamond$ Soient $u = a_1\ldots a_{n+1}$ et $v = b_1\ldots b_{n+1}$ dans A^{n+1}. Posons $u' = a_2\ldots a_{n+1}$ et $v' = b_2\ldots b_{n+1}$, de sorte que $\varphi_n(u) = (a_1,u')$ et $\varphi_n(v) = (b_1,v')$. Ainsi, pour tout $j \in \mathbb{N}_n$, les j-èmes lettres de u' et v' sont a_{j+1} et b_{j+1}.
Supposons que $u \leq_{n+1} v$. Si $u = v$, alors $a_1 = b_1$ et $u' = v'$, donc $\varphi_n(u) \leq_{\text{lex}} \varphi_n(v)$.
Sinon, il existe $k \in \{1,\ldots,n+1\}$ tel que $a_i = b_i$ pour tout $i \in \{1,\ldots,k-1\}$ et $a_k <_A b_k$. Si $k = 1$, alors $a_1 <_A b_1$, donc $\varphi_n(u) \leq_{\text{lex}} \varphi_n(v)$.
Si $k \geq 2$, alors $a_1 = b_1$, $a_{j+1} = b_{j+1}$ pour $j \in \{1,\ldots,k-2\}$ et $a_k <_A b_k$, donc $u' \leq_n v'$. Ainsi, dans tous les cas, $\varphi_n(u) \leq_{\text{lex}} \varphi_n(v)$.
Réciproquement, supposons que $\varphi_n(u) \leq_{\text{lex}} \varphi_n(v)$. Si $a_1 <_A b_1$, alors $u \leq_{n+1} v$.
Sinon, $a_1 = b_1$ et $u' \leq_n v'$: si $u' = v'$, alors $u = v$; sinon, il existe $j \in \{1,\ldots,n\}$ tel que $a_{i+1} = b_{i+1}$ pour $i < j$ et $a_{j+1} <_A b_{j+1}$. On a encore $u \leq_{n+1} v$.
Ainsi, dans tous les cas, $u \leq_{n+1} v$.
On a bien montré que $\boxed{u \leq_{n+1} v \iff \varphi_n(u) \leq_{\text{lex}} \varphi_n(v)}$.

2.b) Raisonnons par récurrence. Pour $n \in \mathbb{N}^*$, notons $R(n)$ l'assertion : $\leq_n$ est un ordre sur A^n, total lorsque $\leq_A$ est un ordre total.
Pour $n = 1$: d'après l'énoncé, $A^1 = A$, donc pour tout $u,v \in A^1$, $u \leq_1 v$ signifie $u = v$ ou $u <_A v$, c'est-à-dire $u \leq_A v$. Ainsi, $\leq_1$ est l'ordre $\leq_A$ et $R(1)$ est donc vraie.
Soit $n \in \mathbb{N}^*$. Supposons que $\leq_n$ soit un ordre sur A^n, total lorsque $\leq_A$ l'est. D'après 1.a et 1.b, appliquées aux ensembles ordonnés $(A,\leq_A)$ et $(A^n,\leq_n)$, $\leq_{\text{lex}}$ est un ordre sur $A \times A^n$, total lorsque $\leq_A$ l'est.
Comme φ_n est bijective et que $u \leq_{n+1} v \iff \varphi_n(u) \leq_{\text{lex}} \varphi_n(v)$, les propriétés de réflexivité, de transitivité et de totalité se transportent de $\leq_{\text{lex}}$ à $\leq_{n+1}$.
Pour l'antisymétrie : soit $u,v \in A^{n+1}$ tels que $u \leq_{n+1} v$ et $v \leq_{n+1} u$.
Alors $\varphi_n(u) = \varphi_n(v)$, donc $u = v$ par injectivité de φ_n. Ceci prouve $R(n+1)$.

Ainsi, d'après le principe de récurrence,
$\boxed{\text{pour tout } n \in \mathbb{N}^*,\ \leq_n \text{ est un ordre sur } A^n, \text{ total lorsque } \leq_A \text{ l'est}}$.

3°) Pour cette question, on fixe une fois pour toutes trois mots de A^*, notés $u = a_1 \dots a_p$, $v = b_1 \dots b_q$ et $w = c_1 \dots c_r$.

