Exercice 1 :

1. Montrer que $(\mathcal{P}(E \times E), \circ, id_E)$, où $R \circ S := RS := \{(x, z) \in E \times E \mid \exists y \in E,\ xRySz\}$ est un monoïde.
2. A quelle condition un treillis est-il un monoïde (commutatif), si on prend la borne supérieure de deux éléments comme loi de composition interne ?
3. Montrer que le produit direct de deux monoïdes est un monoïde.
4. $(\mathbb{Z}/6\mathbb{Z}, \cdot, 1)$ est un monoïde. Montrer que $(\{0, 2, 4\}, \cdot, 4)$ est un monoïde.

Exercice 2 :

Prouver les affirmations suivantes :

1. La composée de deux morphismes de monoïdes est un morphisme.
2. La réciproque d'un morphisme de monoïdes bijectif est un morphisme de monoïde. (On parle alors d'isomorphisme.)

   Solution:
   Soit $f : M \to N$ un tel morphisme. Donc $f(e_M) = e_N$, donc $f^{-1}(e_N) = e_M$. Soit $x, y \in N$, pour montrer que $f^{-1}(xy) = f^{-1}(x)f^{-1}(y)$, il suffit de montrer qu'ils ont la même image par f. On a $f(f^{-1}(xy)) = xy = f(f^{-1}(x))f(f^{-1}(y)) = f(f^{-1}(x)f^{-1}(y))$.
3. L'image d'un sous-monoïde est un sous-monoïde.
4. L'image réciproque d'un sous-monoïde est un sous-monoïde.
5. Le noyau d'un morphisme de monoïde est un sous-monoïde.

Exercice 3 :

Soit $\sim$ une congruence sur un monoïde M. Montrer que $x \sim x' \wedge y \sim y' \Rightarrow xy \sim x'y'$.

Monoïdes libres.

Soit Σ un alphabet fini.

Exercice 4 :

Soit u et v deux mots de Σ^*. Démontrer par récurrence sur $|u| + |v|$ que $uv = vu \Rightarrow \exists w \in \Sigma^*, \{u, v\} \subset w^*$.

Solution:
Si $|u| = 0$, on pose $w = v$. Sinon, supposons par exemple que u est un préfixe de v ; alors $v = ut$ et $uut = uv = vu = utu$ donc $ut = tu$ avec $|u| + |t| < |u| + |v|$, donc par hypothèse, $\exists w \mid \{u, t\} \subset w^*$. Comme $v = tu$, $v \in w^*$.

Exercice 5 :

Soit m et n des entiers naturels > 0. Résoudre dans Σ^* l'équation $u^m = v^n$.

Solution:
On pose $w = u^m = v^n$.
Supposons $|u|$ et $|v|$ premiers entre eux. On peut supposer $|v| > |u|$. Il existe une relation de Bezout $1 = a|v| - b|u|$ avec a et b entiers naturels, $a < |u|$ et $b < |v|$. Alors, soit $s = |w| = m|u| = n|v|$, avec m multiple de $|v|$ et n multiple de $|u|$. Alors pour tout i entre 1 et s, si $w_i = w_{i+k|u|} = w_{i+l|v|}$ tant que $1 \leq i + k|u| \leq s$ et $1 \leq i + l|v| \leq s$. Pour $i \leq |v|$, $i + a|v| \leq (a + 1)|v| \leq |u||v| \leq n|u| = s$ donc $w_i = w_{i+a|v|} = w_{i+a|v|-b|u|} = w_{i+1}$. Ceci

démontre que v donc w donc u s'écrit sur une seule lettre. Le cas général s'en déduit en considérant l'alphabet Σ^d où d est le pgcd de $|u|$ et $|v|$.

Exercice 6 :

Soit Σ un alphabet fini. Deux mots u et v de Σ^* sont dits conjugués s'il existe deux mots x et y tels que $u = xy$ et $v = yx$. Démontrer que les mots u et v sont conjugués si et seulement si il existe un mot z tel que $uz = zv$.

