UNIVERSITÉ MONTPELLIER 2
SCIENCES ET TECHNIQUES

FLMA607 Calcul Formel – 2009–2010

Corrigé de l'examen de seconde session.

Exercice 1

1) Soit A un anneau (commutatif unitaire). Soient $f, g \in A[T]$. Alors il existe $U, V \in A[T]$ tels que

$$\mathrm{Res}\,(f,g) = Uf + Vg.$$

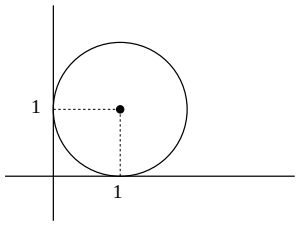
2) On note $A = \mathbb{R}[X,Y]$ et

$$\begin{aligned} f &= (1+T^2)X - 2 \in A[T], \\ g &= (1+T^2)Y - (1+T)^2 \in A[T], \\ P &= \mathrm{Res}_T(f,g) \in A. \end{aligned}$$

D'après le théorème d'élimination, il existe deux polynômes U et V de $A[T]$ tels que $P = Uf + Vg$. Si (x_0, y_0) est un point de $\mathcal{C}$, on a $f(x_0,y_0) = g(x_0,y_0) = 0$ donc $P(x_0,y_0) = 0$ et le polynôme P répond au problème posé. Il ne reste plus qu'à le calculer.

$$\begin{aligned} P(X,Y) &= \begin{vmatrix} X & & Y-1 & \\ 0 & X & -2 & Y-1 \\ X-2 & 0 & Y-1 & -2 \\ & X-2 & & Y-1 \end{vmatrix} = \begin{vmatrix} X & & Y-1 & \\ 0 & X & -2 & Y-1 \\ -2 & 0 & 0 & -2 \\ 0 & -2 & 2 & 0 \end{vmatrix} \quad \begin{matrix} L_3 \leftarrow L_3 - L_1 \\ L_4 \leftarrow L_4 - L_2 \end{matrix} \\ &= (-2)(-2)\begin{vmatrix} X & & Y-1 & \\ 0 & X & -2 & Y-1 \\ 1 & 0 & 0 & 1 \\ & 1 & -1 & 0 \end{vmatrix} = 4\begin{vmatrix} 0 & & Y-1 & -X \\ 0 & 0 & -2+X & Y-1 \\ 1 & 0 & 0 & 1 \\ & 1 & -1 & 0 \end{vmatrix} \\ &= 4\begin{vmatrix} Y-1 & -X \\ -2+X & Y-1 \end{vmatrix} = 4(Y-1)^2 + 4X(X-2) \end{aligned}$$

3) On a $P(x,y) = 0$ si et seulement si $(y-1)^2 + (x-1)^2 = 1$. On reconnaît l'équation du cercle de centre $(1,1)$ et de rayon 1.



Problème

Partie 1

1) D'après le théorème de Lagrange, on a $\alpha^{q-1} = 1$ puisque $\mathbb{F}_q^*$ est un groupe de cardinal $q-1$. Donc $(\alpha^{\frac{q-1}{2}})^2 = 1$. Or les racines du polynôme $X^2 - 1$ sont exactement 1 et -1.
2) Considérons le morphisme de groupes

$$\sigma : \begin{cases} \mathbb{F}_q^* \longrightarrow \mathbb{F}_q^* \\ x \longmapsto x^2 \end{cases}.$$

Si α est un carré, il existe $\beta \in \mathbb{F}_q^*$ tel que $\beta^2 = \alpha$. Alors $\alpha^{\frac{q-1}{2}} = \beta^{q-1} = 1$ donc α appartient à S. On en déduit que $\operatorname{Im}\sigma$ est inclus dans S. Or $\operatorname{Im}\sigma$ est de cardinal $\frac{q-1}{2}$ (puisque le noyau de σ est $\{\pm 1\}$, de cardinal 2) et S est de cardinal inférieur ou égal à $\frac{q-1}{2}$ puisque c'est l'ensemble des racines d'un polynôme de degré $\frac{q-1}{2}$. On en déduit que $\operatorname{Im}\sigma = S$ et que S est lui aussi de cardinal $\frac{q-1}{2}$. Enfin, T est le complémentaire de S dans $\mathbb{F}_q^*$. Il est donc de cardinal $q - 1 - \frac{q-1}{2} = \frac{q-1}{2}$.
3) D'après la question précédente, le polynôme $X^{\frac{q-1}{2}} - 1$ a exactement $\frac{q-1}{2}$ racines distinctes dans $\mathbb{F}_q^*$ (les éléments de S). Or il est de degré $\frac{q-1}{2}$. Donc il est scindé à racines simples, et comme il est de plus unitaire on a l'égalité :

