

Courbes elliptiques pour la cryptographie (partie 1)

Rubén Muñoz--Bertrand

Version 2026.9.10.1175

Ces notes de cours reprennent la première partie du cours « Courbes elliptiques pour la cryptographie », donné en 2026 dans le M2 « Mathématiques de l'information, Cryptographie » de l'Université de Rennes. Cette première partie contient les fondements mathématiques de la théorie des courbes elliptiques. La seconde partie du cours est effectuée par Sylvain Duquesne.

1 Espaces projectifs

Dans cette section, k désigne un corps.

Nous allons introduire de nouveaux types d'espaces dans lesquels nous allons faire de la géométrie, appelés les espaces projectifs. Il s'agira des espaces dans lesquels les courbes elliptiques seront définies.

1.1 Coordonnées projectives

Soit $n \in \mathbb{N}$. On rappelle qu'une droite vectorielle de k^{n+1} est un de ses sous- k -espaces vectoriels de dimension 1.

Soit $D \subset k^{n+1}$ une droite vectorielle. Soit $x = (x_0, \dots, x_n) \in D^*$ un point non-nul de D . Alors :

$$D = \{\lambda x \mid \lambda \in k\}.$$

Cela justifie la notation suivante.

Notation 1.1. Soit $D \subset k^{n+1}$ une droite vectorielle. Soit $(x_0, \dots, x_n) \in D^*$ un point non-nul de D .

On note :

$$[x_0 : \dots : x_n] := D.$$

On prendra garde au fait que, à moins que $k = \mathbb{F}_2$, cette notation n'est jamais uniquement déterminée par D . En d'autres termes, pour toute droite vectorielle D , il existe plusieurs représentations de D sous cette forme ; voire une infinité si k n'est pas un corps fini.

Définition 1.2. L'espace projectif de dimension n sur k est l'ensemble des droites vectorielles de l'espace affine de dimension $n + 1$ sur k :

$$\mathbf{P}_k^n := \left\{ [x_0 : \dots : x_n] \mid (x_0, \dots, x_n) \in k^{n+1*} \right\}.$$

Malgré cette définition, il ne faut pas penser aux éléments d'un espace projectif comme des droites, mais comme des points. De plus, ici, le mot « dimension » fait partie de la définition : il ne s'agit pas de la dimension d'un espace vectoriel par exemple, les espaces projectifs n'en étant pas.

Définition 1.3. Soit $x \in \mathbf{P}_k^n$ un point de l'espace projectif. On appelle coordonnées projectives de x une représentation de la forme $x = [x_0 : \dots : x_n]$, où $(x_0, \dots, x_n) \in k^{n+1*}$.

Nous l'avons vu, contrairement à la géométrie euclidienne, les coordonnées d'un point ne sont pas uniques (sauf si $k = \mathbb{F}_2$). Afin de pouvoir se faire une image mentale de ces espaces, nous allons étudier quelques cas simples.

1.2 La droite projective

Nous allons ici nous intéresser au cas de la dimension 1.

Définition 1.4. La droite projective sur k est l'espace projectif $\mathbf{P}_k^1$ de dimension 1 sur k .

La droite affine $\mathbf{A}_k^1 \cong k$ s'injecte dans la droite projective.

Proposition 1.5. L'application ci-dessous est injective :

$$\iota : \begin{array}{ccc} \mathbf{A}_k^1 & \rightarrow & \mathbf{P}_k^1 \\ (x_1) & \mapsto & [1 : x_1] \end{array}.$$

Démonstration. Il suffit de vérifier que pour $x_1, y_1 \in k$ tels que $[1 : x_1] = [1 : y_1]$, alors $x_1 = y_1$. Si les deux droites vectorielles sont égales, cela signifie qu'il existe $\lambda \in k$ tel que $(1, x_1) = \lambda(1, y_1)$. L'égalité sur la première coordonnée implique que $\lambda = 1$, donc $x_1 = y_1$. $\square$

Il ne s'agit pas de l'unique manière d'obtenir une telle injection. Dans ce qui suit, nous allons identifier $\mathbf{A}_k^1$ à son image par ι .

Proposition 1.6. On a une union disjointe :

$$\mathbf{P}_k^1 = \mathbf{A}_k^1 \cup \{[0 : 1]\}.$$

Démonstration. L'union est disjointe, car pour tout $x_1 \in k$ les points $(0, 1)$ et $(1, x_1)$ ne sont pas colinéaires.

On obtient tout l'espace projectif $\mathbf{P}_k^1$, car si $D \in \mathbf{P}_k^1$, l'un des points ci-dessus appartient à D . En effet, soit $(z_0, z_1) \in D^*$. Si $z_0 = 0$, alors $(0, 1)$ est colinéaire à (z_0, z_1) et donc appartient à D . Sinon, alors $(1, z_1/z_0)$ est colinéaire à (z_0, z_1) . $\square$

Définition 1.7. Avec ce choix d'injection de la droite affine dans la droite projective, on dit que $[0 : 1]$ est point à l'infini, et on note $\infty := [0 : 1]$.

Comme remarqué précédemment, ce choix d'injection n'est pas unique. Mais quel que soit ce choix, on peut toujours décrire la droite projective comme une droite affine avec un point à l'infini.

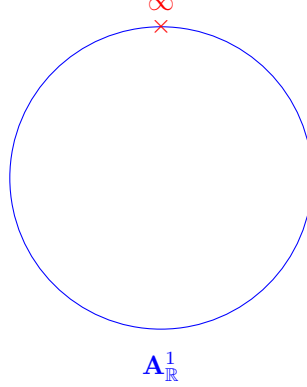


Illustration de la droite projective $\mathbf{P}^1_{\mathbb{R}}$ sur $\mathbb{R}$.

