Université Lyon 1 - ÉNS Lyon M1 2009-2010

Géométrie algébrique élémentaire
Corrigé de l'examen final

Exercice

On fixe dans cet exercice un corps k algébriquement clos.

1. *Soit $C \subset \mathbf{A}^2(k)$ une courbe affine plane. Donner deux définitions équivalentes de la lissité pour un point $P \in C$.*

   Le point $P \in C$ est lisse si et seulement si $(\frac{\partial F}{\partial X}, \frac{\partial F}{\partial Y})(P) \neq (0,0)$, où $F \in k[X,Y]$ est un générateur de $I(C) = \{G \in k[X,Y]; G|_C = 0\}$. De manière équivalente, $P \in C$ est lisse si et seulement si le k-espace vectoriel $\mathfrak{m}/\mathfrak{m}^2$ est de dimension 1, où $\mathfrak{m}$ est l'idéal maximal de $k[C]$ associé à P.

2. *Étudier la courbe $C : y^2 + x^2y + x = 0$ de $\mathbf{A}^2(k)$. On déterminera notamment $I(C)$, la courbe $\overline{C}$, les points à l'infini et les points singuliers éventuels de $\overline{C}$ (on distinguera suivant la caractéristique de k).*

   Le critère d'Eisenstein utilisé avec l'élément irréductible X de $k[X]$ montre que $F = Y^2 + X^2Y + X$ est irréductible dans $(k[X])[Y] \cong k[X,Y]$. Par suite $I(C) = (F)$. D'après le cours, la courbe projective associée à C est donnée par $\overline{C} = V(\widetilde{F})$, où $\widetilde{F} = X^2Y + Y^2Z + Z^2X$ est l'homogénéisé de F. Les points à l'infini de C sont donnés par $C_\infty = \overline{C} \cap V(Z) = V(XY, Z) = \{(0:1:0), (1:0:0)\}$. D'après le cours $P = (x:y:z) \in \overline{C}$ est singulier si et seulement si $\frac{\partial \widetilde{F}}{\partial X}(x,y,z) = \frac{\partial \widetilde{F}}{\partial Y}(x,y,z) = \frac{\partial \widetilde{F}}{\partial Z}(x,y,z) = 0$ c'est-à-dire $2xy + z^2 = 2yz + x^2 = 2zx + y^2 = 0$. Supposons $P = (x:y:z) \in C$ singulier. Si l'une des variables x, y, z est nulle alors les équations entraînent $x = y = z = 0$, ce qui est absurde. Donc $x, y, z \neq 0$. On a $x^2y = (-2yz)y = -2y^2z$ et par symétrie circulaire $y^2z = -2z^2x$ et $z^2x = -2x^2y$. Par suite $x^2y = -8x^2y$ et $9x^2y = 0$. Si $\mathrm{car}(k) \neq 3$, on obtient une contradiction. Si $\mathrm{car}(k) = 3$ alors les équations de départ s'écrivent $z^2 = xy$, $x^2 = yz$ et $y^2 = xz$, d'où l'on tire $(y^2/x)^2 = xy$ et donc $y^3 = x^3$. Par injectivité du morphisme $t \mapsto t^3$ sur k, il vient $x = y$ et par symétrie $y = z$, d'où $P = (1:1:1)$. On vérifie que ce point appartient à $\overline{C}$ et est singulier. En conclusion, $\overline{C}$ est lisse si $\mathrm{car}(k) \neq 3$, et admet l'unique point singulier $(1:1:1)$ si $\mathrm{car}(k) = 3$.

3. *Déterminer l'ordre d'annulation de $x, y, x + y^2 \in k[C]$ en $O = (0,0)$.*

Soit $\mathfrak{m}$ l'idéal maximal de $k[C]$ associé à O. Puisque O est lisse (question précédente), on a $\dim_k \mathfrak{m}/\mathfrak{m}^2 = 1$. L'idéal $\mathfrak{m}$ étant engendré par x et y, l'espace vectoriel $\mathfrak{m}/\mathfrak{m}^2$ est engendré par les classes de x et y. Or $x = -y^2 - x^2y \in \mathfrak{m}^2$ ce qui fait que $y \notin \mathfrak{m}^2$ et donc $\mathrm{ord}_O(y) = 1$. Par suite $\mathrm{ord}_O(-y^2) = 2$ et $\mathrm{ord}_O(-x^2y) \geq 3$, d'où l'on tire $\mathrm{ord}_O(x) = 2$. Enfin $\mathrm{ord}_O(x + y^2) = \mathrm{ord}_O(-x^2y) = 2\,\mathrm{ord}_O(x) + \mathrm{ord}_O(y) = 5$.

