Contrôle de connaissances
Accq203a – Algorithmes pour l'algèbre

2 février 2022
10h15 – 11h45

Documents autorisés : 1 feuille A4 recto-verso manuscrite, dictionnaire de traduction imprimé.
Sont interdits : notes de cours, polycopié et matériel électronique
(calculatrice, ordinateur, téléphone, etc.).

Durée : 1h30.

Exercice 1. On se place dans l'anneau $\mathbb{F}_3[x]$. On cherche à résoudre le système $\mathbf{Az} = \mathbf{b}$ où

$$\mathbf{A} = ((a_{i,j}))_{\substack{1\le i\le 2,\\ 1\le j\le 3}} = \begin{pmatrix} x^2 - x + 1 & x^4 + x^3 - x^2 + x - 1 & x^3 - x^2 + x \\ x + 1 & x^3 + 1 & x^2 + x \end{pmatrix} \in (\mathbb{F}_3[x])^{2\times 3}$$

et

$$\mathbf{b} = \begin{pmatrix} x^3 + 1 \\ x^2 - x + 1 \end{pmatrix} \in (\mathbb{F}_3[x])^2$$

et où $\mathbf{z}$ est inconnu. Afin de simplifier les calculs, on donne dans la figure 1 la liste des polynômes irréductibles de degré 2 et de degré 3 de l'anneau $\mathbb{F}_3[x]$.

1. Calculer la dérivée du polynôme $a_{2,2} = x^3 + 1$. Que peut-on en déduire au sujet de la factorisation du polynôme $a_{2,2}$? (0,5pt)
2. Calculer la dérivée $a'_{1,2}$ du polynôme $a_{1,2} = x^4 + x^3 - x^2 + x - 1$. Que vaut le pgcd entre les polynômes $a_{1,2}$ et $a'_{1,2}$? Que peut-on en déduire ? (0,5pt)
3. Déterminer un polynôme $u \in \mathbb{F}_3[x]$ tel que le pgcd entre $a_{1,2}$ et u révèle le produit des facteurs linéaires de $a_{1,2}$. (0,5pt)
4. Calculer le pgcd entre $a_{1,2}$ et u et en déduire la factorisation complète de $a_{1,2}$. (1pt)
5. Rappeler le nom de l'algorithme de factorisation de polynômes dont s'inspire la question précédente. (0,5pt)
6. Par une opération sur les colonnes entre la première et la deuxième colonne, annuler le coefficient $a_{2,2}$ de la matrice $\mathbf{A}$. (1pt)
7. Par une opération sur les colonnes entre la première et la troisième colonne, annuler le coefficient $a_{2,3}$ de la matrice $\mathbf{A}$. (1pt)
8. Calculer la forme normale de Smith $\boldsymbol{\Delta}$ de la matrice $\mathbf{A}$. On demande trois matrices $\boldsymbol{\Delta}$, $\mathbf{L}$ et $\mathbf{C}$ telles que $\mathbf{LAC} = \boldsymbol{\Delta}$. (2pts)
9. Le système $\mathbf{Az} = \mathbf{b}$ admet-il une solution ? (0,5pt)
10. Donner une solution particulière du système $\mathbf{Az} = \mathbf{b}$. (0,5pt)

Irréductibles de degré 2 dans $\mathbb{F}_3[x]$
x^2+1
x^2+x-1
x^2-x-1

Irréductibles de degré 3 dans $\mathbb{F}_3[x]$
x^3-x+1
x^3-x-1
x^3+x^2-1
x^3+x^2+x-1
x^3+x^2-x+1
x^3-x^2+1
x^3-x^2+x+1
x^3-x^2-x-1

FIGURE 1 – Polynômes irréductibles dans $\mathbb{F}_3[x]$

11. Donner l'ensemble des solutions du système $\mathbf{Az} = \mathbf{b}$. (0,5pt)

Solution 1. 1. La dérivée du polynôme $a_{2,2} = x^3 + 1$ vaut 0 : par conséquent, $a_{2,2}$ est une puissance de la caractéristique, ici 3. On a la factorisation $x^3 + 1 = (x+1)^3$.

