Université de Bretagne Occidentale
UFR Sciences et Techniques
L3 DE MATHEMATIQUES

ARITHMÉTIQUE ET APPLICATIONS

Examen terminal, le 13 mai 2024, 14h00-17h00

CORRIGE

Exercice 1. a. Comme $\deg(P) = 3$, il suffit de montrer que P n'a pas de racine dans $\mathbb{F}_3$. Or, $x^3 - x = 0$ dans $\mathbb{F}_3$ quel que soit $x \in \mathbb{F}_3$, par Fermat. D'où $x^3 - x \neq -1$ quel que soit $x \in \mathbb{F}_3$, i.e., $x^3 - x + 1 \neq 0$ quel que soit $x \in \mathbb{F}_3$. Par conséquent, le polynôme P n'a pas de racine dans $\mathbb{F}_3$.

b. On a

$$\dim_{\mathbb{F}_3} \mathbb{F}_3[X]/(P) = \deg(P) = 3$$

car $\bar{1}, \bar{X}, \bar{X}^2$ est un $\mathbb{F}_3$-base du quotient $\mathbb{F}_3[X]/(P)$ d'après la division euclidienne. Du coup,

$$\mathbb{F}_3[X]/(P) \cong \mathbb{F}_3^3$$

comme espaces vectoriels. En particulier,

$$|\mathbb{F}_3[X]/(P)| = |\mathbb{F}_3^3| = 3^3 = 27.$$

c. On cherche un élément de $K^\times$ d'ordre $27 - 1 = 26 = 2 \times 13$, avec 2 et 13 premiers. Il suffit donc de de chercher un élément $x \in K^\times$ tel que $x \neq 1$, $x^2 \neq 1$ et $x^{13} \neq 1$. Les premières conditions sont vérifiées si on prend $x \neq \pm 1$. Il suffit donc que $x^{13} \neq 1$, avec $x \neq \pm 1$, pour que x soit d'ordre 26.

Regardons si $x = \bar{X} \neq \pm 1$ satisfait $x^{13} \neq 1$. On calcule x^{13} par exponentiation rapide :

$$x^{13} = x^{12} \cdot x = (x^6)^2 \cdot x = ((x^3)^2)^2 \cdot x$$

Notons que $x^3 - x + 1 = 0$ dans K, donc $x^3 = x - 1$ et $x^4 = x^2 - x$ dans K, et du coup

$$\begin{aligned}
(x^3)^2 &= (x-1)^2 = x^2 - 2x + 1 = x^2 + x + 1 \\
((x^3)^2)^2 &= (x^2 + x + 1)^2 = x^4 + 2x^3 + 3x^2 + 2x + 1 = x^4 - x^3 - x + 1 = \\
&\quad x^2 - x - x + 1 - x + 1 = x^2 - 1, \text{ et} \\
x^{13} &= ((x^3)^2)^2 \cdot x = (x^2 - 1) \cdot x = x^3 - x = x - 1 - x = -1 \neq 1!
\end{aligned}$$

Donc $g = \bar{X}$ est bien un générateur de $K^\times$.

d. On vient de voir que $g^{13} = -1$. On a donc $\log_g(-1) = 13 \in \mathbb{Z}/26\mathbb{Z}$.

Exercice 2. La décomposition en facteurs premiers de 210 est $210 = 2 \times 3 \times 5 \times 7$. Le Théorème Chinois donne donc un isomorphisme

$$f \colon \mathbb{Z}/210\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$$

défini par $f(\bar{x}) = (\bar{x}, \bar{x}, \bar{x}, \bar{x})$. On détermine une formule pour $f^{-1}(\bar{x}_1, \bar{x}_2, \bar{x}_3, \bar{x}_4)$. Pour ce faire, on cherche une identité de Bézout :

$$u_1 \times 3 \times 5 \times 7 + u_2 \times 2 \times 5 \times 7 + u_3 \times 2 \times 3 \times 7 + u_4 \times 2 \times 3 \times 5 = 1$$

pour $u = (u_1, \dots, u_4) \in \mathbb{Z}^4$.