Problème – Points d'inflexion sur une cubique

On se donne un polynôme $F \in \mathbf{C}[X_1, X_2, X_3]$ homogène de degré 3, irréductible, et tel que la courbe projective $C = V(F)$ soit lisse.

On note $\mathcal{I}$ l'ensemble des points d'inflexion de C, c'est-à-dire l'ensemble des $P \in C$ tels que $m_P(C, T) > 2$, où T désigne la tangente de C en P.

Pour $i, j \in \{1, 2, 3\}$, on pose $F_i = \frac{\partial F}{\partial X_i}$ et $F_{ij} = \frac{\partial^2 F}{\partial X_i \partial X_j}$. On note H_F le déterminant de la matrice $M = (F_{ij})_{1 \leq i,j \leq 3} \in \mathcal{M}_3(\mathbf{C}[X_1, X_2, X_3])$.

Pour tout entier $d \geq 0$, on note $\mathbf{C}[X_1, X_2, X_3]_d$ le sous-espace vectoriel de $\mathbf{C}[X_1, X_2, X_3]$ formé des polynômes homogènes de degré d.

1. *Montrer que $H_F \in \mathbf{C}[X_1, X_2, X_3]_3$.*
   Pour tout i et j, on a $F_i \in \mathbf{C}[X_1, X_2, X_3]_2$ et $F_{ij} \in \mathbf{C}[X_1, X_2, X_3]_1$. La définition du déterminant montre alors que $H_F \in \mathbf{C}[X_1, X_2, X_3]_3$.
2. *Soit $G \in \mathbf{C}[X_1, X_2, X_3]_e$. Montrer la relation d'Euler $\sum_{i=1}^3 X_i \frac{\partial G}{\partial X_i} = eG$.*
   Par linéarité, il suffit de montrer le résultat lorsque G est un monôme $X_1^{a_1} X_2^{a_2} X_3^{a_3}$ avec $a_1 + a_2 + a_3 = e$. Un calcul direct donne $\sum_{i=1}^3 X_i \frac{\partial G}{\partial X_i} = \sum_{i=1}^3 a_i G = eG$.
3. *En déduire $\sum_{i=1}^3 X_i F_i = 3F$ et $\sum_{j=1}^3 X_j F_{ij} = 2F_i$.*
   Il suffit d'appliquer la question précédente à $G = F \in \mathbf{C}[X_1, X_2, X_3]_3$ et à $G = F_i \in \mathbf{C}[X_1, X_2, X_3]_2$. Noter que $\frac{\partial F_i}{\partial X_j} = F_{ji} = F_{ij}$ car les opérateurs $\frac{\partial}{\partial X_i}$ et $\frac{\partial}{\partial X_j}$ commutent (on le vérifie sur les monômes).
4. *À l'aide d'opérations élémentaires sur M, montrer les identités*

$$X_3^2 H_F = \begin{vmatrix} F_{11} & F_{12} & X_3 F_{13} \\ F_{21} & F_{22} & X_3 F_{23} \\ X_3 F_{31} & X_3 F_{32} & X_3^2 F_{33} \end{vmatrix} = \begin{vmatrix} F_{11} & F_{12} & 2F_1 \\ F_{21} & F_{22} & 2F_2 \\ 2F_1 & 2F_2 & 6F \end{vmatrix}.$$

   La première identité résulte de la linéarité du déterminant par rapport à la dernière ligne et à la dernière colonne. Pour obtenir la seconde identité, on effectue les opérations élémentaires suivantes, ne changeant pas le déterminant : $C_3 \leftarrow C_3 + X_1 C_1 + X_2 C_2$ et $L_3 \leftarrow L_3 + X_1 L_1 + X_2 L_2$ (on a aussi utilisé le fait que $F_{ij} = F_{ji}$).

5. *En déduire* $X_3^2 H_F \equiv 8F_1F_2F_{12} - 4F_1^2F_{22} - 4F_2^2F_{11} \pmod F$.

