Contrôle de connaissances
ACCQ203a – Algorithmes pour l'algèbre

1er février 2023
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 définit la matrice $\mathbf{A}$ suivante

$$\mathbf{A} = \begin{pmatrix} -27 & 40 & -55 \\ -40 & 59 & -82 \\ 15 & -23 & 29 \end{pmatrix} \in \mathbb{Z}^{3\times 3}.$$

On pose $\mathbf{A}' = 10\mathbf{A}$.

1. Donner la forme normale de Smith de $\mathbf{A}$. (On ne demande pas les matrices de passage). (3 pts)
2. On note N le sous-module de $\mathbb{Z}^3$ engendré par les colonnes de la matrice $\mathbf{A}$. Quel est le rang de la partie libre et la suite des facteurs invariants de la partie de torsion du quotient $\mathbb{Z}^3/N$? (1 pt)
3. On note N' le sous-module de $\mathbb{Z}^3$ engendré par les colonnes de la matrice $\mathbf{A}' = 10\mathbf{A}$. Même question pour le quotient $\mathbb{Z}^3/N'$. (½ pt)
4. Quel est l'idéal annulateur de la partie de torsion de $\mathbb{Z}^3/N'$? (½ pt)

Solution 1. 1. On effectue la suite d'opération suivantes. On commence par essayer de faire apparaître un 1 en position de pivot (ce qui semble possible puisque le pgcd entre 27 et 40 est 1).

Avec $C_2 \leftarrow C_2 + C_1$,

$$\mathbf{A} = \begin{pmatrix} -27 & 13 & -55 \\ -40 & 19 & -82 \\ 15 & -8 & 29 \end{pmatrix} \qquad \mathbf{L} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad \mathbf{C} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Avec $C_1 \leftarrow C_1 + 2C_2$,

$$\mathbf{A} = \begin{pmatrix} -1 & 13 & -55 \\ -2 & 19 & -82 \\ -1 & -8 & 29 \end{pmatrix} \qquad \mathbf{L} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad \mathbf{C} = \begin{pmatrix} 3 & 1 & 0 \\ 2 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

On peut rendre le coefficient pivot positif avec $C_1 \leftarrow -C_1$

$$\mathbf{A} = \begin{pmatrix} 1 & 13 & -55 \\ 2 & 19 & -82 \\ 1 & -8 & 29 \end{pmatrix} \qquad \mathbf{L} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad \mathbf{C} = \begin{pmatrix} -3 & 1 & 0 \\ -2 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

On simplifie les lignes en effectuant $L_2 \leftarrow L_2 - 2L_1$ et $L_3 \leftarrow L_3 - L_1$

$$\mathbf{A} = \begin{pmatrix} 1 & 13 & -55 \\ 0 & -7 & 28 \\ 0 & -21 & 84 \end{pmatrix} \qquad \mathbf{L} = \begin{pmatrix} 1 & 0 & 0 \\ -2 & 1 & 0 \\ -1 & 0 & 1 \end{pmatrix} \qquad \mathbf{C} = \begin{pmatrix} -3 & 1 & 0 \\ -2 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

On fait de même sur les colonnes avec $C_2 \leftarrow C_2 - 13C_1$ et $C_3 \leftarrow C_3 + 55C_1$

$$\mathbf{A} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -7 & 28 \\ 0 & -21 & 84 \end{pmatrix} \qquad \mathbf{L} = \begin{pmatrix} 1 & 0 & 0 \\ -2 & 1 & 0 \\ -1 & 0 & 1 \end{pmatrix} \qquad \mathbf{C} = \begin{pmatrix} -3 & 40 & -165 \\ -2 & 27 & -110 \\ 0 & 0 & 1 \end{pmatrix}$$

À ce stade, nous observons que le 1 en pivot divise tous les coefficients restants. On peut donc s'attaquer au prochain sous-bloc. Si nous étions pressés de conclure, on pourrait simplement constater que le bloc 2×2 restant est de rang 1 et de pgcd 7. Directement, on sais que le bloc se réduira simplement en $\begin{pmatrix} 7 & 0 \\ 0 & 0 \end{pmatrix}$

Pour le plaisir de faire des calculs, nous corrigeons les signes avec $C_2 \leftarrow -C_2$.

$$\mathbf{A} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 7 & 28 \\ 0 & 21 & 84 \end{pmatrix} \qquad \mathbf{L} = \begin{pmatrix} 1 & 0 & 0 \\ -2 & 1 & 0 \\ -1 & 0 & 1 \end{pmatrix} \qquad \mathbf{C} = \begin{pmatrix} -3 & -40 & -165 \\ -2 & -27 & -110 \\ 0 & 0 & 1 \end{pmatrix}$$

