TD - Feuille 5

Corrigé ex. 1 (1) Une façon de décrire l'éclatement est comme image schématique de l'application graphe $\varphi : X \dashrightarrow X \times \mathbb{P}^n$ de l'application rationnelle $X \dashrightarrow \mathbb{P}^n$ donné par les fonctions f_i, c'est-à-dire $x \mapsto [f_1(x) : \cdots : f_n(x)]$. (Pour plus de détails sur images et adhérences schématiques, voir Liu, exercice 2.3.17. L'image schématique est l'adhérence schématique de l'image.) L'ensemble de définition de φ est la réunion des ouverts $D(f_i)$, c'est-à-dire, l'ouvert complémentaire du centre de l'éclatement.

Profitons de cette définition pour faire quelques commentaires sur les écritures utilisées. On sait que chaque $f_i \in A$ peut être vu comme un morphisme $X \to \mathbb{A}^1$, et le uplet $f_0, \dots, f_n$ comme un morphisme $X \to \mathbb{A}^{n+1}$. (En l'absence de précision, lorsqu'on écrit $\mathbb{A}^1$ il s'agit de la droite affine sur $\mathbb{Z}$, ou alors de la droite affine sur l'anneau R qui sert d'anneau de base dans le contexte de l'exercice. Dans cet exercice, aucun anneau de base n'est mentionné.) L'application φ est obtenue en composant avec l'application rationnelle $\pi : \mathbb{A}^{n+1} \dashrightarrow \mathbb{P}^n$ qui, lorsqu'on est sur un corps de base k, est le quotient par le groupe multiplicatif k^*. Plus précisément, choisissons des coordonnées $z_0, \dots, z_n$ sur $\mathbb{A}^n$, donc $\mathbb{A}^n = \mathrm{Spec}(\mathbb{Z}[z_0, \dots, z_n])$. Ces coordonnées induisent des coordonnées homogènes $x_0, \dots, x_n$ sur $\mathbb{P}^n$, telles que $\mathbb{P}^n = \mathrm{Proj}(\mathbb{Z}[x_0, \dots, x_n])$ et que π est définie sur l'ouvert $\Omega = \cup_{i=0}^n D(z_i)$ par

$$\pi_{|D(z_i)} : D(z_i) \to D_+(x_i)$$

induit par le morphisme d'anneaux

$$\mathbb{Z}[\frac{x_0}{x_i}, \dots, \frac{x_n}{x_i}] \to \mathbb{Z}[z_0, \dots, z_n, \frac{1}{z_i}]$$

qui envoie x_k/x_i sur z_k/z_i. Une autre description de π en termes de la propriété universelle de $\mathbb{P}^n$ est qu'il y a sur Ω un faisceau inversible engendré par $n+1$ sections, c'est le sous-faisceau du faisceau des fonctions méromorphes $\mathcal{K}_\Omega$ qui sur $D(z_i) = \mathrm{Spec}(\mathbb{Z}[z_0, \dots, z_n, 1/z_i])$ a pour générateur $1/z_i$. (On vérifie que les faisceaux $\mathcal{L}_i$ ainsi définis sur $D(z_i)$ se recollent en un faisceau sur Ω.) À ce faisceau inversible sur Ω engendré par $n+1$ sections correspond, par la propriété universelle de $\mathbb{P}^n$, un morphisme $\Omega \to \mathbb{P}^n$. On peut aussi dire directement qu'il y a sur l'ouvert $U = \cup_{i=0}^n D(f_i) \subset X = \mathrm{Spec}(A)$ un faisceau inversible engendré par $n+1$ sections, ce faisceau étant le sous-faisceau du faisceau des fonctions méromorphes de X qui sur $D(f_i)$ est engendré par $1/f_i$. À ce faisceau inversible sur U engendré par $n+1$ sections correspond un morphisme $\psi : U \to \mathbb{P}^n$.

(2) La restriction de φ à $D(f_i)$ tombe dans l'ouvert affine $X \times U_i$, et dans ces cartes elle est donnée par le morphisme d'anneaux

