Contrôle de connaissances
ACCQ203a – Algorithmes pour l'algèbre

31 janvier 2024
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. Sujet en 9 pages.

Exercice 1. Dans cet exercice, on munit $\mathbb{R}^4$ du produit scalaire et de la norme usuels. On donne les vecteurs

$$\mathbf{v}_1 = \begin{pmatrix} -2 \\ 4 \\ -3 \\ 1 \end{pmatrix} \in \mathbb{Z}^4 \qquad \text{et} \qquad \mathbf{v}_2 = \begin{pmatrix} -9 \\ 3 \\ 7 \\ -1 \end{pmatrix} \in \mathbb{Z}^4.$$

On s'intéresse à l'ensemble Λ des vecteurs de $\mathbb{Z}^4$ orthogonaux à $\mathbf{v}_1$ et à $\mathbf{v}_2$.

1. Exprimer Λ comme le noyau $\ker \mathbf{A} = \{\mathbf{x} \in \mathbb{Z}^4;\ \mathbf{Ax} = \mathbf{0}\}$ d'une certaine matrice $\mathbf{A}$. Donner le nom d'une forme normale de matrice qui permet de calculer un noyau. (1 pt)
2. Mettre la matrice $\mathbf{A}$ sous forme normale citée à la question précédente et donner une base de Λ. (3 pts)
3. Chercher un vecteur $\mathbf{b} \in \mathbb{Z}^4$ non nul et de norme minimale dans Λ . Vérifier que $\|\mathbf{b}\| = 2$. (1,5 pts)
4. On souhaite positionner des boules de rayon identique r centrées en chacun des points de Λ sans qu'elles s'interpénètrent. Pour quelles valeurs de r est-ce possible ? (0,5 pt)

Solution 1.

1. On peut considérer la matrice

$$\mathbf{X} = \begin{pmatrix} -2 & 4 & -3 & 1 \\ -9 & 3 & 7 & -1 \end{pmatrix} \in \mathbb{Z}^{2\times 4}$$

dont on cherche la forme normale d'Hermite.

2. On travaille exclusivement sur les colonnes. On effectue les opérations simultanément sur $\mathbf{X}$ et $\mathbf{U}$

$$\mathbf{X} = \begin{pmatrix} -2 & 4 & -3 & 1 \\ -9 & 3 & 7 & -1 \end{pmatrix} \qquad \mathbf{X} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Comme nous travaillons à la main, nous allons au plus efficace pour obtenir un résultat. Le coefficient -1 placé en dernière ligne et colonne nous tend les bras. Nous commençons par $C_4 \leftarrow -C_4$.

$$\mathbf{X} = \begin{pmatrix} -2 & 4 & -3 & -1 \\ -9 & 3 & 7 & 1 \end{pmatrix} \qquad \mathbf{X} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

Nous simplifions $C_1 \leftarrow C_1 + 9C_4$, $C_2 \leftarrow C_2 - 3C_4$, $C_3 \leftarrow C_3 - 7C_4$:

$$\mathbf{X} = \begin{pmatrix} -11 & 7 & 4 & -1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \qquad \mathbf{X} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ -9 & 3 & 7 & -1 \end{pmatrix}$$

Nous retranchons $C_2 \leftarrow C_2 - 2C_3$:

$$\mathbf{X} = \begin{pmatrix} -11 & -1 & 4 & -1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \qquad \mathbf{X} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & -2 & 1 & 0 \\ -9 & -11 & 7 & -1 \end{pmatrix}$$

Nous replaçons le -1 obtenu en position de pivot $C_3 \leftrightarrow C_2$:

$$\mathbf{X} = \begin{pmatrix} -11 & 4 & -1 & -1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \qquad \mathbf{X} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & -2 & 0 \\ -9 & 7 & -11 & -1 \end{pmatrix}$$

Nous changeons le signe avec $C_3 \leftarrow -C_3$.

$$\mathbf{X} = \begin{pmatrix} -11 & 4 & 1 & -1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \qquad \mathbf{X} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 2 & 0 \\ -9 & 7 & 11 & -1 \end{pmatrix}$$