2. La dérivée $a'_{1,2}$ du polynôme $a_{1,2} = x^4 + x^3 - x^2 + x - 1$ vaut $x^3 + x + 1$. Comme

$$a_{1,2} = (x+1)a'_{1,2} + x^2 - x + 1,$$

$$a'_{1,2} = (x+1)(x^2 - x + 1) + x,$$

$$x^2 - x + 1 = (x-1)x + 1,$$

le pgcd vaut

$$a_{1,2} \wedge a'_{1,2} = 1.$$

Comme $a'_{1,2}$ est non nul, on peut en déduire que $a_{1,2}$ est sans facteur carré.

3. Il est classique de prendre le polynôme $u(x) = x^p - x \in \mathbb{F}_p[x]$ pour révéler le produit des facteurs linéaires. Ici, on choisit donc $u(x) = x^3 - x$.

4. D'après les calculs

$$a_{1,2} = (x+1)u - (x+1)$$

$$u = (x^2 - x)(x+1) + 0,$$

le pgcd vaut ici

$$u \wedge a_{1,2} = x + 1.$$

On en déduit la factorisation complète en divisant $a_{1,2}$ par $x+1$. Il vient

$$a_{1,2} = (x+1)(x^3 - x - 1).$$

On se doute que $(x^3 - x - 1)$ irréductible. En effet, $a_{1,2}$ est sans facteur carré, donc $x^3 - x - 1$ n'admet pas de diviseur de degré 1. Il ne peut pas être factorisé.

5. On s'est inspiré de l'algorithme de Cantor-Zassenhaus.

6. On initialise deux matrices $\mathbf{L} = \mathbf{I}_2$ et $\mathbf{C} = \mathbf{I}_3$ pour noter les opérations.
On applique $C_2 \leftarrow C_2 - (x+1)^2 C_1$. On obtient

$$\mathbf{A} = \begin{pmatrix} x^2+2x+1 & 2x^2+1 & x^3+2x^2+x \\ x+1 & 0 & x^2+x \end{pmatrix} \qquad \mathbf{C} = \begin{pmatrix} 1 & -x^2+x-2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

7. On applique $C_3 \leftarrow C_3 - xC_1$. On obtient

$$\mathbf{A} = \begin{pmatrix} x^2+2x+1 & 2x^2+1 & 0 \\ x+1 & 0 & 0 \end{pmatrix} \qquad \mathbf{C} = \begin{pmatrix} 1 & 2x^2+x+2 & 2x \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

8. On commence par échanger $L_1 \leftrightarrow L_2$. On a alors

$$\mathbf{A} = \begin{pmatrix} 0 & x^2-1 & 0 \\ x+1 & -x^3- & 2x^2-x \end{pmatrix} \qquad \mathbf{L} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \mathbf{C} = \begin{pmatrix} 1 & -x^2+x-2 & 2x \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

On continue avec $L_2 \leftarrow L_2 - (x+1)L_1$.

$$\mathbf{A} = \begin{pmatrix} x+1 & 0 & 0 \\ 0 & 2x^2+1 & 0 \end{pmatrix} \qquad \mathbf{L} = \begin{pmatrix} 0 & 1 \\ 1 & -x-1 \end{pmatrix} \qquad \mathbf{C} = \begin{pmatrix} 1 & -x^2+x-2 & 2x \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

On termine avec $L_2 \leftarrow -L_2$.

$$\mathbf{\Delta} = \begin{pmatrix} x+1 & 0 & 0 \\ 0 & (x-1)(x+1) & 0 \end{pmatrix} \qquad \mathbf{L} = \begin{pmatrix} 0 & 1 \\ -1 & x+1 \end{pmatrix} \qquad \mathbf{C} = \begin{pmatrix} 1 & -x^2+x-2 & 2x \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Point important : on s'assure que le premier coefficient diagonal de $\mathbf{\Delta}$ divise bel et bien le second, ce qui est le point clé d'une forme normale de Smith.