1.3 Le plan projectif

Nous pouvons effectuer une description similaire en dimension 2. Toutefois, il n'y a pas cette fois un unique point à l'infini.

Définition 1.8. Le plan projectif sur k est l'espace projectif $\mathbf{P}^2_k$ de dimension 2 sur k .

Ici aussi, le plan affine $\mathbf{A}^2_k \cong k^2$ s'injecte dans le plan projectif.

Proposition 1.9. L'application ci-dessous est injective :

$$\iota: \begin{array}{ccc} \mathbf{A}^2_k & \rightarrow & \mathbf{P}^2_k \\ (x_1, x_2) & \mapsto & [x_1 : x_2 : 1] \end{array} .$$

Démonstration. Il nous suffit de vérifier que pour tout $x_1, x_2, y_1, y_2 \in k$ vérifiant $[x_1 : x_2 : 1] = [y_1 : y_2 : 1]$, alors $x_1 = y_1$ et $x_2 = y_2$. Si les deux droites vectorielles sont égales, cela signifie qu'il existe $\lambda \in k$ tel que $(x_1, x_2, 1) = \lambda(y_1, y_2, 1)$. L'égalité sur la première coordonnée implique que $\lambda = 1$, et on conclut. $\square$

Qui plus est, la droite projective s'injecte elle aussi dans le plan projectif.

Proposition 1.10. L'application ci-dessous est injective :

$$\tau: \begin{array}{ccc} \mathbf{P}^1_k & \rightarrow & \mathbf{P}^2_k \\ [x_0 : x_1] & \mapsto & [x_0 : x_1 : 0] \end{array} .$$

Démonstration. L'application $k^2 \rightarrow k^3$
 $(x_0, x_1) \mapsto (x_0, x_1, 0)$ est k -linéaire et injective. Deux points de l'image sont donc colinéaires si et seulement si leurs pré-images le sont. Donc, si $[x_0 : x_1 : 0] = [y_0 : y_1 : 0]$ pour deux points de la droite projective $[x_0 : x_1], [y_0 : y_1] \in \mathbf{P}_k^1$, alors $[x_0 : x_1] = [y_0 : y_1]$. $\square$

À nouveau, ces injections ne sont pas uniques ni canoniques. Dans ce qui suit, nous allons identifier $\mathbf{A}_k^2$ à son image par ι , et $\mathbf{P}_k^1$ à son image par τ .

Proposition 1.11. *On a une union disjointe :*

$$\mathbf{P}_k^2 = \mathbf{A}_k^2 \cup \mathbf{P}_k^1.$$

Et donc en particulier :

$$\mathbf{P}_k^2 = \mathbf{A}_k^2 \cup \mathbf{A}_k^1 \cup \{[0 : 1 : 0]\}.$$

Démonstration. L'union est disjointe, car quels que soient $x_1, x_2, y_0, y_1 \in k$ avec $(y_1, y_2) \neq (0, 0)$, les points $(x_1, x_2, 1)$ et $(y_0, y_1, 0)$ ne sont pas colinéaires.

On obtient tout le plan projectif $\mathbf{P}_k^2$, car si $D \in \mathbf{P}_k^2$, l'un des points ci-dessus appartient à D . En effet, soit $(z_0, z_1, z_2) \in D^*$. Si $z_2 = 0$, alors le point est dans l'image de $\mathbf{P}_k^1$. Sinon, alors $(z_0/z_2, z_1/z_2, 1)$ est colinéaire à (z_0, z_1, z_2) .

La dernière partie de la proposition découle de la description de la droite projective. $\square$

Remarquez que dans les propositions précédentes, les mêmes arguments fonctionnent même en dimension supérieure. Cela nous permet d'obtenir des descriptions similaires des espaces projectifs en toute généralité.



Analogie pour $\mathbf{P}_{\mathbb{R}}^2$: le sol est le plan affine $\mathbf{A}_{\mathbb{R}}^2$,
les rails sont des droites parallèles du plan affine,
l'horizon est la droite projective à l'infini.

Les rails se coupent en un unique point à l'horizon.

Attention : il s'agit du *même point* à l'infini si l'on se retourne à 180 degrés.

Dans ce qui suit, nous allons donner un sens à la phrase « deux droites projectives planes distinctes du plan se coupent en un unique point ».

2 Variétés algébriques

Dans cette section, k désigne un corps.

Nous allons définir ici la notion de variété algébrique. Il s'agit des objets géométriques étudiés en géométrie algébrique. Les courbes elliptiques en sont un cas particulier.

Dans certains domaines de la cryptographie, comme par exemple la cryptographie post-quantique à base d'isogénies, des variétés algébriques plus générales sont employées en pratique, par exemple pour des attaques.

2.1 Polynômes homogènes

Dans un espace projectif, les polynômes n'ont pas nécessairement des racines bien définies. Par exemple, le polynôme $P := X^2 + Y \in \mathbb{Q}[X, Y]$ s'annule dans tous les points de la forme $(x, -x^2)$ pour $x \in \mathbb{Q}$. C'est le cas, par exemple, du point $(1, -1)$. Dans $\mathbf{P}_{\mathbb{Q}}^1$, on considérerait alors $[1 : -1]$. Or, $(2, -2)$ est un autre point de la droite vectorielle associée, et $2^2 + (-2) \neq 0$.

