Monoïdes libres

Exercice 1 :

Pour tout $u, v, u', v' \in \Sigma^*$, si $uv \sqsubseteq u'v'$, alors $u \sqsubseteq u'$ ou $u' \sqsubseteq u$.

Solution:

Distinguer selon si $|u| \leq |u'|$ ou $|u'| \leq |u|$.

Exercice 2 :

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, q, pm et mq sur la base B, on obtient que $m \in L$ (écrire $(pm)q = p(mq)$).

   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 :
   - $M_0 = L$
   - $M_{n+1} = \langle {M_n}^{-1}M_n \cap M_n{M_n}^{-1} \rangle$

   Démontrer qu'on définit ainsi une suite croissante 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 de monoïdes. 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 $u \in M_n^{-1}M_n \cap M_nM_n^{-1} \subset M_{n+1} \subset M$. Donc M est libre.

   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 $\langle N^{-1}N \cap NN^{-1} \rangle \subset \langle P \rangle = P$, donc si P contient L, il contient aussi tous les M_n et donc M : M est donc le plus petit sous-monoïde libre contenant L.

Exercice 3 :

Démontrer qu'un monoïde 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.

$$\begin{tikzcd} \Sigma \arrow[rr, "\phi"] \arrow[dr] & & M \\ & \Sigma^* \arrow[ur, "\hat{\phi}"'] & \end{tikzcd}$$

Utilisation de la formule de Burnside.

Exercice 4 :
Considérons l'action $\cdot$ d'un groupe G sur un ensemble E. Montrer que

1. Pour tout $g \in G$, l'application $f_g : E \to E$ telle que $f_g(x) := g \cdot x$ est une bijection d'inverse $f_{g^{-1}}$.
2. L'application $g \mapsto f_g$ est un morphisme, i.e. $f_{gg'} = f_g \circ f_{g'}$.

Exercice 5 :
Montrer que pour tout $x \in E$, on a $|G| = |H_x| \cdot |[x]|$.

Solution:
Soit $x \in E$. L'application

$$\begin{aligned} \theta :& G \to [x] \\ & g \mapsto g \cdot x \end{aligned}$$

On va montrer que chaque élément de l'orbite $[x]$ a $|H_x|$ antécédents par θ, ce qui prouvera la formule.
Pour tout $g, g' \in G$, on note $g \equiv g'$ si $g \cdot x = g' \cdot x$, ce qui est clairement une relation d'équivalence. On remarque que $g \cdot x = g' \cdot x$ ssi $g^{-1}g' \cdot x = x$ ssi $g^{-1}g' \in H_x$ ssi il existe $h \in H_x$ tel que $g' = gh$. Donc $gH_x := \{gh \mid h \in H_x\}$ est la classe d'équivalence de g. Pour tout $g \in G$, l'application

$$\begin{aligned} f_g :& H_x \to gH_x \\ & h \mapsto gh \end{aligned}$$

est une bijection, donc chaque classe d'équivalence a le même nombre d'éléments, i.e. $|H_x|$.

Exercice 6 :
Montrer que pour tout groupe G opérant sur un ensemble E, on a :

$$|G| \cdot |E/G| = \sum_{g \in G} |F_g|$$

Solution:
Soit $X := \{(g, x) \in G \times E \mid g \cdot x = x\}$. On compte les éléments de X en partitionnant d'abord selon E puis selon G. D'une part

$$\begin{aligned} X &= \sqcup_{x \in E} \{(g, y) \in G \times E \mid y = x \wedge g \in G \wedge g \cdot x = x\} \\ &= \sqcup_{x \in E} \{g \in G \mid g \cdot x = x\} \\ &= \sqcup_{x \in E} H_x \end{aligned}$$

Donc

$$\begin{aligned}|X| &= \sum_{x\in E} |H_x| = \sum_{x\in E} \frac{|G|}{|[x]|} \text{ par un lemme ci-dessus,} \\ &= \sum_{\omega\in E/G} \sum_{x\in\omega} \frac{|G|}{|\omega|} = \sum_{\omega\in E/G} |\omega| \cdot \frac{|G|}{|\omega|} \\ &= |E/G| \cdot |G|\end{aligned}$$

D'autre part

$$\begin{aligned}X &= \sqcup_{g\in G}\{(h,x) \in G\times E \mid h = g \wedge g \in G \wedge g\cdot x = x\} \\ &= \sqcup_{g\in G}\{x \in E \mid g\cdot x = x\} \\ &= \sqcup_{g\in G} F_g\end{aligned}$$

Donc $|X| = \sum_{g\in G} |F_g|$.