3.a) $\diamond$ $u \prec_k v$, donc $1 \leq k \leq \min(p, q)$ et $a_k \neq b_k$. Si u était un préfixe de v, on aurait $a_k = b_k$ puisque $k \leq p$; de même, v n'est pas un préfixe de u.
Ainsi, $\boxed{\text{si } u \prec_k v,\ u \text{ et } v \text{ ne sont pas p-comparables}}$.
$\diamond$ *Réflexivité.* u est un préfixe de u, donc $u \leq_* u$.
$\diamond$ *Antisymétrie.* Supposons $u \leq_* v$ et $v \leq_* u$.
Supposons qu'il existe $k \in \mathbb{N}$ tel que $u \prec_k v$. Alors v n'est pas un préfixe de u d'après ce qui précède, or $v \leq_* u$, donc il existe $l \in \mathbb{N}$ tel que $v \prec_l u$. Si $l < k$, $b_l <_A a_l$ contredit $a_l = b_l$; si $k < l$, $a_k <_A b_k$ contredit $a_k = b_k$; si $k = l$, $a_k <_A b_k <_A a_k$ contredit l'antisymétrie de $\leq_A$. Ainsi, il n'existe aucun $k \in \mathbb{N}$ tel que $u \prec_k v$. Or $u \leq_* v$, donc u est un préfixe de v. De même v est un préfixe de u. Ainsi, $p \leq q \leq p$, donc $p = q$ et $u = v$.
$\diamond$ *Transitivité.* Supposons $u \leq_* v$ et $v \leq_* w$.
Premier cas : On suppose que u est un préfixe de v et que v est un préfixe de w.
Alors $p \leq q \leq r$ et $a_i = b_i = c_i$ pour $i \leq p$: u est un préfixe de w, donc $u \leq_* w$.
Second cas : On suppose que u est un préfixe de v et qu'il existe $l \in \mathbb{N}$ tel que $v \prec_l w$.
Si $l \leq p$, alors $a_i = b_i = c_i$ pour $i < l$ et $a_l = b_l <_A c_l$, donc $u \prec_l w$.
Si $l > p$, alors $a_i = b_i = c_i$ pour $i \leq p$ et $p < l \leq r$, donc u est un préfixe de w.
Dans les deux sous-cas, $u \leq_* w$.
Troisième cas : On suppose qu'il existe $k \in \mathbb{N}$ tel que $u \prec_k v$ et que v est un préfixe de w. Alors $k \leq q \leq r$, $a_i = b_i = c_i$ pour $i < k$ et $a_k <_A b_k = c_k$, donc $u \prec_k w$ et $u \leq_* w$.
Dernier cas : On suppose qu'il existe $k, l \in \mathbb{N}$ tels que $u \prec_k v$ et $v \prec_l w$.
Posons $m = \min(k, l)$. Pour $i < m$, $a_i = b_i = c_i$.
Si $k < l$ alors $a_k <_A b_k = c_k$, donc $a_m <_A c_m$.
Si $l < k$, alors $a_l = b_l <_A c_l$ donc $a_m <_A c_m$.
Enfin, si $k = l$, $a_k <_A b_k <_A c_k$, donc $a_m <_A c_m$.
Ainsi, dans tous les sous-cas, $a_i = c_i$ pour tout $i \in \{1, \dots, m-1\}$ et $a_m <_A c_m$. Or $m \leq \min(p, r)$, donc $u \prec_m w$, puis $u \leq_* w$.
Dans tous les cas, $u \leq_* w$, ce qui prouve la transitivité.
En conclusion, $\boxed{\leq_* \text{ est une relation d'ordre sur } A^*}$.

3.b) Supposons que $\leq_A$ soit total. Notons $m = \min(p, q)$. Si $a_i = b_i$ pour tout $i \leq m$, le plus court des deux mots u et v est un préfixe de l'autre, donc $u \leq_* v$ ou $v \leq_* u$. Sinon, $\{i \in \mathbb{N}_m \ / \ a_i \neq b_i\}$ est non vide, donc il possède un minimum noté k. Comme $\leq_A$ est total, $a_k <_A b_k$ ou $b_k <_A a_k$, c'est-à-dire $u \prec_k v$ ou $v \prec_k u$.
Ainsi, $\boxed{\leq_* \text{ est total}}$.

4°) 4.a) Soit $a, b \in E$. L'ensemble $\{a, b\}$ est une partie non vide de E, donc il possède un minimum, noté m. Si $m = a$, alors $a \leq_E b$. Si $m = b$, alors $b \leq_E a$. Ceci prouve que $\leq_E$ est un ordre total.