Solution:

Supposons qu'il existe un mot z tel que $uz = zv$. Si $|z| \leq |u|$, il existe w tel que $u = zw$. Donc $uz = zwz = zv$ et $wz = v$. Sinon, $|z| > |u|$, il existe w tel que $uw = z$. Alors $zv = uwv = uz$ donc $wv = z$; ainsi $uw = wv$ avec $|w| < |z|$, on conclut par récurrence.

Exercice 7 :

Soit Σ un alphabet fini. On considère trois mots x, y, z dans Σ^* tels que $x^2y^2 = z^2$. Justifier qu'il existe un mot w dans Σ et des entiers p et q tels que $x = w^p$, $y = w^q$ et $z = w^{p+q}$.

Solution:

Si $x^2y^2 = z^2$, $|z^2| = |x^2| + |y^2|$, alors $2|z| = 2|x| + 2|y|$, donc $|z| = |x| + |y|$. En particulier, $|z| \leq |x|$ et x est préfixe de z. Posons $z = xu$. Par le même raisonnement, y est suffixe de z et comme $|u| = |y|$, on obtient $y = u$. On a alors $xyxy = xxyy$ donc par simplification dans le monoïde libre Σ^*, $yx = xy$. On sait alors (cf. Exercice 4) qu'il existe un mot $w \in \Sigma^*$ et des entiers p et q tels que $x = w^p$, $y = w^q$. Et $z = xy = w^{p+q}$.

Exercice 8 :

Si M est un monoïde et K, L deux parties de M, on note $L^{-1}K = \{x \in M \mid \exists y \in L, yx \in K\}$.

1. Soit L un sous-monoïde de Σ^*. Démontrer que L est un monoïde libre si et seulement si $L^{-1}L \cap LL^{-1} = L$.

   Solution:

   Supposons L libre de base B. Soit $m \in L^{-1}L \cap LL^{-1}$. Il existe p et q dans L tels que $pm \in L$ et $mq \in L$. En décomposant p et pm sur la base B, on obtient que $m \in L$.

   Réciproquement, supposons que $L^{-1}L \cap LL^{-1} = L$. Soit B la partie génératrice minimale de L (les éléments de L qui ne sont pas des produits de deux éléments distincts de 1). Soit $u_1 \dots u_m = v_1 \dots v_n$ avec les u_i et v_j dans B. Posons par exemple dans Σ^*, $u_m = wv_n$, alors $u_1 \dots u_{m-1}w = v_1 \dots v_{n-1}$, donc $w \in L^{-1}L \cap LL^{-1} = L$. Par minimalité des éléments de B dans L, $w = 1$. On conclut par récurrence.

2. Soit L un sous-monoïde de Σ^*. On définit par récurrence : $M_0 = L$, $M_{n+1} = {M_n}^{-1}M_n \cap M_n{M_n}^{-1}$. Démontrer qu'on définit ainsi une suite croissante de monoïdes et que $\cup_N M_n$ est le plus petit sous-monoïde libre contenant L.

   Solution:

   On remarque que pour tout monoïde M, $L \subset M^{-1}M \cap MM^{-1}$ ($\forall u \in M, 1u \in M$ et $u1 \in M$) donc la suite $(M_n)_n$ est bien une suite croissante et donc $M = \cup_n M_n$ est un monoïde.

   Démontrons que $M^{-1}M \cap MM^{-1} \subset M$: soit $u \in \Sigma^*$ tel qu'il existe v et w dans M tels que $vu \in M$ et $uv \in M$. $M = \cup_n M_n$, donc il existe des entiers l et m tels que $v \in M_l$ et $w \in M_m$. Pour $n = \max(l, m)$, v et w sont dans M_n, donc $u \in M_n^{-1}M_n \cap M_nM_n^{-1} = M_{n+1} \subset M$.

Enfin, si $N \subset P$ est une inclusion de sous-monoïdes, avec P libre, on a $N^{-1}N \cap NN^{-1} \subset P^{-1}P \cap PP^{-1} = P$, donc si P contient L, il contient aussi tous les M_n et donc M.

Monoïdes finis.

Exercice 9 :
Démontrer qu'un monoïde fini est le quotient d'un monoïde libre.

