Let Σ a finite alphabet.

Exercice 1 :
Let u and v two words in Σ^*. Show by induction on $|u|+|v|$ that $uv = vu \Rightarrow \exists w \in \Sigma^*, \{u, v\} \subseteq w^*$.

Exercice 2 :
Let u and v be two words in Σ^* , we say that they are conjugate if there exist x and y such that $u = xy$ and $v = yx$. Show that the words u and v are conjugate iff there exists a word z such that $uz = zv$.

Exercice 3 :
Consider the three words x, y, z in Σ^* such that $x^2y^2 = z^2$. Show that there exists a word w in Σ^* and numbers p and q such that $x = w^p$, $y = w^q$ and $z = w^{p+q}$.

Exercice 4 :
Let m and n natural numbers > 0. Solve in Σ^* the equation $u^m = v^n$. First, solve for $\gcd(|v|, |u|) = 1$.

Exercice 5 :
Let M be a finite monoid and let $x \in M$.

1. Show that there two natural numbers m and n such that $m < n$ and $x^m = x^n$.
2. We choose a minimal l from all the numbers n for which there exists $m < n$ such that $x^m = x^n$.
   (a) Show that $1, x, ..., x^{l-1}$ are all distinct.
   (b) Show that the monoid $< x >$ is of cardinality l.
   (c) Let $k < l$ such that $x^k = x^l$. Let r be the unique integer between k and $l - 1$ divisible by $l - k$. Show that $x^k, ..., x^{l-1}$ is a cyclic group of order $l - k$ where x^r is the natural element.
   (d) Show that there exists n such that $x^n = (x^n)^2$ i.e. idempotent. Are there several ?

Exercice 6 (Syntactic monoid) :
Let $L \subset \Sigma^*$ be a language. This defines the equivalence relation on Σ^* :

$$w \sim_L w' \Leftrightarrow \forall u, v \in \Sigma^*,\ uwv \in L \Leftrightarrow uw'v \in L$$

Justify that $\sim_L$ is a congruence on Σ^* ($x \sim y$ iff $uxv \sim uyv$ $\forall v, u \in M$). We define the Syntactic monoid M_L as the quotient $\Sigma^*|_{\sim_L}$.

Exercice 7 (Star-free languages) :
Let Σ be a finite alphabet. The Star-free family of languages is the smallest family containing empty language, singletons and stable by union, passage to complement and concatenation.

1. Show that Σ^* is star-free.
2. Demonstrate that the intersection of two star-free languages is star-free.
3. Let $a, b \in \Sigma$ where $a \neq b$. Show that $(ab)^*$ is star-free.

We say that a finite monoid is aperiodic if the only group it contains is the trivial group $\{1\}$.

4. Let M be a finite monoid. Show that the following are equivalent :

(a) The monoid M is aperiodic.

(b) For all m in M, there exists a nonzero natural number n such that $m^{n+1} = m^n$,

(c) There exists a non zero natural number n such that for all m in M, $m^{n+1} = m^n$.

5. Let L be a regular language and let M_L be its syntactic monoid. By the definition of a syntactic monoid, we deduce by the previous question that M_L is aperiodic if and only if, for all words u, there exists a non-zero natural number n s.t. for all words v, w, $vu^nw \in L \Leftrightarrow vu^{n+1}w \in L$. In this case we denote it by $i(L)$ the smallest natural non-zero number n such that for all words u, v, w, $vu^nw \in L \Leftrightarrow vu^{n+1}w \in L$.

   (a) Show the following(for languages L with finite $i(L)$) :

      i. $i(\{a\}) = 1$,

      ii. $i(L_1 \cup L_2) \leq \max(i(L_1), i(L_2))$,

      iii. $i(L_1L_2) \leq i(L_1) + i(L_2) + 1$,

      iv. $i(\Sigma^* \setminus L) = i(L)$.

   (b) Deduce that a syntactic monoid of a star-free language is aperiodic.

Groupes

Exercice 8 (8) :
Let G be a cyclic group, show that every sub group $G \subseteq H$ is cyclic

Exercice 9 (9) :
Consider the action $\cdot$ of the group G on the set E. Show that :

1. For all $g \in G$, show that the map $f_g : E \to E$ such as $f_g(x) := g \cdot x$ is an inverse bijection of $f_{g^{-1}}$.
2. The map $g \mapsto f_g$ is a morphism from G to the set of map from E to E with the operation $f_g \circ f_{g'}$.

Exercice 10 (10) :
Let p be a prime number. We denote by $(1, \ldots, p)$ the p-cycle (the permutation of the symmetrical group that sends 1 on 2, 2 on 3, ..., $p-1$ on p and p on 1). We denote by G the group generated by the p-cycle $(1, \ldots, p)$. Assuming that Σ a finite alphabet.

1. Show that G is a group of order p.
2. What are the orders of the elements in G ? For each d, we will specify how many G elements are of order d.
3. We take G to act on Σ^p, the set of words of length p written with the letters of Σ as follows :

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

   (a) Demonstrate that this is a group operation.

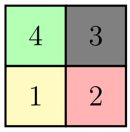
   (b) Determine the fixer of $(1, \ldots, p)$. Deduce the fixer of $(1, \ldots, p)^i$, for any integer i co prime with p.

   (c) Show that the number of orbits, r, of this operation are :

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

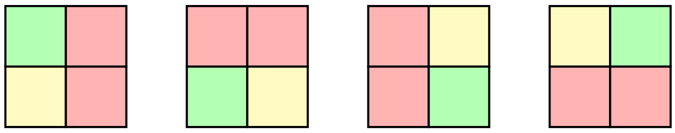
(d) Retrieve Fermat's little theorem ($a^p \equiv_p a$).

Exercice 11 (11) :
On a sheet of paper, a large 2 by 2 square is drawn, consisting of 4 small 1 by 1 squares. We color this large square by coloring each of the small squares with one of the four colors Green (G), yellow (Y), black (B) and red (R). A coloring of this square corresponds to a choice of colors for each of the small squares. For example, in the figure below, having numbered the small squares from the lower left corner, we have chosen to assign the color yellow to the square number 1, the color red to the square number 2, the color black to the square number 3 and the color green squared number 4.



1. How many ways can we color this square in the way described above ?

Once cut, this large square becomes rotatable by 90°, 180° or 270° degrees. We identify the coloring's of the square if they are attainable from each other by rotation. For example, the figure below represents the same coloring of the square after identification :



We now count how many different coloring's we have after this identification.

2. Model this problem using a group operation.
3. For each of the elements of the group, describe their fixers.
4. Conclude the number of possible coloring's.
5. Repeat the exercise with a large 3 by 3 side square formed of 9 small 1 side squares.