Exercice 7 :

Soit p un nombre premier. On note $(1,\ldots,p)$ le p-cycle (la permutation du groupe symétrique qui envoie 1 sur 2, 2 sur 3, …, $p-1$ sur p et p sur 1). On note G le groupe engendré par le p-cycle $(1,\ldots,p)$. Soit Σ un alphabet fini.

1. Démontrer que G est un groupe d'ordre p.

Solution:
La permutation $\tau = (1,\ldots,p)$ est un élément d'ordre p donc il engendre un groupe d'ordre p. Si on veut démontrer que l'ordre de τ est exactement p, on peut remarquer que $\tau(i)$ est congru à $i+1$ modulo p, donc $\tau^j(i)$ est congru à $i+j$ modulo p. Ainsi, $\tau^j = Id$ si et seulement si $\forall i, \tau^j(i) = i$, donc si et seulement si j est un multiple de p.

2. Quels sont les ordres des éléments de G ? Pour chaque ordre d, on précisera combien d'éléments de G sont d'ordre d.

Solution:
Comme p est un nombre premier, par le théorème de Lagrange, les éléments de G sont d'ordre 1 ou p. Seul l'élément neutre est d'ordre 1, donc il y a $p-1$ éléments d'ordre p.

3. On fait opérer G sur Σ^p, l'ensemble des mots de longueur p écrits avec des lettres de Σ de la façon suivante :

$$\begin{array}{lll} G\times\Sigma^p & \to & \Sigma^p \\ (\tau, a_1a_2\ldots a_p) & \to & \tau\cdot(a_1a_2\ldots a_p) = a_{\tau^{-1}(1)}a_{\tau^{-1}(2)}\ldots a_{\tau^{-1}(p)}\end{array}$$

(a) Démontrer qu'il s'agit bien d'une opération de groupe.

Solution:
Soit σ et ρ deux permutations. Soit $a_1a_2\ldots a_p \in \Sigma^p$. Alors :

$$\begin{aligned}\sigma \cdot (\tau \cdot (a_1 a_2 \dots a_p)) &= \sigma \cdot (a_{\tau^{-1}(1)} a_{\tau^{-1}(2)} \dots a_{\tau^{-1}(p)}) \\ &= \sigma \cdot (b_1 b_2 \dots b_p) \text{ avec } b_i = a_{\tau^{-1}(i)}, \forall i \\ &= b_{\sigma^{-1}(1)} b_{\sigma^{-1}(2)} \dots b_{\sigma^{-1}(p)} \\ &= a_{\tau^{-1}(\sigma^{-1}(1))} a_{\tau^{-1}(\sigma^{-1}(2))} \dots a_{\tau^{-1}(\sigma^{-1}(p))} \\ &= a_{(\sigma\tau)^{-1}(1)} a_{(\sigma\tau)^{-1}(2)} \dots a_{(\sigma\tau)^{-1}(p)} \text{ puisque } (\sigma\tau)^{-1} = \tau^{-1}\sigma^{-1}\end{aligned}$$

(b) Déterminer le fixateur de $(1, \dots, p)$. En déduire le fixateur de $(1, \dots, p)^i$, pour tout entier i premier avec p.