Finalement, nous simplifions $C_1 \leftarrow C_1 + 11C_3$, $C_2 \leftarrow C_2 - 4C_3$, $C_4 \leftarrow C_4 + C_3$:

$$\mathbf{X} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \qquad \mathbf{X} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ -11 & 4 & -1 & -1 \\ 22 & -7 & 2 & 2 \\ 112 & -37 & 11 & 10 \end{pmatrix}$$

Nous en déduisons finalement une base

$$\mathbf{u}_1 = \begin{pmatrix} 1 \\ -11 \\ 22 \\ 112 \end{pmatrix} \in \mathbb{Z}^4 \qquad \text{et} \qquad \mathbf{u}_2 = \begin{pmatrix} 0 \\ 4 \\ -7 \\ -37 \end{pmatrix} \in \mathbb{Z}^4.$$

3. Calculons une base LLL réduite de Λ. On a $\|\mathbf{u}_1\|^2 = 13150 > \|\mathbf{u}_2\|^2 = 1434$. On notons que

$$\frac{\langle \mathbf{u}_1, \mathbf{u}_2 \rangle}{\langle \mathbf{u}_2, \mathbf{u}_2 \rangle} = \frac{-4342}{1434} \simeq -3.028\cdots$$

Nous voyons par conséquent que

$$\mathbf{u}_3 = \mathbf{u}_1 - 3\mathbf{u}_2 = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

appartient au réseau.
Nous notons ensuite que

$$\frac{\langle \mathbf{u}_2, \mathbf{u}_3 \rangle}{\langle \mathbf{u}_3, \mathbf{u}_3 \rangle} = \frac{-40}{4} = -10$$

Nous calculons

$$\mathbf{u}_4 = \mathbf{u}_2 + 10\mathbf{u}_3 = \begin{pmatrix} 10 \\ 14 \\ 3 \\ -27 \end{pmatrix}$$

Comme $\|\mathbf{u}_4\|^2 = 1034 > \|\mathbf{u}_3\|^2 = 4$, l'algorithme LLL s'arrête.
Comme nous travaillons avec un réseau de rang 2, le plus court vecteur de Λ apparait dans la réduction est vaut ici $\mathbf{u}_3$.

4. Le vecteur $\mathbf{u}_3$ est de norme $\|\mathbf{u}_3\| = 2$: on peut donc place des boules de rayon $r < 1$.

Exercice 2. Soit $\mathbf{A} \in \mathbb{Z}^{3\times 3}$ la matrice suivante et $\mathbf{b} \in \mathbb{Z}^3$ le vecteur suivant

$$\mathbf{A} = \begin{pmatrix} -16 & -21 & -31 \\ 7 & 9 & 13 \\ -8 & -9 & -11 \end{pmatrix} \in \mathbb{Z}^{3\times 3} \qquad \mathbf{b} = \begin{pmatrix} 1 \\ 0 \\ -3 \end{pmatrix} \in \mathbb{Z}^3$$

1. Déterminer la forme normale de Smith $\mathbf{X}$ de la matrice $\mathbf{A}$. (3 pts)
2. Le système $\mathbf{Ax} = \mathbf{b}$ admet-il une solution dans $\mathbb{Z}^3$? (1 pt)

Solution 2. 1. Nous partons de

$$\mathbf{X} = \begin{pmatrix} -16 & -21 & -31 \\ 7 & 9 & 13 \\ -8 & -9 & -11 \end{pmatrix} \qquad \mathbf{L} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad \mathbf{C} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Nous devinons que le ppcm des coefficients de $\mathbf{A}$ vaut 1. Il est intéressant de faire apparaitre un coefficient 1. Avec $C_1 \leftarrow C_1 - C_2$

$$\mathbf{X} = \begin{pmatrix} 5 & -21 & -31 \\ -2 & 9 & 13 \\ 1 & -9 & -11 \end{pmatrix} \qquad \mathbf{L} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad \mathbf{C} = \begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Nous corrigeons les lignes $L_1 \leftarrow L_1 - 5L_3$ et $L_2 \leftarrow L_2 + 2L_3$