La définition ci-dessus permet de pallier ce problème.

Définition 2.1. Soient $d, n \in \mathbb{N}$. Un polynôme $P \in k[X_0, \dots, X_n]$ est dit homogène de degré d si tous ses monômes ont pour degré total d , où le degré totale d'un monôme est la somme des puissances de chaque indéterminée.

Exemple 2.2. Le polynôme $3XY^2 + Z^3 - XYZ \in \mathbb{Q}[X, Y, Z]$ est homogène de degré 3. En effet, le premier monôme a degré total $1 + 2 + 0 = 3$, le deuxième $0 + 0 + 3 = 3$ et le troisième $1 + 1 + 1$.

Contre-exemple 2.3. Le polynôme $XY + 1 \in \mathbb{Q}[X, Y]$ n'est pas homogène, car ses monômes ont degré total respectifs 2 et 0.

Proposition 2.4. Soient $d, n \in \mathbb{N}$. Soit $P \in k[X_0, \dots, X_n]$ un polynôme homogène de degré d . Soit $x \in \mathbf{P}_k^n$.

Alors, il n'y a que deux situations possibles :

1. soit pour tout $(x_0, \dots, x_n) \in k^{n+1*}$ tel que $x = [x_0 : \dots : x_n]$ nous avons $P(x_0, \dots, x_n) = 0$;
2. soit pour tout $(x_0, \dots, x_n) \in k^{n+1*}$ tel que $x = [x_0 : \dots : x_n]$ nous avons $P(x_0, \dots, x_n) \neq 0$.

Démonstration. Soient $(x_0, \dots, x_n), (y_0, \dots, y_n) \in k^{n+1*}$, et supposons que les coordonnées projectives satisfont $x = [x_0 : \dots : x_n] = [y_0 : \dots : y_n]$. En particulier, il existe $\lambda \in k^*$ tel que $(x_0, \dots, x_n) = \lambda(y_0, \dots, y_n)$.

Comme on a supposé que P est un polynôme homogène de degré d , nous observons que $P(x_0, \dots, x_n) = \lambda^d P(y_0, \dots, y_n)$. En effet, ce résultat se voit immédiatement au niveau des monômes. De cette égalité, le résultat découle immédiatement puisque $\lambda \neq 0$ et que k est un corps. $\square$

Définition 2.5. Soit $n \in \mathbb{N}$. Un idéal $I \subset k[X_0, \dots, X_n]$ est dit homogène s'il est engendré par des polynômes homogènes.

Contre-exemple 2.6. L'idéal $\langle X + 1 \rangle \in \mathbb{Q}[X]$ n'est pas homogène. En effet, si $P_1, \dots, P_l \in \mathbb{Q}[X]$ sont des polynômes homogènes pour lesquels on a $\langle X + 1 \rangle = \langle P_1, \dots, P_l \rangle$, où $l \in \mathbb{N}^*$, alors pour tout $i \in \llbracket 1, m \rrbracket$ il existe $R_i \in \mathbb{Q}[X]$ tels que $(1 + X)R_i = P_i$.

Si M_i est la somme des monômes de plus haut degré de R_i , et m_i la somme des monômes de plus petit degré de R_i , on voit que XM_i est la somme des monômes de plus haut degré de P_i et m_i la somme de ses monômes de plus petit degré. Donc aucun des P_i ne peut être homogène.

Proposition 2.7. Soient $l, m, n \in \mathbb{N}$, et soit $I \subset k[X_0, \dots, X_n]$ un idéal homogène. Soient $P_1, \dots, P_l, Q_1, \dots, Q_m \in k[X_0, \dots, X_n]$ des polynômes homogènes vérifiant $I = \langle P_1, \dots, P_l \rangle = \langle Q_1, \dots, Q_m \rangle$.

Alors quel que soit $[x_0 : \dots : x_n] \in \mathbf{P}_k^n$, les conditions suivantes sont équivalentes :

1. pour tout $i \in \llbracket 1, l \rrbracket$, on a $P_i(x_0, \dots, x_n) = 0$;
2. pour tout $j \in \llbracket 1, m \rrbracket$, on a $Q_j(x_0, \dots, x_n) = 0$.

Démonstration. Soit $[x_0 : \dots : x_n] \in \mathbf{P}_k^n$. Remarquons que chacune des deux conditions implique que pour tout $P \in I$, on a $P(x_0, \dots, x_n) = 0$. Cela suffit à démontrer l'équivalence. $\square$

La proposition précédente implique que la définition suivante a bien un sens.

Définition 2.8. Un ensemble algébrique projectif est un ensemble noté $V(I)$, où $I \subset k[X_0, \dots, X_n]$ est un idéal homogène et $n \in \mathbb{N}$, tel que pour des polynômes homogènes $P_1, \dots, P_l \in k[X_0, \dots, X_n]$ engendrant I , où $l \in \mathbb{N}$, on a :

$$V(I) = \{[x_0 : \dots : x_n] \in \mathbf{P}_k^n \mid \forall i \in \llbracket 1, l \rrbracket, P_i(x_0, \dots, x_n) = 0\}.$$

Exemple 2.9. L'image de $\mathbf{P}_k^1$ par τ dans $\mathbf{P}_k^2$ tel que défini dans la proposition 1.10 est un ensemble algébrique projectif. En effet, il s'agit du lieu des zéros de l'idéal engendré par le polynôme homogène $P(X_0, X_1, X_2) = X_2$.

Bien entendu, on aurait également pu voir $\mathbf{P}_k^1$ comme le lieu des zéros de l'idéal nul dans $\mathbf{P}_k^1$.