4.b) Soit P une partie non vide de $A \times B$. La partie $P_1 = \{a \in A \ / \ \exists b \in B,\ (a,b) \in P\}$ de A n'est pas vide, or $\leq_A$ est bien fondé, donc P_1 possède un minimum, noté a_0. La partie $Q = \{b \in B \ / \ (a_0,b) \in P\}$ de B n'est pas vide, or $\leq_B$ est bien fondé, donc Q possède un minimum, noté b_0.
Soit $(a,b) \in P$. Alors $a \in P_1$, donc $a_0 \leq_A a$.
Si $a_0 <_A a$, alors $(a_0,b_0) \leq_{\text{lex}} (a,b)$.
Sinon, alors $a = a_0$, donc $b \in Q$. Ainsi, $b_0 \leq_B b$, donc on a encore $(a_0,b_0) \leq_{\text{lex}} (a,b)$.
De plus, $(a_0,b_0) \in P$, donc (a_0,b_0) est le minimum de P.
Ceci prouve que toute partie non vide de $A \times B$ possède un minimum pour $\leq_{\text{lex}}$, donc ce dernier est un ordre bien fondé.

4.c) Raisonnons par récurrence : soit $n \in \mathbb{N}^*$.
Notons $R(n)$ l'assertion : $\leq_n$ est bien fondé sur A^n.
Pour $n = 1$, $\leq_1 = \leq_A$ est bien fondé.
Supposons $\leq_n$ bien fondé, et soit P une partie non vide de A^{n+1}.
D'après 4.b, appliquée à $(A, \leq_A)$ et $(A^n, \leq_n)$, $(A \times A^n, \leq_{\text{lex}})$ est bien fondé, donc la partie non vide $\varphi_n(P)$ de $A \times A^n$ possède un minimum, que l'on peut noter $\varphi_n(m)$ avec $m \in P$.
Soit $p \in P$. Alors $\varphi_n(p) \in \varphi_n(P)$, donc $\varphi_n(m) \leq_{\text{lex}} \varphi_n(p)$. Alors, d'après 2.a, $m \leq_{n+1} p$, ce qui prouve $R(n+1)$.

4.d) Lorsque $\leq_A$ est bien fondé, l'ordre $\leq_*$ sur A^* n'est pas toujours bien fondé, ainsi que le montre le contre-exemple suivant : prenons $A = \mathbb{N}$, muni de son ordre usuel, qui est bien fondé d'après le cours.
Pour $k \in \mathbb{N}$, notons $w_k = 0^k 1$ le mot formé de k lettres 0 suivies d'une lettre 1.
Soit $k \in \mathbb{N}$: les mots w_{k+1} et w_k ont les mêmes k premières lettres, et leurs lettres de rang $k+1$ sont 0 et 1, donc $w_{k+1} \prec_{k+1} w_k$, puis $w_{k+1} <_* w_k$ (ces mots sont distincts).
La partie non vide $P = \{w_k \ / \ k \in \mathbb{N}\}$ n'a donc pas de minimum.

5°) 5.a) Soit P une partie non vide de $A \times B = [0,1]^2$.
$\diamond$ Notons $P_1 = \{x \in [0,1] \ / \ \exists y \in [0,1],\ (x,y) \in P\}$. C'est une partie non vide et majorée de $\mathbb{R}$, donc d'après la propriété de la borne supérieure, P_1 possède une borne supérieure, que l'on notera α.
$P_1 \subset [0,1]$, donc d'après le cours, $\alpha = \sup(P_1) \leq \sup([0,1]) = 1$. De plus, il existe $p \in P_1$. $p \geq 0$, donc $\alpha \geq p \geq 0$. Ainsi, $\alpha \in [0,1]$.
$\diamond$ Remarquons que, si $(a,b) \in [0,1]^2$ est un majorant de P, alors $\alpha \leq a$.
En effet, soit $p \in P_1$. Il existe $y \in [0,1]$ tel que $(p,y) \in P$. Alors $(p,y) \leq_{\text{lex}} (a,b)$, donc $p \leq a$. Ainsi, a est un majorant de P_1, donc par définition de la borne supérieure, $\alpha \leq a$ (par la suite, un tel raisonnement sera appelé un passage à la borne supérieure).
$\diamond$ *Premier cas :* supposons que $\alpha \in P_1$.
Posons $Q = \{y \in [0,1] \ / \ (\alpha,y) \in P\}$. Q est une partie non vide de $[0,1]$. Comme on l'a fait pour P_1, on en déduit que Q admet une borne supérieure, notée β, avec $\beta \in [0,1]$.
Posons $M = (\alpha,\beta) \in [0,1]^2$ et montrons que M est la borne supérieure de P.
Soit $(x,y) \in P$. Alors $x \in P_1$, donc $x \leq \alpha$.
Si $x < \alpha$, alors $(x,y) <_{\text{lex}} M$.