Comme $3 + (-1) \times 2 = 1$, on a $3 \times 5 + (-1) \times 2 \times 5 = 5$. Comme $(-1) \times 5 + 2 \times 3 = 1$, on obtient par substition

$$(-1) \times 3 \times 5 + 2 \times 5 + 2 \times 3 = 1.$$

Multiplier par 7 donne $(-1) \times 3 \times 5 \times 7 + 2 \times 5 \times 7 + 2 \times 3 \times 7 = 7$. Comme $13 \times 7 + (-3) \times 2 \times 3 \times 5 = 1$, on obtient encore par substitution :

$$(-13) \times 3 \times 5 \times 7 + 13 \times 2 \times 5 \times 7 + 13 \times 2 \times 3 \times 7 + (-3) \times 2 \times 3 \times 5 = 1.$$

On peut donc prendre $u = (-13, 13, 13, -3)$.

On a donc

$$f^{-1}(\bar{x}_1, \bar{x}_2, \bar{x}_3, \bar{x}_4) = (-13) \times 3 \times 5 \times 7 \times x_1 + 13 \times 2 \times 5 \times 7 \times x_2 + \\ 13 \times 2 \times 3 \times 7 \times x_3 + (-3) \times 2 \times 3 \times 5 \times x_4 \pmod{210}.$$

Le groupe multiplicatif de l'anneau produit $\mathbb{Z}2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$ est

$$(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z})^\times = (\mathbb{Z}/2\mathbb{Z})^\times \times (\mathbb{Z}/3\mathbb{Z})^\times \times (\mathbb{Z}/5\mathbb{Z})^\times \times (\mathbb{Z}/7\mathbb{Z})^\times = \\ \{\bar{1}\} \times (\mathbb{Z}/3\mathbb{Z})^\times \times (\mathbb{Z}/5\mathbb{Z})^\times \times (\mathbb{Z}/7\mathbb{Z})^\times.$$

Comme le premier facteur est trivial, une famille génératrice de ce groupe est

$$(\bar{1}, -\bar{1}, \bar{1}, \bar{1}), (\bar{1}, \bar{1}, \bar{2}, \bar{1}), (\bar{1}, \bar{1}, \bar{1}, -\bar{2}).$$

On calcule les images par f^{-1} :

$$\begin{aligned} f^{-1}(\bar{1}, -\bar{1}, \bar{1}, \bar{1}) &= -13 \times 5 \times 7 \times (3+2) + 2 \times 3 \times (13 \times 7 + (-3) \times 5) = \\ &- 2275 + 456 = 35 + 36 = 71 \pmod{210} \\ f^{-1}(\bar{1}, \bar{1}, \bar{2}, \bar{1}) &= 13 \times 5 \times 7 \times (-3+2) + 2 \times 3 \times (13 \times 7 \times 2 + (-3) \times 5) = \\ &- 455 + 1002 = -35 - 48 = -83 \pmod{210} \\ f^{-1}(\bar{1}, \bar{1}, \bar{1}, -\bar{2}) &= 13 \times 5 \times 7 \times (-3+2) + 2 \times 3 \times (13 \times 7 + (-3) \times 5 \times (-2)) = \\ &- 35 + 726 = -35 + 96 = 61 \pmod{210}. \end{aligned}$$

