Devoir maison no.2, Contrôle Continu M1 4023 Algorithmique Algébrique, Sorbonne Université 2020/2021

Date : distribué le 8 avril 2021, à rendre sur Moodle avant le 15 avril à 23h59.
Enseignant : Pierre CHAROLLOIS, Pierre-Vincent KOSELEFF.
Vous pouvez, si vous le souhaitez, faire vérifier vos calculs au moyen d'un logiciel de calcul formel (par exemple Sage, disponible sur le site https://jupyter.math.upmc.fr/).

Exercice 1 (sommes de Dedekind)

Soit $\sigma \in M_2(\mathbb{Z})$ une matrice de rang 2.

a) Montrer que les colonnes de σ engendrent un sous-groupe $\sigma\mathbb{Z}^2$ de $\mathbb{Z}^2$ d'indice fini, égal à $|\det(\sigma)|$.

correction : C'est la Prop. 10.1 du polycopié de cours.

b) Soit $\sigma_0 = \begin{pmatrix} 11 & 4 \\ 7 & 3 \end{pmatrix}$. Trouver, en expliquant les calculs, des matrices $E, F \in GL_2(\mathbb{Z})$ et D diagonale avec $E\sigma_0 F = D$.

correction : comme dans la preuve de la Prop. 10.1, on fait par exemple les opérations sur les lignes $L_1 \leftarrow L_1 - L_2$ puis $L_2 \leftarrow L_2 - L_1'$ pour arriver à l'étape intermédiaire

$$\begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}\sigma_0 = \begin{pmatrix} 4 & 1 \\ 3 & 2 \end{pmatrix}.$$

A partir de là, on peut faire $L_1 \leftarrow L_1 - L_2$ puis $L_2 \leftarrow L_2 - 3L_1'$ pour arriver à

$$\begin{pmatrix} 1 & 0 \\ -3 & 1 \end{pmatrix}\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}\sigma_0 = \begin{pmatrix} 1 & -1 \\ 0 & 5 \end{pmatrix}.$$

On conclut avec l'opération sur les colonnes $C_2 \leftarrow C_2 + C_1$ pour trouver

$$E = \begin{pmatrix} 1 & 0 \\ -3 & 1 \end{pmatrix}\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & -3 \\ -7 & 11 \end{pmatrix}, \tag{1}$$

$$F = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \tag{2}$$

$$D = \begin{pmatrix} 1 & 0 \\ 0 & 5 \end{pmatrix}. \tag{3}$$

c) Déterminer un système de représentants explicite des classes du groupe quotient $\mathbb{Z}^2/\sigma_0\mathbb{Z}^2$.

correction : On dispose d'un système de représentants de $\mathbb{Z}^2/D\mathbb{Z}^2$ en considérant des vecteurs colonnes $x_k = \begin{pmatrix} 0 \\ k \end{pmatrix}$, avec $k = 0, 1, 2, 3, 4$. En leur appliquant la matrice $E^{-1} = \begin{pmatrix} 11 & 3 \\ 7 & 2 \end{pmatrix}$, ils s'envoient sur un système de représentants $y_k = E^{-1}x_k = k\begin{pmatrix} 3 \\ 2 \end{pmatrix}$ de

$$E^{-1}\mathbb{Z}^2/E^{-1}D\mathbb{Z}^2 = \mathbb{Z}^2/E^{-1}DF\mathbb{Z}^2 = \mathbb{Z}^2/\sigma_0\mathbb{Z}^2.$$

d) On note $<,>$ le produit scalaire usuel sur $\mathbb{R}^2$, et σ^t la transposée de $\sigma \in M_2(\mathbb{Z})$. Montrer que pour tout $h \in \mathbb{Z}^2$,

$$\sum_{r\in\mathbb{Z}^2/\sigma\mathbb{Z}^2} \exp(2i\pi < \sigma^{-1}r, h >) = \begin{cases} \det(\sigma) & \text{si } h \in \sigma^t\mathbb{Z}^2 \\ 0 & \text{si } h \notin \sigma^t\mathbb{Z}^2. \end{cases} \tag{4}$$

correction : lorsque $\sigma = D = diag(d_1, d_2)$ est diagonale, la formule est claire parce que $\sum_{k=0}^{d-1} e^{2i\pi h\frac{k}{d}} = 0$ si d ne divise pas h, et vaut d si d divise h. On se ramène à ce cas diagonal en mettant σ sous forme normale de Smith comme en b).