Si $x = \alpha$, alors $y \in Q$, donc $y \leq \beta$ et $(x, y) \leq_{\text{lex}} M$.
Ainsi M est un majorant de P.
Soit (a, b) un autre majorant de P. D'après la remarque précédente, $\alpha \leq a$.
Si $\alpha < a$, $M \leq_{\text{lex}} (a, b)$.
Sinon, alors $\alpha = a$. Pour tout $y \in Q$, $(\alpha, y) \leq_{\text{lex}} (\alpha, b)$, donc $y \leq b$; ainsi, par passage à la borne supérieure, $\beta = \sup(Q) \leq b$, et $M \leq_{\text{lex}} (a, b)$.
Ceci prouve que M est le plus petit des majorants de P,
donc M est la borne supérieure de P.
$\diamond$ *Second cas :* supposons que $\alpha \notin P_1$.
Posons $M = (\alpha, 0)$ et montrons que M est la borne supérieure de P.
Si $(x, y) \in P$, alors $x \leq \alpha$ et $x \neq \alpha$, donc $(x, y) <_{\text{lex}} M$. Donc M majore P.
Soit (a, b) un majorant de P. Alors d'après la remarque précédente, $\alpha \leq a$, donc $M = (\alpha, 0) \leq_{\text{lex}} (a, b)$. Ainsi, M est la borne supérieure de P.
En conclusion, on a prouvé que toute partie non vide de $[0, 1]^2$ possède une borne supérieure.

5.b) Posons $P = \left\{(x, 1) \ / \ x \in \left[0, \frac{1}{2}\right[\right\}$. P est non vide. Montrons que P ne possède pas de borne supérieure, ce qui répond négativement à la question de l'énoncé.
$\diamond$ Montrons qu'un élément (a, b) de $A \times B$ majore P si et seulement si $a \geq \frac{1}{2}$.
Si $a \geq \frac{1}{2}$, pour tout $x \in \left[0, \frac{1}{2}\right[$, $x < a$, donc $(x, 1) <_{\text{lex}} (a, b)$, donc (a, b) est un majorant de P.
Si $a < \frac{1}{2}$, posons $x = \frac{1}{2}\left(a + \frac{1}{2}\right)$: x est le milieu de a et du réel $\frac{1}{2}$, donc $x \in \left]a, \frac{1}{2}\right[$.
Ainsi $(x, 1) \in P$ et $(a, b) <_{\text{lex}} (x, 1)$, donc (a, b) ne majore pas P, ce qui conclut.
$\diamond$ Supposons que P possède une borne supérieure notée (a, b). C'est un majorant, donc $a \geq \frac{1}{2}$. Comme $\left(\frac{1}{2}, 1\right)$ majore P, $(a, b) \leq_{\text{lex}} \left(\frac{1}{2}, 1\right)$, donc $a \leq \frac{1}{2}$. Ainsi, $a = \frac{1}{2}$.
Mais $b > 0$, donc $\left(\frac{1}{2}, \frac{b}{2}\right)$ est aussi un majorant de P et $\left(\frac{1}{2}, \frac{b}{2}\right) <_{\text{lex}} \left(\frac{1}{2}, b\right)$, ce qui est absurde. Ainsi, $\boxed{P \text{ n'a pas de borne supérieure}}$.

Partie II : Un groupe de mots

6°) 6.a) $\diamond$ La concaténation de deux mots de A^* est un mot de A^*, donc la concaténation est une loi interne sur A^*.
$\diamond$ Soient $u = a_1 \dots a_p$, $v = b_1 \dots b_q$ et $w = c_1 \dots c_r$ trois mots de A^*. Les mots $(uv)w$ et $u(vw)$ sont tous deux égaux au mot $a_1 \dots a_p b_1 \dots b_q c_1 \dots c_r$ de longueur $p+q+r$, même lorsque certains des entiers p, q, r sont nuls, donc la concaténation est associative.
$\diamond$ D'après l'énoncé, $u\varepsilon = \varepsilon u = u$, donc ε est l'élément neutre pour la concaténation.
$\diamond$ Lorsque A possède au moins deux éléments distincts, notés a et b, alors $ab \neq ba$, donc la concaténation n'est pas commutative.