9. Résoudre $\mathbf{Az} = \mathbf{b}$ revient à résoudre $\mathbf{L}^{-1}\mathbf{\Delta}\mathbf{C}^{-1}\mathbf{z} = \mathbf{b}$ ou encore $\mathbf{\Delta z}' = \mathbf{Lb}$ avec $\mathbf{z} = \mathbf{Cz}'$. Ici, on a

$$\mathbf{b}' = \mathbf{Lb} = \begin{pmatrix} x^2-x+1 \\ 0 \end{pmatrix} = \begin{pmatrix} (x+1)^2 \\ 0 \end{pmatrix}.$$

Comme $(x+1)^2$ est divisible par $x+1$, on peut bien trouver $\mathbf{z}'$ qui doit valoir ici $\begin{pmatrix} x+1 \\ 0 \\ 0 \end{pmatrix}$.

10. On en déduit alors $\mathbf{z} = \mathbf{Cz}'$ qui vaut alors

$$\mathbf{z} = \begin{pmatrix} x+1 \\ 0 \\ 0 \end{pmatrix}$$

11. Les solutions homogènes du systèmes sont de la forme $\mathbf{z}'$ qui doit valoir ici $\begin{pmatrix} 0 \\ 0 \\ t(x) \end{pmatrix}$ où $t(x)$ prend n'importe quelle valeur dans $\mathbb{F}_3[x]$, autrement dit de la forme

$$\mathbf{z} = \begin{pmatrix} (x+1) + 2x \cdot t(x) \\ 0 \\ t(x) \end{pmatrix}$$

Exercice 2. On s'intéresse au réseau Λ engendré par les deux vecteurs

$$\mathbf{u}_1 = \begin{pmatrix} 1 \\ 0 \\ 1000 \end{pmatrix} \qquad \mathbf{u}_2 = \begin{pmatrix} 0 \\ 1 \\ -2236 \end{pmatrix} \in \mathbb{R}^3.$$

1. Quel est le rang du réseau Λ en tant que $\mathbb{Z}$-module ? Quelle est sa partie de torsion ? (0,5pt)
2. Calculer une base LLL réduite $\{\mathbf{u}_2'', \mathbf{u}_1'\}$ du réseau Λ. On demande que $\|\mathbf{u}_2''\| \leq \|\mathbf{u}_1'\|$. (2,5pts)
3. Trouver des coefficients α et β tels que $\mathbf{u}_2'' = \alpha \mathbf{u}_1 + \beta \mathbf{u}_2$. (1pt)
4. Proposez une bonne approximation $\frac{a}{b}$ par un rationnel du réel $\sqrt{5} = 2,236067977$ dont le numérateur a et le dénominateur b soient petits. (0,5pt)

Solution 2.