e) On rappelle (Dirichlet) que pour $0 < v < 1$,

$$\lim_{N\to\infty} \sum_{m=-N}^{N} \frac{\exp(-2i\pi vm)}{t+m} = 2i\pi \frac{\exp(2i\pi vt)}{\exp(2i\pi t) - 1}.$$

Démontrer que la somme

$$\frac{1}{\pi^2} \sum_{0\neq n\in\mathbb{Z}} \frac{\exp(2i\pi nv)}{n^2} \tag{5}$$

est un nombre rationnel lorsque v est un nombre rationnel.

correction : On peut dériver terme à terme la série dans la formule de Dirichlet par rapport à t. Au vu du membre de gauche dans la formule de Dirichlet, la quantité

$$\sum_{m\in\mathbb{Z},m\neq 0} \frac{e^{-2i\pi mv}}{m^2}$$

est le coefficient constant du développement de Laurent en $t = 0$. Au vu du membre de droite, ce terme constant est dans $\pi^2\mathbb{Q}$. Le résultat s'ensuit. (il est d'ailleurs encore valable en $v = 0$, par convergence uniforme de la série dérivée).

f) Déduire des questions précédentes que

$$\sum_{(m,n)\in\mathbb{Z}^2,(11m+7n)(4m+3n)\neq 0} \frac{1}{(11m+7n)^2(4m+3n)^2} = \pi^4\lambda,$$

pour un nombre rationnel λ que l'on pourra déterminer. Quel est son dénominateur ? Généraliser.

correction : on pose $(m', n') = (m, n)\sigma_0$, de sorte que la somme demandée s'écrit

$$S = \sum_{(m',n')\in\mathbb{Z}^2\sigma_0,m'n'\neq 0} \frac{1}{m'^2n'^2} \tag{6}$$

$$= \frac{1}{|\det\sigma_0|} \sum_{r\in\mathbb{Z}^2/\sigma_0\mathbb{Z}^2,} \sum_{(m',n')\in\mathbb{Z}^2,m'n'\neq 0} \frac{e^{2i\pi<\sigma_0^{-1}(m',n')^t,r>}}{m'^2n'^2}, \tag{7}$$

la dernière égalité provenant de d).

Pour chaque classe $r \in \mathbb{Z}^2/\sigma_0\mathbb{Z}^2$ fixé, écrivons $v = v(r) = (v_1, v_2) = r^t.\sigma_0^{-1}$. C'est un couple de nombre rationnel. La somme intérieure sur les (m', n') est un produit de deux séries de la forme (5) pour v_1 et pour v_2. D'après le question e), S est donc dans $\pi^4\mathbb{Q}$.

Plus précisément, si l'on note $B_2(v)$ la valeur (rationnelle) de la somme (5), alors

$$\frac{S}{\pi^4} = \frac{1}{5}\sum_{r\in\mathbb{X}} B_2(v_1(r)) \cdot B_2(v_2(r)), \tag{8}$$

où la sommation parcourt le système de représentants obtenu en c). De manière explicite, on trouve $S = \pi^4\lambda$ avec $\lambda = \frac{11\cdot 79}{3^2 5^5}$.

Plus généralement, la même méthode montre que, pour a, b, c, d des entiers fixés, la somme absolument convergente

$$S(a,b,c,d) := \sum_{(m,n)\in\mathbb{Z}^2}{}' \frac{1}{(am+bn)^2(cm+dn)^2},$$

(la somme portant sur les entiers (m, n) tels que le dénominateur est non-nul) est dans $\pi^4\mathbb{Q}$. La forme normale de Smith de la matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ permet de calculer explicitement le nombre rationnel correspondant.

Exercice 2 (factorisation)

Soit $f(x) = x^5 + 100x^4 + 2521x^3 + 78641x^2 + 197118x + 392863$ un polynôme de $\mathbb{Z}[x]$, et $\tilde{f}$ son image dans $\mathbb{F}_5[x]$.

a) Factoriser $\tilde{f}$ en un produit de facteurs irréductibles dans $\mathbb{F}_5[x]$.

correction : $\tilde{f} = x^5 + x^3 + x^2 + 3x + 3$ n'a pas de racine dans $\mathbb{F}_5$ par inspection de cas. Ainsi, $\tilde{f}$ est irréductible, ou bien est un produit d'un facteur irréductible de degré 3 et d'un facteur de degré 2.

