Basics of Algebraic Algorithms (FLAG, MU4IN902, EPU-N8-IAL)

Jérémy Berthomieu, Vincent Neiger and Mohab Safey El Din

Durée : 1h30.
Les calculatrices et les documents sont interdits.
Les téléphones portables doivent être éteints et rangés dans les sacs.
La précision, l'argumentation et la rigueur des réponses sont des facteurs d'appréciation dans l'acquisition des points du barème.
La note sur 20 sera le minimum entre les points obtenus et 20.

Duration: 1h30
Calculators and documents are forbidden.
Phones must be turned off and kept in the bags.
Precision, argumentation and rigour are taken into account for the grade.
The final grade (on the scale 0 . . . 20) will be the minimum between the obtained points and 20.

Problem 1 (Cours/Course – 6 points)**.**

1. *Définir la caractéristique d'un corps. / Define the characteristic of a field.*
2. *Donner la liste des entiers n, $16 \leq n \leq 36$, pour lesquels il n'existe pas de corps à n éléments.*
   Give the list of integers n, $16 \leq n \leq 36$, for which there does not exist any field of size n.
3. *Soit $\mathbb{K}$ un corps. Décrire $\mathbb{K}(z) \cap \mathbb{K}[[z]]$. / Let $\mathbb{K}$ be a field. Describe $\mathbb{K}(z) \cap \mathbb{K}[[z]]$.*
4. *Soient $\mathbb{K}$ un corps et $\mathsf{M}(n)$ le nombre d'opérations dans $\mathbb{K}$ pour multiplier deux polynômes de degré n dans $\mathbb{K}[x]$. Quelle est la complexité, en nombre d'opérations dans $\mathbb{K}$, pour calculer la division euclidienne de deux polynômes de $\mathbb{K}[x]$ de degrés m et n ?*
   Let $\mathbb{K}$ be a field and let $\mathsf{M}(n)$ be the number of operations in $\mathbb{K}$ for multiplying two polynomials of degree n in $\mathbb{K}[x]$. What is the complexity, in number of operations in $\mathbb{K}$, for computing the Euclidean division of two polynomials in $\mathbb{K}[x]$ of degrees m and n?
5. *Soit $\mathbf{u} = (u_i)_{i\in\mathbb{N}}$ à coefficients dans un corps $\mathbb{K}$. Pour un polynôme non nul $P = \sum_{i=0}^{d} p_i x^i \in \mathbb{K}[x]$, on note $[P]_{\mathbf{u}} = \sum_{i=0}^{d} p_i u_i$. Pour le polynôme nul P, on définit $[P]_{\mathbf{u}} = 0$.*
   Let $\mathbf{u} = (u_i)_{i\in\mathbb{N}}$ with coefficients in a field $\mathbb{K}$. For a nonzero polynomial $P = \sum_{i=0}^{d} p_i x^i \in \mathbb{K}[x]$, we let $[P]_{\mathbf{u}} = \sum_{i=0}^{d} p_i u_i$. For the zero polynomial P, we define $[P]_{\mathbf{u}} = 0$.
   a. *Montrer que $\mathbf{u}$ satisfait la relation de récurrence $p_d u_{i+d} + \cdots + p_0 u_i = 0$ pour tout $i \in \mathbb{N}$, si, et seulement si, il existe un polynôme $P \in \mathbb{K}[x]$ (à donner explicitement) tel que pour tout $j \in \mathbb{N}$, $\left[x^j P\right]_{\mathbf{u}} = 0$.*
      Show that $\mathbf{u}$ satisfies the linear recurrence relation $p_d u_{i+d} + \cdots + p_0 u_i = 0$ for all $i \in \mathbb{N}$, if, and only if, there exists a polynomial $P \in \mathbb{K}[x]$ (to describe explicitly) such that for all $j \in \mathbb{N}$, $\left[x^j P\right]_{\mathbf{u}} = 0$.
   b. *Montrer que / Show that $I = \left\{P \in \mathbb{K}[x] \,\middle|\, \forall\, j \in \mathbb{N}, \left[x^j P\right]_{\mathbf{u}} = 0\right\}$ est un idéal de / is an ideal of $\mathbb{K}[x]$.*
   c. *Déduire que si $\mathbf{u}$ est linéairement récurrente, alors il existe une unique relation de récurrence d'ordre minimal $d > 0$ de la forme $\forall\, i \in \mathbb{N}$, $u_{i+d} + q_{d-1} u_{i+d-1} + \cdots + q_0 u_i = 0$.*
      Deduce that if $\mathbf{u}$ is linearly recurrent, then there exists a unique linear recurrence relation of minimal order $d > 0$ of the form $\forall\, i \in \mathbb{N}$, $u_{i+d} + q_{d-1} u_{i+d-1} + \cdots + q_0 u_i = 0$.

Problem 2 (Exercice calculatoire/Computation – 6 points).