1. Le rang est 2. Il n'y a pas de partie de torsion ; elle est triviale.
2. Clairement, $\mathbf{u}_2$ est le plus long des deux vecteurs. On essaie de le raccourcir avec $\mathbf{u}_1$. On peut commencer par établir que
$$\frac{\langle \mathbf{u}_1, \mathbf{u}_2 \rangle}{\|\mathbf{u}_1\|^2} = -\frac{2236000}{1000001} \simeq -2,236.$$
On calcule un nouveau vecteur :
$$\mathbf{u}_2' = \mathbf{u}_2 + 2\mathbf{u}_1 = \begin{pmatrix} 2 \\ 1 \\ -236 \end{pmatrix}$$
On reprend en essayant de raccourcir $\mathbf{u}_1$ avec $\mathbf{u}_2'$. On a
$$\frac{\langle \mathbf{u}_1, \mathbf{u}_2 \rangle}{\|\mathbf{u}_2'\|^2} = -\frac{26222}{6189} \simeq -4,237.$$
On calcule un nouveau vecteur :
$$\mathbf{u}_1' = \mathbf{u}_1 + 4\mathbf{u}_2' = \begin{pmatrix} 9 \\ 4 \\ 56 \end{pmatrix}$$
On reprend en essayant de raccourcir $\mathbf{u}_2'$ avec $\mathbf{u}_1'$. On a
$$\frac{\langle \mathbf{u}_2', \mathbf{u}_1' \rangle}{\|\mathbf{u}_1'\|^2} = -\frac{13194}{3233} \simeq -4,081.$$
$$\mathbf{u}_2'' = \mathbf{u}_2' + 4\mathbf{u}_1' = \begin{pmatrix} 38 \\ 17 \\ 12 \end{pmatrix}$$
Cette fois-ci, le processus s'arrête. Nous avons trouvé un nouvelle base $(\mathbf{u}_2'', \mathbf{u}_1')$.
Remarque de calcul : pour calculer $\mathbf{u}_2'$, on aurait pu alternativement évaluer $\mathbf{u}_2 + \mathbf{u}_1$, $\mathbf{u}_2 + 2\mathbf{u}_1$, $\mathbf{u}_2 + 3\mathbf{u}_1$, etc et noter que la norme est minimisée pour $\mathbf{u}_2 + 2\mathbf{u}_1$. Cela évite de devoir approcher le quotient de deux produits scalaires assez gros.
3. On peut résoudre le système d'équation à l'œil : il suffit de prendre $\alpha = 38$ et $\beta = 17$.
4. Si la fraction $\frac{a}{b}$ est une très bonne approximation par un rationnel du réel $\sqrt{5} = 2,236067977$, on doit notamment avoir que la quantité $1000a - 2236b$ reste très petite. En ce cas, le vecteur $a\mathbf{u}_1 + b\mathbf{u}_2$, qui vaut
$$a\mathbf{u}_1 + b\mathbf{u}_2 = \begin{pmatrix} a \\ b \\ 1000a - 2236b \end{pmatrix},$$
est un vecteur de petite norme (ici, la norme vaut $a^2 + b^2 + (1000a - 2236b)^2$).

Or, lorsqu'on calcule une base LLL d'un réseau de rang 2, on obtient le plus petit vecteur du réseau. Ainsi, le vecteur $\mathbf{u}_1''$ fournit une proposition de court vecteur et fournit, par identification des coefficients, un approximation, qui est ici $38/17 \simeq 2.235294117647$. L'erreur commise est de $8 \cdot 10^{-4}$.

Exercice 3. On donne le polynôme

$$f(x) = x^6 + 3x^5 + x^4 - x^3 - x^2 + 5x + 2 \in \mathbb{Z}[x].$$

On a observé que la factorisation du polynôme $f(x)$, plongé dans $\mathbb{F}_{821}[x]$, est

$$f(x) \equiv (x + 214)(x + 610)(x^4 + 820x + 2) \mod 821.$$

1. Soit $g(x) \in \mathbb{Z}[x]$ un diviseur de $f(x)$ dans $\mathbb{Z}[x]$. Quelles valeurs le degré du polynôme g peut-il prendre ? (0,5pt)

On rappelle que la borne de Mignotte associée à un polynôme $f(x) = \sum_{k=0}^{d} f_k x^k \in \mathbb{Z}[x]$ unitaire a pour expression

$$\sqrt{d+1} \cdot 2^d \cdot \max_{0 \le k \le d} |f_k|.$$

2. On suppose que $g \in \mathbb{Z}[x]$ est un diviseur de f. Que peut-on dire des coefficients du polynôme g ? (1pt)
3. Peut-il exister un polynôme $g \in \mathbb{Z}[x]$ divisant f tel que $g(x) \equiv x + 214 \mod 821$? Même question si $g(x) \equiv x + 610 \mod 821$ ou si $g(x) \equiv x^4 + 820x + 2 \mod 821$. (1pt)
4. En déduire la factorisation complète de $f(x)$ dans $\mathbb{Z}[x]$. (1pt)

Solution 3.