Proposition 2.10. Soient $n \in \mathbb{N}$ et $I \subset J \subset k[X_0, \dots, X_n]$ deux idéaux homogènes. Alors, $V(J) \subset V(I)$.

Démonstration. Soit $x \in V(J)$. Cela signifie que pour tout $P \in J$ on a $P(x) = 0$. Puisque $I \subset J$, cela est vrai en particulier pour tout $P \in I$, ce qui permet de conclure. $\square$

Proposition 2.11. Soient $n \in \mathbb{N}$ et $I \subset k[X_0, \dots, X_n]$ un idéal homogène. Alors $\sqrt{I}$ est un idéal homogène.

Démonstration. Soient $P_1, \dots, P_l \in k[X_0, \dots, X_n]$ des polynômes homogènes engendrant I , où $l \in \mathbb{N}^*$. Soient $Q \in k[X_0, \dots, X_n]$ et $m \in \mathbb{N}$ tels qu'il existe des polynômes $R_1, \dots, R_l \in k[X_0, \dots, X_n]$ tels que $Q^m = \sum_{i=1}^l P_i R_i$.

Soit M la somme des monômes de Q de plus haut degré. Alors M est homogène, tout comme M^m qui est la somme des monômes de Q^m de plus haut degré. Si pour tout $i \in \llbracket 0, l \rrbracket$ on note N_i la somme des monômes de R_i de degré $m \deg(Q) - \deg(P_i)$, alors $M^m = \sum_{i=0}^l P_i N_i$. Donc $M \in \sqrt{I}$.

En considérant $Q - M \in \sqrt{I}$, ce raisonnement permet par récurrence de montrer que Q est somme de polynômes homogènes de $\sqrt{I}$. $\square$

Proposition 2.12. *Soit $n \in \mathbb{N}$. Soit $P \in k[X_0, \dots, X_n]$ un polynôme homogène. Alors, $V(\langle P \rangle) = V(\sqrt{\langle P \rangle})$.*

Démonstration. Puisque $\langle P \rangle \subset \sqrt{\langle P \rangle}$, alors $V(\sqrt{\langle P \rangle}) \subset V(\langle P \rangle)$.

Vérifions l'inclusion réciproque. Soit $x \in V(\langle P \rangle)$. Soient $Q \in k[X_0, \dots, X_n]$ et $m \in \mathbb{N}$ tels que $P \mid Q^m$. On a donc $Q(x)^m = Q^m(x) = 0$. Comme k est un corps, $Q(x) = 0$ et on conclut. $\square$

2.2 Topologie de Zariski

Nous avons désormais tous les outils nécessaires pour introduire une topologie sur les espaces projectifs, et ainsi en particulier les ensembles algébriques projectifs.

Proposition 2.13. *Soit $n \in \mathbb{N}$. Soit $I, J \subset k[X_0, \dots, X_n]$ deux idéaux homogènes.*

Alors $IJ = \langle \{ij \mid i \in I, j \in J\} \rangle$ est un idéal homogène et :

$$V(I) \cup V(J) = V(IJ).$$

Démonstration. L'idéal IJ est engendré par tous les produits de générateurs de I et J . Comme ceux-ci peuvent être des polynômes homogènes, il suffit de vérifier que le produit de polynômes homogènes est homogène, ce qui est le cas en vérifiant monôme par monôme.

De plus, $V(I) \cup V(J) \subset V(IJ)$. Puisque $IJ \subset I$, on a $V(I) \subset V(IJ)$. Par symétrie, on obtient $V(J) \subset V(IJ)$, et donc l'inclusion de l'union.

Réciproquement, soient $P_1, \dots, P_l, Q_1, \dots, Q_m \in k[X_0, \dots, X_n]$ des polynômes homogènes vérifiant $I = \langle P_1, \dots, P_l \rangle$ et $J = \langle Q_1, \dots, Q_m \rangle$, où $l, m \in \mathbb{N}$. Soit $[x_0 : \dots : x_n] \in V(IJ)$. Supposons que $[x_0 : \dots : x_n] \notin V(J)$. En particulier, il existe $j \in \llbracket 1, m \rrbracket$ tel que $Q_j(x_0, \dots, x_n) \neq 0$. Par hypothèse, pour tout $i \in \llbracket 1, l \rrbracket$, on a $P_i(x_0, \dots, x_n)Q_j(x_0, \dots, x_n) = 0$. Donc $P_i(x_0, \dots, x_n) = 0$ puisque k est un corps, et $[x_0 : \dots : x_n] \in V(I)$. Par symétrie de l'argument, nous avons démontré que $V(IJ) \subset V(I) \cup V(J)$. $\square$

Proposition 2.14. *Soit $n \in \mathbb{N}$. Soit J un ensemble. Soit $(I_j)_{j \in J}$ une famille d'idéaux homogènes de $k[X_0, \dots, X_n]$.*

Alors $\sum_{j \in J} I_j$, l'idéal engendré par $\bigcup_{j \in J} I_j$, est un idéal homogène et :

$$\bigcap_{j \in J} V(I_j) = V\left(\sum_{j \in J} I_j\right).$$

Démonstration. Le fait que $\sum_{j \in J} I_j$ soit homogène provient du fait que celui-ci est engendré par l'union des générateurs de tous les I_j , et que l'on peut choisir ces derniers homogènes.