Lorsque A possède une seule lettre notée a, alors $A^* = \{a^n \ / \ n \in \mathbb{N}\}$, or il est clair que, pour tout $n, m \in \mathbb{N}$, $a^{n+m} = a^n a^m = a^m a^n$, donc la concaténation est une loi commutative dans ce cas particulier.
Lorsque $A = \emptyset$, alors $A^* = \{\varepsilon\}$ et la concaténation est encore commutative.

6.b) Pour tous $u, v \in A^*$, $|uv| = |u| + |v|$. Soit $a \in A$. Si a possédait un symétrique v, on aurait $av = \varepsilon$, donc $1 + |v| = 0$, ce qui est absurde.
Ainsi, $\boxed{(A^*, \cdot) \text{ n'est pas un groupe}}$.

7°) 7.a) $baabbbab = b(aa)bbbab \longrightarrow bbbbab = (bb)(bb)ab \longrightarrow (bb)ab \longrightarrow ab$
et $abaa = ab(aa) \longrightarrow ab$ donc $\boxed{baabbbab \, R \, abaa}$.

7.b) Soient $u, v, w \in A^*$.
$\diamond$ *Réflexivité :* Prenons $n = 0$, $w_0 = u = w_n$. Comme $\{0, \dots, n-1\}$ est vide, on a bien que, pour tout $j \in \{0, \dots, n-1\}$, $w_j \longrightarrow w_{j+1}$ ou $w_{j+1} \longrightarrow w_j$. Ainsi, $u \ R \ u$.
$\diamond$ *Symétrie :* Supposons que $u \ R \ v$. 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 $w_{j+1} \longrightarrow w_j$.
Posons, pour tout $j \in \{0, \dots, n\}$, $w'_j = w_{n-j}$. Alors $w'_0 = w_n = v$, $w'_n = w_0 = u$, et pour tout $j \in \{0, \dots, n-1\}$, $w'_j \longrightarrow w'_{j+1}$ ou $w'_{j+1} \longrightarrow w'_j$. Ceci prouve que $v \ R \ u$.
$\diamond$ *Transitivité :* On suppose que $u \ R \ v$ et $v \ R \ w$. 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 $w_{j+1} \longrightarrow w_j$. Il existe également $m \in \mathbb{N}$ et des mots $w'_0, w'_1, \dots, w'_m$ tels que $w'_0 = v$, $w'_m = w$, et pour tout $j \in \{0, \dots, m-1\}$, $w'_j \longrightarrow w'_{j+1}$ ou $w'_{j+1} \longrightarrow w'_j$.
Posons, pour tout $j \in \{1, \dots, m\}$, $w_{n+j} = w'_j$. Comme $w_n = v = w'_0$, la relation $w'_j = w_{n+j}$ est encore vraie pour $j = 0$ et, pour tout $j \in \{0, \dots, n+m-1\}$, $w_j \longrightarrow w_{j+1}$ ou $w_{j+1} \longrightarrow w_j$. Ceci démontre que $u \ R \ w$.
Ainsi, $\boxed{R \text{ est une relation d'équivalence}}$.

7.c) $\diamond$ Commençons par établir le lemme suivant : Soient $u, u', v \in A^*$ tels que $u \longrightarrow u'$. Alors $uv \longrightarrow u'v$ et $vu \longrightarrow vu'$.
En effet, $u \longrightarrow u'$, donc il existe $x, y \in A^*$ et $a \in A$ tels que $u = xaay$ et $u' = xy$. Alors $uv = xaa(yv)$ et $u'v = x(yv)$, donc $uv \longrightarrow u'v$.
De même, $vu = (vx)aay \longrightarrow (vx)y = vu'$.
$\diamond$ Soient maintenant $u, u', v \in A^*$ tels que $u \, R \, u'$.
Il existe $n \in \mathbb{N}$ et des mots $w_0, w_1, \dots, w_n$ tels que $w_0 = u$, $w_n = u'$ et, pour tout $j \in \{0, \dots, n-1\}$, $w_j \longrightarrow w_{j+1}$ ou $w_{j+1} \longrightarrow w_j$.
D'après le lemme, pour tout $j \in \{0, \dots, n-1\}$, $vw_j \longrightarrow vw_{j+1}$ ou $vw_{j+1} \longrightarrow vw_j$. De plus, $vw_0 = vu$ et $vw_n = vu'$, donc $vu \ R \ vu'$.
De même, on montre que $uv \ R \ u'v$.
$\diamond$ Soit $u, u', v, v' \in A^*$ tels que $u \, R \, u'$ et $v \, R \, v'$. Alors $uv \, R \, u'v$ et $u'v \, R \, u'v'$, donc par transitivité de R, $\boxed{uv \, R \, u'v'}$.

