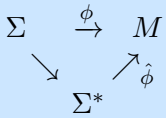
Monoïdes finis

Exercice 1 :
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.



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 $x^m = x^n$.

   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 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 $\Sigma^*|_{\sim_L}$.

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 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.

   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 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.

   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 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 $w = u_1 u_2 ... u_p, u_i \in \Sigma \sqcup \bar{\Sigma}$:

- *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 $w = \hat{\sigma}(w)(\varepsilon) = \hat{\sigma}(w')(\varepsilon) = w'$.

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 $\mathbb{Z}/n\mathbb{Z}$.

   Solution:
   Soit $H_m = \{x \in \mathbb{Z}/n\mathbb{Z} \mid \overline{m}x = \underbrace{x + x + \cdots + x}_{m} = 0\}$
   Démontrons que H_m est un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$:
   - $\forall p \in \mathbb{N}, \overline{p} \cdot 0 = 0$, donc $0 \in H_m$.
   - Soit $x, y \in H_m$.

   $$\begin{aligned}\overline{m}(x-y) &= \underbrace{x - y + x - y + \cdots + x - y}_{m} \\ &= \underbrace{x + x + \cdots + x}_{m} - \underbrace{y + y + \cdots + y}_{m} \\ &= 0\end{aligned}$$

   Donc $x - y \in H_m$.

   (b) H_m est un sous-groupe cyclique de $\mathbb{Z}/n\mathbb{Z}$ de cardinal $\text{pgcd}(m, n)$.

   Solution:
   Soit $a \in \mathbb{Z}$ relevant $x \in \mathbb{Z}/n\mathbb{Z}$.
   Alors $x \in H_m \iff ma \in n\mathbb{Z} \iff a \in n/\text{pgcd}(m,n)\mathbb{Z}$ (en utilisant le théorème de Gauss). Donc H_m est un sous-groupe cyclique engendré par la classe de $n/\text{pgcd}(m, n)$ dans $\mathbb{Z}/n\mathbb{Z}$.
   De plus, pour tout $d \in \mathbb{N}$, $dn/\text{pgcd}(m,n) \in n\mathbb{Z} \iff \text{pgcd}(m,n)|d$, donc la classe de $n/\text{pgcd}(m, n)$ dans $\mathbb{Z}/n\mathbb{Z}$ est exactement d'ordre $\text{pgcd}(m, n)$. Et donc H_m est d'ordre $\text{pgcd}(m, n)$.

   (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.

   Solution:
   Pour d diviseur de n, H_d est un sous-groupe d'ordre $d = \text{pgcd}(m, n)$. Soit H un sous-groupe d'ordre d. Alors $H \subset H_d$ par le théorème de Lagrange. Or $d = |H| = |H_d|$ donc $H = H_d$, d'où l'unicité.

2. On considère l'application suivante :

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

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

Solution:
$\forall x \in \mathbb{Z}/n\mathbb{Z}, \psi(\overline{1})(x) = \overline{1}x = x$, donc $\psi(\overline{1})$ est l'identité de $\mathbb{Z}/n\mathbb{Z}$.
$\forall \overline{m_1}, \overline{m_2} \in (\mathbb{Z}/n\mathbb{Z})^*, \overline{m_1} \cdot \overline{m_2} = \overline{m_1 m_2}$ donc $\psi(\overline{m_1 m_2}) = \psi(\overline{m_1}) \circ \psi(\overline{m_2})$.

(b) Démontrer l'égalité :

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

Solution:
On démontre qu'il y a $d(n)$ orbites. Soit $x, y \in \mathbb{Z}/n\mathbb{Z}$. x et y sont dans une même orbite sous l'action de $(\mathbb{Z}/n\mathbb{Z})^*$ si et seulement si $\langle x \rangle = \langle y \rangle$ ($\exists m \in \mathbb{N}, y = \overline{m}x \Rightarrow y \in \langle x \rangle$). L'orbite de x est l'ensemble des générateurs du sous-groupe $\langle x \rangle$. Il y a donc autant d'orbites que de sous-groupes cycliques de $\mathbb{Z}/n\mathbb{Z}$, soit $d(n)$ (question 1(c)).

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 $\{1, \ldots, n\}$:

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

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 $\{1, \ldots, n\}$. En faisant opérer le sous-groupe $< \sigma >$ par restriction sur $\{1, \ldots, n\}$, 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.

Solution:
Soit ω une orbite pour cette opération. Si $i \in \omega$, alors $\forall l > k \geq 0$, $\sigma^k(i) = \sigma^l(i)$ impose $i = \sigma^{l-k}(i)$ (en appliquant σ^{-k}), donc $\omega = \{i, \sigma(i), \sigma^2(i), \cdots, \sigma^{k-1}(i)\}$ avec k l'entier minimal > 0 tel que $\sigma^k(i) = i$. Ainsi, la restriction de σ à ω est une permutation circulaire : $\tau_\omega + (i, \sigma(i), \sigma^2(i), \cdots, \sigma^{k-1}(i))$.
Les permutations τ_ω, ω parcourant l'ensemble des orbites, commutent deux à deux puisque à supports disjoints. Et si $\forall i \in [\![1, n]\!], (\prod_\omega \tau_\omega)(i) = \tau_{\omega^{(i)}}(i)$, en notant $\omega^{(i)}$ l'orbite de i. Donc $(\prod_\omega \tau_\omega)(i) = \tau_{\omega^{(i)}}(i) = \sigma(i)$. Donc $\prod_\omega \tau_\omega = \sigma$.