L'égalité provient du fait que $[x_0 : \dots : x_n] \in \bigcap_{j \in J} V(I_j)$ si et seulement si $P(x_0, \dots, x_n) = 0$ pour tout $P \in \bigcup_{j \in J} I_j$. $\square$

Proposition 2.15. *Soit $n \in \mathbb{N}$ et plaçons-nous dans $\mathbf{P}_k^n$. On a $V(\emptyset) = \mathbf{P}_k^n$ et $V(k[X_0, \dots, X_n]) = \emptyset$.*

En particulier, les ensembles algébriques projectifs de $\mathbf{P}_k^n$ sont les fermés d'une topologie sur $\mathbf{P}_k^n$.

Démonstration. Les deux premières égalités sont claires puisque k est un corps, et la conclusion découle des propositions précédentes. $\square$

Définition 2.16. *La topologie de $\mathbf{P}_k^n$ dont les fermés sont les ensembles algébriques projectifs est appelée topologie de Zariski.*

Remarquez que dans cette topologie, les ouverts sont gros et les fermés petits.

2.3 Nullstellensatz

Le Nullstellensatz, ou en français le théorème des zéros de Hilbert, est un résultat qui possède de nombreuses variantes dans la littérature. Ici, nous allons en énoncer deux versions non générales, adaptées à nos besoins, afin de simplifier la présentation.

Tout d'abord, nous avons besoin de deux cas particulier de la théorie des éléments dits « entiers ».

Lemme 2.17. *Soit R une $k[X]$ -algèbre commutative. Soient $y, y' \in R$ tels qu'il existe des polynômes unitaires $P, Q \in k[X][Y]$ vérifiant $P(y) = Q(y') = 0$. Alors il existe un polynôme unitaire $S \in k[X][Y]$ tel que $S(y + y') = 0$.*

Démonstration. Soit Z une indéterminée, et considérons le résultant défini par rapport à cette variable $S := \text{Res}_Z(P(Z), Q(Y - Z)) \in k[X][Y]$. Nous avons $S(y + y') = 0$, parce que les polynômes $P(Z)$ et $Q(y + y' - Z)$ ont x comme racine commune. De plus, S n'est pas le polynôme nul car, par définition de la matrice de Sylvester, son coefficient dominant est $1^{\deg_Y(Q)} Y^{\deg_Y(Q) \deg_Y(P)}$. $\square$

Lemme 2.18. *Soit R une $k[X]$ -algèbre commutative. Tout produit et toute combinaison $k[X]$ -linéaire d'éléments de R annulés par des polynômes unitaires de $k[X][Y]$ est également annulée par un tel polynôme.*

Démonstration. Par récurrence sur le lemme précédent, il suffit de vérifier que le produit de deux $y, y' \in R$ tels qu'il existe $P, Q \in k[X][Y]$ unitaires vérifiant $P(y) = Q(y') = 0$ est également annulé par un tel polynôme.

Soit Z une indéterminée, et considérons le résultant défini par rapport à cette variable $S := \text{Res}_Z(P(Z), Z^{\deg_Y(Q)} Q(Y/Z)) \in k[X][Y]$. Remarquons que $S(yy') = 0$, car les polynômes $P(Z)$ et $Z^{\deg_Y(Q)} Q(yy'/Z)$ ont x comme racine

commune. De plus, S n'est pas le polynôme nul car son coefficient dominant est $1^{\deg_Y(Q)} Y^{\deg_Y(Q)} 1^{\deg_Y(P)}$. $\square$

Lemme de Zariski 2.19. *Soit $n \in \mathbb{N}$. Soit $\mathfrak{m} \subset k[X_1, \dots, X_n]$ un idéal maximal.*

Alors $k[X_1, \dots, X_n]/\mathfrak{m}$ est une extension de corps finie de k . En particulier, si k est algébriquement clos, il s'agit d'un isomorphisme.

Démonstration. Le lemme se démontre par récurrence sur n . Si $n = 0$, alors $\mathfrak{m} = \{0\}$ et l'extension est triviale.

Supposons que nous avons démontré le lemme pour un certain $n \in \mathbb{N}$. Soit $\mathfrak{m} \subset k[X_1, \dots, X_{n+1}]$ un idéal maximal. Posons $K := k[X_1, \dots, X_{n+1}]/\mathfrak{m}$. Pour tout $i \in \llbracket 1, n+1 \rrbracket$, notons x_i la classe de X_i modulo $\mathfrak{m}$. Nous avons deux extensions de corps $k \subset k(x_1) \subset K$. Par hypothèse de récurrence, la deuxième extension est finie.

Il existe donc des polynômes unitaires $P_1, \dots, P_{n+1} \in k(x_1)[Y]$ tels que $P_i(x_i) = 0$ pour tout $i \in \llbracket 1, n+1 \rrbracket$. Notons $D \in k[x_1]$ le produit des dénominateurs des coefficients de tous les P_i . Pour $i \in \llbracket 1, n+1 \rrbracket$ fixé, nous avons donc $D^{\deg_Y(P_i)} P_i(x_i) = 0$ qui peut se réécrire sous la forme $R_i(Dx_i) = 0$ pour un certain $R_i \in k[x_1][Y]$ unitaire.

Soit $P \in k[X_1, \dots, X_{n+1}]$ tel que $x_1^{-1} = P(x_1, \dots, x_{n+1})$. On peut alors trouver $R \in k[X_1, \dots, X_{n+1}]$ tel que $D^{\deg(P)} x_1^{-1} = R(Dx_1, \dots, Dx_{n+1})$. Si l'on suppose que x_1 n'est pas algébrique, alors d'après le lemme précédent, nous pouvons trouver un polynôme unitaire $Q \in k[x_1][Y]$ tel que $Q(D^{\deg(P)} x_1^{-1}) = 0$. En multipliant cette égalité par $x_1^{\deg_Y(Q)}$, on voit que x_1 est une racine d'un polynôme unitaire à coefficients dans k , ce qui contredit l'hypothèse que x_1 n'est pas algébrique. Ainsi, les extensions sont finies.