   D'après la question précédente $X_3^2 H_F \equiv \begin{vmatrix} F_{11} & F_{12} & 2F_1 \\ F_{21} & F_{22} & 2F_2 \\ 2F_1 & 2F_2 & 0 \end{vmatrix} \pmod F$.

   En développant suivant la dernière colonne et en tenant compte de $F_{12} = F_{21}$, on obtient le résultat annoncé.

Dans les questions (6) à (15), on suppose que $P_0 = (0:0:1) \in C$ *et que la tangente de* C *en* P_0 *est la droite* $T : X_2 = 0$. *On pose* $\widetilde{P_0} = (0,0,1)$.

6. *Montrer que* $F_1(\widetilde{P_0}) = 0$ *et* $F_2(\widetilde{P_0}) \neq 0$.

   D'après le cours T admet pour équation $\sum_{i=1}^3 F_i(\widetilde{P_0}) \cdot X_i = 0$. Comme on a aussi $T : X_2 = 0$, il vient $F_1(\widetilde{P_0}) = 0$ et $F_2(\widetilde{P_0}) \neq 0$ (et $F_3(\widetilde{P_0}) = 0$).

7. *En déduire que* $P_0 \in V(H_F)$ *équivaut à* $F_{11}(\widetilde{P_0}) = 0$.

   La condition $P_0 \in V(H_F)$ équivaut à $H_F(\widetilde{P_0}) = 0$. D'après (5) et (6) et comme $F(\widetilde{P_0}) = 0$, il vient $H_F(\widetilde{P_0}) = (X_3^2 H_F)(\widetilde{P_0}) = -4F_2^2(\widetilde{P_0})F_{11}(\widetilde{P_0})$. Toujours d'après (6), on a $F_2(\widetilde{P_0}) \neq 0$, d'où le résultat.

On considère la carte affine $\{(x:y:1); x,y \in \mathbf{C}\} \cong \mathbf{A}^2(\mathbf{C})$ *de* $\mathbf{P}^2(\mathbf{C})$. *On pose* $f = F(X,Y,1) \in \mathbf{C}[X,Y]$ *et on note* $C_f = V(f) \subset \mathbf{A}^2(\mathbf{C})$ *la courbe affine associée à* f. *On désigne par* x *(resp.* y*) l'image de* X *(resp.* Y*) dans* $\mathbf{C}[C_f]$. *Enfin, on pose* $O = (0,0) \in C_f$.

8. *Montrer que* $\frac{\partial f}{\partial X}(O) = 0$ *et* $\frac{\partial f}{\partial Y}(O) \neq 0$.

   On a $\frac{\partial f}{\partial X} = F_1(X,Y,1)$ d'où $\frac{\partial f}{\partial X}(O) = F_1(\widetilde{P_0}) = 0$. De même $\frac{\partial f}{\partial Y}(O) \neq 0$.

9. *Quelle est l'équation de* T *dans cette carte affine ? En déduire* $\mathrm{ord}_O(y) = m_{P_0}(C,T)$ *et* $\mathrm{ord}_O(y) \in \{2,3\}$.

   L'équation de $T' := T \cap \mathbf{A}^2(\mathbf{C})$ est $y = 0$. En tant que courbe, T est irréductible et n'est pas une composante irréductible de C (par hypothèse de l'énoncé). Donc $m_{P_0}(C,T)$ est un entier bien défini, et le cours permet d'écrire $m_{P_0}(C,T) = m_O(C_f, T') = \mathrm{ord}_{O\in C_f}(y)$, la dernière égalité étant justifiée par le fait que $O \in C_f$ est lisse et que $I(T') = (Y)$. Comme T est tangente à C en P_0, le cours donne $m_{P_0}(C,T) \geq 2$. Les courbes C et T n'ayant pas de composante commune, on peut leur appliquer le théorème de Bézout. Les idéaux $I(C) = (F)$ et $I(T) = (X_2)$ étant engendrés par des polynômes de degrés respectifs 3 et 1, on obtient $\sum_{P\in C\cap T} m_P(C,T) = 3$. En particulier $m_{P_0}(C,T) \leq 3$ et on a bien $\mathrm{ord}_O(y) \in \{2,3\}$.

10. *Montrer que* x *est une uniformisante de* C_f *en* O.