Solution:
Soit Σ un alphabet en bijection avec M (par une application ϕ). Alors le morphisme de monoïdes $\hat{\phi}$ qui prolonge ϕ est surjectif.

$$\begin{array}{ccc} \Sigma & \xrightarrow{\phi} & M \\ & \searrow \quad \nearrow_{\hat{\phi}} & \\ & \Sigma^* & \end{array}$$

Exercice 10 :
Soit M un monoïde fini et soit $x \in M$.

1. Démontrer qu'il existe deux entiers naturels m et n avec $m < n$ et $x^m = x^n$.

   Solution:
   Principe des tiroirs.

2. On choisit alors l minimal parmi les entiers n tels qu'il existe $m < n$ vérifiant $x^m = x^n$.
   (a) Démontrer que $1, x, ..., x^{l-1}$ sont des éléments distincts.

   Solution:
   Supposons $x^h = x^k$ pour $h < k < l$, alors l n'est pas minimal.

   (b) Démontrer que le monoïde $< x >$ est de cardinal l.

   Solution:
   Soit $k < l$ tel que $x^l = x^k$. Si $i \geq l$, $x^i = x^{k+i-l}$ donc par récurrence sur i, $x^i \in \{1, \ldots, x^{l-1}\}$. Donc $< x >= \{1, \ldots, x^{l-1}\}$ est de cardinal l.

   (c) Soit $k < l$ tel que $x^k = x^l$. Soit r l'unique entier compris entre k et $l-1$ divisible par $l-k$. Démontrer que $x^k, ..., x^{l-1}$ est un groupe cyclique d'ordre $l-k$ d'élément neutre x^r.

   Solution:
   Pour $i \geq n$, soit j le reste positif et q le quotient de la division euclidienne de i par $l-k$. Alors $x^i = x^{k+q(l-k)+j} = x^{k+j}$. Donc $\{x^k, \ldots, x^{l-1}\}$ est multiplicativement stable et x^r est élément neutre. De plus, $x^i \times x^{(q+1)(l-k)-i} = x^{(q+1)(l-k)} = x^r$, donc $\{x^k, \ldots, x^{l-1}\}$ est un groupe.

   (d) Démontrer que x admet une puissance qui est un idempotent(i.e. un élément y tel que $y^2 = y$). Y en a-t-il plusieurs ?

Solution:
Avec les notations précédentes, x^r est idempotent. Soit s tel que x^s est idempotent. Alors $x^{2s} = x^s$, donc $2s \geq l$. Donc $x^s = x^{2s} = x^{3s} = \cdots = x^{rs} = \cdots = x^r$.

Monoide syntaxique et Langages sans étoile.

Exercice 11 (Définition du monoïde syntaxique) :
Soit $L \subset \Sigma^*$ un langage. Il définit une relation d'équivalence sur Σ^* :

$$w \sim_L w' \Leftrightarrow \forall u, v \in \Sigma^*,\ uwv \in L \Leftrightarrow uw'v \in L$$

Justifier que $\sim_L$ est une congruence sur Σ^*. On définit alors le monoïde syntaxique M_L comme le quotient $\Sigma^*|_{\sim_L}$.

Solution:
Soit w, w' tels que $w \sim_L w'$. Soit $s, t \in \Sigma^*$. $\forall u, v \in \Sigma^*, u(swt)v = (us)w(tv)$ donc $u(swt)v \in L \Rightarrow (us)w'(tv) \in L$. Comme $(us)w'(tv) = u(sw't)v$, alors on a $u(sw't)v \in L$. Par symétrie, $u(swt)v \in L \iff u(sw't)v \in L$, donc $swt \sim_L sw't$.

Exercice 12 (Langage reconnu par un monoïde) :
Soit $L \subset \Sigma^*$ un langage. Soit M un monoïde. On dit que le langage L est reconnu par M s'il existe un morphisme de monoïdes φ de Σ^* dans M et une partie X de M tels que $L = \varphi^{-1}(X)$.