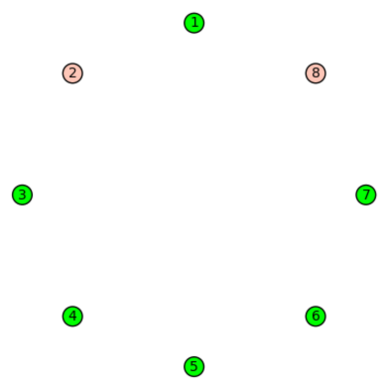
Donc une famille génératrice à 3 éléments de $(\mathbb{Z}/210\mathbb{Z})^\times$ est

$$\overline{71}, -\overline{83}, \overline{61}.$$

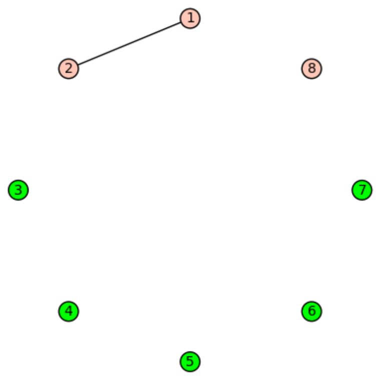
Exercice 3. On applique les règles de calcul du symbole de Jacobi

$$\begin{aligned} \left(\frac{263}{646}\right) &= \left(\frac{263}{323}\right) && \text{car } 646 = 2 \times 323 \\ &= -\left(\frac{323}{263}\right) && \text{car } 263, 323 \equiv 3 \pmod 4 \\ &= -\left(\frac{60}{263}\right) && \text{car } 323 \equiv 60 \pmod{263} \\ &= -\left(\frac{2}{263}\right)^2 \left(\frac{15}{263}\right) && \text{car } 60 = 2^2 \times 15 \\ &= -\left(\frac{15}{263}\right) && \text{car } (\pm 1)^2 = 1 \\ &= \left(\frac{263}{15}\right) && \text{car } 15, 263 \equiv 3 \pmod 4 \\ &= \left(\frac{8}{15}\right) && \text{car } 263 \equiv 8 \pmod{15} \\ &= \left(\frac{2}{15}\right)^3 && \text{car } 8 = 2^3 \\ &= 1 && \text{car } 15 \equiv -1 \pmod 8 \end{aligned}$$

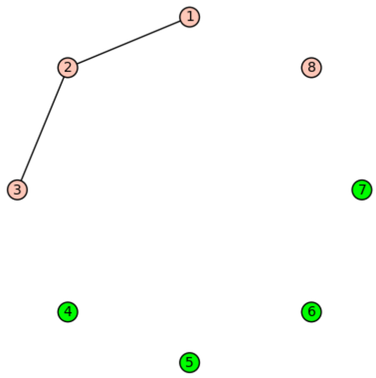
Exercice 4. a. Comme le code de Prüfer $t = (2, 2, 2, 8, 8, 8)$ est de longueur 6, l'arbre correspondant possède 8 sommets. Comme ce code ne contient que 2 et 8, les sommets $1, 3, 4, 5, 6, 7$ sont des feuilles de l'arbre. On commence avec le graphe sans arête sur les sommets $1, \ldots, 8$ où on colorie les feuilles en vert :



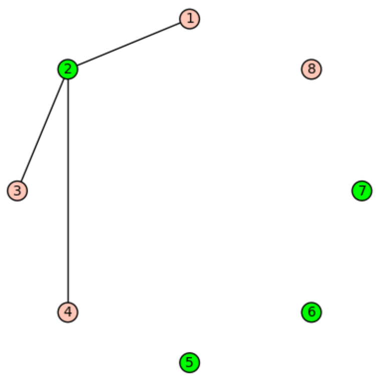
Comme $t_1 = 2$, la plus petite feuille 1 est reliée au sommet 2. Comme il y a des indices $i > 1$ tels que $t_i = 2$, le sommet 2 ne devient pas une feuille à cette étape. On obtient



