Plongements grassmanniens et arithmétique jacobienne rapide

Nicolas Mascot, d'après Kamal Khuri-Makdisi

Université de Bordeaux 1

Février 2011

Table des matières

Table des matières

Table des matières

Table des matières

Rappels sur les courbes algébriques

Notations

Nous travaillerons sur un corps parfait K.

Considérons une courbe algébrique X sur K, réduite, géométriquement irréductible, non singulière, de genre g.

Nous noterons $H^i(\cdot) = R^i\Gamma(X, \cdot)$ la cohomologie des faisceaux sur X.

Diviseurs

Un *diviseur* sur X est une somme formelle finie $D = \sum_{P \in X} n_P P$ de points de X.

Diviseurs

Un *diviseur* sur X est une somme formelle finie $D = \sum_{P \in X} n_P P$ de points de X.
Le diviseur est *effectif* (noté $D \geqslant 0$) si $n_P \geqslant 0$, et son *degré* est $\deg D = \sum n_P \big[K(P) : K\big]$.

Diviseurs

Un *diviseur* sur X est une somme formelle finie $D = \sum_{P \in X} n_P P$ de points de X.
Le diviseur est *effectif* (noté $D \geqslant 0$) si $n_P \geqslant 0$, et son *degré* est $\deg D = \sum n_P \big[K(P) : K\big]$.
Les *diviseurs principaux* sont les

$$(\alpha) = \sum_{P \in X} \mathrm{ord}_P(\alpha) P, \quad \alpha \in K(X)^*.$$

Diviseurs

Un *diviseur* sur X est une somme formelle finie $D = \sum_{P \in X} n_P P$ de points de X.
Le diviseur est *effectif* (noté $D \geqslant 0$) si $n_P \geqslant 0$, et son *degré* est $\deg D = \sum n_P \big[K(P) : K\big]$.
Les *diviseurs principaux* sont les

$$(\alpha) = \sum_{P \in X} \mathrm{ord}_P(\alpha) P, \quad \alpha \in K(X)^*.$$

Ils sont tous de degré nul.

Diviseurs

Un *diviseur* sur X est une somme formelle finie $D = \sum_{P \in X} n_P P$ de points de X.
Le diviseur est *effectif* (noté $D \geqslant 0$) si $n_P \geqslant 0$, et son *degré* est $\deg D = \sum n_P \big[K(P) : K\big]$.
Les *diviseurs principaux* sont les

$$(\alpha) = \sum_{P \in X} \mathrm{ord}_P(\alpha) P, \quad \alpha \in K(X)^*.$$

Ils sont tous de degré nul.

Le *groupe de Picard* de X est

$$\mathrm{Pic}(X) = \text{Diviseurs} \ / \ \text{Diviseurs principaux}.$$

Diviseurs

Un *diviseur* sur X est une somme formelle finie $D = \sum_{P \in X} n_P P$ de points de X.
Le diviseur est *effectif* (noté $D \geqslant 0$) si $n_P \geqslant 0$, et son *degré* est $\deg D = \sum n_P \big[K(P) : K\big]$.
Les *diviseurs principaux* sont les

$$(\alpha) = \sum_{P \in X} \mathrm{ord}_P(\alpha) P, \quad \alpha \in K(X)^*.$$

Ils sont tous de degré nul.

Le *groupe de Picard* de X est

$$\mathrm{Pic}(X) = \text{Diviseurs} \ / \ \text{Diviseurs principaux}.$$

Les diviseurs sont les sections globales de $K(X)^*/\mathcal{O}_X^*$, donc

$$\mathrm{Pic}(X) \simeq H^1(\mathcal{O}_X^*).$$

Fibrés en droites

On appelle *fibré en droites* sur X tout $\mathcal{O}_X$-module localement libre de rang 1.

Fibrés en droites

On appelle *fibré en droites* sur X tout $\mathcal{O}_X$-module localement libre de rang 1.
Le produit tensoriel de deux fibrés en droites sur X est un fibré en droites sur X.

Fibrés en droites

On appelle *fibré en droites* sur X tout $\mathcal{O}_X$-module localement libre de rang 1.
Le produit tensoriel de deux fibrés en droites sur X est un fibré en droites sur X.
Si $\mathcal{L}$ est un fibré en droites, on notera $\mathcal{L}^\vee$ le *fibré dual*

$$\mathcal{L}^\vee = \mathcal{H}om_{\mathcal{O}_X}(\mathcal{L}, \mathcal{O}_X);$$

il vérifie $\mathcal{L} \otimes \mathcal{L}^\vee \simeq \mathcal{O}_X$.

Fibrés en droites

On appelle *fibré en droites* sur X tout $\mathcal{O}_X$-module localement libre de rang 1.
Le produit tensoriel de deux fibrés en droites sur X est un fibré en droites sur X.
Si $\mathcal{L}$ est un fibré en droites, on notera $\mathcal{L}^\vee$ le *fibré dual*

$$\mathcal{L}^\vee = \mathcal{H}om_{\mathcal{O}_X}(\mathcal{L}, \mathcal{O}_X);$$

il vérifie $\mathcal{L} \otimes \mathcal{L}^\vee \simeq \mathcal{O}_X$.
Les fibrés en droites sur X modulo isomorphisme forment donc un groupe abélien pour $\otimes$.