1. Démontrer qu'un langage reconnu par un monoïde fini est rationnel.

   Solution:
   Soit L reconnu par M à l'aide d'un morphisme de monoïdes φ de Σ^* dans M et X une partie de M telle que $L = \varphi^{-1}(X)$. Alors L est le langage reconnu par l'automate dont les états sont les éléments de M, l'état initial est 1, les états finals sont les éléments de X, et les transitions sont :

   $$\forall m \in M, \forall a \in \Sigma, m \xrightarrow{a} m\varphi(a)$$

2. Démontrer qu'un langage L est reconnu par son monoïde syntaxique.

   Solution:
   Soit φ la surjection canonique de Σ^* sur $\Sigma^*|_{\sim_L}$. Alors $L = \varphi^{-1}(\varphi(L))$.

3. Démontrer qu'un langage L est reconnu par un monoïde M si et seulement si M_L est isomorphe à un quotient d'un sous-monoïde de M.

   Solution:
   Soit L reconnu par M à l'aide d'un morphisme de monoïdes φ de Σ^* dans M et X une partie de M telle que $L = \varphi^{-1}(X)$. Soit $w, w' \in \Sigma^*$. Si $\varphi(w) = \varphi(w')$, alors $\forall u, v \in \Sigma^*, uwv \in L \iff \varphi(uwv) \in X \iff \varphi(u)\varphi(w)\varphi(v) \in X$ donc $uwv \in L \iff \varphi(uw'v) = \varphi(u)\varphi(w')\varphi(v) \in X$ et donc $uwv \in L \iff uw'v \in L$. On a montré : $\varphi(w) = \varphi(w') \Rightarrow w \sim_L w'$.

4. En déduire une caractérisation des langages rationnels portant sur leurs monoïdes syntaxiques.

Solution:
Un langage est rationnel si et seulement si son monoïde syntaxique est fini.

Exercice 13 (Langages sans étoile) :
Soit Σ un alphabet fini. La famille des langages sans étoile est la plus petite famille contenant le langage vide, les singletons et stable par union, passage au complémentaire et concaténation.

1. Démontrer que l'intersection de deux langages sans étoile est sans étoile.

Solution:
$$L \cap L' = \Sigma^* \setminus (\Sigma^* \setminus L \cup \Sigma^* \setminus L')$$

2. Démontrer que Σ^* est sans étoile.

Solution:
Σ^* est le complémentaire du langage vide.

3. Soit $a, b \in \Sigma$ distincts. Démontrer que $(ab)^*$ est sans étoile.

Solution:
$$(ab)^* = (a\Sigma^* \cap \Sigma^* b) \setminus (\Sigma^* a^2 \Sigma^* \cup \Sigma^* b^2 \Sigma^*)$$

On dit qu'un monoïde fini est apériodique si le seul groupe qu'il contient est le groupe trivial $\{1\}$.

4. Soit M un monoïde fini. Démontrer l'équivalence des assertions :
   (a) Le monoïde M est apériodique.
   (b) Pour tout m dans M, il existe un entier naturel non nul n tel que $m^{n+1} = m^n$,
   (c) Il existe un entier naturel non nul n tel que pour tout m dans M, $m^{n+1} = m^n$.

Solution:
$(a) \Rightarrow (b)$: supposons qu'il existe $m \in M$ tel que pour tout $n > 0$, $m^{n+1} \neq m^n$. Par le principe des tiroirs, il existe des entiers $0 < k < l$ tels que $m^k = m^l$. On prend alors k le plus petit possible et on pose $p = l - k$. Alors $m, m^2, \ldots, m^{l-1}$ sont des éléments tous distincts et $\{m^k, \ldots, m^{l-1}\}$ est un groupe d'ordre p (d'élément neutre m^r, r étant le multiple de p entre k et $l - 1 = k + p - 1$). L'hypothèse assure que $p \geq 2$.
$(b) \Rightarrow (c)$: on prend le maximum sur les éléments de M.
$(c) \Rightarrow (a)$: s'il existe un $n > 0$ tel que $\forall m \in M, m^{n+1} = m^n$, le seul élément inversible de M est 1 donc M est apériodique.