On continue avec l'opération $C_3 \leftarrow C_3 - 4C_2$

$$\mathbf{A} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 7 & 0 \\ 0 & 21 & 0 \end{pmatrix} \qquad \mathbf{L} = \begin{pmatrix} 1 & 0 & 0 \\ -2 & 1 & 0 \\ -1 & 0 & 1 \end{pmatrix} \qquad \mathbf{C} = \begin{pmatrix} -3 & -40 & -5 \\ -2 & -27 & -2 \\ 0 & 0 & 1 \end{pmatrix}$$

Il reste à faire $L_3 \leftarrow L_3 - 3L_2$

$$\mathbf{A} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 7 & 0 \\ 0 & 0 & 0 \end{pmatrix} \qquad \mathbf{L} = \begin{pmatrix} 1 & 0 & 0 \\ -2 & 1 & 0 \\ 5 & -3 & 1 \end{pmatrix} \qquad \mathbf{C} = \begin{pmatrix} -3 & -40 & -5 \\ -2 & -27 & -2 \\ 0 & 0 & 1 \end{pmatrix}$$

On pose

$$\mathbf{\Delta} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 7 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

2. On peut observer que $\mathbf{LAC} = \mathbf{\Delta}$ équivaut à $\mathbf{A} = \mathbf{L}^{-1}\mathbf{\Delta}\mathbf{C}^{-1}$. Comme $\mathbf{C}$ est une matrice de $\mathbf{GL}_3(\mathbb{Z})$, l'image N de $\mathbf{A}$ est aussi l'image de la matrice $\mathbf{L}^{-1}\mathbf{\Delta}$. Appelons $\mathbf{l}_1$, $\mathbf{l}_2$, $\mathbf{l}_3$ les vecteurs colonne de la matrice $\mathbf{L}^{-1}$. Ainsi une base de N est simplement $(\mathbf{l}_1, 7\mathbf{l}_2)$. Comme $\mathbf{L}$ est une matrice de $\mathbf{GL}_3(\mathbb{Z})$, $\mathbf{l}_1$, $\mathbf{l}_2$, $\mathbf{l}_3$ forme une base de $\mathbb{Z}^3$.
   On peut alors facilement identifier le quotient $\mathbb{Z}^3/N$ à
   $$0\mathbf{l}_1 \oplus (\mathbb{Z}/7\mathbb{Z})\mathbf{l}_2 \oplus \mathbb{Z}\mathbf{l}_3 \simeq (\mathbb{Z}/7\mathbb{Z}) \oplus \mathbb{Z}.$$
   La partie libre est $\mathbb{Z}$, de rang 1. La partie de torsion est $(\mathbb{Z}/7\mathbb{Z})$, les facteurs invariants sont simplement (7).

3. Le raisonnement est le même avec $10\boldsymbol{\Delta}$ à la place de $\boldsymbol{\Delta}$. La base de N' est $(10\mathbf{l}_1, 70\mathbf{l}_2)$. Le quotient $\mathbb{Z}^3/N'$ s'identifie à

$$(\mathbb{Z}/10\mathbb{Z})\mathbf{l}_1 \oplus (\mathbb{Z}/70\mathbb{Z})\mathbf{l}_2 \oplus \mathbb{Z}\mathbf{l}_3 \simeq (\mathbb{Z}/10\mathbb{Z}) \oplus (\mathbb{Z}/70\mathbb{Z}) \oplus \mathbb{Z}.$$

La partie libre est $\mathbb{Z}$, de rang 1. La partie de torsion est $(\mathbb{Z}/10\mathbb{Z}) \oplus (\mathbb{Z}/70\mathbb{Z})$, les facteurs invariants sont désormais $(10, 70)$.

4. Il s'agit de l'ensemble des multiples de 70, à savoir l'idéal $70\mathbb{Z}$.

Exercice 2. On définit les vecteurs

$$\mathbf{u} = \begin{pmatrix} -9 \\ 10 \\ 6 \\ 11 \end{pmatrix} \quad \text{et} \quad \mathbf{v} = \begin{pmatrix} -3 \\ 3 \\ 2 \\ 2 \end{pmatrix} \in \mathbb{Z}^4.$$

On munit $\mathbb{Z}^4$ du produit scalaire usuel. On appelle Λ le sous-$\mathbb{Z}$-module de $\mathbb{Z}^4$ engendré par les vecteurs $\mathbf{u}$ et $\mathbf{v}$.