Pour l'unicité : si $\sigma = \sigma_1\sigma_2\cdots\sigma_k$, les σ_j étant à supports disjoints. Alors $\forall i \in [\![1, n]\!]$, i est au plus dans le support d'une permutation σ_j, et dans ce cas $\sigma(i) = \sigma_j(i)$. Donc l'orbite de i est le support de σ_j et la restriction de σ à ce support est σ_j. Sinon, i est fixe par σ.

2. Comment calculer l'ordre de σ ?

Solution:
C'est le ppcm des longueurs des cycles dans sa décomposition en cycles à supports disjoints.

3. Déterminer le maximum des ordres des permutations de $\mathcal{S}_6$.

Solution:
On fait l'inventaire des décompositions possibles :

décomposition	ordre
id	1
$(a,b),\ (a,b)(c,d),\ (a,b)(c,d)(e,f)$	2
$(a,b,c), (a,b,c)(d,e,f)$	3
$(a,b,c,d), (a,b,c,d)(e,f)$	4
(a,b,c,d,e)	5
(a,b,c,d,e,f)	6
$(a,b)(c,d,e)$	6

Donc 6. En fait, dans le cas général, c'est le maximum des $\text{ppcm}(l_1, \cdots, l_k), k \in \mathbb{N}$, $l_1 + \cdots + l_k = n$.

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 $\{1, \ldots, 52\}$:

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

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

Solution:
$(1)(2, 3, 5, 9, 17, 33, 14, 27)(4, 7, 13, 25, 49, 46, 40, 28)(6, 11, 21, 41, 30, 8, 15, 29)$
$(10, 19, 37, 22, 43, 34, 16, 31)(12, 23, 45, 38, 24, 47, 42, 32)(18, 35)$
$(20, 39, 26, 51, 50, 48, 44, 36)(52)$

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

Solution:
L'ordre de la permutation σ est le ppcm des longueurs des cycles intervenant dans sa décomposition, soit 8.

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.

   Solution:
   $(a_1, \cdots, a_k) = (a_1, a_2)(a_2, a_3) \cdots (a_{k-1}, a_k)$

2. Démontrer que $\mathfrak{S}_n$ est engendré par les transpositions $(1,2), (2,3), \ldots, (n-1, n)$.

   Solution:
   Si $a < b$, $(a, b) = (a, a+1)(a+1, a+2) \cdots (b-1, b)(b-1, b-2) \cdots (a, a+1)$.

3. Démontrer que $\mathfrak{S}_n$ est engendré par les transpositions $(1,2), (1,3), \ldots, (1, n)$.

   Solution:
   $(a, b) = (1, a)(1, b)(1, a)$

4. Soit E un sous-ensemble de $\{1, \ldots, n\}$. On note $\mathcal{S}_E$ le sous-groupe de $\mathfrak{S}_n$ formé par les permutations qui fixent tous les points de $\{1, \ldots, n\} \setminus E$. 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 $\{1, \ldots, n\}$ 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.

   Solution:
   Notons $\langle X \rangle$ le sous-groupe de $\mathfrak{S}_n$ engendré par X. Le graphe G_X vérifie la propriété suivante pour deux sommets i et j :

$$\text{Il existe un chemin entre } i \text{ et } j \iff \exists \sigma \in \langle X \rangle,\ \sigma(i) = j$$

   Donc $\langle X \rangle = \mathfrak{S}_n$ implique la connexité de G_X.
   Réciproquement, supposons G_X connexe et montrons que $\langle X \rangle = \mathfrak{S}_n$ par récurrence sur $|X|$. Soit $(m, n) \in X$ et $Y = X \setminus \{(m, n)\}$. Deux cas sont possibles :
   - G_Y est connexe. Alors, par récurrence, $\langle Y \rangle = \mathfrak{S}_n$ et a fortiori $\langle X \rangle = \mathfrak{S}_n$.
   - G_Y possède deux composantes connexes E et F qui partitionnent $[\![1, n]\!]$. Alors, si $(i, j) \in Y$, soit i et j sont dans E, soit i et j sont dans F et quitte à échanger les notations, on peut supposer $m \in E$ et $n \in F$. Par hypothèse de récurrence, $\mathcal{S}_E = \langle \{(i, j) \in Y \mid i, j \in E\} \rangle$ et $\langle \mathcal{S}_E, (m, n) \rangle = \mathcal{S}_{E \cup \{n\}}$. De même, $\mathcal{S}_{F \cup \{m\}} = \langle (m, n), \{(i, j) \in Y \mid i, j \in F\} \rangle$, et $\langle X \rangle = \langle \mathcal{S}_{E \cup \{n\}}, \mathcal{S}_{E \cup \{n\}} \rangle = \langle \{(n, i) \mid i < n\} \rangle = \mathfrak{S}_n$.

6. Démontrer qu'une partie génératrice du groupe symétrique $\mathfrak{S}_n$ formée de transpositions contient au moins $n - 1$ transpositions.

   Solution:
   On démontre par récurrence sur un nombre de sommets n qu'un graphe connexe a au moins $n - 1$ arêtes.
   Soit G un graphe à n sommets $1, 2, \cdots, n$ connexes. On retire n et ses arêtes (i, n) avec $i < n$ (il y en a au moins une, sinon n est isolé). Soit H le graphe ainsi obtenu.

- Si H est connexe, on lui applique l'hypothèse de récurrence. Il a au moins $n-2$ arêtes, donc G en a au moins $n-1$.
- Sinon, H a k composantes connexes de cardinal respectifs $n_1, \cdots, n_k$ avec par récurrence au moins $\sum_{i\leq k}(n_i-1) = (\sum_{i\leq k} n_i) - k = n-1-k$ arêtes. Chaque composante connexe disposait dans G d'une arête (i,n), sinon elle reste une composante connexe dans G. On obtient ainsi les k arêtes manquantes.