ALGORITHMIQUE ALGÉBRIQUE **MU4MA023** **Examen**

P. V. Koseleff – P. Charollois

Corrigé de l'examen du 6 mai 2021

Solution 1.1. —

1. (a) On démontre la propriété par récurrence. Elle est vraie pour $n = 1$. Soit $n \geq 0$ est supposons la propriété vérifiée, alors

$$(X-1)\cdot\prod_{i=0}^{n}(X^{2^i}+1) = (X-1)\cdot\prod_{i=0}^{n-1}(X^{2^i}+1)\cdot(X^{2^n}+1) = (X^{2^n}-1)\cdot(X^{2^n}+1) = (X^{2^{n+1}}+1).$$

   Donc la propriété est vraie au rang $n+1$. Elle est héréditaire et par le théorème de récurrence, elle est vraie pour tout $n \in \mathbf{N}$.

   (b) On a d'une part $X^{2^n}-1 = \prod_{d|2^n}\Phi_d$ et d'autre part $X^{2^n}-1 = \Phi_1\cdot\prod_{i=0}^{n-1}(X^{2^i}+1)$. Les diviseurs de 2^n sont les $d_i = 2^i$, et par conséquent, on démontre par récurrence que $\Phi_{d_i} = X^{2^{i-1}}+1$. En particulier $\Phi_{2^n} = X^{2^{n-1}}+1$.

2. (a) Démontrons la propriété par récurrence. On a, pour $n = 3$, $5^{2^{n-3}} = 5 \equiv 1+4 \pmod 8 = 1+2^{n-1} \pmod{2^n}$. Supposons la propriété vérifiée pour n. Alors $5^{2^{n-3}} = 1+2^{n-1}+\lambda 2^n$, donc $5^{2^{n-2}} = \left(1+2^{n-1}+\lambda 2^n\right)^2 = 1+2^n+\lambda 2^{2n}+2^{2n-2}+\lambda^2 2^{2n} \equiv 1+2^n \pmod{2^{n+1}}$. Donc la propriété est vraie au rang $n+1$. Elle est héréditaire et par le théorème de récurrence, elle est vraie pour tout $n \geq 3$.

   (b) On déduit alors que $5^{2^{n-2}} \equiv 1 \pmod{2^n}$ donc que l'ordre de 5 dans $(\mathbf{Z}/2^n\mathbf{Z})^*$ divise 2^{n-2}. Mais $5^{2^{n-3}} \not\equiv 1 \pmod{2^n}$ donc l'ordre de 5 ne divise pas 2^{n-3}.

3. (a) On a $\Phi_4 = X^2+1 = (X-2)(X+2)$ dans $\mathbf{F}_5[X]$.

   (b) On a alors $\Phi_{2^n} = \Phi_4(X^{2^{n-2}}) = (X^{2^{n-2}}-2)(X^{2^{n-2}}+2)$.

   (c) Les facteurs irréductibles de Φ_{2^n} sont de degré l'ordre de 5 dans $(\mathbf{Z}/2^n\mathbf{Z})^*$, c'est-à-dire, 2^{n-2}. $\Phi_{2^n} = (X^{2^{n-2}}-2)(X^{2^{n-2}}-3)$ est donc la décomposition de $\Phi_{2^n} \in \mathbf{F}_5[X]$ en produits de facteurs irréductibles.

4. (a) $P_n = X^{2^n}-2$ est irréductible : c'est un des 2 facteurs de $\Phi_{2^{n+2}}$. K_n est donc un corps. Son cardinal est $q = 5^{2^n}$.

   (b) α vérifie $\alpha^{2^n} = 2$ donc $\alpha^{2^{n+1}} = -1$ et $\alpha^{2^{n+2}} = 1$. α est donc d'ordre un diviseur d de 2^{n+2}. d est une puissance de 2, mais $d \nmid 2^{n+1}$, donc $d = 2^{n+2}$. *Autre solution : les racines de Φ_N sont d'ordre N, si $(q,N) = 1$.*

5. (a) La division euclidienne de A par B_N peut s'effectuer en $O(\deg B_N(\deg A - \deg B_N + 1)) = O(N(d-N+1)) = O(Nd)$ opérations arithmétiques.

   (b) Si $A = A_0 + X^{2^n}A_1 + \cdots + X^{r\cdot 2^n}A_r$, avec $\deg A_i < 2^n$, alors $A \pmod{P_n} = \sum_{i=0}^{r} 3^i A_i$ que l'on peut calculer en calculant de proche en proche $u_0 = 1$, $R_0 = 0$, puis $R_i = R_{i-1} + u_i A_i$, $u_i = 3u_{i-1}$, pour $i = 1,\ldots,r+1$.