5. Soit L un langage rationnel et soit M_L son monoïde syntaxique. Par définition du monoïde syntaxique, on déduit de la question précédente que M_L est apériodique si et seulement si, pour tout mot u, il existe un entier naturel non nul n tel que pour tous mots v, w, $vu^n w \in L \Leftrightarrow vu^{n+1} w \in L$. Dans ce cas, on appelle indice de L et on note $i(L)$ le plus petit entier naturel non nul n tel que pour tous mots v, w, $vu^n w \in L \Leftrightarrow vu^{n+1} w \in L$.
   (a) Démontrer les propriétés suivantes :
      i. $i(\{a\}) = 1$,
      ii. $i(L \cup L') \leq \max(i(L), i(L'))$,

iii. $i(LL') \leq i(L) + i(L') + 1$,

iv. $i(\Sigma^* \setminus L) = i(L)$.

(b) En déduire que le monoïde syntaxique d'un langage sans étoile est apériodique.

6. Soit M un monoïde fini apériodique. Démontrer les propriétés suivantes :

(a) Règles de simplification : Pour tous k, l, m dans M, $m = kml \Rightarrow m = km = ml$.

Solution:
$m = kml$ donc $m = k^n m l^n$; si n vérifie $k^{n+1} = k^n$ et $l^{n+1} = l^n$, on a $m = km = ml$.

(b) 1 est le seul élément inversible à droite ou à gauche

Solution:
Soit m inversible à droite d'inverse l. $1 = ml = 1ml \Rightarrow 1m = ml = 1$.

(c) $\forall m \in M, (mM \cap Mm) \setminus \{k \in M \mid m \notin MkM\} = \{m\}$.

Solution:
Soit $p \in (mM \cap Mm) \setminus \{k \in M \mid m \notin MkM\}$. Soit $k, l \in M$ tels que $p = km = ml$. Comme $p \notin \{k \in M \mid m \notin MkM\}$, $m \in MpM$, donc il existe $r, s \in M$ tels que $m = rps$. Ainsi, $m = rps = r(ml)s = mls$ par simplification, donc $m = ps$; $p = km = kps = ps$ par simplification donc $p = m$.
L'inclusion inverse est évidente.

7. Soit M un monoïde fini apériodique. Soit $m \in M$. On définit $\rho(m) = |MmM|$.

(a) Démontrer que le seul m tel que $\rho(m) = |M|$ est $m = 1$.

Solution:
$\rho(m) = |M|$ si et seulement si $MmM = M$ si et seulement si $1 \in MmM$. Or $1 \in MmM$ implique $1 = m$ par simplification.

(b) Si m et n vérifient : $m \in nM$ et $n \notin mM$, alors $\rho(n) > \rho(m)$.

Solution:
Comme $m \in nM$, $MmM \subset MnM$. Si $n \in MmM$, alors il existe p et q tels que $n = pmq$; soit k tel que $m = nk$. Alors $n = pnkq$, par simplification $n = nkq = mq \in mM$. On obtient une contradiction. L'inclusion $MmM \subset MnM$ est donc stricte.

(c) Si m et n vérifient : il existe a, b dans M tels que $m \in ManM \cap MnbM$ et $m \notin ManbM$, alors $\rho(n) > \rho(m)$.

Solution:
De même, on écrit : $m = panq = rnbs$ et $n = umv$ (par l'absurde). Alors, par simplification$n = urnbs = nbs$ et $m = panbsq \in MambM$, contradiction.

8. Soit μ un morphisme de Σ^* dans un monoïde apériodique fini M. Soit $m \in M$. On pose :

$$U = \bigcup_{\substack{(a,n) \in \Sigma \times N \\ n\mu(a)M = mM \\ n \notin mM}} \mu^{-1}(n)a \qquad V = \bigcup_{\substack{(a,n) \in \Sigma \times N \\ M\mu(a)n = Mm \\ n \notin Mm}} a\mu^{-1}(n)$$

$$W = \{a \in \Sigma \mid m \notin MaM\} \cup \bigcup_{\substack{(a,b,n) \in \Sigma \times \Sigma \times N \\ m \in M\mu(a)nM \cap Mn\mu(b)M \\ m \notin M\mu(a)n\mu(b)M}} a\mu^{-1}(n)b$$

(a) Soit $m \in M$ tel que $m \neq 1$. Soit $x \in \Sigma^*$ tel que $\mu(x) \in mM$. Démontrer que x se factorise sous la forme uay, avec $\mu(u) \notin mM, \mu(ua) \in mM$. On pose $n = \mu(u)$. Établir une réciproque.