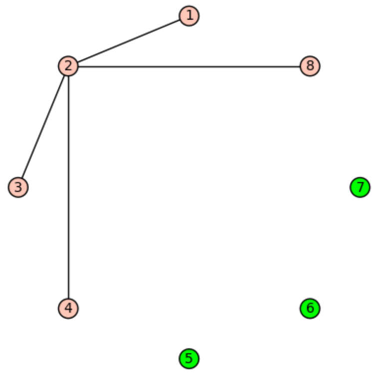
Comme $t_2 = 2$, la plus petite feuille restante 3 est reliée au sommet 2. Comme il y a un indice $i > 2$ tels que $t_i = 2$, le sommet 2 ne devient pas une feuille à cette étape. On obtient



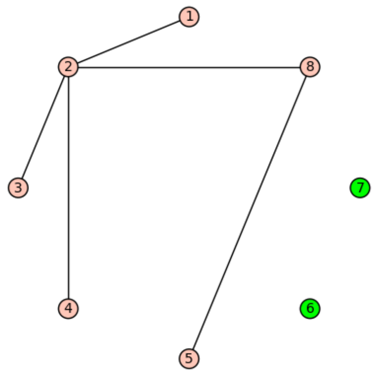
Comme $t_3 = 2$, la plus petite feuille restante 4 est reliée au sommet 2. Comme il n'y a plus d'indice $i > 3$ tels que $t_i = 2$, le sommet 2 devient une feuille à cette étape-ci. On obtient



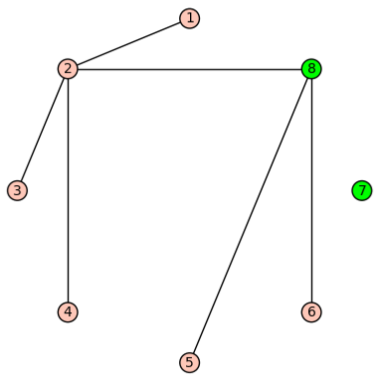
Comme $t_4 = 8$, la plus petite feuille restante 2 est reliée au sommet 8. Comme il y a des indices $i > 4$ tels que $t_i = 8$, le sommet 8 ne devient pas une feuille à cette étape. On obtient



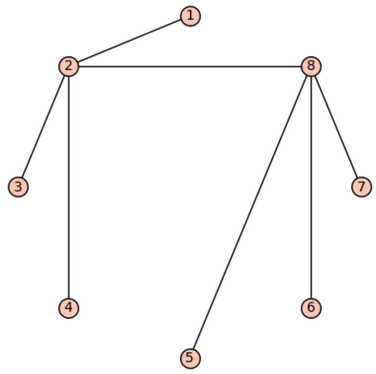
Comme $t_5 = 8$, la plus petite feuille restante 5 est reliée au sommet 8. Comme il y a encore un indice $i > 5$ tels que $t_i = 8$, le sommet 8 ne devient pas une feuille à cette étape. On obtient



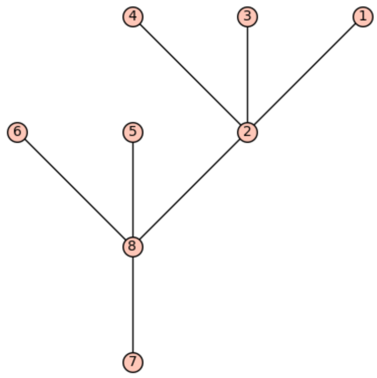
Comme $t_6 = 8$, la plus petite feuille restante 6 est reliée au sommet 8. Comme il n'y a plus d'indice $i > 6$ tels que $t_i = 8$, le sommet 8 devient une feuille à cette étape-ci. On obtient



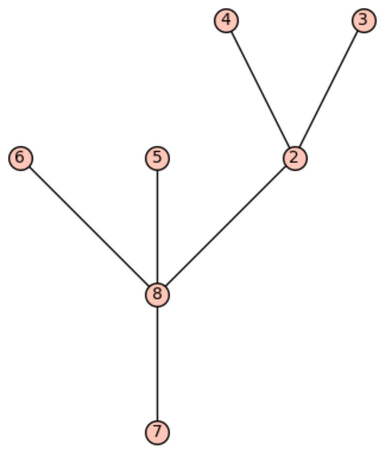
On a épuisé le code de Prüfer, et il nous reste les feuilles 7 et 8 qu'il faut relier pour obtenir le graphe



