Monoïdes finis

Exercice 1 :
Démontrer qu'un monoïde fini est le quotient d'un monoïde libre.

Exercice 2 :
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 3 (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 4 (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 5 (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 6 (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 $w = u_1u_2...u_p, u_i \in \Sigma \sqcup \bar{\Sigma}$:

- *Une insertion* : $u_1u_2..u_i\, u\bar{u}\, u_{i+1}...u_p$ pour un i entre 0 et p et $u \in \Sigma \sqcup \bar{\Sigma}$.
- *Une suppression* : $u_1u_2..u_{i-1}u_{i+2}...u_p$ 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 : $w_{i-1} = u_1u_2..u_p$, $w_i = u_1u_2..u_sa\bar{a}u_{s+1}...u_p = v_1....v_{p+2}$ 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.

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.

Groupes

Exercice 7 (7) :

On note φ la fonction d'Euler.

Soit n un entier naturel > 1. On note $d(n)$ le nombre d'entiers naturels diviseurs de n.

1. Soit m un entier naturel compris entre 1 et n. Soit H_m l'ensemble des éléments de $\mathbb{Z}/n\mathbb{Z}$ dont l'ordre est un diviseur de m, c'est-à-dire l'ensemble des éléments x de $\mathbb{Z}/n\mathbb{Z}$ tels que $\overline{m}x = \underbrace{x + x + \cdots + x}_{m} = 0$. Démontrer :
   (a) H_m est un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$.
   (b) H_m est un sous-groupe cyclique de $\mathbb{Z}/n\mathbb{Z}$ de cardinal $\text{pgcd}(m, n)$.
   (c) Montrer que l'ensemble des sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ est exactement l'ensemble des sous-groupes H_d pour $d \in \mathbb{N}$, d diviseur de n.
2. On considère l'application suivante :

$$\begin{array}{rcccc} \psi & : & (\mathbb{Z}/n\mathbb{Z})^* \times \mathbb{Z}/n\mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \\ & & (\overline{m}, x) & \to & \overline{m}x \end{array}$$

   (a) Justifier que le groupe $(\mathbb{Z}/n\mathbb{Z})^*$ opère ainsi sur $\mathbb{Z}/n\mathbb{Z}$.

   (b) Démontrer l'égalité :

$$\sum_{\substack{m \in \{1,\ldots,n\} \\ \text{pgcd}(m,n)=1}} \text{pgcd}(m-1, n) = \varphi(n)d(n)$$

Exercice 8 (Décomposition en cycles disjoints d'une permutation) :

Rappels de vocabulaire : Soit $\{i_1, \ldots, i_k\}$ une partie de $\{1, \ldots, n\}$ de cardinal k La permutation notée $(i_1, \ldots, i_k)$ est la permutation σ telle que $\sigma(i_1) = i_2, \cdots \sigma(i_{k-1}) = i_k$, $\sigma(i_k) = i_1$ et $\sigma(i) = i, \forall i \notin \{i_1, \ldots, i_k\}$. Une telle permutation est appelée un k-cycle (une transposition si $k = 2$) et l'ensemble $\{i_1, \ldots, i_k\}$ est appelé son *support*. On vérifiera que l'ordre de $(i_1, \ldots, i_k)$ dans $\mathfrak{S}_n$ est k.

Plus généralement, on appelle *support* d'une permutation σ le complémentaire de ses points fixes, i.e, $\{i \in \{1, \ldots, n\} \ ; \ \sigma(i) \neq i\}$.

On fait opérer le groupe symétrique $\mathfrak{S}_n$ naturellement sur l'ensemble $\{1, \ldots, n\}$:

$$\begin{array}{rcl} \mathfrak{S}_n \times \{1, \ldots, n\} & \to & \{1, \ldots, n\} \\ (\sigma, i) & \mapsto & \sigma(i) \end{array}$$

On pourra remarquer qu'il s'agit simplement de l'opération définie par le morphisme de groupes :

$$\mathfrak{S}_n \overset{id}{\to} \mathfrak{S}_n$$

avec le seconde définition.

1. Soit σ une permutation de $\{1,\dots,n\}$. En faisant opérer le sous-groupe $<\sigma>$ par restriction sur $\{1,\dots,n\}$, démontrer que σ se décompose de façon unique (à l'ordre près) comme une composition de cycles à supports disjoints. On remarquera que sur chaque orbite de cette opération, σ agit comme une permutation circulaire.
2. Comment calculer l'ordre de σ ?
3. Déterminer le maximum des ordres des permutations de $\mathcal{S}_6$.
4. Un mélange dit *parfait* d'un jeu de cartes se fait en prenant les 26 cartes du dessus du paquet, les 26 suivantes et les entrelaçant. En ayant numéroté les 52 cartes de 1 à 52, du haut vers le bas du paquet, on peut représenter ce mélange par l'action de la permutation sur $\{1,\dots,52\}$:

$$\sigma(x) = \begin{cases} 2x-1, & \text{si } x \in \{1,\dots,26\} \\ 2(x-26), & \text{si } x \in x \in \{27,\dots,52\} \end{cases}$$

   (a) Déterminer la décomposition en cycles disjoints de la permutation σ.

   (b) En déduire l'ordre de la permutation σ.

Exercice 9 (Parties génératrices du groupe symétrique) :
On remarque que l'exercice 1 assure que $\mathfrak{S}_n$ est engendré par les cycles.

1. Démontrer que $\mathfrak{S}_n$ est engendré par les transpositions.
2. Démontrer que $\mathfrak{S}_n$ est engendré par les transpositions $(1,2),(2,3),\dots,(n-1,n)$.
3. Démontrer que $\mathfrak{S}_n$ est engendré par les transpositions $(1,2),(1,3),\dots,(1,n)$.
4. Soit E un sous-ensemble de $\{1,\dots,n\}$. On note $\mathcal{S}_E$ le sous-groupe de $\mathfrak{S}_n$ formé par les permutations qui fixent tous les points de $\{1,\dots,n\} \setminus E$. Soit (i,j) une transposition de $\mathfrak{S}_n$. Démontrer que :

$$<\mathcal{S}_E,(i,j)> = \begin{cases} \mathcal{S}_E \times <(i,j)> & \text{si } i \notin E \text{ et } j \notin E \\ \mathcal{S}_{E\cup\{j\}} & \text{si } i \in E \text{ et } j \notin E \end{cases}$$

5. Soit X une famille de transpositions dans $\mathfrak{S}_n$. On note G_X le graphe dont l'ensemble des sommets est l'ensemble $\{1,\dots,n\}$ et dont l'ensemble des arêtes est $\{(i,j) \mid (i,j) \in X\}$.

   (a) Dessiner les graphes correspondant aux trois parties génératrices ci-dessus.

   (b) Démontrer que X est une partie génératrice du groupe symétrique $\mathfrak{S}_n$ si et seulement si G_X est connexe.
6. Démontrer qu'une partie génératrice du groupe symétrique $\mathfrak{S}_n$ formée de transpositions contient au moins $n-1$ transpositions.