8°) 8.a) Soit $u, v \in A^*$. Il s'agit de vérifier que $\overline{uv}$ ne dépend que de $\overline{u}$ et $\overline{v}$.
Soit $u', v' \in A^*$ tels que $\overline{u} = \overline{u'}$ et $\overline{v} = \overline{v'}$. Alors $u \ R \ u'$ et $v \ R \ v'$, donc d'après la question précédente, $uv \, R \, u'v'$, donc $\overline{uv} = \overline{u'v'}$, ce qu'il fallait démontrer.

8.b) $\diamond$ Pour tous $u, v, w \in A^*$, $(\overline{u}\cdot\overline{v})\cdot\overline{w} = \overline{(uv)w} = \overline{u(vw)} = \overline{u}\cdot(\overline{v}\cdot\overline{w})$ et $\overline{u}\cdot\overline{\varepsilon} = \overline{\varepsilon}\cdot\overline{u} = \overline{u}$, d'après 6.a. Ainsi la loi sur G est associative et admet $\overline{\varepsilon}$ comme élément neutre.
$\diamond$ Soit $n \in \mathbb{N}$. Notons $R(n)$ l'assertion : pour tout $a_1, \dots, a_n \in A$, $a_1 \dots a_n a_n \dots a_1 \, R \, \varepsilon$.
Pour $n = 0$, $R(0) \iff \varepsilon \, R \, \varepsilon$, ce qui est vrai.
Pour $n \geq 0$, supposons $R(n)$. Soit $a_1, \dots, a_{n+1} \in A$.
Posons $x = a_1 \dots a_n$ et $y = a_n \dots a_1$. Alors $a_1 \dots a_{n+1} a_{n+1} \dots a_1 = x a_{n+1} a_{n+1} y \longrightarrow xy$, or d'après $R(n)$, $xy \, R \, \varepsilon$, donc par transitivité, $a_1 \dots a_{n+1} a_{n+1} \dots a_1 \, R \, \varepsilon$, ce qui prouve $R(n+1)$.
$\diamond$ Soit $u = a_1 \dots a_n \in A^*$. Posons $u' = a_n \dots a_1$. D'après le point précédent, $uu' \, R \, \varepsilon$, donc $\overline{\varepsilon} = \overline{uu'} = \overline{u}\cdot\overline{u'}$. De même, $u'u = a_n \dots a_1 a_1 \dots a_n \, R \, \varepsilon$, donc $\overline{u'}\cdot\overline{u} = \overline{\varepsilon}$. Ceci prouve que tout élément $\overline{u}$ de G possède un symétrique, que l'on notera $(\overline{u})^{-1}$.
On a établi que, pour tout $n \in \mathbb{N}$, pour tout $a_1, \dots, a_n \in A$, $\boxed{(\overline{a_1 \dots a_n})^{-1} = \overline{a_n \dots a_1}}$.
En conclusion, on a prouvé que $\boxed{(G, \cdot) \text{ est un groupe}}$.

9°) Soit u un préfixe de w.
D'après l'énoncé, après la question 6, il existe $v \in A^*$ tel que $w = uv$.
Supposons que u n'est pas réduit. Alors il existe $x, y \in A^*$ et $a \in A$ tels que $u = xaay$.
On en déduit que $w = xaa(yv)$, donc w n'est pas réduit, ce qui est faux. Ainsi u est réduit.