    Comme $O \in C_f$ est lisse et $\mathrm{ord}_O(y) \geq 2$, le même raisonnement que la question (3) de l'exercice montre que x est une uniformisante en O.

11. *En utilisant la relation* $\frac{\partial f}{\partial X}(x,y)\ \mathrm{d}x + \frac{\partial f}{\partial Y}(x,y)\ \mathrm{d}y = 0$ *dans* $\Omega^1(C_f)$, *montrer que* $\mathrm{ord}_O(\mathrm{d}y) = \mathrm{ord}_O(\frac{\partial f}{\partial X}(x,y))$.

 Rappelons qu'on obtient cette relation en différentiant l'identité tautologique $f(x,y) = 0$ dans $\mathbf{C}[C_f]$. Comme x est une uniformisante en O, on a d'après le cours $\mathrm{ord}_O(\mathrm{d}y) = \mathrm{ord}_O(\frac{\mathrm{d}y}{\mathrm{d}x}) = \mathrm{ord}_O(-\frac{\partial f/\partial X(x,y)}{\partial f/\partial Y(x,y)})$. Le dernier quotient a bien un sens dans $\mathbf{C}(C_f)$ car $\frac{\partial f}{\partial Y}(x,y)(O) \neq 0$, ce qui montre du même coup $\mathrm{ord}_O(\frac{\partial f}{\partial Y}(x,y)) = 0$ et le résultat.

12. *Établir le développement limité* $\frac{\partial f}{\partial X}(x,y) = \frac{\partial^2 f}{\partial X^2}(O) \cdot x + O(x^2)$ *à l'ordre 2 au point* O.

 Écrivons le développement de Taylor du *polynôme* $\frac{\partial f}{\partial X}$ au point O. Vu (8), on a $\frac{\partial f}{\partial X} = \frac{\partial^2 f}{\partial X^2}(O) \cdot X + \frac{\partial^2 f}{\partial X \partial Y}(O) \cdot Y + h$ avec $h \in \langle X^2, XY, Y^2\rangle$. En appliquant le morphisme de k-algèbres $X, Y \mapsto x, y$ et en tenant compte du fait que $y = O(x^2)$ et donc $h(x,y) = O(x^2)$, le résultat suit.

13. *Démontrer que* $\mathrm{ord}_O(\mathrm{d}y) = \mathrm{ord}_O(y) - 1$.

 Posons $e = \mathrm{ord}_O(y) \in \{2,3\}$. Écrivons $y = \lambda x^e + O(x^{e+1})$ avec $\lambda \in \mathbf{C}^*$. D'après le cours, on peut dériver ce développement limité, ce qui donne $\frac{\mathrm{d}y}{\mathrm{d}x} = e\lambda x^{e-1} + O(x^e)$. Comme $e\lambda \neq 0$, on obtient bien $\mathrm{ord}_O(\mathrm{d}y) = e-1$.

14. *Déduire des questions précédentes que* $P_0 \in \mathcal{I}$ *équivaut à* $P_0 \in V(H_F)$.

 On a les équivalences successives $P_0 \in \mathcal{I} \overset{\text{déf}}{\Leftrightarrow} m_{P_0}(C,T) \geq 3 \overset{(9)}{\Leftrightarrow} \mathrm{ord}_O(y) \geq 3 \overset{(13)}{\Leftrightarrow} \mathrm{ord}_O(\mathrm{d}y) \geq 2 \overset{(11)}{\Leftrightarrow} \mathrm{ord}_O(\frac{\partial f}{\partial X}(x,y)) \geq 2 \overset{(12)}{\Leftrightarrow} \frac{\partial^2 f}{\partial X^2}(O) = 0 \Leftrightarrow F_{11}(\widetilde{P_0}) = 0 \overset{(7)}{\Leftrightarrow} P_0 \in V(H_F)$.