Solution:
Notons $\mathrm{Fix}((1, \cdots, p))$ le fixateur de $(1, \cdots, p)$. $a_1 a_2 \dots a_p \in \mathrm{Fix}((1, \cdots, p))$ si $(1, \cdots, p) \cdot a_1 a_2 \dots a_p = a_1 a_2 \dots a_p$. Or $(1, \cdots, p) \cdot a_1 a_2 \dots a_p = a_2 a_3 \dots a_p a_1$. Donc $a_1 a_2 \dots a_p \in \mathrm{Fix}((1, \cdots, p))$ si et seulement si $a_1 = a_2$, $a_2 = a_3$, …, $a_p = a_1$. Donc $\mathrm{Fix}((1, \cdots, p)) = \{a^p \mid a \in \Sigma\}$.
Un mot dans le fixateur de $(1, \cdots, p)$ est dans le fixateur de $(1, \cdots, p)^i$, pour tout entier i. Si i est premier avec p, il existe des entiers a et b tels que $ap + bi = 1$ donc $(1, \cdots, p) = ((1, \cdots, p)^p)^a ((1, \cdots, p)^i)^b = ((1, \cdots, p)^i)^b$, donc un mot dans le fixateur de $(1, \cdots, p)^i$ est dans le fixateur de $(1, \cdots, p)$. Donc pour i premier avec p, $\mathrm{Fix}((1, \cdots, p)) = \mathrm{Fix}((1, \cdots, p))^i$.

(c) Démontrer que le nombre d'orbites r de cette opération est :

$$r = \frac{1}{p}(|\Sigma|^p + (p-1)|\Sigma|)$$

Solution:
On écrit la formule de Burnside :

$$r = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}(g)|$$

L'identité fixe tout élément de Σ^p, les autres éléments de G sont les $(1, \cdots, p)^i$ pour $i \in \{1, \cdots, p-1\}$ et ont comme fixateur $\{a^p \mid a \in \Sigma\}$, de cardinal $|\Sigma|$. Et G est d'ordre p, donc la formule de Burnside s'écrit dans ce cas précis :

$$r = \frac{1}{p}(|\Sigma|^p + (p-1)|\Sigma|)$$

(d) Retrouver ainsi le petit théorème de Fermat.

Solution:
Comme le nombre d'orbites est un entier naturel, on en déduit que p divise l'entier $|\Sigma|^p + (p-1)|\Sigma| = (|\Sigma|^{p-1} + (p-1))|\Sigma|$. Lorsque l'alphabet Σ est de cardinal premier avec p, p est inversible modulo p et $p - 1 \equiv -1 \mod p$, donc $|\Sigma|^{p-1} \equiv 1 \mod p$. En considérant pour tout $n \in \mathbb{N}$ tel que $n \wedge p = 1$ un alphabet de cardinal n, on retrouve ainsi le petit théorème de Fermat.

Exercice 8 :

Soit n un entier naturel ≥ 1. On considère l'ensemble E_n des graphes dont l'ensemble des sommets est $[\![1,n]\!]$. Un tel graphe G est représenté par une application $\delta_G : [\![1,n]\!] \to \mathcal{P}([\![1,n]\!])$ où $\delta_G(i)$ est l'ensemble dans $[\![1,n]\!] \setminus \{i\}$ des sommets de G reliés à i par une arête. Comme le graphe est non orienté, on a l'équivalence :

$$\forall i,j \in [\![1,n]\!], i \neq j,\ i \in \delta_G(j) \Leftrightarrow j \in \delta_G(j)$$

Soit σ une permutation de $[\![1,n]\!]$ ($\sigma \in \mathcal{S}_n$). Si G est un graphe dans E_n, $G = ([\![1,n]\!], \delta_G)$, On note $\sigma.G$ le graphe $([\![1,n]\!], \delta_{\sigma.G})$ où $\delta_{\sigma.G}$ est définie par :

$$\forall i \in [\![1,n]\!], \delta_{\sigma.G}(\sigma(i)) = \{\sigma(j), j \in \delta_G(i)\}$$

On vérifierait (c'est juste fastidieux !) qu'on a bien ainsi défini une opération du groupe $\mathcal{S}_n$ sur l'ensemble E_n.

1. On suppose dans cette question $n = 3$. Dessiner les différents graphes à trois sommets à isomorphisme près (il y en a 4).

Solution:
Il y en a quatre : 0, 1, 2 ou 3 arêtes.

2. On se propose de faire le calcul pour $n = 4$ en utilisant la formule de Burnside. Pour cela on passe en revue les éléments du groupe symétrique $\mathcal{S}_4$ et détermine pour chacun le cardinal du fixateur.

   (a) Soit τ la transposition $(1,2)$. Démontrer que le graphe G est dans $\mathrm{Fix}(\tau)$ si et seulement si $\delta_G(1) \cap \{3,4\} = \delta_G(2) \cap \{3,4\}$. En déduire que $\mathrm{Fix}(\tau)$ est de cardinal 2^4.