Solution:
Comme $1 \notin mM$ (par simplification), on prend pour u le plus grand préfixe de m tel que $\mu(u) \notin mM$. Comme $m \in mM$, c'est un préfixe strict.

(b) On démontre de la même façon que $x \in \Sigma^*$ est tel que $\mu(x) \in Mm$ si et seulement s'il se factorise sous la forme $u'a'v'$ avec $\mu(v') \notin Mm$ et $\mu(a'v') \in Mm$. Démontrer que $m \notin M\mu(x)M$ si et seulement si $x \notin \Sigma^* W \Sigma^*$.

Solution:
Soit x tel que $m \notin M\mu(x)M$. Soit y le plus petit facteur de x tel que $m \in M\mu(y)M$. Soit y est une lettre a et $x = uav$ avec $m \notin M\mu(a)M$, soit y se factorise en azb avec $m \in M\mu(a)\mu(z)M \cap M\mu(z)\mu(b)M$.

(c) Conclure par récurrence sur $\rho(M)$.

Solution:
On vient de montrer avec les notations précédentes que $\mu^{-1}(m) = U\Sigma^* \cap \Sigma^* V \setminus (\Sigma^* W \Sigma^*)$. La question 7 ci dessus montre qu'on peut appliquer l'hypothèse de récurrence à chacun des langages.

Exercice 14 (Groupes libres) :

Soit Σ un alphabet fini. On note $\bar{\Sigma}$ une copie de Σ ; $\bar{\Sigma} = \{\bar{a} \mid a \in \Sigma\}$. Pour chaque lettre $a \in \Sigma$, on note $\bar{\bar{a}} = a$. L'application $x \to \bar{x}$ ainsi définit une involution de $\Sigma \sqcup \bar{\Sigma}$ qui échange Σ et $\bar{\Sigma}$.

On note L le monoïde libre sur l'alphabet $\Sigma \sqcup \bar{\Sigma}$.

On appelle *opération élémentaire* sur un mot $w = u_1 u_2 ... u_p, u_i \in \Sigma \sqcup \bar{\Sigma}$:

- *Une insertion* : $u_1 u_2 .. u_i \, u\bar{u} \, u_{i+1} ... u_p$ pour un i entre 0 et p et $u \in \Sigma \sqcup \bar{\Sigma}$.
- *Une suppression* : $u_1 u_2 .. u_{i-1} u_{i+2} ... u_p$ pour un i entre 1 et $p-1$ tel que $u_{i+1} = \bar{u_i}$.

1. On définit sur L une relation en posant $w \sim w'$ s'il existe une suite finie de mots $w_1 = w, w_2, ..., w_{n-1}, w_n = w'$ tels que w_{i+1} est obtenu à partir de w_i par une opération élémentaire.

   Démontrer que $\sim$ est une congruence.

2. On dit qu'un mot w est *réduit* si on ne peut pas faire de suppression dans w.

   (a) Démontrer que toute classe de congruence contient un mot réduit.

   Solution:
   Un mot de longueur minimale dans une classe de congruence est réduit.

   (b) On se propose de justifier que toute classe de congruence contient un unique mot réduit. Soit w et w' deux mots réduits congruents. Soit $w_1 = w, w_2, ..., w_{n-1}, w_n = w'$ tels que w_{i+1} est obtenu à partir de w_i par une opération élémentaire et tels que $\sum_i |w_i|$ est minimal parmi les suites finies de mots vérifiant cette propriété. On suppose $w \neq w'$ donc $n > 1$.

i. Justifier que $|w| < |w_2|$ et $|w'| < |w_{n-1}|$.