1. Calculer une base LLL réduite de Λ. (2 pts)
2. On souhaite placer une famille de boules de ouvertes de rayon r, de centre $\mathbf{x}$ avec $\mathbf{x} \in \Lambda$ et qui ne s'interpénètrent pas. Pour quelles valeurs de r est-ce possible ? (1pt)
3. Combien de voisins la frontière d'une boule touche-t-elle dans le (les) empilement(s) décrit(s) à la question précédente ? (½ pt)

Solution 2.

1. Le vecteur $\mathbf{v}$ a l'air d'être le plus court des deux (on se passe du calcul). On a $\|\mathbf{v}\|^2 = 26$ et

$$\frac{\langle \mathbf{u}, \mathbf{v} \rangle}{\|\mathbf{v}\|^2} = \frac{91}{26} = 3 + \frac{1}{2}$$

On décide de retrancher $\mathbf{w} \leftarrow \mathbf{u} - 3\mathbf{v}$. On obtient

$$\mathbf{w} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 5 \end{pmatrix}$$

qui est aussi de norme 26.

La famille $(\mathbf{v}, \mathbf{w})$ est donc une base LLL réduite.

2. Le premier minimum est de longueur $\sqrt{26}$. On peut donc placer des boules de rayon $r \leq \frac{1}{2}\sqrt{26}$.
3. On est ici dans une configuration très particulière. On a un troisième vecteur de norme $\sqrt{26}$ qui est

$$\mathbf{w} - \mathbf{v} = \begin{pmatrix} 3 \\ -2 \\ -2 \\ 3 \end{pmatrix}$$

On retrouve la configuration du réseau $\mathbb{A}_2$ (à une homothétie près). Lorsque $r = \frac{1}{2}\sqrt{26}$, il y a 6 boules qui touchent chaque boule centrale. Sinon, si $r < \frac{1}{2}\sqrt{26}$, il y a 0 boules qui touchent chaque boule centrale.

Exercice 3. On donne le polynôme

$$h(z) = z^8 + z^7 + z^3 - 1 \in \mathbb{Z}[z]$$

et le polynôme

$$f(x) = x^8 + x^7 + x^3 - 1 \in \mathbb{F}_3[x].$$

1. Vérifier que f ne possède pas de facteurs de degré 1. (½ pt)
2. Déterminer la factorisation sans facteurs carrés de $f \in \mathbb{F}_3[x]$. (½ pt)
3. On a calculé le pgcd suivant (½ pt)

$$f(x) \wedge \left(x^9 - x\right) = x^4 + 1.$$

   Que peut-on dire des degrés des facteurs irréductibles du polynôme $f \in \mathbb{F}_3[x]$?
4. Vérifier que le polynôme $z^4 + 1$ divise le polynôme $h(z)$ dans $\mathbb{Z}[z]$. (1 pt)
5. Que peut-on dire des degrés des facteurs irréductibles du polynôme $h \in \mathbb{Z}[z]$? (½ pt)
6. Calculer la matrice de Petr-Berlekamp $\mathbf{Q}$ associée au polynôme $x^4 + 1$. (½ pt)
7. Calculer une base $\mathcal{B}$ du noyau de $(\mathbf{Q} - \mathbf{I})$. Pouvait-on prévoir le cardinal de $\mathcal{B}$? (½ pt)
8. Quels sont les éléments de la sous-algèbre de Petr-Berlekamp $\mathcal{A} \subseteq \mathbb{F}_3[x]$? (½ pt)
9. Déterminer un élément $u(x)$ de $\mathcal{A}$ tel que $(x^4 + 1) \wedge u$ n'est pas trivial et factoriser $x^4 + 1$ dans $\mathbb{F}_3[x]$. (½ pt)
10. Nous rappelons que $3^8 = 6561$ et nous observons l'identité suivante

$$z^4 + 1 = \left(z^2 + 2695z - 1\right)\left(z^2 - 2695z - 1\right) \mod 3^8.$$

   Nous rappelons l'expression de la borne de Mignotte pour un polynôme unitaire de degré d et à coefficients entiers dans l'intervalle $[-M, M]$:

$$\sqrt{d+1} \cdot 2^d \cdot M.$$

   Montrer que le polynôme $z^4 + 1 \in \mathbb{Z}[z]$ est irréductible. (½ pt)
11. Donner la factorisation complète de $h \in \mathbb{Z}[z]$. (½ pt)

Solution 3.