   Solution:
   Soit $i \in \{3,4\}$. Alors i est fixe par σ donc $i \in \delta_G(1)$ si et seulement si $i \in \delta_G(2)$. Il n'y a pas d'autre condition.

   Il y a 4 possibilités pour les arêtes reliant le sommet 1 à un sommet 3, 4 et cela fixe les arêtes reliant le sommet 2 à un sommet 3, 4. Il y a ensuite 2 possibilités entre 3 et 4 (une arête ou non) et 2 possibilités entre 1 et 2 (une arête ou non). Donc 2^4 en tout.

   (b) Soit σ le 3-cycle $(1,2,3)$.

      i. Soit G un graphe dans $\mathrm{Fix}(\sigma)$. Démontrer que si on efface les arêtes d'extrémité 4 dans G, il y a exactement deux graphes possibles.

      Solution:
      La présence de l'arête entre 1 et 2 impose celle entre 2 et 3 et celle entre 3 et 1, donc le graphe est complet. De même, l'arête entre 1 et 3 impose le graphe complet. Donc le graphe restreint aux sommets $1,2,3$ est vide ou complet.

      ii. En déduire qu'il y a exactement 4 graphes dans $\mathrm{Fix}(\sigma)$.

      Solution:
      On choisit le graphe restreint aux sommets $1,2,3$ (deux choix) et l'existence d'au moins une arête vers 4 (il y aura alors les trois) ou non (deux choix).

(c) Soit μ le produit de deux transpositions disjointes $(1, 2)(3, 4)$. Décrire les différentes possibilités pour l'ensemble des arêtes ayant une extrémité dans $\{1, 2\}$ et une dans $\{3, 4\}$. En déduire que $\text{Fix}(\mu)$ est de cardinal 2^4.

Solution:
De même on choisit la présence de l'arête entre 1 et 2 ou non (2 choix), la présence de l'arête entre 3 et 4 ou non (2 choix), la présence de l'arête entre 1 et 3 ou non (2 choix), la présence de l'arête entre 1 et 4 ou non (2 choix). Il y en a 2^4 en tout.

(d) Soit ρ le cycle $(1, 2, 3, 4)$. Calculer le cardinal $\text{Fix}(\rho)$. On pourra démontrer qu'un graphe G dans $\text{Fix}(\rho)$ est totalement déterminé par $\delta_G(1)$.

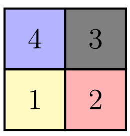
Solution:
Si on choisit la présence de l'arête entre 1 et 2 , alors on a les arêtes entre 2 et 3, entre 3 et 4 et entre 4 et 1. Il reste le choix entre l'arête entre 1 et 3 (graphe complet) ou non. Si on choisit la non présence de l'arête entre 1 et 2 on a aucune des arêtes entre 2 et 3, entre 3 et 4 et entre 4 et 1. Il reste le choix entre l'arête entre 1 et 3 (avec celle entre 2 et 4) ou aucune arête.

(e) Conclure.

Solution:
On applique la formule de Burnside :

$$\begin{aligned}\frac{1}{|G|}\sum_{g\in G}|\text{Fix}(g)| &= \frac{1}{24}(\text{Fix}(Id) + \binom{4}{2}|\text{Fix}(\text{transposition})| + 2\binom{4}{1}|\text{Fix}(\text{3-cycle})| \\ &\quad + 3!|\text{Fix}(\text{4-cycle})| + 3|\text{Fix}(\text{prod. de 2 transpositions disjointes})|) \\ &= \frac{1}{24}(2^{3+2+1} + \binom{4}{2}2^4 + 2\binom{4}{1}4 + 3! \times 4 + 3 \times 2^4) \\ &= 11\end{aligned}$$

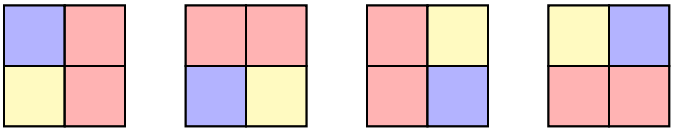
Exercice 9 :
Sur une feuille de papier, on dessine un grand carré de coté 2 formé de 4 petits carrés de côté 1. On colorie ce grand carré en coloriant chacun des petits carrés avec l'une des quatre couleurs bleu (B), jaune (J), noir (N), rouge (R). Une coloration de ce carré correspond à un choix de couleurs pour chacun des petits carrés. Par exemple, dans la figure ci-dessous, en ayant numéroté les petits carrés circulairement en partant du coin inférieur gauche, on a choisi d'attribuer la couleur jaune au carré numéro 1, la couleur rouge au carré numéro 2, la couleur noire au carré numéro 3 et la couleur bleue au carré numéro 4.