$$\mathbf{X} = \begin{pmatrix} 0 & 24 & 24 \\ 0 & -9 & -9 \\ 1 & -9 & -11 \end{pmatrix} \qquad \mathbf{L} = \begin{pmatrix} 1 & 0 & -5 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix} \qquad \mathbf{C} = \begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Nous corrigeons les colonnes $C_2 \leftarrow C_2 + 9C_1$ et $C_3 \leftarrow C_3 + 11C_1$

$$\mathbf{X} = \begin{pmatrix} 0 & 24 & 24 \\ 0 & -9 & -9 \\ 1 & 0 & 0 \end{pmatrix} \qquad \mathbf{L} = \begin{pmatrix} 1 & 0 & -5 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix} \qquad \mathbf{C} = \begin{pmatrix} 1 & 9 & 11 \\ -1 & -8 & -11 \\ 0 & 0 & 1 \end{pmatrix}$$

Il est tentant d'effectuer $C_2 \leftarrow C_2 - C_3$

$$\mathbf{X} = \begin{pmatrix} 0 & 24 & 0 \\ 0 & -9 & 0 \\ 1 & 0 & 0 \end{pmatrix} \qquad \mathbf{L} = \begin{pmatrix} 1 & 0 & -5 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix} \qquad \mathbf{C} = \begin{pmatrix} 1 & 9 & 2 \\ -1 & -8 & -3 \\ 0 & 0 & 1 \end{pmatrix}$$

Avant de continuer, échangeons $L_1 \leftrightarrow L_3$

$$\mathbf{X} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -9 & 0 \\ 0 & 24 & 0 \end{pmatrix} \qquad \mathbf{L} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 2 \\ 1 & 0 & -5 \end{pmatrix} \qquad \mathbf{C} = \begin{pmatrix} 1 & 9 & 2 \\ -1 & -8 & -3 \\ 0 & 0 & 1 \end{pmatrix}$$

Puis $L_3 \leftarrow L_3 + 3L_2$

$$\mathbf{X} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -9 & 0 \\ 0 & -3 & 0 \end{pmatrix} \qquad \mathbf{L} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 2 \\ 1 & 3 & 1 \end{pmatrix} \qquad \mathbf{C} = \begin{pmatrix} 1 & 9 & 2 \\ -1 & -8 & -3 \\ 0 & 0 & 1 \end{pmatrix}$$

Puis $L_2 \leftarrow L_2 - 3L_2$

$$\mathbf{X} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & -3 & 0 \end{pmatrix} \qquad \mathbf{L} = \begin{pmatrix} 0 & 0 & 1 \\ -3 & -8 & -1 \\ 1 & 3 & 1 \end{pmatrix} \qquad \mathbf{C} = \begin{pmatrix} 1 & 9 & 2 \\ -1 & -8 & -3 \\ 0 & 0 & 1 \end{pmatrix}$$

Enfin $L_3 \leftrightarrow L_2$ et $L_2 \leftarrow -L_2$

$$\mathbf{X} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 0 \end{pmatrix} \qquad \mathbf{L} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & -3 & 1 \\ -3 & 8 & -1 \end{pmatrix} \qquad \mathbf{C} = \begin{pmatrix} 1 & 9 & 2 \\ -1 & -8 & -3 \\ 0 & 0 & 1 \end{pmatrix}$$