Diviseurs et fibrés en droites

A un diviseur $D = \sum_{P \in X} n_p P$ de X, on associe le faisceau

$$\mathcal{O}_X(D) : U \longmapsto \left\{ f \in K(X)^* \;\middle|\; \forall P \in U, \mathrm{ord}_P(f) + n_P \geqslant 0 \right\} \cup \{0\}.$$

C'est un fibré en droites sur X, et tout fibré en droites sur X est isomorphe à un $\mathcal{O}_X(D)$.

Diviseurs et fibrés en droites

A un diviseur $D = \sum_{P \in X} n_p P$ de X, on associe le faisceau

$$\mathcal{O}_X(D) : U \longmapsto \left\{ f \in K(X)^* \;\middle|\; \forall P \in U, \mathrm{ord}_P(f) + n_P \geqslant 0 \right\} \cup \{0\}.$$

C'est un fibré en droites sur X, et tout fibré en droites sur X est isomorphe à un $\mathcal{O}_X(D)$.

On sait calculer effectivement $H^0\big(O_X(D)\big)$.

Diviseurs et fibrés en droites

A un diviseur $D = \sum_{P \in X} n_p P$ de X, on associe le faisceau

$$\mathcal{O}_X(D) : U \longmapsto \left\{ f \in K(X)^* \;\middle|\; \forall P \in U, \mathrm{ord}_P(f) + n_P \geqslant 0 \right\} \cup \{0\}.$$

C'est un fibré en droites sur X, et tout fibré en droites sur X est isomorphe à un $\mathcal{O}_X(D)$.

On sait calculer effectivement $H^0\big(O_X(D)\big)$.

On notera $l(D) = \dim_K H^0\big(O_X(D)\big)$.

Diviseurs et fibrés en droites

A un diviseur $D = \sum_{P \in X} n_p P$ de X, on associe le faisceau

$$\mathcal{O}_X(D) : U \longmapsto \left\{ f \in K(X)^* \;\middle|\; \forall P \in U, \mathrm{ord}_P(f) + n_P \geqslant 0 \right\} \cup \{0\}.$$

C'est un fibré en droites sur X, et tout fibré en droites sur X est isomorphe à un $\mathcal{O}_X(D)$.

On sait calculer effectivement $H^0\big(O_X(D)\big)$.

On notera $l(D) = \dim_K H^0\big(O_X(D)\big)$.

On a $\mathcal{O}_X(D) \otimes \mathcal{O}_X(D') \simeq \mathcal{O}_X(D + D')$ et $\mathcal{O}_X(D)^\vee \simeq \mathcal{O}_X(-D)$.

Groupe de Picard et fibrés en droites

$\mathcal{O}_X(D) \simeq \mathcal{O}_X(D')$ si et seulement si $D \sim D'$; par conséquent, $\mathrm{Pic}(X)$ s'identifie aux classes d'isomorphisme des fibrés en droites sur X, et on a un isomorphisme de groupes

$$\big(\mathrm{Pic}(X), +\big) \quad \simeq \quad \big(\text{fibrés en droites}, \otimes\big)/\text{isomorphisme}.$$

On peut donc parler du degré d'un fibré en droites.

Caractéristique d'Euler

Définissons la *caractéristique d'Euler* d'un fibré en droites $\mathcal{L}$ sur X par

$$\chi(\mathcal{L}) = \dim_K H^0(\mathcal{L}) - \dim_K H^1(\mathcal{L}).$$

Caractéristique d'Euler

Définissons la *caractéristique d'Euler* d'un fibré en droites $\mathcal{L}$ sur X par

$$\chi(\mathcal{L}) = \dim_K H^0(\mathcal{L}) - \dim_K H^1(\mathcal{L}).$$

Proposition

Pour tout fibré en droites $\mathcal{L}$ sur X, on a

$$\chi(\mathcal{L}) = \deg \mathcal{L} + 1 - g.$$

Dualité de Serre

La *classe canonique* est la classe des coefficients des 1-formes différentielles sur X. Soit $\mathcal{K}_X$ un fibré en droites représentant la classe canonique de X.

Dualité de Serre

La *classe canonique* est la classe des coefficients des 1-formes différentielles sur X. Soit $\mathcal{K}_X$ un fibré en droites représentant la classe canonique de X.

Proposition

On a un accouplement parfait

$$H^1(\mathcal{L}) \underset{K}{\otimes} H^0(\mathcal{K}_X \otimes \mathcal{L}^\vee) \longrightarrow K.$$

Dualité de Serre

La *classe canonique* est la classe des coefficients des 1-formes différentielles sur X. Soit $\mathcal{K}_X$ un fibré en droites représentant la classe canonique de X.