Solution:
Comme w est réduit, la suite commence par une insertion. De même, comme w' est réduit, la suite finit par une suppression.

ii. En déduire qu'il existe i tel que w_i obtenu à partir de w_{i-1} à partir d'une insertion et w_{i+1} est obtenu à partir de w_i à partir d'une suppression.

Solution:
Comme $|w| < |w_2|$ et $|w'| < |w_{n-1}|$, il existe i tel que $|w_i| > |w_{i-1}|$ et $|w_i| > |w_{i+1}|$.

iii. Soit $a, b \in \Sigma \sqcup \bar{\Sigma}$ et s, t tels que : $w_{i-1} = u_1u_2..u_p$, $w_i = u_1u_2..u_sa\bar{a}u_{s+1}...u_p = v_1....v_{p+2}$ et $w_{i+1} = v_1...v_{t-1}v_{t+1}...v_{p+2}$ avec $v_t = b$ et $V_{t+1} = \bar{b}$. En étudiant les cas où ces deux opérations se chevauchent ou non, aboutir à une contradiction.

Solution:
Si les deux opérations ne se chevauchent pas, on aurait pu commencer par la suppression puis effectuer l'insertion. Dans ce cas, la suite $w_1 = w, w_2, \dots, w_{i-1}, w_i', w_{i+1}, \dots, w_{n-1}, w_n = w'$ représenterait une suite d'opérations élémentaires avec $|w_i'| = |w_i| - 4$, ce que contredit la minimalité de $\sum_i |w_i|$.
Si les deux opérations de font au même endroit, alors $w_{i-1} = w_{i+1}$, on peut supprimer w_i et w_{i+1} de la suite $w_1 = w, w_2, \dots, w_{i-1}, w_i', w_{i+1}, \dots, w_{n-1}, w_n = w'$, ce que contredit la minimalité de $\sum_i |w_i|$.
Si les deux opérations se chevauchent sur une lettre :
$w_i = u_1u_2 \dots u_sa\bar{a}u_{s+1} \dots u_p$, $u_{s+1} = a$ et $w_{i+1} = u_1u_2 \dots u_sau_{s+2} \dots u_p$.
Mais alors $w_{i-1} = u_1u_2 \dots u_sau_{s+2} \dots u_p = w_{i+1}$ et à nouveau on peut supprimer w_i et w_{i+1} de la suite. De même, si $u_s = \bar{a}$ et
$w_{i+1} = u_1u_2 \dots u_{s-1}\bar{a}u_{s+2} \dots u_p = w_{i-1}$.

3. On note GF le monoïde $L/\sim$ et π la surjection canonique de L sur GF.
   (a) Démontrer que π injecte Σ dans GF.

   Solution:
   Une lettre est un mot réduit.

   (b) Démontrer que GF est un groupe engendré par $\pi(\Sigma)$.

   Solution:
   On remarque que $u\bar{u} \sim \varepsilon\bar{u}u$, pour tout $u \in \Sigma \sqcup \bar{\Sigma}$, donc $\pi(u)\pi(\bar{u}) = \pi(\bar{u})\pi(u) = 1$, les éléments de $\pi(\Sigma)$ sont tous inversibles.
   Si $w = u_1 \dots u_n \in L$, $u_i \in \Sigma \sqcup \bar{\Sigma}$, on a $\pi(w) = \pi(u_1) \cdots \pi(u_n) \in \langle \pi(\Sigma) \rangle$. De plus, $\pi(w)\pi(u_n)^{-1} \cdots \pi(u_1)^{-1} = 1$ et $\pi(u_n)^{-1} \cdots \pi(u_1)^{-1}\pi(w) = 1$

   (c) Quel est ce groupe lorsque Σ est un singleton ?

   Solution:
   $\mathbb{Z}$.

4. Soit ϕ une application de l'ensemble Σ dans un groupe G. On étend ϕ sur $\bar{\Sigma}$ en posant $phi(\bar{u}) = \phi(u)^{-1}$, pour tout u dans Σ. Démontrer qu'il existe un unique morphisme de groupes de GF dans G prolongeant ϕ.