2. Nous effectuons un changement de base dans l'espace des solutions en posant $\mathbf{x} = \mathbf{C}\mathbf{x}'$. Cette transformation est bien valide car $\mathbf{C}$ appartient à $\mathbf{GL}_3(\mathbb{Z})$. L'équation $\mathbf{A}\mathbf{x} = \mathbf{b}$ équivaut à l'équation $\mathbf{A}\mathbf{C}\mathbf{x}' = \mathbf{b}$. Nous multiplions à gauche par $\mathbf{L}$, ce qui ne change pas les solutions puisque $\mathbf{L} \in \mathbf{GL}_3(\mathbb{Z})$. Nous obtenons l'équation $\mathbf{L}\mathbf{A}\mathbf{C}\mathbf{x}' = \mathbf{X}\mathbf{x}' = \mathbf{L}\mathbf{b}$. Calculons $\mathbf{b}' = \mathbf{L}\mathbf{b}$ explicitement :

$$\mathbf{b}' = \begin{pmatrix} -3 \\ -2 \\ 0 \end{pmatrix}$$

Le système $\mathbf{X}\mathbf{x}' = \mathbf{b}'$ s'écrit comme

$$\begin{cases} x'_1 &= -3, \\ 3x'_2 &= -2 \\ x'_3 &= 0 \end{cases}$$

où $\mathbf{x}' = (x'_1, x'_2, x'_3) \in \mathbb{Z}^3$. Ce système n'a pas de solutions entières puisque -2 n'est pas un multiple de 3.

Exercice 3. Dans tout cet exercice, on se donne un premier $p \geq 3$.

1. Soient ℓ un entier et x un élément de $\mathbb{F}_{p^\ell}$. Rappeler un critère d'algèbre linéaire permettant de savoir si $x \in \mathbb{F}_p$. (0,5 pt)

La notation $(\mathbb{F}_{p^2}^\times, \cdot)$ désigne le groupe des éléments non nuls de $\mathbb{F}_{p^2}$ muni de la loi de multiplication.

2. Vérifier les faits suivants :
   (a) L'application (0,5 pt)
   $$\mathcal{N} : \begin{cases} (\mathbb{F}_{p^2}^\times, \cdot) & \to & \mathbb{F}_{p^2}^\times \\ t & \to & t^{p+1} \end{cases}$$
   est un homomorphisme (de groupe abélien) à valeur dans $\mathbb{F}_p^\times$.
   (b) L'image $\mathcal{N}(\mathbb{F}_p)$ est le groupe des carrés non nuls de $\mathbb{F}_p^\times$. (0,5 pt)
3. Montrer que le polynôme $f(x) = x^{p+1} - a \in \mathbb{F}_p[x]$, où a est un élément de $\mathbb{F}_p^\times$, est sans facteur carré. (0,5 pt)
4. Compter le nombre de racines du polynôme $x^{p+1} - a \in \mathbb{F}_p[x]$ (0,5 pt)
   (a) dans le corps $\mathbb{F}_{p^2}$, (0,5 pt)
   (b) puis dans le corps $\mathbb{F}_p$. (0,5 pt)
5. En déduire les degrés des facteurs irréductibles de $x^{p+1} - a \in \mathbb{F}_p[x]$. (0,5 pt)
6. Dans cette question, nous supposons que $p = 5$. Écrire la matrice $\mathbf{Q}$ de Petr-Berlekamp du polynôme $x^6 - 2 \in \mathbb{F}_5[X]$. Calculer le rang de la matrice $\mathbf{Q} - \mathbf{I}$. (0,5 pt)
7. Peut-on, plus généralement, prévoir le rang de la matrice $\mathbf{Q} - \mathbf{I}$ relative au polynôme $x^{p+1} - a \in \mathbb{F}_p[X]$ lorsque a décrit l'ensemble $\mathbb{F}_p^\times$? (0,5 pt)
8. Identifier le polynôme (0,5 pt)
   $$h(x) = \prod_{a \in \mathbb{F}_p^\times} x^p - a$$
   c'est-à-dire donner la forme développée de $h(x)$.
9. Nous souhaitons factoriser dans $\mathbb{Z}[z]$ le polynôme
   $$k(z) = z^{24} - 1 \in \mathbb{Z}[z].$$
   (a) Nous rappelons qu'il y a autant de facteurs irréductibles du polynôme $z^n - 1$ dans $\mathbb{Z}[z]$ que de diviseurs de n (ce sont les polynômes cyclotomiques). Combien le polynôme $k(z)$ possède-t-il de facteurs irréductibles dans $\mathbb{Z}[z]$? (0,5 pt)
   (b) Nous plongeons $k(z)$ dans $\mathbb{Z}/5^{16}\mathbb{Z}[z]$ et factorisons $k(z)$ modulo 5^{16}. Combien de facteurs obtient-on ? (0,5 pt)

Solution 3.