Proposition

On a un accouplement parfait

$$H^1(\mathcal{L}) \underset{K}{\otimes} H^0(\mathcal{K}_X \otimes \mathcal{L}^\vee) \longrightarrow K.$$

Corollaire

En particulier, $\dim_K H^1\big(\mathcal{O}_X(D)\big) = \dim_K H^0\big(\mathcal{K}_X(-D)\big)$.

Le théorème de Riemann-Roch

Théorème de Riemann-Roch

Soit K un corps parfait, et soit X une courbe projective non singulière réduite absolument irréductible de genre g sur K.

Le théorème de Riemann-Roch

Théorème de Riemann-Roch

Soit K un corps parfait, et soit X une courbe projective non singulière réduite absolument irréductible de genre g sur K. Le degré de la classe canonique est

$$\deg(\mathcal{K}_X) = 2g - 2.$$

Le théorème de Riemann-Roch

Théorème de Riemann-Roch

Soit K un corps parfait, et soit X une courbe projective non singulière réduite absolument irréductible de genre g sur K. Le degré de la classe canonique est

$$\deg(\mathcal{K}_X) = 2g - 2.$$

Pour tout diviseur D,

$$l(D) = \deg(D) + 1 - g + l(\mathcal{K}_X - D).$$

Le théorème de Riemann-Roch

Théorème de Riemann-Roch

Le degré de la classe canonique est

$$\deg(\mathcal{K}_X) = 2g - 2.$$

Pour tout diviseur D,

$$l(D) = \deg(D) + 1 - g + l(\mathcal{K}_X - D).$$

Corollaire

Si $\deg(D) \geqslant g$, alors $H^0\big(\mathcal{O}_X(D)\big) \neq 0$.

Le théorème de Riemann-Roch

Théorème de Riemann-Roch

Le degré de la classe canonique est

$$\deg(\mathcal{K}_X) = 2g - 2.$$

Pour tout diviseur D,

$$l(D) = \deg(D) + 1 - g + l(\mathcal{K}_X - D).$$

Corollaire

Si $\deg(D) \geqslant g$, alors $H^0\big(\mathcal{O}_X(D)\big) \neq 0$.

Corollaire

Si $\deg(D) \geqslant 2g - 1$, alors $l(D) = \deg(D) + 1 - g$.

Applications du théorème de Riemann-Roch

Un fibré en droites $\mathcal{L} \simeq \mathcal{O}_X(D)$ est *sans points-base* si

$$\inf_{f \in H^0(\mathcal{L})} (f) + D = 0.$$

Applications du théorème de Riemann-Roch

Un fibré en droites $\mathcal{L} \simeq \mathcal{O}_X(D)$ est *sans points-base* si

$$\inf_{f \in H^0(\mathcal{L})} (f) + D = 0.$$

Corollaire

Si $\deg \mathcal{L} \geqslant 2g$, alors $\mathcal{L}$ est sans points-base.

Applications du théorème de Riemann-Roch

Un fibré en droites $\mathcal{L} \simeq \mathcal{O}_X(D)$ est *sans points-base* si

$$\inf_{f \in H^0(\mathcal{L})} (f) + D = 0.$$

Corollaire

Si $\deg \mathcal{L} \geqslant 2g$, alors $\mathcal{L}$ est sans points-base.

Soit $\phi_{\mathcal{L}} : \begin{array}{ccc} X & \longrightarrow & \mathbb{P}_K^{\deg \mathcal{L} - g} \\ x & \longmapsto & [\cdots, f_i(x), \cdots] \end{array}$, où (f_i) est une K-base de $H^0(\mathcal{L})$.

Applications du théorème de Riemann-Roch

Un fibré en droites $\mathcal{L} \simeq \mathcal{O}_X(D)$ est *sans points-base* si

$$\inf_{f \in H^0(\mathcal{L})} (f) + D = 0.$$

Corollaire

Si $\deg \mathcal{L} \geqslant 2g$, alors $\mathcal{L}$ est sans points-base.

Soit $\phi_{\mathcal{L}} : \begin{array}{ccc} X & \longrightarrow & \mathbb{P}_K^{\deg \mathcal{L} - g} \\ x & \longmapsto & [\cdots, f_i(x), \cdots] \end{array}$, où (f_i) est une K-base de $H^0(\mathcal{L})$.

Corollaire

Si $\deg \mathcal{L} \geqslant 2g + 1$, alors $\phi_{\mathcal{L}}$ est un plongement.

Jacobienne d'une courbe

Théorème

Pour toute courbe projective absolument irréductible non singulière X de genre $g \geqslant 1$ sur un corps K, admettant au moins un point rationnel O, il existe une variété abélienne J_X sur K, dite *jacobienne de la courbe* X, qui est de dimension g et munie d'un plongement $\jmath : X \hookrightarrow J_X$, défini sur K, et qui, étendu par linéarité au groupe des diviseurs de X, induit un isomorphisme entre $\mathrm{Pic}^0(X)$ et $J_X(K)$.