$$u : A[\frac{x_0}{x_i}, \dots, \frac{x_n}{x_i}] \to A[\frac{1}{f_i}]$$

qui préserve les éléments de A et envoie x_k/x_i sur f_k/f_i. Il est clair que $(J : (f_i)^\infty) \subset \ker(u)$ puisque si $P = P(x_0/x_i, \ldots, x_n/x_i)$ et $f_i^n P \in J$ pour un certain entier $n \geq 1$, alors on voit immédiatement que $u(f_i^n P) = 0$, et comme f_i est inversible dans $A[1/f_i]$, on trouve $P \in \ker(u)$. C'est la réciproque qui est moins évidente. Soit $P = P(x_0/x_i, \ldots, x_n/x_i) \in \ker(u)$. Il est clair que si n est plus grand que le degré total de P en les variables x_k/x_i, alors $f_i^n P$ est un polynôme en les variables $f_i x_k/x_i$, i.e. $f_i^n P(x_0/x_i, \ldots, x_n/x_i) = Q(f_i x_0/x_i, \ldots, f_i x_n/x_i)$. Dans $A[x_0/x_i, \ldots, x_n/x_i]/J$ on a donc

$$f_i^n P(x_0/x_i, \ldots, x_n/x_i) = Q(f_0, \ldots, f_n) =: a$$

qui est un élément $a \in A$. Dire que $P \in \ker(u)$ implique que $a = 0$. Il s'ensuit que $f_i^n P(x_0/x_i, \ldots, x_n/x_i)$ est nul modulo J, donc $P \in (J : (f_i)^\infty)$.

(3) Ici $A = k[x, y]/(f)$ où $f = y^2 - x^2(x + 1)$, et on éclate l'idéal $I = (x, y)$. L'éclatement $\widetilde{X}$ est un sous-schéma fermé de $X \times \mathbb{P}^1$. Notons z_0, z_1 des coordonnées homogènes sur $\mathbb{P}^1$, $u = z_1/z_0$, $v = z_0/z_1$. On note aussi $\mathcal{U}_0 = X \times U_0 = \operatorname{Spec}(A[u])$ et $\mathcal{U}_1 = X \times U_1 = \operatorname{Spec}(A[v])$, qui sont les ouverts standards de $X \times \mathbb{P}^1$ vu comme la droite affine $\mathbb{P}^1_A$ sur A. Il faut calculer les équations de $\widetilde{X}$ dans $\mathcal{U}_0$ et $\mathcal{U}_1$.

Regardons dans $\mathcal{U}_0$. Dans l'anneau quotient $A[u]/(y - ux)$ on a $(ux)^2 = x^2(x + 1)$, donc l'élément $u^2 - (x + 1)$ est de x-torsion. On a :

$$A[u]/(y - ux, u^2 - (x + 1)) \simeq k[x, u]/(u^2 - (x + 1)) \simeq k[u]\ .$$

Cet anneau n'a pas de x-torsion, autrement dit $\widetilde{X} \cap \mathcal{U}_0 \simeq \operatorname{Spec}(k[u])$.

Regardons maintenant dans l'ouvert $\mathcal{U}_1$. Dans l'anneau quotient $A[v]/(x - vy)$ on a $y^2 = (vy)^2(vy + 1)$, donc $1 - v^2(vy + 1)$ est de y-torsion. On a :

$$A[v]/(x - vy, 1 - v^2(vy + 1)) \simeq k[y, v]/(1 - v^2(vy + 1))\ .$$

Cet anneau n'a pas de y-torsion, donc $\widetilde{X} \cap \mathcal{U}_1 \simeq \operatorname{Spec}(k[y, v]/(1 - v^2(vy + 1)))$.

En fait, puisque la fonction v est inversible sur $\widetilde{X} \cap \mathcal{U}_1$, on voit que $\widetilde{X} \cap \mathcal{U}_1 \subset \widetilde{X} \cap \mathcal{U}_0$. Donc finalement $\widetilde{X} = \widetilde{X} \cap \mathcal{U}_0$ est la droite affine de coordonnée u. On pouvait anticiper cela en observant que :

a) dans X on a $D(y) \subset D(x)$, donc l'ensemble de définition de l'application rationnelle graphe $X \dashrightarrow X \times \mathbb{P}^n$ est simplement $D(x)$,

b) l'image schématique de $D(x) \to X \times \mathcal{U}_0$ est fermée dans $X \times \mathbb{P}^1$, donc c'est l'image schématique dans $X \times \mathbb{P}^1$ i.e. c'est $\widetilde{X}$. Précisément, en coordonnées homogènes z_0, z_1 c'est le sous-schéma fermé d'équations $z_0 y - z_1 x$ et $z_1^2 - z_0^2(x + 1)$.