$$X^{\frac{q-1}{2}} - 1 = \prod_{\alpha \in S} (X - \alpha).$$

Le même raisonnement avec T et le polynôme $X^{\frac{q-1}{2}} + 1$ montre que

$$X^{\frac{q-1}{2}} + 1 = \prod_{\alpha \in T} (X - \alpha).$$

4) Comme S et T forment une partition de $\mathbb{F}_q^*$, le produit des égalités ci-dessus donne

$$X^{q-1} - 1 = \prod_{\alpha \in \mathbb{F}_q^*} (X - \alpha).$$

En multipliant par X on obtient l'égalité demandée.

Partie 2

5) Le polynôme g est scindé puisqu'il divise $X^q - X$, lui-même scindé d'après la question 4). Soit $\alpha \in \mathbb{F}_q$. Montrons que $g(\alpha) = 0$ si et seulement si $f(\alpha) = 0$. La partie « seulement si » est évidente puisque g divise f. Réciproquement, si $f(\alpha) = 0$, alors $X - \alpha$ divise f. Comme $X - \alpha$ divise aussi $X^q - X$ (d'après 4), il divise g et l'on en déduit $g(\alpha) = 0$.
6) Les s_i sont deux à deux distincts si et seulement si le polynôme f est sans facteur carré. Il suffit donc d'utiliser l'algorithme (vu en cours) de factorisation d'un polynôme en produit de polynômes sans facteurs carrés.
Entrée : un polynôme f scindé.
Sortie : $g_1, \ldots, g_n$ scindés à racines simples tels que $f = g_1 \ldots g_n$.
Début :

1. Si $f' = 0$, aller en 2. Sinon, aller en 3.
2. Dans ce cas, f est la puissance $p^{\text{ième}}$ d'un polynôme h, où p est la caractéristique du corps. On trouve h tel que $f = h^p$ puis on retourne en 1 avec h à la place de f.
3. $f_1 := \operatorname{pgcd}(f, f')$
4. Si $f_1 = 1$, f est séparable, sinon on pose $g_1 := \frac{f}{f_1}$ et on recommence en 1 avec f_1 pour obtenir les polynômes $g_2, \ldots, g_n$.

Fin
7) Il suffit de regarder le terme constant de f. S'il est nul, on retient que 0 est une racine de f et on divise f par X^k avec k aussi grand que possible (en pratique, une telle division ne coûte presque rien puisqu'il suffit de translater les coefficients). On se ramène ainsi à un polynôme dont le terme constant est non nul, ce qui signifie que les s_i sont non nuls.

Partie 3

8) Vu les factorisations en irréductibles $f = \prod_{i=1}^{d}(X - s_i)$ et $X^{\frac{q-1}{2}} - 1 = \prod_{\alpha \in S}(X - \alpha)$, on a l'égalité

$$\operatorname{pgcd}(f, X^{\frac{q-1}{2}} - 1) = \prod_{\substack{i=1 \\ s_i \in S}}^{d} (X - s_i).$$

On a de même

$$\operatorname{pgcd}(f, X^{\frac{q-1}{2}}+1) = \prod_{\substack{i=1\\ s_i\in T}}^{d}(X-s_i).$$

D'où

$$\operatorname{pgcd}(f, X^{\frac{q-1}{2}}-1).\operatorname{pgcd}(f, X^{\frac{q-1}{2}}+1) = \left(\prod_{\substack{i=1\\ s_i\in S}}^{d}(X-s_i)\right).\left(\prod_{\substack{i=1\\ s_i\in T}}^{d}(X-s_i)\right) = f.$$