1. De combien de façons peut-on colorier ainsi ce grand carré ?

Solution:
On a 4 choix de couleurs par petit carré, soit 4^4 choix.

Une fois découpé, ce grand carré devient mobile et peut être tourné de 90^o, 180^o ou 270^o. Deux colorations qui se déduisent l'une de l'autre en tournant le grand carré deviennent une même coloration du grand carré mobile. On cherche combien de colorations différentes on obtient ainsi. Par exemple, la figure ci-dessous représente une même coloration du grand carré mobile :



2. Modéliser ce problème en utilisant une opération d'un groupe qu'on précisera sur l'ensemble des colorations du carré statique.

Solution:
On représente une coloration du carré statique comme un application de l'ensemble $[\![1, 4]\!]$ (chaque numéro d'un petit carré) dans l'ensemble des couleurs $\{B, J, N, R\}$.
Soit G le groupe formé par l'identité et les rotations de 90°, 180° et 270°.

3. Pour chacun des éléments du groupe, décrire les colorations fixes.

Solution:

- Toute coloration est fixe par l'identité. Le fixateur de l'identité est de cardinal 4^4.
- La rotation d'angle 180° échange les carrés 1 et 3, et les carrés 2 et 4. Une coloration fixe par cette rotation a donc des carrés 1 et 3 de la même couleur et les carrés 2 et 4 de la même couleur. Le fixateur de cette rotation est de cardinal 4^2.
- La rotation d'angle 90° échange circulairement les carrés 1, 2, 3, 4. Une coloration fixe par cette rotation a donc les carrés 1 et 2 de la même couleur, les carrés 2 et 3 de la même couleur, et carrés 3 et 4 de la même couleur. La seule possibilité est que les 4 petits carrés soient de la même couleur. Le fixateur de cette rotation est de cardinal 4.
- De même, la rotation d'angle 270° échange circulairement les carrés 1, 2, 3, 4. La seule possibilité est que les 4 petits carrés soient de la même couleur. Le fixateur de cette rotation est de cardinal 4.

4. Conclure en utilisant la formule de Burnside.

Solution:
Le nombre de colorations du grand carré mobile est

$$\frac{1}{4}(4^4 + 4^2 + 4 + 4) = 70$$

5. Reprendre l'exercice avec un grand carré de coté 3 formé de 9 petits carrés de côté 1.

Solution:
On représente une coloration du carré statique comme une application de l'ensemble $[\![1, 9]\!]$ (chaque numéro d'un petit carré) dans l'ensemble des couleurs $\{B, J, N, R\}$.
Pour chacun des éléments du groupe, on décrit les colorations fixes.

- Toute coloration est fixe par l'identité. Le fixateur de l'identité est de cardinal 4^9.

- La rotation d'angle 180° fixe le carré central, échange les autres carrés deux par deux, par symétrie par rapport au centre : 1 et 5, les carrés 3 et 7, les carrés 2 et 6, et les carrés 4 et 8. Une coloration fixe par cette rotation a donc les carrés échangés de la même couleur. Le fixateur de cette rotation est de cardinal 4^5.
- La rotation d'angle 90° fixe le carré central, échange circulairement les carrés diagonaux 1, 3, 5, 7, et échange circulairement les autres carrés 2, 4, 6, 8. Le fixateur de cette rotation est de cardinal 4^3.
- De même, pour la rotation d'angle 270°. Le fixateur de cette rotation est de cardinal 4^3.

Le nombre de colorations du grand carré mobile est :

$$\frac{1}{4}(4^9 + 4^5 + 4^3 + 4^3) = 65824$$