Corrigé ex. 2 (1) Soit $(u : v)$ des coordonnées dans $X = \mathbb{P}^1_R$. On utilisera le plongement de Segre $\mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^3$ donné par $((u : v), (x : y)) \mapsto (a : b : c : d) = (ux : uy : vx : vy)$. L'équation de $\mathbb{P}^1 \times \mathbb{P}^1$ dans $\mathbb{P}^3$ est $ad = bc$. On peut supposer que le point qu'on éclate est défini dans la carte $v \neq 0$ par l'idéal $(u/v, \pi)$ donc le morphisme graphe qui définit l'éclatement est $X \to X \times \mathbb{P}^1$, $(u : v) \mapsto ((u : v), (x : y) = (u : \pi v))$. On voit que l'équation $\pi v x = u y$ donne $\pi c = b$ dans $\mathbb{P}^3$. Finalement les équations pour $\widetilde{X}$ dans $\mathbb{P}^3$ sont $ad = bc$ et $\pi c = b$. Il s'agit de la conique $\{ad = \pi c^2\}$ du plan projectif $\mathbb{P}^2_R = \operatorname{Proj}(R[a, c, d])$.

(2) La fibre fermée a pour équation $ad = 0$, c'est une réunion de deux $\mathbb{P}^1$ se coupant en un point. Elle est singulière.

Corrigé ex. 3 On éclate la courbe en le point singulier $x = y = 0$. Lorsqu'on éclate, il y a deux cartes. Dans la première carte on pose $y = ux$ et on obtient l'équation $u^a x^{a-b} = 1$. Ici, il n'y a plus de singularité. Dans la deuxième carte, on pose $x = vy$ et on obtient l'équation $y^{a-b} = v^b$. Ici, il y a encore une singularité et on se concentre dans la suite sur cette seule carte. On voit qu'en itérant, dans la seule carte intéressante, l'exposant de y décroît de b unités à chaque étape. Si on fait la division euclidienne $a = bq + r$ avec $0 \leq r < b$, après q éclatements l'exposant $a - qb = r$ est strictement inférieur à b. Ensuite, la carte intéressante est celle qui n'était pas intéressante avant. Par ailleurs, on voit qu'on peut éviter ces q éclatements en éclatant dès le départ le sous-schéma non réduit d'idéal (x, y^q) au lieu d'éclater le point singulier réduit. En effet, si l'on fait cela, dans la première carte on pose $y^q = ux$ et on obtient l'équation $u^b y^r = 1$, il n'y a plus de singularité. Dans la deuxième carte, on pose $x = vy^q$ et on obtient l'équation $y^r = v^b$. On recommence alors en faisant la division euclidienne de b par r, etc. En résumé, il s'agit d'appliquer l'algorithme d'Euclide du calcul du pgcd, de la manière suivante :

1) Faire $A := a$, $B := b$, et $A = BQ + R$ avec $0 \leq R < B$ (division euclidienne de A par B).

2) Éclater l'idéal $I = (x, y^Q)$ dans la courbe d'équation $y^A = x^B$.

3) Tant que $R \geq 2$, une singularité $y^R = v^B$ persiste (dans la carte telle que $x = vy^Q$). Faire $A := B$, $B := R$ et retourner en 2).

Corrigé ex. 4 On doit noter tout d'abord que la loi d'addition de E_K est décrite par des expressions rationnelles, c'est-à-dire valables sur un ouvert $U \subset E_K$, mais on sait qu'elle s'étend en une loi sur E_K. De même, on sait qu'une application rationnelle non constante entre deux courbes projectives lisses s'étend de manière unique en un morphisme, bien défini partout, c'est pourquoi on peut se permettre de décrire un tel morphisme de manière rationnelle. En revanche, lorsque les courbes ne sont pas propres, ou pas lisses, ou qu'il s'agit de courbes sur R (de dimension 2, donc des surfaces), les choses ne sont plus aussi simples. Pour définir des morphismes, il est alors important d'écrire des expressions « sans pôles » en tout point.

(1) Si la loi de groupe s'étendait à E, alors la fibre spéciale E_k serait munie d'une loi de groupe. Comme E_k est géométriquement réduite, elle devrait être lisse, comme tout groupe algébrique, ce qui n'est pas le cas puisque le point $x = y = 0$ est singulier. Donc la loi de groupe de E_K ne s'étend pas à E.

(2) Un point $P \in E(K)$ est de 2-torsion si et seulement si $2P = 0$, ou encore $-P = P$. Le point origine $P = O$ est de 2-torsion, considérons maintenant les points $P \neq O$. Si $P = (x, y)$, on a $-P = (x, -y)$, donc les points de 2-torsion non triviaux sont ceux pour lesquels $y = 0$ (noter que comme la caractéristique de k est différente de 2, celle de K aussi). On trouve que x vaut 0, 1 ou λ et donc les points de 2-torsion sont :

$$O = \infty \quad , \quad A = (0,0) \quad , \quad B = (\lambda, 0) \quad , \quad C = (1,0) \ .$$

Ainsi tous les points de 2-torsion sont rationnels et $G = E_K[2] \simeq (\mathbb{Z}/2\mathbb{Z})^2$.