La dernière assertion de l'énoncé provient du fait que toute extension finie d'un corps algébriquement clos est triviale. $\square$

Nullstellensatz faible 2.20. *Supposons que k est algébriquement clos. Soit $n \in \mathbb{N}$. Les idéaux maximaux de $k[X_0, \dots, X_n]$ sont tous les idéaux de la forme $\langle X_0 - x_0, \dots, X_n - x_n \rangle$, où $x_0, \dots, x_n \in k$.*

Démonstration. Tout d'abord, le morphisme d'évaluation $k[X_0, \dots, X_n] \rightarrow k$ qui envoie chaque indéterminée X_i vers x_i se factorise à travers le quotient $k[X_0, \dots, X_n]/\langle X_0 - x_0, \dots, X_n - x_n \rangle$. Nous avons donc une surjection de ce quotient vers k , et il s'agit d'un isomorphisme car, par divisions euclidiennes successives, on voit que chaque polynôme est dans la même classe qu'un scalaire de k . L'idéal est donc bien maximal.

Réciproquement, si $\mathfrak{m}$ est un idéal maximal de $k[X_0, \dots, X_n]$, alors d'après le lemme de Zariski $k[X_0, \dots, X_n]/\mathfrak{m}$ est isomorphe à k . En notant x_i les images de X_i dans k , on observe alors que $\langle X_0 - x_0, \dots, X_n - x_n \rangle \subset \mathfrak{m}$, et on conclut. $\square$

Nullstellensatz univarié 2.21. *Supposons que k est un corps algébriquement clos. Soient $P, Q \in k[X_0, \dots, X_n]$ deux polynômes homogènes tels que $V(\langle P \rangle) \subset V(\langle Q \rangle)$. Alors, $\langle Q \rangle \subset \sqrt{\langle P \rangle}$.*

Démonstration. Nous allons employer l'astuce dite de Rabinowitsch. Introduisons une nouvelle indéterminée Y . Soit $I := \langle 1 - YQ, P \rangle$. Remarquons que le polynôme $1 - YQ \in k[X_0, \dots, X_n, Y]$ ne peut avoir aucune racine en commun avec P , vu comme un polynôme avec cette variable supplémentaire. D'après le Nullstellensatz faible, cela implique que $1 \in I$, car sinon I serait inclus dans un idéal maximal fournissant une racine commune.

Il existe donc $A, B \in k[X_0, \dots, X_n, Y]$ tels que $A - AYQ + BP = 1$. En substituant Y par Q^{-1} , on obtient $B(X_0, \dots, X_n, Q^{-1})P = 1$. En multipliant par une puissance suffisamment élevée de Q , cela implique que P divise cette puissance de Q dans $k[X_0, \dots, X_n]$. $\square$

2.4 Irréductibilité

Nous allons désormais introduire une notion topologique d'irréductibilité, et nous allons voir comment celle-ci se comporte avec l'irréductibilité des polynômes.

Définition 2.22. *Un ensemble algébrique projectif V est dit réductible s'il existe deux ensembles algébriques projectifs W et W' tels que $V = W \cup W'$ et $W \neq V$ et $W' \neq V$.*

Si cette propriété n'est jamais vérifiée, V est dit irréductible.

Exemple 2.23. *L'ensemble algébrique projectif $V(\langle (X - Y)^2 \rangle) \subset \mathbf{P}_{\mathbb{Q}}^2$ est irréductible.*

En effet, il s'agit de l'ensemble $\{[0 : 0 : 1]\} \cup \{[1 : 1 : z] \mid z \in \mathbb{Q}\}$. Si cet ensemble était la réunion de deux ensembles algébriques projectifs W et W' , alors l'un des deux aurait une infinité de points de la forme $[1 : 1 : z]$ avec $z \in \mathbb{Q}$. Supposons sans perte de généralité qu'il s'agit de W .

Si P est un polynôme homogène dans l'idéal définissant W , alors on a $P(1, 1, z) = 0$ pour une infinité de $z \in \mathbb{Q}$. En particulier, cela implique que le polynôme $P(1, 1, Z) \in \mathbb{Q}[Z]$ est nul. Donc $\{[1 : 1 : z] \mid z \in \mathbb{Q}\} \subset W$.

Comme P est un polynôme homogène, nous trouvons également qu'il n'a pas de monôme ne contenant que l'indéterminée Z . Ainsi, $P(0, 0, 1) = 0$ et nous avons démontré l'irréductibilité.

Exemple 2.24. *L'ensemble algébrique projectif $V(\langle (X^2 - Y^2)^2 + Z^4 \rangle) \subset \mathbf{P}_{\mathbb{Q}}^2$ est réductible.*

Il s'agit en effet de l'ensemble $\{[x : x : 0] \mid x \in \mathbb{Q}\} \cup \{[x : -x : 0] \mid x \in \mathbb{Q}\}$. C'est donc la réunion de $V(\langle (X - Y)^2 + Z^2 \rangle)$ et de $V(\langle (X + Y)^2 + Z^2 \rangle)$.

