Soit Σ un alphabet fini.

Exercice 1 :
Soit u et v deux mots de Σ^*. Démontrer par récurrence sur $|u| + |v|$ que $uv = vu \Rightarrow \exists w \in \Sigma^*, \{u, v\} \subset w^*$.

Exercice 2 :
Soit m et n des entiers naturels > 0. Résoudre dans Σ^* l'équation $u^m = v^n$.

Exercice 3 :
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 $uz = zv$.

Exercice 4 :
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 $z = w^{p+q}$.

Exercice 5 :
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 $L^{-1}L \cap LL^{-1} = L$.
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.

Monoïdes finis

Exercice 6 :
Démontrer qu'un monoïde fini est le quotient d'un monoïde libre.

Exercice 7 :
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 $x^m = x^n$.
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.
   (b) Démontrer que le monoïde $< x >$ 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.
   (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 ?

Monoide syntaxique et Langages sans étoile

Exercice 8 (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 $\Sigma^*|_{\sim_L}$.

Exercice 9 (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.
2. Démontrer qu'un langage L est reconnu par son monoïde syntaxique.
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.
4. En déduire une caractérisation des langages rationnels portant sur leurs monoïdes syntaxiques.

Exercice 10 (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.
2. Démontrer que Σ^* est sans étoile.
3. Soit $a, b \in \Sigma$ distincts. Démontrer que $(ab)^*$ est sans étoile.

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, $m^{n+1} = m^n$.
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, $m = kml \Rightarrow m = km = ml$.
   (b) 1 est le seul élément inversible à droite ou à gauche
   (c) $\forall m \in M, (mM \cap Mm) \setminus \{k \in M \mid m \notin MkM\} = \{m\}$.
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 $m = 1$.
   (b) Si m et n vérifient : $m \in nM$ et $n \notin mM$, alors $\rho(n) > \rho(m)$.
   (c) Si m et n vérifient : il existe a, b dans M tels que $m \in ManM \cap MnbM$ et $m \notin ManbM$, alors $\rho(n) > \rho(m)$.
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.
   (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 $x \notin \Sigma^* W \Sigma^*$.
   (c) Conclure par récurrence sur $\rho(M)$.

Exercice 11 (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.

(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 $|w'| < |w_{n-1}|$.

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.

iii. Soit $a, b \in \Sigma \sqcup \bar{\Sigma}$ et s, t tels que : $w_{i-1} = u_1u_2..u_p$, $w_i = u_1u_2..u_s a\bar{a} u_{s+1}...u_p = v_1....v_{p+2}$ 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.

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.

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

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

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.

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 :

$$\sigma_u : w \to \begin{cases} uw & \text{si } uw \in L_R, \\ v & \text{si } w = \bar{u}v. \end{cases}$$

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

(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 $\sigma_w(\varepsilon) = w$.

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