Pour le savoir, il suffit de calculer son pgcd avec $x^{5^2} - x$ au moyen de l'algorithme d'Euclide :

$$\begin{aligned}
(x^{25} - x, \tilde{f}) &= (2x^4 + 4x^3 + 4x^2 + 2x + 4, x^5 + x^3 + x^2 + 3x + 3) && (9)\\
&= (x^4 + 2x^3 + 2x^2 + x + 2, 3x^3 + 4x^2 + 3x + 2) && (10)\\
&= (3x^2 + x + 2, 3x^3 + 4x^2 + 3x + 2) && (11)\\
&= (3x^2 + x + 2) && (12)\\
&= (x^2 + 2x + 4). && (13)
\end{aligned}$$

Ainsi

$$\tilde{f} = (x^2 + 2x + 4) \cdot \frac{\tilde{f}}{(3x^2 + x + 2)} = (x^2 + 2x + 4)(x^3 + 3x^2 + x + 2)$$

est la factorisation de $\tilde{f}$ en facteurs irréductibles.

b) Démontrer que f ne possède pas de racine rationnelle.

correction : soit $x_0 = p/q$ une fraction irréductible racine de f. De $f(p/q) = 0$ on déduit, en chassant les dénominateurs, que q divise 1. Ainsi x_0 est une racine entière de f. Mais alors $f \mod 5$ aurait une racine ce qui n'est pas le cas d'après le a).

c) Soit g un facteur irréductible de f dans $\mathbb{Z}[x]$. Donner une majoration des coefficients de g.

correction : La borne de Mignotte dit que

$$||g_|||_\infty \leq 2^{\deg g}||f_2|| < 2^{\deg g}500000.$$

d) Au moyen du relevé de Hensel, déduire des questions précédentes la factorisation de f dans $\mathbb{Z}[x]$ en facteurs irréductibles. (On détaillera les étapes du calcul).

correction : On procède comme en TD. On pose $A_1 = x^2 + 2x + 4, B_1 = x^3 + 3x^2 + x + 2$. On a, pour $U = (3x + 3$ et $V = 2$, l'égalité $UA + VB = 1$ dans $\mathbb{F}_5[X]$. On pose, en prenant le relevé dans $\mathbb{Z}[X]$ du polynôme modulo 5, $D_1 = (f - A_1B_1)/5 \equiv 4x^4 + 2x^3 + 2x + 1$ et $S_1 = D_1U \mod B_1 = x^2 + 2x + 2, T_1 = D_1V \mod A_1 = 3x + 4$. Puis $A_2 = A_1 + 5T_1 = x^2 + 17x + 24, B_2 = B_1 + 5S_1 = x^3 + 8x^2 + 11x + 12$ (on choisit un relevé mod 5^2).

On itère en posant $D_2 = (f - A_2B_2)/25 \equiv 3x^4 + 4x^3 + x + 3$ et $S_2 = D_2U \mod B_2 = 3x^2 + 3x + 2$ $T_2 = D_2V \mod A_2 = 0$ (on prend un relevé modulo 5). Puis on pose $A_3 = A_2 + 5^2T_2 = A_2$ et $B_3 = B_2 + 5^2S_2 = x^3 + 83x^2 + 86x + 62$. (on est en train de découvrir les chiffres des coefficients des facteurs de f en base 5.

On itère avec $D_3 = (f - A_3B_3)/5^3$ puis $S_3 = D_3U \mod B_3 = x + 3$ en prenant un relevé modulo 5, et $T_3 = D_3V \mod A_3 = 2$.

On pose alors

$$A_4 = A_3 + 5^3T_3 = x^2 + 17x + 274, \tag{14}$$
$$B_4 = B_3 + 5^3S_3 = x^3 + 83x^2 + 211x + 437. \tag{15}$$

On pose ensuite $D_4 = (f - A_4B_4)/5^4 = x^3 + 83x^2 + 211x + 437$, ou plutôt $D_4 = x^3 + 3x^2 + x + 2$ car seul son reste modulo 5 est pertinent. $S_4 = D_4U \mod B_4 = 0$, et $T_4 = D_4V \mod A_4 = 1$ en prenant le relevé modulo 5. On trouve alors des facteurs à la précision 5^5 : $A_5 = A_4 + 5^4T_4 = x^2 + 17x + 899$, et $B_5 = B_4$. Finalement $f - A_5B_5 = 0$, non seulement à la précision 5^5 mais vraiment dans $\mathbb{Z}[X]$, et les deux facteurs irréductibles de f dans $\mathbb{Z}[X]$ sont

$$f = (x^2 + 17x + 899)(x^3 + 83x^2 + 211x + 437). \tag{16}$$

Exercice 3 (résultant) :

Soit $P(x, y) = x^3 - y^2 + 1$ et $Q(x, y) = x^2 + y^2 + xy - 1$.