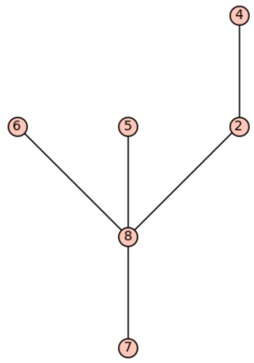
qu'on dresse en arbre comme celui-ci par exemple



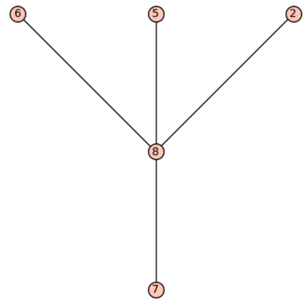
b. On commence avec l'arbre ci-dessus qu'on vient de déterminer. Ses feuilles sont $1, 3, 4, 5, 6, 7$. La plus petite est 1 qui est reliée au sommet 2. On a donc $t_1 = 2$. On supprime la feuille 1 et on obtient



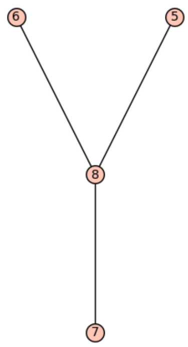
Ses feuilles sont $3, 4, 5, 6, 7$. La plus petite est 3 qui est reliée au sommet 2. On a donc $t_2 = 2$. On supprime la feuille 3 et on obtient



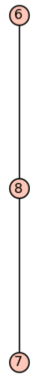
Ses feuilles sont $4, 5, 6, 7$. La plus petite est 4 qui est reliée au sommet 2. On a donc $t_3 = 2$. On supprime la feuille 4 et on obtient



Ses feuilles sont $2, 5, 6, 7$. La plus petite est 2 qui est reliée au sommet 8. On a donc $t_4 = 8$. On supprime la feuille 2 et on obtient



Ses feuilles sont $5, 6, 7$. La plus petite est 5 qui est reliée au sommet 8. On a donc $t_5 = 8$. On supprime la feuille 5 et on obtient



Ses feuilles sont $6, 7$. La plus petite est 6 qui est reliée au sommet 8. On a donc $t_6 = 8$. On supprime la feuille 6 et on obtient

et l'algorithme est terminé ! On obtient bien le code de Prüfer $t = (2, 2, 2, 8, 8, 8)$.

Exercice 5. L'ensemble des sommets du graphe g en question est

$$V = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}.$$

On pose $W = \emptyset$ et

$$\ell(v) = \begin{cases} +\infty & \text{si } v \neq 0, \text{ et} \\ 0 & \text{si } v = 0, \end{cases}$$

Le complementaire W^c de W dans V est

$$\{0, 1, 2, 3, 4, 5, 6, 7, 8\}.$$

Les valeurs de ℓ sont respectivement

$$\{0, +\infty, +\infty, +\infty, +\infty, +\infty, +\infty, +\infty, +\infty\}.$$

Le minimum de ℓ sur W^c est 0. Ce minimum est atteint 1 fois pour le(s) sommet(s) : $\{0\}$. On prend le sommet $u = 0$. On rajoute le sommet 0 a W. Les voisins du sommet 0 dans W^c est/sont le(s) sommet(s) $\{2, 5, 7\}$. La valeur de $l(u) + w(uv)$ pour le sommet $v = 2$ est 3. Comme c'est inferieur strict a la valeur $l(v) = +\infty$, on remplace $l(v)$ par $l(u) + w(uv)$. Et on pose $p(2) = 0$. La valeur de $l(u) + w(uv)$ pour le sommet $v = 5$ est 1. Comme c'est inferieur strict a la valeur $l(v) = +\infty$, on remplace $l(v)$ par $l(u) + w(uv)$. Et on pose $p(5) = 0$. La valeur de $l(u) + w(uv)$ pour le sommet $v = 7$ est 2. Comme c'est inferieur strict a la valeur $l(v) = +\infty$, on remplace $l(v)$ par $l(u) + w(uv)$. Et on pose $p(7) = 0$. Et on réitère.