15. *Montrer que si* $P_0 \in \mathcal{I}$ *alors* $m_{P_0}(C, V(H_F)) = 1$ *(on pourra commencer par établir que* $\frac{\partial^3 f}{\partial X^3}(O) \neq 0$*).*

 Supposons $P_0 \in \mathcal{I}$. D'après la question (9), on a $\mathrm{ord}_O(y) = 3$. D'après les équivalences démontrées dans la question (14), on sait aussi que $\frac{\partial^2 f}{\partial X^2}(O) = 0$. En poussant le développement de Taylor de $\frac{\partial f}{\partial X}$ en O un cran plus loin, on trouve $\frac{\partial f}{\partial X} = \frac{1}{2}\frac{\partial^3 f}{\partial X^3}(O)X^2 + h'$ avec $h' \in \langle X^3, Y\rangle$. Comme $h'(x,y) = O(x^3)$ et $\mathrm{ord}_O(\frac{\partial f}{\partial X}(x,y)) = 2$ (questions (11) et (13)), il vient $\frac{\partial^3 f}{\partial X^3}(O) \neq 0$. On pouvait également remarquer (vu sur une seule copie) que $\frac{\partial^2 f}{\partial X^2}(O) = \frac{\partial^3 f}{\partial X^3}(O) = 0$ et $\deg(f) = 3$ entraînent que Y divise f, ce qui contredirait l'irréductibilité de C_f.

 Pour l'instant, on n'a toujours pas montré que $H_F \neq 0$. On va établir que $\mathrm{ord}_O(H_F(x,y,1)) = 1$, ce qui montrera d'un coup le fait que C et $V(H_F)$ n'ont pas de composante commune (si elles en avaient une, H_F s'annulerait identiquement sur C) et la multiplicité souhaitée (noter qu'il n'est pas nécessaire ici de montrer que H_F engendre l'idéal de

$V(H_F)$: si tel n'était pas le cas, cela ne ferait que diminuer la multiplicité). D'après la question (14), on sait que $\mathrm{ord}_O(H_F(x,y,1)) \geq 1$. En appliquant le morphisme $X_1, X_2, X_3 \mapsto x, y, 1$ à l'identité de la question (5) (ce qui est licite car $F(x,y,1) = f(x,y) = 0$), on obtient $H_F(x,y,1) = \frac{\partial f}{\partial X}(x,y) \cdot g - 4(\frac{\partial f}{\partial Y}(x,y))^2 \frac{\partial^2 f}{\partial X^2}(x,y)$ pour une certaine $g \in \mathbf{C}[C_f]$. D'une part, on sait que $\mathrm{ord}_O(\frac{\partial f}{\partial X}(x,y) \cdot g) \geq \mathrm{ord}_O(\frac{\partial f}{\partial X}(x,y)) \geq 2$ et $\mathrm{ord}_O(\frac{\partial f}{\partial Y}(x,y)) = 0$. D'autre part, la considération du développement de Taylor de $\frac{\partial^2 f}{\partial X^2}$ mène à $\mathrm{ord}_O(\frac{\partial^2 f}{\partial X^2}(x,y)) = 1$. Le résultat suit des propriétés de l'ordre d'annulation.

16. *Soit $g \in \mathrm{GL}_3(\mathbf{C})$ et $F_g \in \mathbf{C}[X_1, X_2, X_3]$ l'unique polynôme tel que $F_g(x) = F(gx)$ pour tout $x = (x_1, x_2, x_3) \in \mathbf{C}^3$. Montrer que $H_{F_g}(x) = (\det g)^2 \cdot H_F(gx)$ pour tout $x \in \mathbf{C}^3$.*

    Posons $g = (g_{ij})_{1 \leq i,j \leq 3}$. Notons gX le vecteur $(\sum_{j=1}^3 g_{ij} X_j)_{1 \leq i \leq 3}$, qui est à coordonnées dans $\mathbf{C}[X_1, X_2, X_3]$. Le polynôme F_g n'est autre que le polynôme composé $F(gX)$. On sait dériver un tel poynôme, et cela donne $(F_g)_k = \sum_{i=1}^3 g_{ik} F_i(gX) = \sum_{i=1}^3 g_{ik} (F_i)_g$. En continuant à dériver, il vient $(F_g)_{k\ell} = \sum_{i=1}^3 g_{ik} ((F_i)_g)_\ell = \sum_{i=1}^3 g_{ik} \sum_{j=1}^3 g_{j\ell} F_{ij}(gX)$. En notant M_g la matrice qui est au polynôme F_g ce que M est à F, nous venons en fait de montrer $(M_g)_{k\ell} = \sum_{i,j=1}^3 g_{ik} g_{j\ell} M_{ij}(gX)$ c'est-à-dire $M_g = {}^t g \cdot M(gX) \cdot g$. En prenant le déterminant, il vient $H_{F_g} = (\det g)^2 H_F(gX)$.