a) Calculer le résultant, en y, $\mathrm{Res}_y(P, Q) \in \mathbb{Z}[x]$.

correction : On a deux polynômes de degré 2 en y, la matrice de Sylvester de taille 4 associée est

$$\begin{pmatrix} -1 & 0 & 1 & 0 \\ 0 & -1 & x & 1 \\ x^3+1 & 0 & x^2-1 & x \\ 0 & x^3+1 & 0 & x^2-1 \end{pmatrix}. \tag{17}$$

Son déterminant est

$$\mathrm{Res}_y(P,Q) = x^6 + x^5 + x^4 - x^2 = x^2(x^4 + x^3 + x^2 - 1). \tag{18}$$

b) Déterminer tous les couples $(x_i, y_i) \in \mathbb{Q}^2$ de nombres rationnels qui sont solutions du système

$$\begin{cases} P(x,y) = 0 \\ Q(x,y) = 0. \end{cases} \tag{19}$$

Combien ce système possède-t'il de solutions rationnelles ?

correction : si $(x_0, y_0) \in K$ est racine du système, alors $P(x_0, Y)$ et $Q(x_0, Y)$, chacun de degré 2, ont une racine commune (y_0) dans K, donc leur résultant est nul. Ce résultant est, par définition, $R(x_0) \in K$. Donc x_0 est à chercher parmi les racines dans $K = \mathbb{Q}$ de R. Dans le cas rationnel, on écrit x_0 sous la forme $p/q, p \in \mathbb{Z}, q \in \mathbb{N}$ premiers entre eux. En reportant on trouve alors $x_0 = 0$ ou $p^4 + p^3q + p^2q^2 - q^4 = 0$, donc q divise p, ie $q = 1$, et p divise q donc $p = \pm 1$. Réciproquement, on voit que $x_0 = 0, x_2 = -1$ sont racines rationnelles de R (avec 0 racine double). Pour chacun de ces deux choix, en reportant on trouve la liste de solutions rationnelles $(0,1), (0,-1), (-1,0)$. Il y a 3 solutions rationnelles au système ; et ce sont des solutions entières.

c) Soit $p = 11$. A l'aide des questions a) et b), déterminer toutes les paires $(x', y') \in \mathbb{F}_p \times \mathbb{F}_p$ qui sont solutions du système

$$\begin{cases} P(x',y') = 0 \\ Q(x',y') = 0. \end{cases} \tag{20}$$

Combien ce système possède-t'il de solutions dans $\mathbb{F}_p$?

correction : Chaque solution entière conduit, par réduction modulo 11, à une solution dans $\mathbb{F}_{11} \times \mathbb{F}_{11}$, ce qui fournit déjà 3 solutions distinctes. Le raisonnement de b) avec $K = \mathbb{F}_{11}$ conduit à chercher les racines x_j de $R(x)$ dans $\mathbb{F}_{11}$. On trouve $x - j \in \{0, -1, -2\} = \{0, 10, 9\}$, et $R(x) \mod 11$ se factorise en facteurs irréductibles sous la forme

$$R(x) = x^2(x+1)(x+2)(x^2 - 2x + 5) \in \mathbb{F}_{11}[x].$$

Pour le choix $x_0 = -2$, on est conduit à résoudre dans $\mathbb{F}_{11}$ le système $(4 = y^2, 3 + y^2 - 2y = 0)$ dont la seule solution est $y_0 = -2$. Finalement on trouve 4 solutions dans $\mathbb{F}_{11}^2$, à savoir $(0,1), (0,-1), (-1,0), (-2,-2)$.

d) (question bonus). Même question que la précédente, mais pour $p = 31$. Expliquez.

correction : dans $\mathbb{F}_{31}$ le polynôme R est complètement scindé,

$$R(x) = x^2(x+1)(x+3)(x+14)^2 \in \mathbb{F}_{31}[x].$$

Pour le choix $x_0 = -3$, on est conduit à résoudre dans $\mathbb{F}_{31}$ le système $(36 = y^2, 8+y^2-3y = 0)$ dont la seule solution est $y_0 = -6$.

Pour le choix $x_0 = -14 = 17$, on est conduit à résoudre dans $\mathbb{F}_{31}$ le système $(16 = y^2, y^2 + 17y + 9 = 0)$ dont la seule solution est $y_0 = 4$. Finalement on trouve 5 solutions dans $\mathbb{F}_{11}^2$, à savoir $(0,1), (0,-1), (-1,0), (-3,-6), (17,4)$, ce qui s'approche de la borne de Bezout.