Arithmétique jacobienne naïve : Brill-Noether

Construction de la jacobienne

Notons, pour $n \in \mathbb{N}^*$,

$$\mathrm{Sym}^n X = X^n / \mathfrak{S}_n.$$

Construction de la jacobienne

Notons, pour $n \in \mathbb{N}^*$,

$$\mathrm{Sym}^n X = X^n / \mathfrak{S}_n.$$

Application d'Abel-Jacobi

Si X admet un point rationnel $O \in X(K)$, alors

$$\begin{array}{rccc} \jmath : & \mathrm{Sym}^n X & \longrightarrow & J_X \\ & (P_1, \cdots, P_n) & \longmapsto & \left[\sum_{i=1}^{n} P_i - nO \right] \end{array}$$

est surjective pour $n \geqslant g$, et birationnelle pour $n = g$.

Représentation explicite

Les plongements effectifs de J_X dans $\mathbb{P}^n_K$ demandent traditionnellement $n = 4^g - 1$, et un nombre d'équations définissant l'image de J_X encore plus grand.

Par conséquent, il est plus raisonnable de représenter les éléments de $J_X(K)$ sous la forme

$$\sum_{i=1}^{g} P_i - gO,$$

autrement dit par des g-uplets non ordonnés de points.

Représentation explicite

Les plongements effectifs de J_X dans $\mathbb{P}^n_K$ demandent traditionnellement $n = 4^g - 1$, et un nombre d'équations définissant l'image de J_X encore plus grand.

Par conséquent, il est plus raisonnable de représenter les éléments de $J_X(K)$ sous la forme

$$\sum_{i=1}^{g} P_i - gO,$$

autrement dit par des g-uplets non ordonnés de points.

On doit "voir" la loi d'addition sur $\mathrm{Sym}^g(X)$.

Calculs dans la jacobienne : test d'égalité

Test d'égalité : $\sum_{i=1}^{g} P_i - gO \sim \sum_{i=1}^{g} Q_i - gO$

Calculs dans la jacobienne : test d'égalité

Test d'égalité : $\displaystyle\sum_{i=1}^{g} P_i - gO \sim \sum_{i=1}^{g} Q_i - gO$

$$\iff \quad H^0\big(\mathcal{O}_X(\textstyle\sum P_i - \sum Q_i)\big) \neq 0.$$

(Ce H^0 est alors de dimension 1 sur K.)

Brill-Noether : addition

Soit D de degré $\geqslant 3g$, posons $\mathcal{L} = \mathcal{O}_X(D)$ et calculons une bonne fois pour toutes une K-base de $H^0(\mathcal{L})$.

Brill-Noether : addition

Soit D de degré $\geqslant 3g$, posons $\mathcal{L} = \mathcal{O}_X(D)$ et calculons une bonne fois pour toutes une K-base de $H^0(\mathcal{L})$.

Addition : $\displaystyle\sum_{i=1}^{g} P_i - gO + \sum_{i=1}^{g} Q_i - gO \sim \sum_{i=1}^{g} R_i - gO.$

Brill-Noether : addition

Soit D de degré $\geqslant 3g$, posons $\mathcal{L} = \mathcal{O}_X(D)$ et calculons une bonne fois pour toutes une K-base de $H^0(\mathcal{L})$.

Addition : $\displaystyle\sum_{i=1}^{g} P_i - gO + \sum_{i=1}^{g} Q_i - gO \sim \sum_{i=1}^{g} R_i - gO.$

- Soit $\alpha \in H^0\big(\mathcal{L}(-\sum P_i - \sum Q_i)\big)$, $\alpha \neq 0$:

$$D' = (\alpha) + D - \sum_{i=1}^{g} P_i - \sum_{i=1}^{g} Q_i \geqslant 0.$$

Brill-Noether : addition

Soit D de degré $\geqslant 3g$, posons $\mathcal{L} = \mathcal{O}_X(D)$ et calculons une bonne fois pour toutes une K-base de $H^0(\mathcal{L})$.

Addition : $\displaystyle\sum_{i=1}^{g} P_i - gO + \sum_{i=1}^{g} Q_i - gO \sim \sum_{i=1}^{g} R_i - gO.$

- Soit $\alpha \in H^0\big(\mathcal{L}(-\sum P_i - \sum Q_i)\big)$, $\alpha \neq 0$:

$$D' = (\alpha) + D - \sum_{i=1}^{g} P_i - \sum_{i=1}^{g} Q_i \geqslant 0.$$

- Soit $\beta \in H^0\big(\mathcal{L}(-D' - gO)\big)$, $\beta \neq 0$:

$$D'' = (\beta) + D - D' - gO \geqslant 0.$$

Brill-Noether : addition

Soit D de degré $\geqslant 3g$, posons $\mathcal{L} = \mathcal{O}_X(D)$ et calculons une bonne fois pour toutes une K-base de $H^0(\mathcal{L})$.