1. *Soit/Let* $\mathbb{F}_4 = \mathbb{F}_2[\alpha]/\langle \alpha^2 + \alpha + 1 \rangle$.
   a. *Montrer que* $x^3 + \alpha x + 1 \in \mathbb{F}_4[x]$ *est irréductible. / Show that* $x^3 + \alpha x + 1 \in \mathbb{F}_4[x]$ *is irreducible.*
   b. *Calculer l'inverse de* $\alpha\beta^2$ *dans / Compute the inverse of* $\alpha\beta^2$ *in* $\mathbb{F}_4[\beta]/\langle \beta^3 + \alpha\beta + 1 \rangle$.

2. *Montrer l'exécution de l'algorithme d'*interpolation rapide *pour trouver* $P \in \mathbb{F}_9[x]$ *tel que*
   Show the execution of the fast interpolation *algorithm to find* $P \in \mathbb{F}_9[x]$ *such that*
   $$P(1) = 1, \quad P(2) = 1, \quad P(\gamma) = 2, \quad P(2\gamma) = 2, \qquad \text{où / where } \mathbb{F}_9 = \mathbb{F}_3[\gamma]/\langle \gamma^2 + 1 \rangle .$$

Problem 3 (Problème/Problem – 12 points). *La résolution d'un système d'équations polynomiales en* n *variables* $x_1, \ldots, x_n$ *à coefficients dans* $\mathbb{K}$ *ayant un nombre fini de solutions se fait en plusieurs étapes. La première consiste en le calcul d'une certaine matrice* $M \in \mathbb{K}^{D \times D}$, *pour un entier* $D > 0$. *Ensuite on utilise le fait que, pour* $a_n \in \mathbb{K}$, *le système possède une solution de la forme* $(a_1, \ldots, a_n)$ *si, et seulement si,* a_n *est une racine du polynôme minimal de* M. *Dans la suite,* $\mathbb{K} = \mathbb{F}_5$ *and* $n = 3$.
Solving a system of polynomial equations in n *variables* $x_1, \ldots, x_n$ *with coefficients and* $\mathbb{K}$ *and with finitely many solutions is done in several steps. The first one consists in computing a certain matrix* $M \in \mathbb{K}^{D \times D}$, *for some integer* $D > 0$. *The second step is based on the fact that, for* $a_n \in \mathbb{K}$, *the system admits a solution of the form* $(a_1, \ldots, a_n)$ *if, and only if,* a_n *is a root of the minimal polynomial of* M. *We now assume that* $\mathbb{K} = \mathbb{F}_5$ *and* $n = 3$.

$$M = \begin{pmatrix} 0 & 0 & 0 & 0 & 4 & 0 \\ 1 & 0 & 0 & 0 & 3 & 1 \\ 0 & 0 & 0 & 0 & 3 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 4 & 4 \\ 0 & 0 & 0 & 1 & 4 & 3 \end{pmatrix}, \quad u = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad v = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}.$$

1. *Montrer que le polynôme minimal de* M *est de degré au plus* 6.
   Show that the minimal polynomial of M *has degree at most* 6.

2. *Calculer un candidat pour le polynôme minimal de* M *à l'aide de l'algorithme de Wiedemann et* u *pour le vecteur à droite et* v *pour celui à gauche.*
   Compute a candidate for the minimal polynomial of M *using the Wiedemann algorithm and* u *for the vector on the right and* v *for the one on the left.*

3. *Montrer que le polynôme calculé divise le polynôme minimal de* M.
   Show that the computed polynomial divides the minimal polynomial of M.

4. *En déduire que le polynôme calculé est le polynôme minimal* M.
   Deduce that the computed polynomial is the minimal polynomial of M.

5. *On admet que les solutions satisfont aussi* $x_2 + 2x_3^5 + x_3^4 + 2x_3^3 + 4x_3 + 3 = x_1 + 2x_3^5 + x_3^4 + 2x_3^3 + 2 = 0$.
   Généralement, on peut s'intéresser aux solutions dont les coefficients sont dans une extension de corps $\mathbb{L}$ *de* $\mathbb{F}_5$.
   Soit $(a_1, a_2, a_3) \in \mathbb{L}^3$ *une telle solution. Montrer que cette solution est dans* $\mathbb{F}_5^3$ *si, et seulement si,* $a_3^5 = a_3$.
   We admit that the solutions also satisfy $x_2 + 2x_3^5 + x_3^4 + 2x_3^3 + 4x_3 + 3 = x_1 + 2x_3^5 + x_3^4 + 2x_3^3 + 2 = 0$. *Generally, we can consider solutions whose coefficients are in a field extension* $\mathbb{L}$ *of* $\mathbb{F}_5$. *Let* $(a_1, a_2, a_3) \in \mathbb{L}^3$ *be such a solution. Show that this solution is in* $\mathbb{F}_5^3$ *if, and only if,* $a_3^5 = a_3$.

6. *Calculer les solutions du système dans* $\mathbb{F}_5^3$. */ Compute all the solutions of the system in* $\mathbb{F}_5^3$.

7. *Montrer que les autres solutions sont dans* $\mathbb{F}_{25}^3$ *puis les calculer.*
   Show that the other solutions are in $\mathbb{F}_{25}^3$ *and compute them.*