1. On calcule les valeurs $f(0) = -1$, $f(1) = -1$ et $f(-1) = 1$ qui sont toutes non nulles.
2. Il faut commencer par calculer la dérivée

$$f'(x) = -x^7 + x^6 = -x^6(x - 1).$$

   Le pgcd $f \wedge f'$ vaut 1, car ni 0 ni 1 ne sont des racines de f. En conséquence, f est déjà sous forme sans facteurs carrés.
3. Le pgcd $f(x) \wedge \left(x^{3^2} - x\right)$ attrape tous les facteurs de degré divisant 2. Mais, nous avons vu qu'il n'y a pas de facteurs de degré 1. Donc f possède deux facteurs irréductible de degré 2 (et dont le produit est $x^4 + 1$) et des facteurs irréductibles de degré qui ne divisent pas 2. La somme des degrés de ces derniers facteurs valant 4, la seule possibilité est qu'il y ait un seul facteur irréductible de degré 4.
4. On a (en posant la division)

$$z^8 + z^7 + z^3 - 1 = (z^4 + 1)(z^4 + z^3 - 1).$$

5. On en déduit que (z^4+z^3-1) est forcément un facteur irréductible de h et que soit (z^4+1) est irréductible, soit se factorise en deux morceaux sur $\mathbb{Z}[z]$.
6. On obtient la matrice
$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \in \mathbb{F}_3^{4\times 4}.$$
7. Une base de
$$\mathbf{Q}-\mathbf{I} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix} \in \mathbb{F}_3^{4\times 4}$$
est donnée par les vecteurs $(1,0,0,0)$ et $(0,1,0,1)$. On savait déjà que x^4+1 avait deux facteurs, donc ce cardinal était prévisible.
8. Il y a neuf éléments dans $\mathcal{A}$ qui sont
$$\alpha+\beta x+\beta x^3$$
avec $\alpha,\beta\in\mathbb{F}_3$.
9. Pour trouver u, on a intérêt à choisir un polynôme non constant et unitaire, donc prendre $\beta=1$. Ensuite, si $\alpha=0$, on a $x^3+x=x(x^2+1)$ qui contient les racine carrées de -1 alors que x^4+1 contient les racine quartiques primitives de -1. Mieux vaut prendre
$$u=1+x+x^3$$
On a dans ce cas
$$x^4+1=x\cdot(x^3+x+1)-(x^2+x-1)$$
et
$$x^3+x+1=(x+2)\cdot(x^2+x-1)$$
Donc
$$(x^4+1)\wedge(x^3+x+1)=(x^2+x-1)$$
On en déduit la factorisation
$$x^4+1=(x^2+x-1)(x^2-x-1)$$
10. Si z^4+1 était réductible, on aurait un facteur $g(z)\in\mathbb{Z}$ avec des coefficients compris entre $-B$ et B avec
$$B=\sqrt{5}\cdot 2^5\cdot 1$$
d'après la borne de Mignotte. Mais alors ce facteur apparaîtrait tel quel modulo 3^8. Or ce n'est pas le cas. Donc z^4+1 est irréductible.
11. La factorisation complète de $h(z)$ est finalement
$$z^8+z^7+z^3-1=(z^4+1)(z^4+z^3-1).$$

Exercice 4. On considère les polynômes suivants
$$\begin{cases} g_1(x,y) &=& x-4y^2-y \\ g_2(x,y) &=& xy+x+3y^2 \end{cases}$$
dans $\mathbb{F}_{11}[x,y]$ muni de l'ordre lexicographique sur les monômes (avec $x>y$).

1. Calculer le polynôme de syzygie $s = S(g_1, g_2)$. (½ pt)
2. Calculer le reste r du polynôme s dans sa pseudo-divsion par g_1. (1 pt)
3. Montrer que $\{g_1, r\}$ engendre le même idéal que l'idéal $\mathfrak{I} = \langle g_1, g_2 \rangle$. (½ pt)
4. Montrer que $\{g_1, r\}$ est une base de Gröbner minimale et réduite de l'idéal $\mathfrak{I}$. On conseille de donner le principe avant d'effectuer le calcul. (1½ pts)
5. Déterminer l'ensemble des racines de r dans $\mathbb{F}_{11}$. (½ pt)
6. En déduire l'ensemble des racines du système (1 pt)

$$(\mathcal{S}) \quad \begin{cases} g_1(x, y) &= 0 \\ g_2(x, y) &= 0 \end{cases}$$

7. Proposer une base vectorielle et calculer la dimension, en tant que $\mathbb{F}_{11}$-espace vectoriel, du quotient $\mathbb{F}_{11}[x, y]/\mathfrak{I}$. (½ pt)

Solution 4.