Addition : $\displaystyle\sum_{i=1}^{g} P_i - gO + \sum_{i=1}^{g} Q_i - gO \sim \sum_{i=1}^{g} R_i - gO.$

- Soit $\alpha \in H^0\big(\mathcal{L}(-\sum P_i - \sum Q_i)\big)$, $\alpha \neq 0$:

$$D' = (\alpha) + D - \sum_{i=1}^{g} P_i - \sum_{i=1}^{g} Q_i \geqslant 0.$$

- Soit $\beta \in H^0\big(\mathcal{L}(-D' - gO)\big)$, $\beta \neq 0$:

$$D'' = (\beta) + D - D' - gO \geqslant 0.$$

- Alors $\displaystyle D'' = \sum_{i=1}^{g} R_i$.

Brill-Noether : opposition

Opposition : $gO - \sum_{i=1}^{g} P_i \sim \sum_{i=1}^{g} Q_i - gO$.

Brill-Noether : opposition

Opposition : $gO - \sum_{i=1}^{g} P_i \sim \sum_{i=1}^{g} Q_i - gO.$

- Soit $\alpha \in H^0\big(\mathcal{L}(-2gO)\big)$, $\alpha \neq 0$:

$$D' = (\alpha) + D - 2gO \geqslant 0.$$

Brill-Noether : opposition

Opposition : $gO - \sum_{i=1}^{g} P_i \sim \sum_{i=1}^{g} Q_i - gO.$

- Soit $\alpha \in H^0\big(\mathcal{L}(-2gO)\big)$, $\alpha \neq 0$:

$$D' = (\alpha) + D - 2gO \geqslant 0.$$

- Soit $\beta \in H^0\big(\mathcal{L}(-D' - \sum P_i)\big)$, $\beta \neq 0$:

$$D'' = (\beta) + D - D' - \sum_{i=1}^{g} P_i \geqslant 0.$$

Brill-Noether : opposition

Opposition : $gO - \sum_{i=1}^{g} P_i \sim \sum_{i=1}^{g} Q_i - gO.$

- Soit $\alpha \in H^0\big(\mathcal{L}(-2gO)\big)$, $\alpha \neq 0$:

$$D' = (\alpha) + D - 2gO \geqslant 0.$$

- Soit $\beta \in H^0\big(\mathcal{L}(-D' - \sum P_i)\big)$, $\beta \neq 0$:

$$D'' = (\beta) + D - D' - \sum_{i=1}^{g} P_i \geqslant 0.$$

- Alors $D'' = \sum_{i=1}^{g} Q_i$.

Plongements grassmanniens

Une nouvelle représentation des diviseurs

Fixons un fibré en droites $\mathcal{L}$ de degré $N \gg 0$, $N \geqslant 2g$ sur X, et soit $V = H^0(\mathcal{L})$. Pour tout diviseur effectif D, notons

$$W_D = H^0\big(\mathcal{L}(-D)\big) \subset H^0(\mathcal{L}) = V.$$

Une nouvelle représentation des diviseurs

Fixons un fibré en droites $\mathcal{L}$ de degré $N \gg 0$, $N \geqslant 2g$ sur X, et soit $V = H^0(\mathcal{L})$. Pour tout diviseur effectif D, notons

$$W_D = H^0\big(\mathcal{L}(-D)\big) \subset H^0(\mathcal{L}) = V.$$

Proposition

Si $d \leqslant N - 2g$, alors

$$\begin{array}{ccc} \mathrm{Sym}^d X & \longrightarrow & \mathrm{Grass}_d(V) \\ D & \longmapsto & W_D \end{array}$$

est injective.

Une nouvelle représentation des diviseurs

Fixons un fibré en droites $\mathcal{L}$ de degré $N \gg 0$, $N \geqslant 2g$ sur X, et soit $V = H^0(\mathcal{L})$. Pour tout diviseur effectif D, notons

$$W_D = H^0\big(\mathcal{L}(-D)\big) \subset H^0(\mathcal{L}) = V.$$

Proposition

Si $d \leqslant N - 2g$, alors

$$\begin{array}{ccc} \mathrm{Sym}^d X & \longrightarrow & \mathrm{Grass}_d(V) \\ D & \longmapsto & W_D \end{array}$$

est injective.

Ceci permet de représenter les diviseurs effectifs de degré au plus $N - 2g$ sur X, une fois une K-base de V calculée.

Lemme de multiplication

Soient $\mathcal{L}_1$ et $\mathcal{L}_2$ deux fibrés en droites sur X, et soit

$$\mu : H^0(\mathcal{L}_1) \underset{K}{\otimes} H^0(\mathcal{L}_2) \longrightarrow H^0(\mathcal{L}_1 \otimes \mathcal{L}_2).$$

Lemme de multiplication

Soient $\mathcal{L}_1$ et $\mathcal{L}_2$ deux fibrés en droites sur X, et soit

$$\mu : H^0(\mathcal{L}_1) \underset{K}{\otimes} H^0(\mathcal{L}_2) \longrightarrow H^0(\mathcal{L}_1 \otimes \mathcal{L}_2).$$

Lemme

Si $\deg \mathcal{L}_1 \geqslant 2g+1$ et $\deg \mathcal{L}_2 \geqslant 2g+1$, alors μ est surjective.