1. Un élément $x \in \mathbb{F}_{p^k}$ appartient à $\mathbb{F}_p$ si et seulement si $\sigma = \mathrm{Frob}_{[\mathbb{F}_{p^k}:\mathbb{F}_p]}(x) = x$ c'est-à-dire $x^p = x$.
2. (a) On peut constater que $\varphi(1) = 1$ et $\varphi(ab) = \varphi(a)\varphi(b)$ ce qui montrer que nous avons bien un morphisme.
   D'autre part, on sait que $\sigma^2 = \mathrm{Id}$ dans $\mathbb{F}_{p^2}$. Ainsi, pour tout élément x de $\mathbb{F}_{p^2}$
   $$\sigma(\mathcal{N}(x)) = \sigma(x\sigma(x)) = \sigma(x)\sigma^2(x) = \sigma(x)x = \mathcal{N}(x)$$
   ce qui prouve que $\mathcal{N}(x)$ appartient toujours $\mathbb{F}_p$.

(b) Nous observons que, si $x \in \mathbb{F}_p$, on a

$$\mathcal{N}(x) = x \cdot \sigma(x) = x \cdot x = x^2$$

ce qui prouve notre point.

3. Nous calculons $f'(x) = (p+1)x^p = x^p$. Ainsi, comme a est non nul,

$$f \wedge f' = 1$$

ce qui prouve que f est sans facteur carré.

4. (a) Nous savons que $\operatorname{im}\mathcal{N} \subseteq \mathbb{F}_p^\times$, donc $|\operatorname{im}\mathcal{N}| \leq p-1$. Par ailleurs, $\ker\mathcal{N} = \{x \in \mathbb{F}_{p^2}^\times; \mathcal{N}(x) = 1\}$ possède $p+1$ éléments au plus (puisqu'on cherche les racines d'un polynôme de degré $p+1$ dans un corps). Or $|\mathbb{F}_{p^2}^\times| = |\ker\mathcal{N}| \cdot |\operatorname{im}\mathcal{N}|$. Ceci force les égalités $|\ker\mathcal{N}| = p+1$ et $\operatorname{im}\mathcal{N} = \mathbb{F}_p^\times$.
Nous en déduisons que $f(x) = x^{p+1} - a$ possède exactement $p+1$ racines distinctes.

(b) Si a n'est pas un carré, $x^{p+1} - a$ ne peut pas avoir de racine $t \in \mathbb{F}_p$, car $\mathcal{N}(t)$ est toujours un carré.
Inversement, deux éléments x et x' de $\mathbb{F}_p^\times$ satisfont $\mathcal{N}(x) = \mathcal{N}(x')$ si et seulement si $x^{p+1} = x'^{p+1}$ soit encore si et seulement si $x^2 = x'^2$ ce qui équivaut à $x = \pm x'$. Donc un même polynôme $f(x) = x^{p+1} - a$ ne peut avoir qu'au maximum deux racines issues de $\mathbb{F}_p$. Pour des raisons de cardinalité, nous pouvons conclure que tous les polynômes de la forme $f(x) = x^{p+1} - a$, où a est un carré, possèdent exactement 2 racines distinctes dans $\mathbb{F}_p^\times$.

5. Il s'en suit que :
   — si a est un non carré, $f(x) = x^{p+1} - a$ possède $(p+1)/2$ facteurs irréductibles quadratiques.
   — si a est un carré, $f(x) = x^{p+1} - a$ possède $(p-1)/2$ facteurs irréductibles quadratiques et deux facteurs linéaires.