1. On calcule le polynôme

$$s = S(g_1, g_2) = y\, g_1 - g_2 = -x - 4y^3 - 4y^2.$$

2. On a

$$s + g_1 = -4y^3 + 3y^2 - y$$

Donc $r = -4y^3 + 3y^2 - y$.

3. Clairement, $r = (y + 1)g_1 - g_2$ appartient à $\mathfrak{I}$, donc $\{g_1, r\}$ engendre un idéal contenu dans l'idéal $\mathfrak{I}$. Par ailleurs,

$$g_2 = (y + 1)g_1 - r.$$

ce qui montre que l'idéal $\mathfrak{I}$ est inclus dans l'idéal engendré par $\{g_1, r\}$.

4. On commence par calculer le polynôme de syzygie entre g_1 et r. Il s'agit de

$$t = y^3 f_1 - xr = 5xy^3 - 3xy^2 + xy - 4y^5 - y^4$$

On cherche ensuite à simplifier t en le réduisant par une pseudo-division par f_1 et par r. Pour se simplifier la tâche, on note que

$$\frac{1}{5} t = xy^3 - 5xy^2 - 2xy - 3y^5 + 2y^4$$

et que

$$\frac{1}{-4} r = y^3 + 2y^2 + 3y.$$

On commence avec

$$\frac{1}{5} t - y^3 f_1 = -5xy^2 - 2xy + y^5 + 3y^4.$$

Puis

$$\frac{1}{5} t - (y^3 - 5y^2) f_1 = -2xy + y^5 + 5y^4 - 5y^3.$$

Puis

$$\frac{1}{5} t - (y^3 - 5y^2 - 2y) f_1 = y^5 + 5y^4 - 2y^3 - 2y^2.$$

Puis

$$\frac{1}{5} t - (y^3 - 5y^2 - 2y) f_1 - y^2 \frac{1}{-4} r = 3y^4 - 5y^3 - 2y^2.$$

Et finalement

$$\frac{1}{5}t - (y^3 - 5y^2 - 2y)f_1 - (y^2 + 3y)\frac{1}{-4}r = 3y^4 - 5y^3 - 2y^2.$$

Ceci démontre que la base $\{g_1, r\}$ est une base de Groebner minimale réduite.

5. Les racines de
$$r = 7y^3 + 3y^2 - y = -4y(y + 4)(y - 2)$$
sont 0, -4 et 2.

6. On substitue les trois valeurs dans le système. Pour $y = 0$, on obtient
$$(\mathcal{S}_0) \quad \begin{cases} g_1(x, 0) & = & x \\ g_2(x, 0) & = & x \end{cases}$$
qui est s'annule pour $x = 0$.
Pour $y = -4$, on obtient
$$(\mathcal{S}_{-4}) \quad \begin{cases} g_1(x, 0) & = & x - 5 \\ g_2(x, 0) & = & -3x + 4 \end{cases}$$
qui est s'annule pour $x = 5$.
Pour $y = 2$, on obtient
$$(\mathcal{S}_{-4}) \quad \begin{cases} g_1(x, 0) & = & x + 4 \\ g_2(x, 0) & = & 3x + 1 \end{cases}$$
qui est s'annule pour $x = -4$.
Il y a trois solutions $(0, 0)$, $(5, -4)$ et $(-4, 2)$.

7. On peut utiliser le fait que $\{g_1, r\}$ est une base de Groebner et dessiner un diagramme en escalier pour déterminer les monômes qui ne sont pas plus réduits. Il reste 1, y et y^2, qui forment une base. Le quotient est de dimension 3.

	1	2	3	4	5	−5	−4	−3	−2	−1
1	1	2	3	4	5	−5	−4	−3	−2	−1
2	2	4	−5	−3	−1	1	3	5	−4	−2
3	3	−5	−2	1	4	−4	−1	2	5	−3
4	4	−3	1	5	−2	2	−5	−1	3	−4
5	5	−1	4	−2	3	−3	2	−4	1	−5
−5	−5	1	−4	2	−3	3	−2	4	−1	5
−4	−4	3	−1	−5	2	−2	5	1	−3	4
−3	−3	5	2	−1	−4	4	1	−2	−5	3
−2	−2	−4	5	3	1	−1	−3	−5	4	2
−1	−1	−2	−3	−4	−5	5	4	3	2	1

FIGURE 1 – Table des produits dans $\mathbb{F}_{11}$

x	1	2	3	4	5	-5	-4	-3	-2	-1
x^{-1}	1	-5	4	3	-2	2	-3	-4	5	-1

FIGURE 2 – Table des inverses dans $\mathbb{F}_{11}$