Lemme de division

Soient $\mathcal{L}_1$, $\mathcal{L}_2$ et μ comme précédemment, et soient D_1 et D_2 deux diviseurs effectifs sur X.

Lemme de division

Soient $\mathcal{L}_1$, $\mathcal{L}_2$ et μ comme précédemment, et soient D_1 et D_2 deux diviseurs effectifs sur X.
Supposons connus les sous-espaces

$$H^0\big((\mathcal{L}_1 \otimes \mathcal{L}_2)(-D_1 - D_2)\big) \subset H^0(\mathcal{L}_1 \otimes \mathcal{L}_2)$$

et

$$H^0\big(\mathcal{L}_2(-D_2)\big) \subset H^0(\mathcal{L}_2).$$

Lemme de division

Soient $\mathcal{L}_1$, $\mathcal{L}_2$ et μ comme précédemment, et soient D_1 et D_2 deux diviseurs effectifs sur X.
Supposons connus les sous-espaces

$$H^0\big((\mathcal{L}_1 \otimes \mathcal{L}_2)(-D_1 - D_2)\big) \subset H^0(\mathcal{L}_1 \otimes \mathcal{L}_2)$$

et

$$H^0\big(\mathcal{L}_2(-D_2)\big) \subset H^0(\mathcal{L}_2).$$

Lemme

Si $\mathcal{L}_2(-D_2)$ est sans points-base, alors on peut calculer $H^0\big(\mathcal{L}_1(-D_1)\big)$

Lemme de division

Soient $\mathcal{L}_1$, $\mathcal{L}_2$ et μ comme précédemment, et soient D_1 et D_2 deux diviseurs effectifs sur X.
Supposons connus les sous-espaces

$$H^0\big((\mathcal{L}_1 \otimes \mathcal{L}_2)(-D_1 - D_2)\big) \subset H^0(\mathcal{L}_1 \otimes \mathcal{L}_2)$$

et

$$H^0\big(\mathcal{L}_2(-D_2)\big) \subset H^0(\mathcal{L}_2).$$

Lemme

Si $\mathcal{L}_2(-D_2)$ est sans points-base, alors on peut calculer

$$H^0\big(\mathcal{L}_1(-D_1)\big) = \Big\{ s \in H^0(\mathcal{L}_1) \;\Big|\; \forall t \in H^0\big(\mathcal{L}_2(-D_2)\big), \\ \mu(s \otimes t) \in H^0\big((\mathcal{L}_1 \otimes \mathcal{L}_2)(-D_1 - D_2)\big) \Big\}.$$

Addition de diviseurs

Soient D et D' deux diviseurs effectifs de degrés $\deg D, \deg D' \leqslant N - 2g - 1$, donnés par W_D et $W_{D'}$. Notons

$$\mu : V \underset{K}{\otimes} V \longrightarrow H^0(\mathcal{L}^{\otimes 2}).$$

Addition de diviseurs

Soient D et D' deux diviseurs effectifs de degrés $\deg D, \deg D' \leqslant N - 2g - 1$, donnés par W_D et $W_{D'}$. Notons

$$\mu : V \underset{K}{\otimes} V \longrightarrow H^0(\mathcal{L}^{\otimes 2}).$$

Addition de diviseurs

- Calculer $H^0\big((\mathcal{L}^{\otimes 2}(-D - D')\big) = \mu(W_D \otimes W_{D'})$.

Addition de diviseurs

Soient D et D' deux diviseurs effectifs de degrés $\deg D, \deg D' \leqslant N - 2g - 1$, donnés par W_D et $W_{D'}$. Notons

$$\mu : V \underset{K}{\otimes} V \longrightarrow H^0(\mathcal{L}^{\otimes 2}).$$

Addition de diviseurs

- Calculer $H^0\big((\mathcal{L}^{\otimes 2}(-D - D')\big) = \mu(W_D \otimes W_{D'})$.
- Calculer $W_{D+D'}$

$$= \left\{ s \in V \;\middle|\; \forall t \in V,\ \mu(s \otimes t) \in H^0\big((\mathcal{L}^{\otimes 2}(-D - D')\big) \right\}.$$

Addition de diviseurs

Soient D et D' deux diviseurs effectifs de degrés $\deg D, \deg D' \leqslant N - 2g - 1$, donnés par W_D et $W_{D'}$. Notons

$$\mu : V \underset{K}{\otimes} V \longrightarrow H^0(\mathcal{L}^{\otimes 2}).$$

Addition de diviseurs

- Calculer $H^0\big((\mathcal{L}^{\otimes 2}(-D - D')\big) = \mu(W_D \otimes W_{D'})$.
- Calculer $W_{D+D'}$

$$= \left\{ s \in V \;\middle|\; \forall t \in V,\ \mu(s \otimes t) \in H^0\big((\mathcal{L}^{\otimes 2}(-D - D')\big) \right\}.$$

Remarque : Ceci ne permet de récupérer $D + D'$ que si N est assez grand.