Exemple 2.25. *Soit $n \in \mathbb{N}$. Tout ensemble réduit à un point de $\mathbf{P}_k^n$ est un ensemble algébrique projectif irréductible.*

En effet, si $[x_0 : \dots : x_n] \in \mathbf{P}_k^n$, alors si $i \in \llbracket 0, n \rrbracket$ est le premier entier tel que $x_i \neq 0$, si $I := \langle X_0, \dots, X_{i-1}, X_{i+1} - x_{i+1}x_i^{-1}X_i, \dots, X_n - x_nx_i^{-1}X_i \rangle$, on vérifie que $V(I) = \{[x_0 : \dots : x_n]\}$.

Proposition 2.26. *Supposons que k est algébriquement clos. Soit $n \in \mathbb{N}$. Soit $P \in k[X_0, \dots, X_n]$ un polynôme homogène irréductible. Alors, $V(\langle P \rangle)$ est irréductible.*

Démonstration. Soient I et J deux idéaux homogènes de $k[X_0, \dots, X_n]$ dont les lieux des zéros ne coïncident pas avec $V(\langle P \rangle)$, et tels que $V(\langle P \rangle) = V(I) \cup V(J)$. Soient $Q \in I$ et $R \in J$ deux polynômes homogènes tels qu'il existe $x \in V(I)$ et $y \in V(J)$ vérifiant $Q(y) \neq 0$ et $R(x) \neq 0$. Par hypothèse, nous avons $V(\langle P \rangle) \subset V(\langle Q \rangle) \cup V(\langle R \rangle) = V(\langle QR \rangle)$.

D'après le Nullstellensatz univarié, P divise une puissance de QR dans $k[X_0, \dots, X_n]$. Comme l'anneau est factoriel, et que P est irréductible, cela signifie que P divise Q ou R , donc que $V(\langle P \rangle) \subset V(\langle Q \rangle)$ ou que $V(\langle P \rangle) \subset V(\langle R \rangle)$. Cela contredit nos hypothèses sur Q et R , donc $V(\langle P \rangle)$ est irréductible. $\square$

La précédente proposition est fausse sans l'hypothèse sur k .

Proposition 2.27. *Sur un corps fini, tout ensemble algébrique projectif avec au moins deux points est réductible.*

Démonstration. Tout espace projectif sur un corps fini est un ensemble fini. Ainsi, tout ensemble algébrique projectif est la réunion finie des points qui le compose. Puisqu'un point est un ensemble algébrique projectif, on conclut. $\square$

La proposition précédente justifie la définition suivante.

Définition 2.28. *Un ensemble algébrique projectif V d'un espace projectif sur k est dit géométriquement irréductible si les équations qui le définissent engendrent un ensemble algébrique projectif sur les clôtures algébriques de k .*

Si tel est le cas, on dira que V est une variété algébrique projective.

Proposition 2.29. *Supposons que k est un corps algébriquement clos. Soit $n \in \mathbb{N}$. Soit $P \in k[X_0, \dots, X_n]$ un polynôme homogène tel que $V(\langle P \rangle)$ soit une variété algébrique projective. Alors P est une puissance d'un polynôme homogène irréductible.*

Démonstration. Soit $\mathcal{H}$ l'ensemble des polynômes homogènes de $k[X_0, \dots, X_n]$. Considérons l'idéal $I := \langle \{Q \in \mathcal{H} \mid \forall x \in \mathbf{P}_k^n, P(x) = 0 \implies Q(x) = 0\} \rangle$. Remarquons que $V(\langle P \rangle) = V(I)$, car $P \in I$ et $V(\langle P \rangle) \subset V(I)$ par définition.

De plus, I est un idéal premier. Si tel n'était pas le cas, alors on pourrait trouver des polynômes $R, S \in k[X_0, \dots, X_n] \setminus I$ tels que $RS \in I$. Quitte à considérer la somme de leurs termes de plus haut degré, on peut les supposer homogènes. Cela impliquerait alors que $V(I) \subset V(\langle RS \rangle) = V(\langle R \rangle) \cup V(\langle S \rangle)$. D'où une écriture comme réunion de deux ensembles algébriques projectifs $V(I) = (V(I) \cap V(\langle R \rangle)) \cup (V(I) \cap V(\langle S \rangle))$. Ces deux ensembles algébriques projectifs étant des sous-ensembles stricts de $V(I)$, on arrive à la contradiction, donc I est bien premier.

Supposons qu'il existe $Q \in I \setminus \langle P \rangle$. Comme I est premier et que $k[X_0, \dots, X_n]$ est factoriel, on peut supposer que Q est irréductible. Alors $V(\langle P \rangle) \subset V(\langle Q \rangle)$, et d'après le Nullstellensatz univarié P divise une puissance de Q . $\square$

3 Courbes projectives planes

Dans cette section, k désigne un corps.

Nous allons désormais restreindre notre étude à de certaines variétés algébriques, qui sont les courbes projectives planes. Certains des résultats énoncés ici possèdent des versions plus générales, mais nous nous restreignons à ce cadre afin de simplifier l'exposition. Les courbes elliptiques sont un cas particulier de courbe projective plane.

3.1 Dimension et degré

Nous allons introduire deux invariants importants associés à certains ensembles algébriques projectifs.

Définition 3.1. *Une hypersurface projective est un ensemble algébrique projectif défini par un idéal homogène principal.*

En d'autres termes, une hypersurface projective est le lieu des zéros d'un polynôme homogène.

Définition 3.2. *Soit $n \in \mathbb{N}$. Soit $V \subset \mathbf{P}_k^n$ une hypersurface projective. La dimension de V est l'entier $n - 1$.*

À nouveau, ici, le mot « dimension » possède un sens nouveau.