6. On effectue les calculs suivants

$$\begin{cases} \sigma(1) &= & & & 1 \\ \sigma(x) &= & & & x^5 \\ \sigma(x^2) &= & x^{10} = x^{6+4} & = & 2x^4 \\ \sigma(x^3) &= & x^{15} = x^{2\cdot 6+3} & = & -x^3 \\ \sigma(x^4) &= & x^{20} = x^{3\cdot 6+2} = 2^3x^2 & = & -2x^3 \\ \sigma(x^5) &= & x^{25} = x^{4\cdot 6+1} = 2^{5-1}x & = & x \end{cases}$$

On obtient la matrice

$$\mathbf{Q} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & -2 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

On en tire

$$\mathbf{Q} - \mathbf{I}_6 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 & -2 & 0 \\ 0 & 0 & 0 & -2 & 0 & 0 \\ 0 & 0 & 2 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 & 0 & -1 \end{pmatrix}$$

Il est facile de voir que cette matrice est de rang 3. On regarde le bloc aux lignes [2,3,4] et colonnes [2,3,4]. Le noyau est donc de dimension $6-3=3$.

7. Plus généralement, le rang de la matrice $\mathbf{Q}-\mathbf{I}_6$ est 3 ou 4 selon que a est un non carré ou un carré. On a ici

a	carré	rang
1	oui	4
2	non	3
3	non	3
4	oui	4

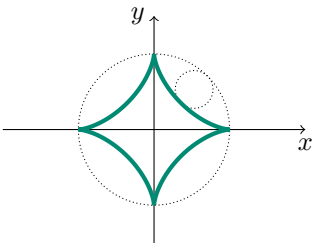
8. Ce qui précède montre que $h(x)=\prod_{a\in\mathbb{F}_5^\times} x^{p+1}-a$ a pour facteur l'ensemble des irréductibles de degré 1 ou 2 avec multiplicité 1 sauf le facteur x. On a donc

$$h(x)=x^{p^2-1}-1$$

9. (a) On compte les diviseurs de 24 : 1, 2, 3, 4, 6, 8, 12. Ainsi $z^{24}-z$ se factorise en 8 irréductibles.

   (b) Dans $\mathbb{F}_5[x]$ on obtient $4+20/2=14$ irréductibles, qui se relèvent par le lemme d'Hensel en 14 irréductibles dans $\mathbb{Z}/5^{16}\mathbb{Z}[z]$.

Exercice 4. Une *astroïde* est une courbe plane $\mathscr{A}$, que l'on peut obtenir en faisant rouler un cercle de rayon $\frac{1}{4}$ à l'intérieur d'un cercle de rayon 1.



La mise en équation de ce mouvement conduit à la paramétrisation

$$\mathscr{A}=\left\{(x(t),y(t))\in\mathbb{R}^2\,;\ t\in\mathbb{R}\right\}$$

où

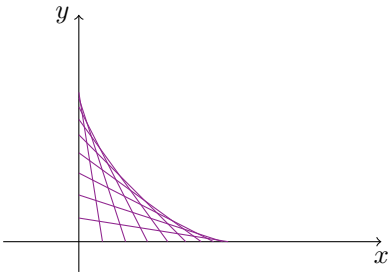
$$\begin{cases} x(t) &= \sin^3(t) \\ y(t) &= \cos^3(t) \end{cases} \qquad (t\in\mathbb{R})$$

1. Nous nous proposons de retrouver une équation cartésienne $f(x,y)=0$ de la courbe $\mathscr{A}$. Nous introduisons quatre variables polynomiales x, y, s et c.
   Proposer trois polynômes $g_1(x,y,s,c)$, $g_2(x,y,s,c)$ et $g_3(x,y,s,c)\in\mathbb{Q}[x,y,s,c]$ tels que (1 pt)

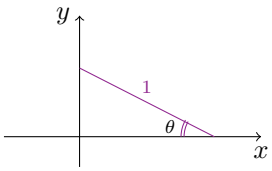
$$\mathscr{A}=\{(x,y)\in\mathbb{R}^2;\exists(s,c)\in\mathbb{R}^2, g_1(x,y,s,c)=g_2(x,y,s,c)=g_3(x,y,s,c)=0\}.$$

2. Nous notons $\mathfrak{I}$ l'idéal engendré $\mathfrak{I}=\langle g_1,g_2,g_3\rangle$. Suggérer un ordre $\preceq$ sur les monômes de $\mathbb{Q}[x,y,s,c]$ tel que, si on calcule une base de Groebner de $\mathfrak{I}$, le ou les derniers polynômes de cette base forment une base de Groebner de $\mathfrak{I}\cap\mathbb{Q}[x,y]$ (idéal d'élimination des variables s et c). (0,5 pt)
   Écrire les monômes x, y, s et c par ordre décroissant.