Arithmétique jacobienne rapide

Notations

Choisissons un diviseur effectif D_0 de degré $d_0 = \deg D_0 \geqslant 2g+1$, qui servira d'origine dans la jacobienne.
Fixons $\mathcal{L} = \mathcal{O}_X(3D_0)$. $\mathcal{L}$ est très ample et fournira un plongement projectif de X ; calculons une fois pour toutes une K-base de $V = H^0(\mathcal{L})$, une K-base de $H^0(\mathcal{L}^{\otimes 2})$, et la matrice de

$$\mu : V \underset{K}{\otimes} V \longrightarrow H^0(\mathcal{L}^{\otimes 2})$$

dans ces bases, qui donne les équations définissant X pour le plongement associé à $\mathcal{L}$.
Les points sur la jacobienne sont des classes de forme $x_D = [D - D_0]$, où D est un diviseur effectif de degré d_0, et représenté par l'espace W_D.

Test d'égalité

Soient x_D et x'_D deux points de la jacobienne, représentés par W_D et $W_{D'}$. L'algorithme suivant teste si $x_D = x_{D'}$.

Test d'égalité

Soient x_D et x'_D deux points de la jacobienne, représentés par W_D et $W_{D'}$. L'algorithme suivant teste si $x_D = x_{D'}$.

Test d'égalité

- Choisir $\alpha \in W_D$, $\alpha \neq 0$; soit $E = (\alpha) + 3D_0 - D$.
  E est effectif de degré $2d_0$.

Test d'égalité

Soient x_D et x'_D deux points de la jacobienne, représentés par W_D et $W_{D'}$. L'algorithme suivant teste si $x_D = x_{D'}$.

Test d'égalité

- Choisir $\alpha \in W_D$, $\alpha \neq 0$; soit $E = (\alpha) + 3D_0 - D$.
  E est effectif de degré $2d_0$.
- Calculer $H^0\big(\mathcal{L}^{\otimes 2}(-D - D' - E)\big) = \mu(\alpha \otimes W_{D'})$.

Test d'égalité

Soient x_D et x'_D deux points de la jacobienne, représentés par W_D et $W_{D'}$. L'algorithme suivant teste si $x_D = x_{D'}$.

Test d'égalité

- Choisir $\alpha \in W_D$, $\alpha \neq 0$; soit $E = (\alpha) + 3D_0 - D$.
  E est effectif de degré $2d_0$.
- Calculer $H^0\big(\mathcal{L}^{\otimes 2}(-D - D' - E)\big) = \mu(\alpha \otimes W_{D'})$.
- Calculer $W_{E+D'}$

$$= \left\{ s \in V \;\middle|\; \forall t \in W_D,\ \mu(s \otimes t) \in H^0\big(\mathcal{L}^{\otimes 2}(-D-D'-E)\big) \right\}.$$

Test d'égalité

Soient x_D et x'_D deux points de la jacobienne, représentés par W_D et $W_{D'}$. L'algorithme suivant teste si $x_D = x_{D'}$.

Test d'égalité

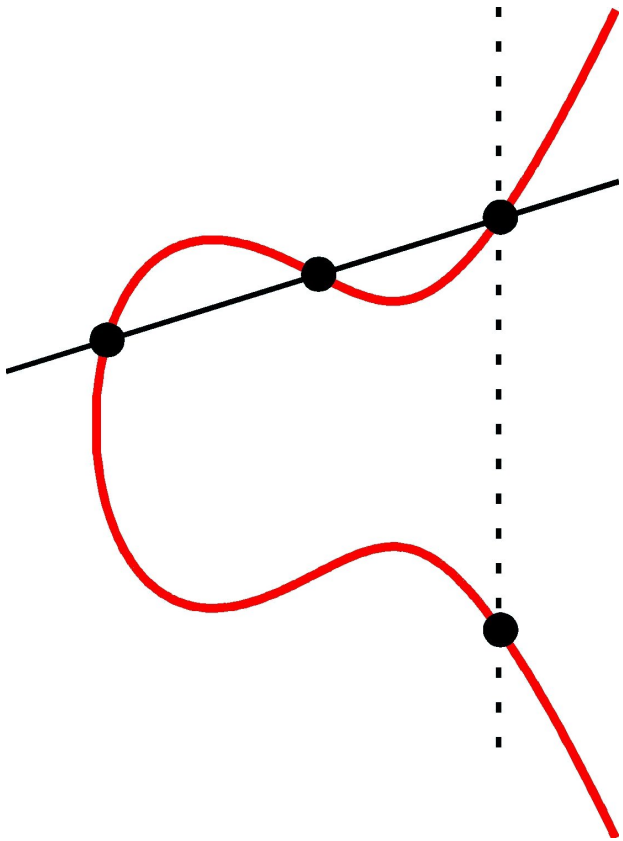
- Choisir $\alpha \in W_D$, $\alpha \neq 0$; soit $E = (\alpha) + 3D_0 - D$.
  E est effectif de degré $2d_0$.
- Calculer $H^0\big(\mathcal{L}^{\otimes 2}(-D - D' - E)\big) = \mu(\alpha \otimes W_{D'})$.
- Calculer $W_{E+D'}$
  $$= \left\{ s \in V \;\middle|\; \forall t \in W_D,\ \mu(s \otimes t) \in H^0\big(\mathcal{L}^{\otimes 2}(-D-D'-E)\big) \right\}.$$
- $x_D = x_{D'} \iff W_{E+D'} \neq 0$.
  ($W_{E+D'}$ est alors de dimension 1.)