17. *Montrer que $\mathcal{I} = C \cap V(H_F)$ et que $m_P(C, V(H_F)) = 1$ pour tout $P \in \mathcal{I}$.*

    Comme $\mathcal{I} \subset C$ par définition, il suffit de montrer que pour $P \in C$, on a l'équivalence $P \in \mathcal{I} \Leftrightarrow P \in V(H_F)$. Dans le question (14), on l'a montré dans un cas particulier. On va se ramener à ce cas par un changement projectif de coordonnées convenable. Soit $P \in C$. Désignons par T la tangente de C en P. Soit $g \in \mathrm{GL}_3(\mathbf{C})$ tel que $g(P) = (0:0:1)$ et tel que $g(T)$ soit la droite $X_2 = 0$. Il en existe car $\mathrm{GL}_3(\mathbf{C})$ agit 2-transitivement sur $\mathbf{P}^2(\mathbf{C})$ (on prend un point $P' \neq P$ sur T, et on choisit g tel que $g(P) = (0:0:1)$ et $g(P') = (1:0:0)$; comme g envoie droite projective sur droite projective, on a bien $g(T) = V(X_2)$). La courbe $C' = g(C) = g(V(F)) = V(F_{g^{-1}})$ vérifie les conditions du cas particulier. Comme une transformation projective préserve les tangentes et les multiplicités d'intersection, le point P est un point d'inflexion de C si et seulement si $g(P)$ est un point d'inflexion de C', c'est-à-dire si et seulement si $g(P) \in V(H_{F_{g^{-1}}}) = gV(H_F)$ d'après la question précédente. D'où la première partie de l'assertion. Enfin, pour $P \in \mathcal{I}$ on a $m_P(C, V(H_F)) = m_{g(P)}(g(C), g(V(H_F))) = 1$.

18. *Déduire du théorème de Bézout que $\#\mathcal{I} = 9$.*

On a déjà vu que C et $V(H_F)$ n'ont pas de composante commune. On peut donc leur appliquer le théorème de Bézout. Vu la question précédente, on a $\#\mathcal{I} = \sum_{P \in C \cap V(H_F)} m_P(C, V(H_F))$. Pour obtenir $\#\mathcal{I} = 9$, encore faut-il montrer que H_F (qui est non nul et homogène de degré 3) engendre l'idéal de $V(H_F)$, c'est-à-dire montrer que H_F est sans facteur carré. Si tel n'était pas le cas, alors H_F serait divisible par λ^2 avec $\lambda \in \mathbf{C}[X_1, X_2, X_3]_1 - \{0\}$. En considérant un point $P \in C \cap V(\lambda)$ (il en existe par Bézout) et en se ramenant par transformation projective au cas $P = P_0$ et $T : X_2 = 0$, on aurait avec les notations de la démonstration de la question (15) l'inégalité $\mathrm{ord}_O(H_F(x, y, 1)) \geq 2\,\mathrm{ord}_O(\lambda(x, y, 1)) \geq 2$, ce qui est absurde. D'où finalement $\#\mathcal{I} = 9$.

19. *Soit $P_1, P_2 \in \mathcal{I}$ distincts. Montrer que la droite $D = (P_1P_2)$ coupe C en un troisième point $P_3 \notin \{P_1, P_2\}$ et que l'on a $P_3 \in \mathcal{I}$.*