3. Nous voudrions confirmer que la courbe $\mathscr{A}$ est également l'enveloppe de l'ensemble des segments $(S_u)_{u\in\mathbb{R}}$ de longueur 1 dont les extrémités glissent le long des axes (Ox) et (Oy) (on pourra imaginer une échelle qui glisse le long d'un mur). Le rôle du paramètre u sera précisé plus loin.



(a) Donner l'équation de la droite dessinée ci-dessous en fonction de l'angle θ (1 pt)



(b) En introduisant un paramètre u tel que $\tan\theta = \dfrac{2u}{1-u^2}$, introduire une famille de fonctions polynomiales $h(x,y,u)$ telle que, pour chaque valeur fixée u_0, l'équation $h(x,y,u_0)=0$ soit l'équation cartésienne de l'un des segments S_u dessiné plus haut. (1 pt)

(c) Décrire une manipulation à l'aide de bases de Groebner qui permettrait de retrouver l'équation $f(x,y)=0$ qui décrit l'astroïde. (0,5 pt)

Solution 4. 1. Nous introduisons les trois équations

$$g_1(x,y,c,s) = c^2+s^2-1, \quad g_2(x,y,c,s) = x-s^3, \quad g_3(x,y,c,s) = y-c^3$$

2. Nous munissons $\mathbb{Q}[x,y,c,s]$ de l'ordre lexicographique dans lequel

$$c > s > x > y$$

On pourrait aussi utiliser un autre ordre tel que $c,s > x,y$.

3. (a) L'abscisse à l'origine est $\cos\theta$, l'ordonnée à l'origine est $\sin\theta$. La droite a, par conséquent, pour équation :

$$\frac{x}{\cos\theta} + \frac{y}{\sin\theta} = 1.$$

(b) Avec la paramétrisation

$$\tan\theta = \frac{2u}{1-u^2},$$

on a, selon les formules classiques de paramétrisation du cercle,

$$\sin\theta = \frac{2u}{1+u^2} \qquad \text{et} \qquad \cos\theta = \frac{1-u^2}{1+u^2}.$$

On propose donc l'équation

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

qui est celle de la question précédente où l'on a chassé les dénominateurs.

(c) Ici encore, on souhaite chasser la variable u de l'ensemble des équations

$$\left\{ h(x,y,u) = 0 \quad \text{et} \quad \frac{\partial h}{\partial u}(x,y,u) = 0 \right\}$$

On déclare l'idéal $\mathfrak{E}$ engendré par h et $\frac{\partial h}{\partial u}$ dans $\mathbb{Q}[x,y,u]$. On munit $\mathbb{Q}[x,y,u]$ de l'ordre lexicographique. On cherche une base de Groebner de $\mathfrak{E}$. La dernière équation doit être égale à $f(x,y)$.

Voici le code si on veut vérifier les calculs :

```
Pol.<s,c,x,y> = PolynomialRing(QQ,4, order = 'lex')
g1 = c^2 + s^2 - 1
g2 = x-s^3
g3 = y-c^3
I = Ideal([g1, g2, g3])
f(x,y) = I.groebner_basis()[-1].subs(c=0,s=0)
implicit_plot( f, (x, -2,2), (y, -2,2))

Pol.<u,x,y> = PolynomialRing(QQ,3, order = 'lex')
h = (1+u^2)*2*u*x + (1+u^2)*(1-u^2)*y - 2*u*(1-u^2)
E = Ideal([h, h.derivative(u)])
E.groebner_basis()[-1]
```