Le complementaire W^c de W est

$$\{1, 2, 3, 4, 5, 6, 7, 8\}.$$

Les valeurs de ℓ sur W^c sont respectivement

$$\{+\infty, 3, +\infty, +\infty, 1, +\infty, 2, +\infty\}.$$

Le minimum de ℓ sur W^c est 1. Ce minimum est atteint 1 fois pour le(s) sommet(s) : $\{5\}$. On prend le sommet $u = 5$. On rajoute le sommet 5 a W. Les voisins du sommet 5 dans W^c est/sont le(s) sommet(s) $\{2, 6\}$. La valeur de $l(u) + w(uv)$ pour le sommet $v = 2$ est 2. Comme c'est inferieur strict a la valeur $l(v) = 3$, on remplace $l(v)$ par $l(u) + w(uv)$. Et on pose $p(2) = 5$. La valeur de $l(u) + w(uv)$ pour le sommet $v = 6$ est 2. Comme c'est inferieur strict a la valeur $l(v) = +\infty$, on remplace $l(v)$ par $l(u) + w(uv)$. Et on pose $p(6) = 5$. Et on réitère.

Le complementaire W^c de W est

$$\{1, 2, 3, 4, 6, 7, 8\}.$$

Les valeurs de ℓ sur W^c sont respectivement

$$\{+\infty, 2, +\infty, +\infty, 2, 2, +\infty\}.$$

Le minimum de ℓ sur W^c est 2. Ce minimum est atteint 3 fois pour le(s) sommet(s) : $\{2, 6, 7\}$. On prend le sommet $u = 2$. On rajoute le sommet 2 a W. Les voisins du sommet 2 dans W^c est/sont le(s) sommet(s) $\{3, 8\}$. La valeur de $l(u) + w(uv)$ pour le sommet $v = 3$ est 8. Comme c'est inferieur strict a la valeur $l(v) = +\infty$, on remplace $l(v)$ par $l(u) + w(uv)$. Et on pose $p(3) = 2$. La valeur de $l(u) + w(uv)$ pour le sommet $v = 8$ est 3. Comme c'est inferieur strict a la valeur $l(v) = +\infty$, on remplace $l(v)$ par $l(u) + w(uv)$. Et on pose $p(8) = 2$. Et on réitère.

Le complementaire W^c de W est

$$\{1, 3, 4, 6, 7, 8\}.$$

Les valeurs de ℓ sur W^c sont respectivement

$$\{+\infty, 8, +\infty, 2, 2, 3\}.$$

Le minimum de ℓ sur W^c est 2. Ce minimum est atteint 2 fois pour le(s) sommet(s) : $\{6, 7\}$. On prend le sommet $u = 6$. On rajoute le sommet 6 a W. Les voisins du sommet 6 dans W^c est/sont le(s) sommet(s) $\{1, 8\}$. La valeur de $l(u) + w(uv)$

pour le sommet $v = 1$ est 4. Comme c'est inferieur strict a la valeur $l(v) = +\infty$, on remplace $l(v)$ par $l(u) + w(uv)$. Et on pose $p(1) = 6$. La valeur de $l(u) + w(uv)$ pour le sommet $v = 8$ est 4. Ce n'est pas inferieur strict a la valeur $l(v) = 3$. Et on réitère.