10°) *Analyse :* Supposons qu'existe une application ρ de A^* dans A^* vérifiant : $\rho(\varepsilon) = \varepsilon$ et, pour tous $u \in A^*$ et $a \in A$, $\rho(ua) = T_a(\rho(u))$.
Par récurrence sur $k \in \mathbb{N}$, on montre que, pour tous $u \in A^*$, pour tout $a_1, \dots, a_k \in A$, $\rho(ua_1 \dots a_k) = T_{a_k} \circ T_{a_{k-1}} \circ \dots \circ T_{a_1}(\rho(u))$, en convenant qu'une composée d'un nombre nul d'applications est égale à l'identité.
On en déduit que, pour tout $k \in \mathbb{N}$, $\rho(a_1 \dots a_k) = T_{a_k} \circ T_{a_{k-1}} \circ \dots \circ T_{a_1}(\varepsilon)$. Ceci prouve l'unicité de ρ sous condition d'existence.
Synthèse : Notons ρ l'application de A^* dans A^* définie par : pour tout $k \in \mathbb{N}$, pour tout $a_1, \dots, a_k \in A$, $\rho(a_1 \dots a_k) = T_{a_k} \circ T_{a_{k-1}} \circ \dots \circ T_{a_1}(\varepsilon)$.
Avec la convention précédente, on a bien $\rho(\varepsilon) = \varepsilon$ et il est clair que, pour tous $u \in A^*$ et $a \in A$, $\rho(ua) = T_a(\rho(u))$, ce qui prouve l'existence.

11°) 11.a) $\diamond$ Supposons d'abord que w est de la forme $w = w'a$, où $w' \in A^*$.
w est réduit, donc d'après la question 9, w' est aussi réduit. Or $T_a(w) = w'$, donc $T_a(w)$ est réduit.
De plus, si la dernière lettre de w' est égale à a, alors w se termine par aa, ce qui est impossible car w est réduit. Ainsi, w' ne finit pas par la lettre a, donc $T_a(w') = w'a = w$.
Dans ce cas, on a montré que $T_a(T_a(w)) = w$.
$\diamond$ Il reste à étudier le cas où w ne se termine pas par la lettre a. Alors $T_a(w) = wa$.
Supposons que wa n'est pas réduit. Alors il existe $x, y \in A^*$ et $c \in A$ tels que $wa = xccy$.
Si $y = \varepsilon$, alors $c = a$, puis $w = xc = xa$ se termine par la lettre a, ce qui est faux.
Ainsi, $y \neq \varepsilon$, et $wa = xccy$, donc il existe $y' \in A^*$ tel que $y = y'a$. Alors $w = xccy'$, ce qui est exclu car w est réduit. Ainsi, $T_a(w) = wa$ est réduit.
De plus, $T_a(T_a(w)) = T_a(wa) = w$.

En conclusion, dans tous les cas,
$\boxed{\text{lorsque } w \text{ est réduit, } T_a(w) \text{ est réduit et } T_a(T_a(w)) = w}$.

12°) Soit $n \in \mathbb{N}$. Notons $R(n)$ l'assertion suivante : pour tout $u \in A^*$ tel que $|u| = n$, $\rho(u)$ est réduit et si u est un mot réduit, alors $\rho(u) = u$.
Pour $n = 0$, $\rho(\varepsilon) = \varepsilon$ est réduit, donc $R(0)$ est vraie.
Pour $n \geq 0$, supposons $R(n)$. Soit u un mot de longueur $n+1$.
Il existe $u' \in A^*$ et $a \in A$ tels que $u = u'a$. Alors $\rho(u) = T_a(\rho(u'))$.
u' est de longueur n, donc d'après l'hypothèse de récurrence, $\rho(u')$ est réduit. Alors d'après la question précédente, $\rho(u)$ est réduit.
De plus, si l'on suppose que u est réduit, alors d'après la question 9, u' est réduit, donc d'après $R(n)$, $\rho(u') = u'$. Alors $\rho(u) = T_a(u') = T_a(T_a(u))$, donc d'après la question précédente, $\rho(u) = u$.
Ceci prouve $R(n+1)$, ce qui conclut d'après le principe de récurrence.

13°) On raisonne à nouveau par récurrence sur la longueur de u.
Soit $n \in \mathbb{N}$. Notons $R(n)$ l'assertion suivante : pour tout $u \in A^n$, $u \,R\, \rho(u)$.
Pour $n = 0$, $\rho(\varepsilon) = \varepsilon \,R\, \varepsilon$, donc $R(0)$ est vraie.
Pour $n \geq 0$, supposons $R(n)$. Soit u un mot de longueur $n+1$.
Il existe $u' \in A^*$ et $a \in A$ tels que $u = u'a$.
D'après $R(n)$, $u' \,R\, \rho(u')$. Alors, d'après 7.c, $u = u'a \,R\, \rho(u')a$.
Si $\rho(u')$ ne se termine pas par a, alors $\rho(u'a) = \rho(u')a$, donc $\rho(u) = \rho(u')a \,R\, u$.
Sinon, il existe $w' \in A^*$ tel que $\rho(u') = w'a$. Alors $\rho(u')a = w'aa \longrightarrow w'$
et $\rho(u) = \rho(u'a) = T_a(\rho(u')) = T_a(w'a) = w'$, donc on a encore $u \,R\, \rho(u)$, ce qui conclut.