9) Cette factorisation est triviale si et seulement si l'un des deux facteurs vaut 1, c'est-à-dire si et seulement si les racines de f sont toutes dans S, ou toutes dans T. On suppose maintenant $d=2$, donc $f=(X-s_1)(X-s_2)$. Il y a $\binom{q-1}{2}$ configurations possibles (choix de deux éléments dans $\mathbb{F}_q^*$). Le nombre de configurations dans lesquelles les deux racines ont été choisies dans S (resp. dans T) est $\binom{\frac{q-1}{2}}{2}$. La probabilité pour que la factorisation soit triviale est donc :

$$\frac{2\binom{\frac{q-1}{2}}{2}}{\binom{q-1}{2}} = \frac{2\times\frac{(\frac{q-1}{2})(\frac{q-1}{2}-1)}{2}}{\frac{(q-1)(q-2)}{2}} = \frac{\frac{q-1}{2}-1}{q-2} = \frac{1}{2}\frac{q-1-2}{q-2} < \frac{1}{2}$$

et l'on a au moins une chance sur deux d'obtenir une factorisation non triviale.
10) Soit $f_a = gh$ une factorisation de f_a. Alors $f(X) = f_a(X+a) = g(X+a)h(X+a)$ est une factorisation de f.
11) Pour ne pas avoir réussi à factoriser f, il faut avoir obtenu une factorisation triviale à chaque fois. Vu l'hypothèse, la probabilité d'un tel événement est de l'ordre de $(2^{1-d})^{10} = (2^{-2})^{10} = 2^{-20}$, donc très faible (moins d'une chance sur 1 million !).

Partie 4

12) On note $d = \deg f$. D'après le cours, le calcul du pgcd de f et de $X^q - X$ par l'algorithme d'Euclide requiert $O((d+1)(q+1))$ opérations dans $\mathbb{F}_q$. Ce coût *n'est pas* polynomial en la taille des entrées. En effet, l'entier q est de taille $\log(q)$, et q est exponentiel en $\log q$.
13) On calcule $X^q \mod f$ par l'algorithme d'exponentiation rapide. D'après le cours, on va effectuer $O(\log q)$ multiplications dans $\mathbb{F}_q[X]/(f)$. Pour chaque multiplication dans $\mathbb{F}_q[X]/(f)$, on fait :

(i) une multiplication dans $\mathbb{F}_q[X]$ de deux polynômes de degrés $< d$;
(ii) une division euclidienne d'un polynôme de degré $< 2d$ par f.

Chacune de ces deux étapes coûte $O(d^2)$ opérations dans le corps $\mathbb{F}_q$. Au total, on fait donc $O(d^2\log q)$ opérations dans le corps $\mathbb{F}_q$ pour calculer $X^q \mod f$. Ensuite on calcule le pgcd de f avec ce reste, ce qui demande encore $O(d^2)$ opérations dans $\mathbb{F}_q$. Finalement, le calcul de g requiert un total de $O(d^2\log q)$ opérations dans $\mathbb{F}_q$.
14) Vu le résultat de la question précédente, on peut calculer $\operatorname{pgcd}(f, X^{\frac{q-1}{2}}+1)$ en $O(d^2\log(\frac{q-1}{2})) = O(d^2\log q)$ opérations dans $\mathbb{F}_q$.
15) On note $C(k)$ le coût de la détermination par l'algorithme probabiliste décrit dans la partie 3 des d racines d'un polynôme unitaire f de degré $d=2^k$ scindé, séparable et tel que $f(0)\neq 0$ (sous les hypothèses de la présente question). Pour un polynôme de degré 1 il n'y a rien à faire (la racine est l'opposé du terme constant) donc $C(0)=0$. Dans le cas général, on commence par calculer $f_1 := \operatorname{pgcd}(f, X^{\frac{q-1}{2}}+1)$ puis $f_2 := f/f_1$. Vu l'hypothèse, ces deux polynômes sont de degré $\frac{d}{2} = 2^{k-1}$. Le calcul de f_1 demande $O(d^2\log q)$ opérations d'après la question 14, et le calcul de f_2 demande $O(d^2)$ opérations d'après le cours. On en déduit l'existence d'une constante K telle que

$$C(k) \leq Kd^2\log q + 2C(k-1) = K4^k\log q + 2C(k-1).$$

Une récurrence immédiate montre alors que $C(k) \leq 2K4^k\log q = 2Kd^2\log q$. On a donc bien $C(k) = O(d^2\log q)$, cqfd.
16) D'après la question 12, la première étape de l'algorithme (le calcul de g à la question 5) requiert $O(d^2\log q)$ opérations dans $\mathbb{F}_q$. On admet qu'il en est de même pour l'étape décrite à la question 6. L'étape de la question 7 est négligeable. Enfin la partie probabiliste demande elle aussi $O(d^2\log q)$ opérations. En conclusion, sous les hypothèses optimistes faites au fil des questions, cet algorithme permet de déterminer les racines d'un polynôme de degré d à coefficients dans $\mathbb{F}_q$ en $O(d^2\log q)$ opérations dans $\mathbb{F}_q$.