1. Quand on plonge le polynôme g dans $\mathbb{F}_{821}[x]$, il se factorise avec des facteurs de f, qui sont de degrés 1, 1 et 4. Donc g peut être degré 1, $2 = 1 + 1$, 4, $5 = 4 + 1$ ou 6.
2. On calcule la borne de Mignotte qui vaut ici $320\sqrt{7} \simeq 846,5$. On peut en déduire ici que tout coefficient de g est de valeur absolue inférieure à 847.
   NB : en préparant le sujet, j'avais obtenu une borne de Mignotte valant 108. Il s'agit d'une erreur de ma part. La suite fonctionne pas du coup. Voici le raisonnement qui aurait été attendu.
3. Supposons qu'il existe un diviseur $g(x)$ tel que $g(x) \equiv x + 214 \mod 821$. A cause de la borne de Mignotte, ses coefficients sont compris entre -108 et 108. Or ni $x + 214$ a déjà des coefficients centrés en zéro : ceux-ci ne peuvent pas être diminués en jouant avec des congruences modulo 821. Donc il n'existe pas de diviseur $g(x)$ tel que $g(x) \equiv x + 214 \mod 821$.

   On peut centrer le polynôme $x + 610$ avec la congruence $x + 610 \equiv x - 211 \mod 821$, mais pour autant, même en le centrant, on ne parvient pas à lui faire passer la borne de Mignotte. Donc il n'existe pas de diviseur $g(x)$ tel que $g(x) \equiv x + 610 \mod 821$.

   Enfin, on note que $x^4 + 820x + 2 \equiv x^4 - x + 2 \mod 821$, qui passe la borne de Mignotte. Donc il est possible qu'il existe un diviseur $g(x)$ tel que $g(x) \equiv x^4 + 820x + 2 \mod 821$.
4. De la question précédente, on peut déjà noter qu'il n'y pas de facteur de degré 1 et noter que $x^4 - x + 2$ est irréductible dans $\mathbb{Z}[x]$ (sinon, il serait réductible dans $\mathbb{F}_{821}[x]$) . De plus, on peut diviser f par $x^4 - x + 2$. On obtient alors

   $$f = (x^2 + 3x + 1)(x^4 - x + 2)$$

   qui est la factorisation de f en produit de polynômes irréductibles.

Exercice 4. On considère les polynômes suivants de $\mathbb{F}_5[x,y]$:

$$f_1 = y^6 + 2y^4 + y^3 + 2y^2 - y,$$
$$f_2 = y^5 + y^4 + y^2 + 2x + y - 2,$$
$$f_3 = y^4 + xy - y^2 - x - y + 1,$$
$$f_4 = x^3 + x^2 - x - 1,$$
$$f_5 = xy^2 - y^3 + 2y^2 + 2x - y - 2,$$
$$f_6 = x^2 + 2xy + y^2 - x - y.$$

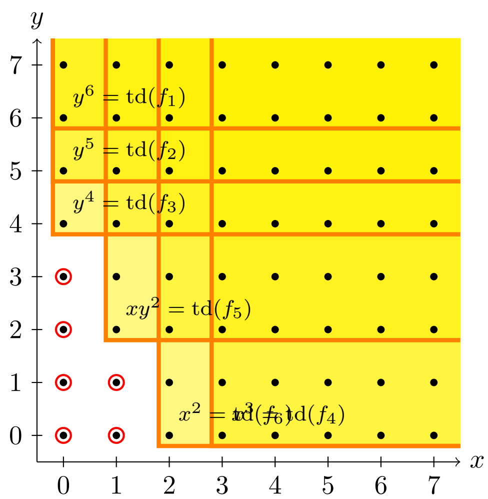
On note $\mathfrak{I} \subseteq \mathbb{F}_5[x,y]$ l'idéal engendré par les six polynômes f_1, f_2, …, f_6. On affirme que $(f_1, f_2, \ldots, f_6)$ est une base de Gröbner de $\mathfrak{I}$, à la fois pour l'ordre deglex (on compare le degré total d'abord, puis l'ordre lexicographique) mais aussi pour l'ordre lex (ordre lexicographique avec $x > y$) et invlex (ordre lexicographique avec $y > x$). On ne demande pas de prouver ce fait.