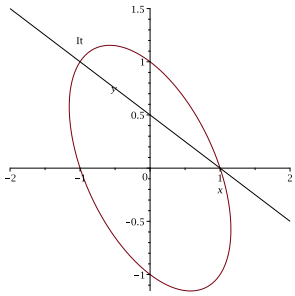
   A chaque étape on effectue 2^n+1 multiplications, et $O(2^n)$ additions, soit au total $O(r2^n) = O(d)$ opérations arithmétiques

Solution 1.2. —

1. (a) Les 6 polynômes F^2, FG, G^2, FH, GH et H^2 sont liés dans $\mathbf{R}_{\leq 4}[t]$, de dimension 5.

   (b) On en déduit qu'il existe des coefficients réels tels que $aF^2+bG^2+cFG+dFH+eGH+fH^2$, soit $ax^2+by^2+cxy+dx+ey+f = 0$. L'équation de $\mathcal{C}_1$ n'est pas de degré 1 car les polynômes $F = t^2-1$, $G = t^2+2t$ et $H = t^2+t+1$ forment une famille libre.

   (c) On doit éliminer t entre x et y. Pour cela, on écrit $x(t^2+t+1)+1-t^2 = 0, y(1+t+t^2)+t(t+2) = 0$, soit $t^2(x+1)+tx+x+1 = 0, t^2(y+1)+t(y+2)+y = 0$. Un point $(x(t),y(t))$ appartient à la courbe recherchée si et seulement si le paramètre t vérifie ces deux conditions polynomiales. t est une racine commune de



$P = T^2(x+1)+Tx+(x+1)$ et de $Q = T^2(y+1)+T(y+2)+y$. Ces deux polynômes ont une racine commune t si et seulement si leur résultant est nul. L'équation recherchée est donc $\mathrm{Res}_T(T^2(x+1)+Tx+(x+1), T^2(y+1)+T(y+2)+y) = 0$, soit

$$3(x^2+y^2+xy-1) = 0.$$

2. (a) On vérifie que les points $I = (1,0)$, $I' = (-1,0)$, $J = (0,1)$ et $J' = (-1,0)$ appartiennent à $\mathcal{C}_a$.

   (b) Si $(x,y) \in \mathcal{D}_t \cap \mathcal{C}_a$, alors on a $y = t(x-1)$, et

   $$x^2+t^2(x-1)^2+atx(x-1)-1 = (x^2-1)+t^2(x-1)^2+atx(x-1) = (x-1)(x+1+t^2(x-1)+atx) = 0.$$

   On en déduit que $x = 1$ ou $x(t^2+at+1) = t^2-1$. Le point $I(t)$ admet pour coordonnées

   $$x(t) = \frac{t^2-1}{t^2+at+1}, y(t) = t(x-1) = -\frac{t(at+2)}{t^2+at+1}.$$

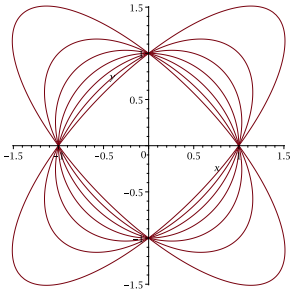
   (c) On vérifie Montrer que $I(0) = I', I(-1) = J, I(1) = J$.

   (d) On a $I(t) = I$ lorsque $x(t) = 1$ et $y(t) = 0$. On obtient $t(at+2) = 0$ et $t^2-1 = t^2+at+1$. Soit $at+2 = 0$ et $t = -2/a$. Si $a = 0$, on obtient la droite $x = 1$. $\mathcal{D}_t$ est tangente à $\mathcal{C}_a$ en I lorsque $\mathcal{D}_t$ coupe $\mathcal{C}_a$ en 2 points confondus, ce qui est le cas pour $t = -2/a$. L'équation de la tangente en I est donc $y = -2/a(x-1)$, soit $2x-21+ay = 0$.

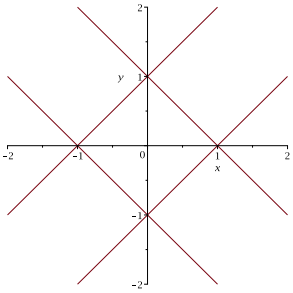
3. (a) Tout point M de $\mathcal{C}_a$ appartient à la droite IM qui est de la forme $y = t(x-1)$, sauf peut-être lorsque IM est vertical (c'est le cas pour le point $M = I(\infty) = (1,-a)$. Tout point de $\mathcal{C}_a$ est de la forme $I(t)$, y compris $I(\infty)$.

   (b) La courbe est bornée lorsque t^2+at+1 ne s'annule pas, c'est-à-dire, t^2+at+1 est irréductible, c'est-à-dire, $a^2 < 4$.

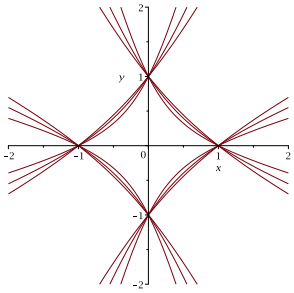
   Lorsque $|a| < 2$, on obtient une ellispe. Lorsque $a = \pm 2$, on obtient 2 droites parallèles : $2x+ay = \pm 1$. Lorsque $|a| > 2$, on obtient une hyperbole



Ellipses



Droites



Hyperboles