La droite D n'étant pas incluse dans C, le théorème de Bézout donne $\sum_{P \in C \cap D} m_P(C, D) = 3$. Il suffit de montrer que pour $i \in \{1, 2\}$, on a $m_{P_i}(C, D) = 1$. On a déjà $m_{P_i}(C, D) \geq 1$, et $m_{P_i}(C, D) \geq 2$ entraînerait que D est la tangente de C en P_i, d'où $m_{P_i}(C, D) \geq 3$ et $\sum_{P \in C \cap D} m_P(C, D) > 3$, absurde. Par suite il existe $P_3 \in C \cap D$ tel que $P_3 \notin \{P_1, P_2\}$. Pour montrer que $P_3 \in \mathcal{I}$, utilisons la loi de groupe sur une cubique irréductible lisse (TD n°10, exercice 7). Fixons $O \in \mathcal{I}$ et considérons la loi de groupe abélien sur C d'élément neutre O. Commençons par montrer que si une droite D' intersecte C en des points (non nécessairement distincts) P, Q, R, alors $P + Q + R = O$. Avec les notations de l'exercice, on a $\varphi(P, Q) = R$ d'où $P + Q = \varphi(O, R)$. La droite (OR) coupe C en O, R et $\varphi(O, R)$, d'où $\varphi(\varphi(O, R), R) = O$ et donc $(P + Q) + R = \varphi(O, \varphi(P + Q, R)) = \varphi(O, O) = O$ car $O \in \mathcal{I}$. On obtient en particulier $P_1 + P_2 + P_3 = O$. En appliquant également le résultat à la tangente T_i de C en P_i, il vient $3P_i = O$ pour $i \in \{1, 2\}$ puisque dans ce cas $C \cap T_i = \{P_i\}$. Par suite $3P_3 = O$. Par l'absurde, supposons que $P_3 \notin \mathcal{I}$. Alors $C \cap T_3 = \{P_3, P_3'\}$ avec $P_3' \neq P_3$. Mais on aurait $2P_3 + P_3' = O$, ce qui contredit $3P_3 = O$. Ainsi $P_3 \in \mathcal{I}$.

Remarque : on vient en fait de montrer que $\mathcal{I}$ est un sous-groupe de C. Comme $\mathcal{I}$ est d'ordre 9 et que tout point $P \in \mathcal{I}$ vérifie $3P = O$, on a en fait $\mathcal{I} \cong (\mathbf{Z}/3\mathbf{Z})^2$.

On suppose que C est une cubique réelle, i. e. $F \in \mathbf{R}[X_1, X_2, X_3]$.

20. *Montrer que C possède au moins un point d'inflexion réel (on pourra utiliser la conjugaison complexe $c : (x : y : z) \mapsto (\overline{x} : \overline{y} : \overline{z})$ de $\mathbf{P}^2(\mathbf{C})$).*

Comme F et donc H_F sont à coefficients réels, l'ensemble $\mathcal{I} = V(F, H_F)$ est stable par c. L'application $c|_{\mathcal{I}}$ étant une involution sur un ensemble à

9 éléments, et 9 étant impair, elle possède nécessairement un point fixe. D'où l'existence d'un point d'inflexion réel (si $(x:y:z) = (\overline{x}:\overline{y}:\overline{z})$ alors $(\overline{x},\overline{y},\overline{z}) = \lambda(x,y,z)$ avec $\lambda \in \mathbf{C}^*$; comme $|\lambda| = 1$ on peut écrire $\lambda = \mu/\overline{\mu}$ ce qui fait que $(x:y:z) = (\mu x : \mu y : \mu z) \in \mathbf{P}^2(\mathbf{R})$).

21. *Montrer que* $\#(\mathcal{I} \cap \mathbf{P}^2(\mathbf{R})) = 3$.

On a vu à la question précédente que $\mathcal{I} \cap \mathbf{P}^2(\mathbf{R})$ est non vide. Choisissons $O \in \mathcal{I} \cap \mathbf{P}^2(\mathbf{R})$ comme origine sur C. Comme c préserve l'alignement des points et $c(O) = O$, on a $c(P+Q) = c(P) + c(Q)$ pour tout $P, Q \in C$. Par suite $\mathcal{I} \cap \mathbf{P}^2(\mathbf{R})$ est un sous-groupe de $\mathcal{I}$ et est de cardinal 1, 3 ou 9. Quitte à appliquer un élément convenable de $\mathrm{GL}_3(\mathbf{R})$, on peut supposer que $O = (0:1:0)$ et que la tangente T de C en O est $T = V(Z)$ (on note maintenant $(x:y:z)$ les coordonnées homogènes sur $\mathbf{P}^2(\mathbf{C})$). D'après les calculs qui ont déjà été faits, l'équation de C prend la forme

$$\alpha y^2 z + \beta xyz + \gamma x^2 z + \delta x^3 + \epsilon x^2 z + \zeta x z^2 + \eta z^3 = 0$$

avec $\alpha, \delta \neq 0$. Quitte à appliquer un changement de variables de la forme $y' = \lambda y + \mu x + \nu z$, $x' = \xi x + \rho z$ et $z' = z$ avec $\lambda, \xi \in \mathbf{R}^*$ (cette transformation fixe O et laisse stable T), on peut supposer $\alpha = 1$, $\delta = -1$, $\beta = \gamma = \epsilon = 0$, d'où $C : y^2 z = x^3 + axz^2 + bz^3$ avec $a, b \in \mathbf{R}$.