14°) Soit $u \in A^*$. Soit $n \in \mathbb{N}$.
Notons $R(n)$ l'assertion suivante : pour tout $v \in A^n$, $\rho(uv) = \rho(\rho(u)v)$.
Lorsque $n = 0$: d'après la question 12, $\rho(u)$ est réduit et donc, toujours d'après la question 12, $\rho(\rho(u)) = \rho(u)$, ce qui prouve $R(0)$, avec $v = \varepsilon$.
Lorsque $n \geq 0$, supposons $R(n)$. Soit $v' \in A^{n+1}$. Il existe $a \in A$ et $v \in A^n$ tels que $v' = va$.
Alors $\rho(uva) = T_a(\rho(uv)) = T_a\Big(\rho(\rho(u)v)\Big) = \rho(\rho(u)va)$, donc $\rho(uv') = \rho(\rho(u)v')$, ce qui prouve $R(n+1)$ et permet de conclure d'après le principe de récurrence.

15°) $\diamond$ Soit $u, v \in A^*$ tels que $\rho(u) = \rho(v)$.
Alors, d'après la question 13 et la symétrie de R, $u \,R\, \rho(u) = \rho(v) \,R\, v$, donc par transitivité de R, $u \,R\, v$.
$\diamond$ Soit $u, v \in A^*$ tels que $u \longrightarrow v$.
Ainsi, il existe $x, y \in A^*$ et $a \in A$ tels que $u = xaay$ et $v = xy$.
D'après la question précédente, $\rho(u) = \rho(xaay) = \rho(\rho(xaa)y)$, or d'après la question 10, $\rho(xaa) = T_a(T_a(\rho(x)))$, mais d'après la question 12, $\rho(x)$ est réduit, donc d'après la question 11, $\rho(xaa) = \rho(x)$. Ainsi, $\rho(u) = \rho(\rho(x)y)$, puis à nouveau à l'aide de la question précédente,
$\rho(u) = \rho(xy) = \rho(v)$.
Ainsi, $u \longrightarrow v$ implique $\rho(u) = \rho(v)$.

$\diamond$ Soit $u, v \in A^*$. Supposons maintenant que $u\,R\,v$. Ainsi, il existe $n \in \mathbb{N}$ et des mots $w_0, w_1, \ldots, w_n$ tels que $w_0 = u$, $w_n = v$ et, pour tout $j \in \{0, \ldots, n-1\}$, $w_j \longrightarrow w_{j+1}$ ou $w_{j+1} \longrightarrow w_j$. Alors, d'après le point précédent,
$\rho(u) = \rho(w_0) = \rho(w_1) = \cdots = \rho(w_n) = \rho(v)$.
En conclusion, on a bien montré que, pour tout $u, v \in A^*$, $u\,R\,v \iff \rho(u) = \rho(v)$.

16°) $\diamond$ Soit $\mathcal{C}$ une classe d'équivalence de R. Il existe $u \in A^*$ tel que $\mathcal{C} = \overline{u}$. D'après la question 13, $u\,R\,\rho(u)$ donc $\rho(u) \in \mathcal{C}$, or d'après la question 12, $\rho(u)$ est réduit, donc $\mathcal{C}$ contient au moins un mot réduit.
$\diamond$ Supposons que w et w' sont deux mots réduits appartenant à $\mathcal{C}$. Alors, d'après la question précédente et la question 12, $w = \rho(w) = \rho(w') = w'$.
Ainsi, $\mathcal{C}$ contient un unique mot réduit.
$\diamond$ On suppose que A contient au moins deux lettres distinctes, notées a et b.
Les mots ab et ba ne contiennent aucun motif de la forme cc avec $c \in A$, donc ils sont réduits. Or ils sont distincts, donc ils n'appartiennent pas à la même classe d'équivalence. Ainsi, $\overline{ab} \neq \overline{ba}$, puis $\overline{a} \cdot \overline{b} \neq \overline{b} \cdot \overline{a}$, donc G n'est pas commutatif.