(3) Soit $P = (x, y)$, l'expression de $\tau(P) = P + A$ en coordonnées non homogènes est :

$$\left\{ \begin{array}{l} x' = (y/x)^2 - x + \lambda + 1 \\ y' = -(y/x)x' = -(y/x)((y/x)^2 - x + \lambda + 1) \ . \end{array} \right.$$

Il s'agit d'exprimer τ en coordonnées homogènes, et de voir si on peut l'étendre à E tout entière. Notons que E est un schéma normal : c'est clair partout sauf peut-être au point singulier de la fibre spéciale, mais en ce point, on peut voir que l'anneau local est encore normal, soit par un calcul direct, soit en utilisant le fait que E est plate sur R, à fibre générique normale (car lisse) et à fibre spéciale réduite, voir Liu, lemme 4.1.18. On sait que les schémas normaux ont la propriété que leurs fonctions rationnelles définies en codimension ≤ 1 sont définies partout. Cependant, il n'est pas vrai que si X est normal, toute application rationnelle $X \dashrightarrow Y$ définie en codimension ≤ 1 s'étend en un morphisme $X \to Y$ (les fonctions sur X correspondent au cas particulier $Y = \mathbb{A}^1$). À ce sujet, lire Liu, theorem 4.1.14 et proposition 4.1.16.

L'équation homogène de E est $y^2z = x(x-z)(x-\lambda z)$. Pour passer en coordonnées homogènes, on chasse les dénominateurs dans les composantes du point image $(x' : y' : 1)$, et pour cela on multiplie par x^3z. Pour x', cela fait apparaître

$$x(y^2z - x^3 + (\lambda+1)x^2z)$$

qui vaut λx^2z^2. Finalement,

$$\tau(x:y:z) = (\lambda x^2z^2 : -\lambda xyz^2 : x^3z) = (\lambda xz : -\lambda yz : x^2) \ .$$

Cette expression a un sens au moins sur l'ouvert $U = \{x \neq 0\}$, essayons de l'étendre. On peut réécrire l'équation de E en $(y^2 + (1+\lambda)x^2 - \lambda xz)z = x^3$, donc on a

$$\tau(x:y:z) = (\lambda x^2z : -\lambda xyz : x^3) = (\lambda x^2 : -\lambda xy : y^2 + (1+\lambda)x^2 - \lambda xz) \ .$$

Cette expression a un sens au moins sur l'ouvert $V = \{y^2 + (1+\lambda)x^2 - \lambda xz \neq 0\}$. Il ne reste qu'un point qui n'est ni dans E_K, ni dans U, ni dans V, c'est le point de la fibre spéciale de coordonnées $x = y = 0$ et $z = 1$, notons-le Q. J'affirme que τ ne peut pas s'étendre sur un voisinage de Q. En effet, si cétait le cas, comme τ envoie $E_k \setminus \{Q\}$ sur Q, alors par continuité on doit avoir $\tau(Q) = Q$. Soit $m_Q = (\lambda, x, y)$ l'idéal maximal de Q et

$$\mathcal{O}_{E,Q} = \left(\frac{R[x,y]}{y^2 - x(x-1)(x-\lambda)}\right)_{m_Q}$$

l'anneau local de Q dans E. Alors τ induit un morphisme $\tau^\sharp : \mathcal{O}_{E,Q} \to \mathcal{O}_{E,Q}$, ce morphisme est connu sur les corps de fractions et l'on a

$$\tau^\sharp(x) = (y/x)^2 - x + \lambda + 1 \quad , \quad \tau^\sharp(y) = -(y/x)((y/x)^2 - x + \lambda + 1) \ .$$

Comme $(y/x)^2 - x + \lambda + 1 = \lambda/x \notin \mathcal{O}_{E,Q}$, on a une contradiction.

En conclusion τ ne s'étend pas en un morphisme $E \to E$. On note, au passage, que la restriction de τ à $E_k \setminus \{q\}$ s'étend en un morphisme $E_k \to E_k$, à savoir le morphisme constant de valeur q. Donc lorsqu'on part d'une application rationnelle f définie sur un schéma X/R, dont l'ensemble de définition intersecte toute les fibres, ce n'est pas la même chose d'étendre f en un morphisme, ou d'étendre en des morphismes les restrictions de f fibre à fibre.

(4)