“Corde” (Addition opposée)

Soient x_D et x'_D deux points de la jacobienne, représentés par W_D et $W_{D'}$. L'algorithme suivant calcule W_E tel que $x_D + x_{D'} + x_E = 0$.

“Corde” (Addition opposée)

Soient x_D et x'_D deux points de la jacobienne, représentés par W_D et $W_{D'}$. L'algorithme suivant calcule W_E tel que $x_D + x_{D'} + x_E = 0$.



“Corde” (Addition opposée)

Soient x_D et x'_D deux points de la jacobienne, représentés par W_D et $W_{D'}$. L'algorithme suivant calcule W_E tel que $x_D + x_{D'} + x_E = 0$.

Corde

- Calculer $W_{D+D'}$ à l'aide de l'algorithme d'addition de diviseurs.

“Corde” (Addition opposée)

Soient x_D et x'_D deux points de la jacobienne, représentés par W_D et $W_{D'}$. L'algorithme suivant calcule W_E tel que $x_D + x_{D'} + x_E = 0$.

Corde

- Calculer $W_{D+D'}$ à l'aide de l'algorithme d'addition de diviseurs.
- Choisir $\alpha \in W_{D+D'}$, $\alpha \neq 0$; soit $E = (\alpha) + 3D_0 - D - D'$. E est effectif de degré d_0.

“Corde” (Addition opposée)

Soient x_D et x'_D deux points de la jacobienne, représentés par W_D et $W_{D'}$. L'algorithme suivant calcule W_E tel que $x_D + x_{D'} + x_E = 0$.

Corde

- Calculer $W_{D+D'}$ à l'aide de l'algorithme d'addition de diviseurs.
- Choisir $\alpha \in W_{D+D'}$, $\alpha \neq 0$; soit $E = (\alpha) + 3D_0 - D - D'$. E est effectif de degré d_0.
- Calculer $H^0\big(\mathcal{L}^{\otimes 2}(-D - D' - E)\big) = \mu\big(\alpha \otimes H^0(\mathcal{L})\big)$.

“Corde” (Addition opposée)

Soient x_D et x'_D deux points de la jacobienne, représentés par W_D et $W_{D'}$. L'algorithme suivant calcule W_E tel que $x_D + x_{D'} + x_E = 0$.

Corde

- Calculer $W_{D+D'}$ à l'aide de l'algorithme d'addition de diviseurs.
- Choisir $\alpha \in W_{D+D'}$, $\alpha \neq 0$; soit $E = (\alpha) + 3D_0 - D - D'$. E est effectif de degré d_0.
- Calculer $H^0\big(\mathcal{L}^{\otimes 2}(-D-D'-E)\big) = \mu\big(\alpha \otimes H^0(\mathcal{L})\big)$.
- Calculer W_E

$$= \left\{ s \in V \;\middle|\; \forall t \in W_{D+D'},\ \mu(s \otimes t) \in H^0\big(\mathcal{L}^{\otimes 2}(-D-D'-E)\big) \right\}.$$

Opposition

Soit x_D un point de la jacobienne, représenté par W_D.
L'algorithme suivant calcule W_{D^-} tel que $x_{D^-} = -x_D$.

Opposition

Soit x_D un point de la jacobienne, représenté par W_D.
L'algorithme suivant calcule W_{D^-} tel que $x_{D^-} = -x_D$.

Opposition

Appliquer l'algorithme "corde" à D et à D_0.

Addition et soustraction, bilan

Pour l'addition, appliquer l'algorithme "corde", puis opposer le résultat.
Pour la soustraction, opposer le premier membre, puis appliquer l'algorithme "corde".

Addition et soustraction, bilan

Pour l'addition, appliquer l'algorithme "corde", puis opposer le résultat.
Pour la soustraction, opposer le premier membre, puis appliquer l'algorithme "corde".

On ne fait que de l'algèbre linéaire sur des espaces de dimension $O(g)$ et $O(g^2)$, d'où une complexité de $O(g^4)$ opérations dans K.