Le complementaire W^c de W est

$$\{1, 3, 4, 7, 8\}.$$

Les valeurs de ℓ sur W^c sont respectivement

$$\{4, 8, +\infty, 2, 3\}.$$

Le minimum de ℓ sur W^c est 2. Ce minimum est atteint 1 fois pour le(s) sommet(s) : $\{7\}$. On prend le sommet $u = 7$. On rajoute le sommet 7 a W. Les voisins du sommet 7 dans W^c est/sont le(s) sommet(s) $\{3\}$. La valeur de $l(u) + w(uv)$ pour le sommet $v = 3$ est 10. Ce n'est pas inferieur strict a la valeur $l(v) = 8$. Et on réitère.

Le complementaire W^c de W est

$$\{1, 3, 4, 8\}.$$

Les valeurs de ℓ sur W^c sont respectivement

$$\{4, 8, +\infty, 3\}.$$

Le minimum de ℓ sur W^c est 3. Ce minimum est atteint 1 fois pour le(s) sommet(s) : $\{8\}$. On prend le sommet $u = 8$. On rajoute le sommet 8 a W. Les voisins du sommet 8 dans W^c est/sont le(s) sommet(s) $\{1, 3, 4\}$. La valeur de $l(u) + w(uv)$ pour le sommet $v = 1$ est 4. Ce n'est pas inferieur strict a la valeur $l(v) = 4$. La valeur de $l(u) + w(uv)$ pour le sommet $v = 3$ est 7. Comme c'est inferieur strict a la valeur $l(v) = 8$, on remplace $l(v)$ par $l(u) + w(uv)$. Et on pose $p(3) = 8$. La valeur de $l(u) + w(uv)$ pour le sommet $v = 4$ est 4. Comme c'est inferieur strict a la valeur $l(v) = +\infty$, on remplace $l(v)$ par $l(u) + w(uv)$. Et on pose $p(4) = 8$. Et on réitère.

Le complementaire W^c de W est

$$\{1, 3, 4\}.$$

Les valeurs de ℓ sur W^c sont respectivement

$$\{4, 7, 4\}.$$

Le minimum de ℓ sur W^c est 4. Ce minimum est atteint 2 fois pour le(s) sommet(s) : $\{1, 4\}$. On prend le sommet $u = 1$. On rajoute le sommet 1 a W. Les voisins du sommet 1 dans W^c est/sont le(s) sommet(s) $\{4\}$. La valeur de $l(u) + w(uv)$ pour le sommet $v = 4$ est 6. Ce n'est pas inferieur strict a la valeur $l(v) = 4$. Et on réitère.

Le complementaire W^c de W est

$$\{3, 4\}.$$

Les valeurs de ℓ sur W^c sont respectivement

$$\{7, 4\}.$$

Le minimum de ℓ sur W^c est 4. Ce minimum est atteint 1 fois pour le(s) sommet(s) : $\{4\}$. On prend le sommet $u = 4$. On rajoute le sommet 4 a W. Les voisins du sommet 4 dans W^c est/sont le(s) sommet(s) $\{3\}$. La valeur de $l(u) + w(uv)$ pour le sommet $v = 3$ est 6. Comme c'est inferieur strict a la valeur $l(v) = 7$, on remplace $l(v)$ par $l(u) + w(uv)$. Et on pose $p(3) = 4$. Et on réitère.

Le complementaire W^c de W est

$$\{3\}.$$

Les valeurs de ℓ sur W^c sont respectivement

$$\{6\}.$$

Le minimum de ℓ sur W^c est 6. Ce minimum est atteint 1 fois pour le(s) sommet(s) : $\{3\}$. On prend le sommet $u = 3$. On rajoute le sommet 3 a W. Les voisins du sommet 3 dans W^c est/sont le(s) sommet(s) $\{\}$. Et on a terminé !

Voici le tableau correspondant

v	$\ell(v), p(v)$
0	|
1	4, 6 |
2	3, 0 2, 5 |
3	8, 2 7, 8 6, 4 |
4	4, 8 |
5	1, 0 |
6	2, 5 |
7	2, 0 |
8	3, 2 |