Un calcul explicite donne $M = \begin{pmatrix} -6X & 0 & -2aZ \\ 0 & 2Z & 2Y \\ -2aZ & 2Y & -2aX - 6bZ \end{pmatrix}$ d'où

$$H_F = 24X(aXZ + 3bZ^2 + Y^2) - 8a^2 Z^3.$$

Considérons la carte affine $\{(x:y:1); x, y \in \mathbf{C}\}$. La cubique $V(H_F)$ possède deux points à l'infini $(0:1:0)$ et $(1:0:0)$, mais ce dernier n'est pas sur C car O est l'unique point à l'infini de C. Pour $x, y \in \mathbf{R}$, on a l'équivalence

$$(x:y:1) \in \mathcal{I} \Leftrightarrow \begin{cases} y^2 = x^3 + ax + b \\ 24x(ax + 3b + y^2) - 8a^2 = 0. \end{cases}$$

Ces deux conditions entraînent $g(x) := 3x^4 + 6ax^2 + 12bx - a^2 = 0$. Remarquons que $g'(x) = 12(x^3 + ax + b)$ est à racines simples (dans $\mathbf{C}$) par lissité de C.

Premier cas : $a = 0$. On a $b \neq 0$ et les racines réelles de $g(x) = 3x(x^3 + 4b)$ sont 0 et $-\sqrt[3]{4b}$. La première équation donne alors $y^2 = b$ (resp. $y^2 = -3b$). D'où $\#(\mathcal{I} \cap \mathbf{P}^2(\mathbf{R})) = 3$ quel que soit le signe de b.

Deuxième cas : $a \neq 0$ et x^3+ax+b possède une unique racine réelle. Comme $g(0) = -a^2 < 0$, le polynôme g possède au moins deux racines réelles. Le tableau de variations de $g(x)$ montre que g a exactement 2 racines réelles ξ_1 et ξ_2, et qu'une seule de ces racines vérifie $g'(\xi_i) > 0$. D'où encore $\#(\mathcal{I} \cap \mathbf{P}^2(\mathbf{R})) = 3$.

Troisième cas : $a \neq 0$ et $x^3 + ax + b$ possède trois racines réelles $x_1 < x_2 < x_3$. Par l'absurde, supposons d'abord $\#(\mathcal{I} \cap \mathbf{P}^2(\mathbf{R})) = 1$. D'après le tableau de variations de $g(x)$, on a nécessairement $g(x_3) > 0$ (sinon g aurait une racine $x \in [x_3, +\infty[$ qui vérifierait $x^3 + ax + b \geq 0$, d'où un point d'inflexion réel autre que O). Par suite $g(x_2) > 0$ et de même $g(x_1) > 0$. Mais alors $g > 0$ sur $\mathbf{R}$, ce qui contredit $g(0) = -a^2 < 0$. Toujours par l'absurde, supposons maintenant $\#(\mathcal{I} \cap \mathbf{P}^2(\mathbf{R})) = 9$. Alors g serait scindé à racines simples dans $\mathbf{R}$, et d'après le tableau de variations de $g(x)$ on aurait $g(x_1) < 0$, $g(x_2) > 0$ et $g(x_3) < 0$. Mais alors les racines x de g dans les intervalles $]-\infty, x_1[$ et $]x_2, x_3[$ vérifieraient $x^3 + ax + b < 0$, ce qui est absurde. Cela achève la démonstration du fait que $\#(\mathcal{I} \cap \mathbf{P}^2(\mathbf{R})) = 3$.

Remarque. Plus généralement, Felix Klein a démontré en 1876 que pour une courbe réelle « générique » de degré d, le nombre de ses points d'inflexion réels ne peut dépasser $d(d-2)$, c'est-à-dire le tiers du nombre total de ses points d'inflexion (il est facile de voir que dans cette situation H_F est homogène de degré $3(d-2)$, d'où $3d(d-2)$ points d'inflexion complexes en général).