1. Dans cette question, on munit $\mathbb{F}_5[x,y]$ de l'ordre deglex. Décrire l'ensemble des monômes qui appartiennent à l'idéal monomial des termes dominants de $\mathfrak{I}$. (1pt)
2. En déduire un sous-ensemble de $(f_1, f_2, \ldots, f_6)$ qui forme une base de Gröbner minimale réduite de $\mathfrak{I}$ pour deglex. (0,5pt)
3. Quelle est la dimension du quotient $\mathbb{F}_5[x,y]/\mathfrak{I}$ en tant qu'espace vectoriel sur $\mathbb{F}_5$? (0,5pt)
4. Dans cette question, on munit $\mathbb{F}_5[x,y]$ de l'ordre lex. Lequel des polynômes f_1, f_2, …, f_6 appartient forcément à une base de Gröbner minimale réduite de $\mathfrak{I}$? (1pt)
5. On note $\mathcal{V}(\mathfrak{I})$ l'ensemble des racines du système (0,5pt)

$$f_1(x,y) = f_2(x,y) = \cdots = f_6(x,y) = 0.$$

Soit $h(x) \in \mathbb{F}_5[x]$ un polynôme qui s'annule sur tout $\mathcal{V}(\mathfrak{I})$. Est-il vrai que le polynôme h appartient forcément à l'idéal $\mathfrak{I}$?

Solution 4. 1. Puisque $(f_1, f_2, \ldots, f_6)$ est une base de Gröbner de $\mathfrak{I}$, l'idéal des termes dominants de $\mathfrak{I}$ est engendré par l'idéal des termes dominants de $(f_1, f_2, \ldots, f_6)$, c'est-à-dire est engendré par y^6, y^5, y^4, x^3, xy^2 et x^2. On peut, par conséquent, dessiner le diagramme en escalier suivant pour le décrire. Les monômes qui appartiennent à $\mathrm{td}(\mathfrak{I})$ sont les multiples de y^6, y^5, y^4, x^3, xy^2 & x^2 et ont été coloriés en jaune.



2. Il suffit de conserver les monômes dominants de f_3, f_5 et f_6 pour engendrer le même idéal monômial. Par contre, si on retire l'un des trois polynômes restants, l'idéal engendré par les monômes change. Aussi (f_3, f_5, f_6) forme une base de Groebner minimale réduite pour $\mathfrak{I}$ pour l'ordre deglex.
3. Il suffit de compter les monômes entourés en rouge qui fournissent une base vectorielle du quotient. On a $\dim \mathbb{F}_5[x,y]/\mathfrak{I} = 6$.
4. On observe que f_1 est un polynôme qui ne dépend que de y : ceci montre que $\mathfrak{I} \cap \mathbb{F}_5[y]$ est non-vide. Or, si G_{lex} est une base de Groebner pour l'ordre lex, on a doit avoir que $G' \cap \mathbb{F}_5[y]$ est une base de Groebner de $\mathfrak{I} \cap \mathbb{F}_5[y]$. Donc $G_{\mathsf{lex}} \cap \cap \mathbb{F}_5[y]$ est non vide. Mais f_1 est le seul polynôme qui ne dépend que de y et il est le seul dans ce cas là. Comme la base de Groebner minimale réduite peut être obtenue à partir de f_1, f_2, …, f_6, c'est forcément f_1 qui en fait partie.
5. Non ce n'est pas vrai ici et nous allons en donner un contre-exemple. On peut noter que f_4 se factoriser en $f_4(x) = (x-1)(x+1)^2$. Donc si $(x,y) \in \mathcal{V}(\mathfrak{I})$, alors $x \in \{-1, 1\}$. Ainsi le polynôme $h_0(x) = x^2 - 1 = (x-1)(x+1)$ s'annule aussi sur $\mathcal{V}(\mathfrak{I})$. Mais, pour les mêmes raisons qu'à la question 5, une base de Groebner G_{invlex} pour invlex contient forcément f_4 et d'autres polynômes qui dépendent de x et de y. Quand on essaie de diviser le polynôme h_0 par G_{invlex}, le reste de la division demeure h_0. Donc $h_0 \notin \mathfrak{I}$.

