Monoïdes

Exercice 1 :
Soit M un monoïde. Montrer que toute intersection de congruences sur M est une congruence.

Exercice 2 :
Soit $f : M \to N$ un morphisme de monoïdes. Montrer que si $x \sim y \Leftrightarrow f(x) = f(y)$, alors $\sim$ est une congruence.

Solution:
$\sim$ est bien une relation d'équivalence (réflexive, symétrique, transitive) car $=$ en est une.
Soit $x \sim y$, et soit $u, v \in M$.

$$\begin{aligned} f(uxv) &= f(u)f(x)f(v) \\ &= f(u)f(y)f(v) \text{ car } x \sim y \text{ donc } f(x) = f(y) \\ &= f(uyv) \end{aligned}$$

Donc $uxv \sim uyv$. $\sim$ est donc bien une congruence.

Exercice 3 :
Montrer qu'un isomorphisme de monoïdes libres envoie la base sur la base.

Solution:
Soit $f : M \to N$ un isomorphisme de monoïdes libres et B la base de M. La base B est un code et est donc envoyée sur un code $f[B]$, car f est injective. On a $\langle f[B]\rangle = f[\langle B\rangle]$ par un lemme du cours. Or $\langle B\rangle = M$ et f est surjective, donc $\langle f[B]\rangle = N$.

Exercice 4 :
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 : $M_0 = L$, $M_{n+1} = {M_n}^{-1}M_n \cap M_n{M_n}^{-1}$. 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 plus $M = \cup_n M_n$ 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 $u \in M_n^{-1}M_n \cap M_nM_n^{-1} = M_{n+1} \subset M$. 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 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 5 :
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 6 :
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 $x^s = x^{2s} = x^{3s} = \cdots = x^{rs} = \cdots = x^r$.

Groupes

Exercice 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.