Exemple 3.3. *Soit $n \in \mathbb{N}^*$. On peut voir $\mathbf{P}_k^{n-1}$ comme l'ensemble des zéros du polynôme homogène X_n . Sa dimension en tant qu'hypersurface projective est $n - 1$, coïncidant ainsi avec sa dimension en tant qu'espace projectif.*

Définition 3.4. *Une courbe projective plane est une hypersurface projective de dimension 1.*

Proposition 3.5. *Soit $n \in \mathbb{N}$. Soit $V \subset \mathbf{P}_k^n$ une hypersurface projective géométriquement irréductible. Alors il existe un polynôme homogène irréductible $P \in k[X_0, \dots, X_n]$ tel que :*

$$V = V(\langle P \rangle).$$

Démonstration. Soit $\bar{k}$ une clôture algébrique de k . Par hypothèse sur V , il existe un polynôme homogène $P \in k[X_0, \dots, X_n]$ tel que $V = V(\langle P \rangle)$. On peut de plus supposer sans perte de généralité que P n'est pas la puissance d'un autre polynôme de $k[X_0, \dots, X_n]$.

Notons $P_{\bar{k}}$ le polynôme P vu comme un polynôme dans $\bar{k}$. Par définition, V est une variété algébrique projective, donc $V(\langle P_{\bar{k}} \rangle)$ est irréductible. En particulier, $P_{\bar{k}} = Q^l$ avec $Q \in \bar{k}[X_0, \dots, X_n]$ homogène irréductible et $l \in \mathbb{N}^*$ car $\bar{k}[X_0, \dots, X_n]$ est factoriel.

Soit $m \in \mathbb{N}^*$ le plus petit entier naturel non nul tel qu'il existe $c \in \bar{k}$ pour lequel $(cQ)^m \in k[X_0, \dots, X_n]$. Soit R le PGCD dans $k[X_0, \dots, X_n]$ de P et de $(cQ)^m$. Puisque $\bar{k}[X_0, \dots, X_n]$ est factoriel, R doit être une puissance de Q à

un scalaire près, donc par hypothèse sur m on doit avoir $(cQ)^m$ divisant R , et donc $m = l$.

En particulier, si l'on prend $A, B \in k[X_0, \dots, X_n]$ tels que $P = AB$, alors toujours par factorialité, A et B sont dans cet anneau des puissances de Q à un scalaire près. Par hypothèse sur m , l'un des deux doit donc être un multiple de P , qui est donc irréductible. $\square$

Les résultats vus précédemment, dont le Nullstellensatz univarié, nous assurent que la définition suivante ne dépend pas de choix.

Définition 3.6. Soit $n \in \mathbb{N}$. Soit $V \subset \mathbf{P}_k^n$ une hypersurface projective géométriquement irréductible. Posons $P \in k[X_0, \dots, X_n]$ un polynôme homogène irréductible définissant V .

Alors le degré de V est le degré de P .

Définition 3.7. Une droite projective plane est une courbe projective plane de degré 1.

Exemple 3.8. La droite projective est une droite projective plane.

Exemple 3.9. Comme tout polynôme homogène de $k[X_0, \dots, X_2]$ de degré 1 est irréductible, alors celui-ci définit une droite projective plane, et réciproquement.

Proposition 3.10. Deux droites projectives planes distinctes se croisent en un unique point de $\mathbf{P}_k^2$.

Démonstration. Une droite projective plane est le lieu des zéros d'un polynôme homogène de degré 1 de $k[X_0, \dots, X_2]$. Ce polynôme peut être vu comme un endomorphisme linéaire de k^3 , et l'ensemble des droites vectorielles de son noyau correspond à la droite projective plane étudiée. Or, le théorème du rang nous assure que ces noyaux sont de dimension 2. L'intersection de deux de ces noyaux est donc de dimension 1 ou 2.

Si cette intersection était de dimension 2, cela signifie que les noyaux coïncident, et donc les droites projectives planes aussi, ce qui est exclu par hypothèse. L'intersection est donc une droite vectorielle : il s'agit ainsi d'un unique point de $\mathbf{P}_k^2$. $\square$

3.2 Lisseté

Définition

Lisse implique irréductible (pour les courbes ?)

Toute courbe de degré 1 est lisse

Morphismes ? Homographies ?

Toute courbe lisse de degré 2 est isomorphe à $\mathbf{P}^1$

3.3 Courbes elliptiques

Définition 3.11. Une courbe elliptique est une courbe projective plane lisse de degré 3.

Remarque : plane inutile, degré c'est pareil que genre 1.

4 Reste

- loi de groupe + construction des formules à partir de la description géométrique
- forme de Weierstrass courte (d'où ça vient, enfin pas Riemann-Roch quand même), forme longue, changements de variables, discriminant, j-invariant
- isomorphismes
- torsion, polynômes de division
- Théorème appli rationnelle + $f(0)=0$ + $f(E)=E \Rightarrow$ morphisme
- isogénies + duale + degré + théorème de Tate
- endomorphismes ([m] et Frobenius comme exemples)
- ordinaires/supersingulières
- tordue quadratique
- Théorème de Hasse (sans preuve)

Références

- [1] William FULTON, *Algebraic Curves, An Introduction to Algebraic Geometry*.
- [2] Qing LIU, *Algebraic Geometry and Arithmetic Curves*.
- [3] Joseph Hillel SILVERMAN, *The Arithmetic of Elliptic Curves*.