Supplément pour comprendre : On pourrait se demander quels polynômes forment chaque base de Gröbner de l'idéal $\mathfrak{I}$ en fonction des ordres possibles. Nous avons déjà traité le cas de l'ordre deglex.

Dans le cas de lex, les polynômes sont, par ordre décroissant,

$$f_4 = x^3 + x^2 - x - 1,$$

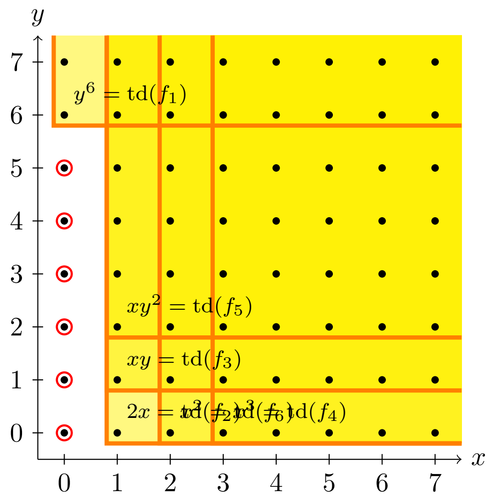
$$f_6 = x^2 + 2xy + y^2 - x - y.$$

$$f_5 = xy^2 - y^3 + 2y^2 + 2x - y - 2,$$

$$f_3 = xy - x + y^4 - y^2 - y + 1,$$

$$f_2 = 2x + y^5 + y^4 + y^2 + y - 2,$$

$$f_1 = y^6 + 2y^4 + y^3 + 2y^2 - y,$$



La base de Gröbner minimale réduite est $G_{\mathsf{lex}} = \{f_2, f_1\}$.

Dans le cas de invlex, les polynômes sont, par ordre décroissant,

$$f_1 = y^6 + 2y^4 + y^3 + 2y^2 - y,$$

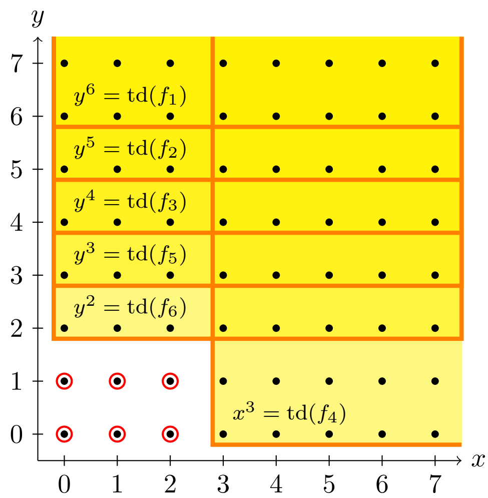
$$f_6 = y^2 + 2xy - y + x^2 - x.$$

$$f_5 = -y^3 + xy^2 + 2y^2 - y + 2x - 2,$$

$$f_3 = y^4 - y^2 + xy - y - x + 1,$$

$$f_2 = y^5 + y^4 + y^2 + y + 2x - 2,$$

$$f_4 = x^3 + x^2 - x - 1,$$



La base de Gröbner minimale réduite est $G_{\mathsf{invlex}} = \{f_6, f_4\}$

Dans les deux cas supplémentaires, on observe que le calcul du quotient donne bien la même dimension que celle calculée à la question 3.