**Corrigé de l'exercice 3 du TD2 (Automates et Langages Formels)**
**1.** On vérifie la symmétrie, la réflexivité et la transitivité.
**2.** Si $u$ n'est pas un préfixe de $v$ et que $u < v$ alors $u = xay$ et $v = xbz$ pour certains $x, y, z \in \Sigma^*$ et $a < b \in \Sigma$.
Donc pour tous $w_1, w_2 \in \Sigma^*$, on a

$$uw_1 = xa(yw_1) < xb(yw_2) = vw_2$$

**3.** ($i \Rightarrow ii$) On suppose $i$)
Si $u$ est égal à un de ses conjugués propres, alors $u = ts = st$ pour $t, s \neq \epsilon$ et donc $t$ et $s$ commutent et sont donc puissance d'un même mot (cf. cours) :

$$t = w^k, s = w^{k'}(k, k' \geq 1)$$

et donc $u = w^{k+k'}$ n'est pas primitif. Contradiction avec $i$).
Ainsi, $u$ est strictement inférieur à chacun de ses conjugués propres ($ii$).

($ii \Rightarrow iii$) Par contraposée, on suppose $\neg iii$).
Alors $u = xy, x, y \neq \epsilon$ et $y < u$.
Si $yx < u$, on a montré $\neg ii$)
sinon, $yx \geq u$ donc $y$ est préfixe de $u$ (par $y < u$ et question 2)
donc $u = yw$, donc $yw \leq yx$ (c'est $u \leq yx$)
donc $w \leq x$ et puisque $w$ et $x$ ont même longueur ($|u| - |y|$), on a
$wy \leq xy = u$ ce qui est une négation de $ii$).
(c'était pas si long que ça finalement !)

($iii \Rightarrow i$) Encore une contraposée, on suppose $\neg i$).
Deux cas :
- $u = w^m(w \neq \epsilon, m \geq 2) \Rightarrow w < u : \neg iii)$
- $u = xy, (x, y \neq \epsilon)$ et $yx < u \Rightarrow y < yx < u : \neg iii)$

**4.** Montrons d'abord que $uv < v$.
Si $u$ n'est pas préfixe de $v$, alors $u < v \Rightarrow uv < v$ (question 2)
si par contre $v = ux$, alors $v < x$ (car $v \in L$) et donc

$$uv < ux = v$$

Soit $w$ un suffixe propre de $uv$. Si c'est un suffixe de $v$, alors

$$uv < v \leq w$$

Si par contre $w = xv$ (avec $|x| < |u|$), alors $u$ n'est pas préfixe de $x$ et l'on a

$$u < x \quad (\text{car } u \in L)$$

donc on a bien (question 2) $uv < xv = w$.
Ainsi, $uv$ est inférieur à tous ses suffixes propres et est donc un mot de Lyndon.
**5.** On a $w = uv$ où $w \in L$ et $v$ est le plus long suffixe de $w$ qui soit dans $L$.
Raisonnons par l'absurde en supposant $u \notin L$.
Soit $x$ le plus court suffixe de $u$ non vide tel que $x < u$ (il existe puisque $u \notin L$).
On va montrer qu'alors $xv \in L$

Regardons tous les suffixes de $xv$. Deux cas :

– Soit $z$ un suffixe de $v$. On a (par relation de préfixe, ou par propriété des mots de Lyndon)

$$x < u < w < v \leq z$$

Donc $x < z$ et si $x$ est préfixe de $z$, on a $z = xz'$ avec $z' < v$ et donc $xv < xz' = z$, et sinon, par application de la question 1, on a $xv < z$.

– Soit $x = ab$, $(a, b \neq \epsilon)$. On considère le suffixe $bv$.
Puisque $x$ est le plus court suffixe de $u$ tel que $x < u$, on a

$$x < u < b$$

Or $x$ n'est pas préfixe de $b$ donc $xv < bv$.

On a bien montré que $xv$ était un mot de Lyndon, ce qui contredit la maximalité de $v$.

**6. unicité.** Supposons que l'on ait un mot $w$ qui se décompose de deux manières différentes en mots de Lyndon décroissants. De la même manière que l'on avait fait pour les codes, on peut se ramener à deux décomposition d'un mot $w'$ dont les premiers termes diffèrent (en supprimant tous les mots de la décomposition de $w$ qui sont égaux au début).
On est donc dans la situation

$$\begin{aligned} w' &= u_1 u_2 \dots u_n \\ &= v_1 v_2 \dots v_m \end{aligned}$$

avec $u_1 \neq v_1$. On suppose $|v_1| > |u_1|$.
On considère $k$ tel que

$$v_1 = u_1 u_2 \dots u_{k-1} x$$

où $x$ est un préfixe de $u_k$ ($u_k$ est le dernier $u_i$ que $v_1$ touche).
Par décroissance des décompositions, et relation de préfixe, on a

$$x \leq u_k \leq u_1 \leq v_1$$

et donc $v_1$ n'est pas un mot de Lyndon (contradiction).
**existence.** Par récurrence sur la longueur de $w$. On considère $u$ le plus long suffixe de $w$ qui est dans $L$ ($u$ est non vide car une lettre est dans $L$).

$$w = xu$$

et par hypothèse de récurrence $x = a_1 a_2 \dots a_k$ (décomposition décroissante en mots de $L$).
Si $a_k < u$, alors $a_k u \in L$ (question 4) ce qui contredit la maximalité de $u$, donc $a_k \geq u$ et

$$w = a_1 a_2 \dots a_k u$$

est une décomposition décroissante en mots de $L$.
**7.** On a vu à la question précédente, que $u_n$ est le plus long suffixe de $u$ qui est dans $L$ (preuve de l'existence).
Considérons maintenant $v$ le plus petit suffixe de $u$ (au sens de $\leq$).
Alors $v \in L$ puisqu'aucun de ses suffixes n'est plus petit que lui et pour tout suffixe $xv$ de $u$ plus long, $xv \notin L$ (puisque $v < xv$). Donc $v$ est le plus long suffixe de $u$ qui est dans $L$, c'est donc $u_n$.