Solution:
On sait déjà qu'il existe un morphisme de monoïdes de L dans G qui prolonge ϕ. Notons $\hat{\phi}$ ce morphisme.

$$\begin{array}{ccc} \Sigma \sqcup \bar{\Sigma} & \xrightarrow{\phi} & G \\ & \searrow \quad \nearrow_{\hat{\phi}} & \\ & L & \end{array}$$

Or on vérifie qu'en passant d'un mot w à un mot w' par une opération élémentaire, $\hat{\phi}(w) = \hat{\phi}(w')$, donc deux mots congruents ont une même image par $\hat{\phi}$. Donc $\hat{\phi}$ passe au quotient. On note $\tilde{\phi}$ l'application ainsi obtenue de GF dans G.

$$\begin{array}{ccccc} \Sigma \sqcup \bar{\Sigma} & \xrightarrow{\phi} & & & G \\ & \searrow & & \nearrow_{\hat{\phi}} & \uparrow \tilde{\phi} \\ & & L & \xrightarrow{\pi} & GF \end{array}$$

Comme $\tilde{\phi}(\pi(a)) = \phi(a)$ pour tout $a \in \Sigma$ et que $GF = \langle \pi(\Sigma) \rangle$, on a l'unicité.

5. On note L_R l'ensemble des mots réduits.
   (a) Démontrer que tout facteur d'un mot réduit est réduit.
   (b) Soit $u \in \Sigma$. Justifier qu'on peut définir une application σ_u de L_R dans lui-même en posant :
   $$\sigma_u : w \to \begin{cases} uw & \text{si } uw \in L_R, \\ v & \text{si } w = \bar{u}v. \end{cases}$$

   Solution:
   Soit $w \in L_R$, $w = u_1 \dots u_p$, $u_i \in \Sigma \sqcup \bar{\Sigma}$.
   $v = u_2 \dots u_p$ est réduit car suffixe de w, donc si $u_1 = \bar{u}$, $w = \bar{u}v$ avec $v \in L_R$. Sinon, $u_1 \neq \bar{u}$, donc uw est réduit car comme w est réduit, la seule suppression à envisager aurait été uu_1. On a donc bien défini une application de L_R dans L_R.

   (c) Démontrer que σ_u est une permutation de L_R.

   Solution:
   Par définition, on a $\sigma_{\bar{u}} \circ \sigma_u = Id$ et $\sigma_u \circ \sigma_{\bar{u}} = Id$, donc σ_u est une permutation.

   (d) Soit $\sigma : \Sigma \to L$ l'application telle que $\sigma(u) = \sigma_u$. On note $\hat{\sigma}$ le morphisme de groupes prolongement de σ de L dans $\mathfrak{S}(L_R)$. Si $w \in L_R$, démontrer que $\sigma_w(\varepsilon) = w$.

   Solution:
   Soit $w = u_1 \dots u_p$ un mot réduit. Justifions par récurrence sur p que $\hat{\sigma}_w(\varepsilon) = w$: $\hat{\sigma}_w = \hat{\sigma}_{u_1}\hat{\sigma}_{u_2 \dots u_p} = \sigma_{u_1}\hat{\sigma}_{u_2 \dots u_p}$. Par hypothèse de récurrence, $v = \hat{\sigma}_{u_2 \dots u_p}(\varepsilon) = u_2 \dots u_p$, donc $\hat{\sigma}_w(\varepsilon) = \sigma_{u_1}(v)$. Comme w est réduit, $u_1 \neq \bar{u_2}$, donc $\sigma_{u_1}(v)u_1v = w$.

   (e) Retrouver ainsi l'unicité du mot réduit dans une classe de congruence.

   Solution:
   On note $\tilde{\sigma}$ le morphisme de groupes prolongement de σ de GF dans $\mathfrak{S}(L_R)$. Soit w, w' deux mots congruents, ils définissent un même élément dans GF, $\hat{\sigma}(w) = \tilde{\sigma}(\pi(w)) = \tilde{\sigma}(\pi(w')) = \hat{\sigma}(w')$. Donc $w = \hat{\sigma}(w)(\varepsilon) = \hat{\sigma}(w')(\varepsilon) = w'$.