Implémentation d'algorithmes pour la résolution du problème du logarithme discret dans les courbes elliptiques sur des corps finis

Salim Rostam

Sous la direction de Claus Diem
Universität Leipzig (Allemagne)

Du 13 mai au 5 juillet 2013

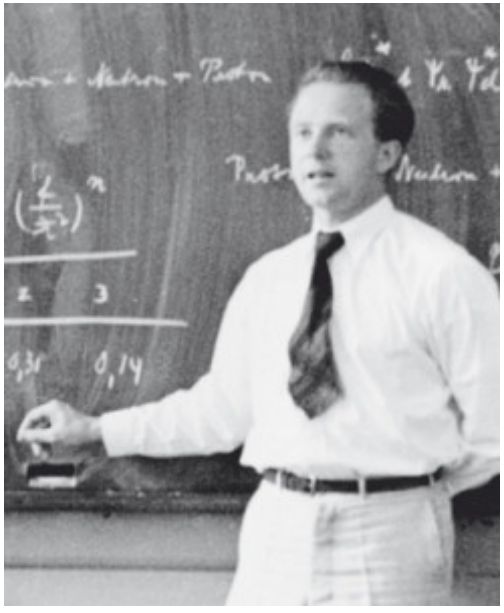

Danemark
Mer du Nord
Mer Baltique
Hambourg
Brême
Pays-
Bas
Pologne
Hanovre
BERLIN
ALLEMAGNE
Leipzig
Cologne
Dresde
Bonn
République
tchèque
Francfort
Luxembourg
Stuggart
France
Munich
Suisse
Autriche


UNIVERSITÄT LEIPZIG

Leibniz (droit)

Möbius

Klein

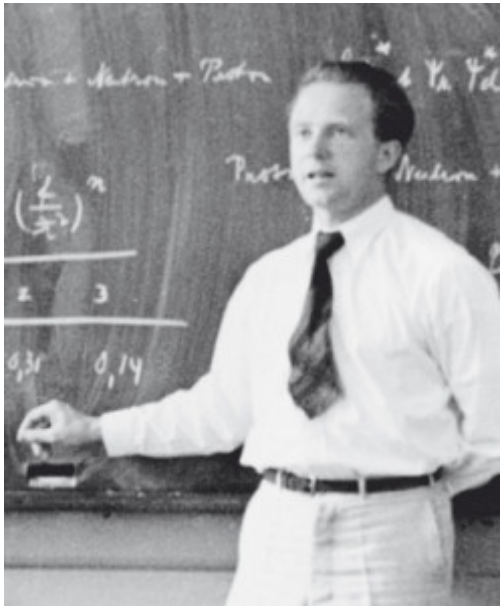


Heisenberg

Leibniz (droit)

Möbius

Klein



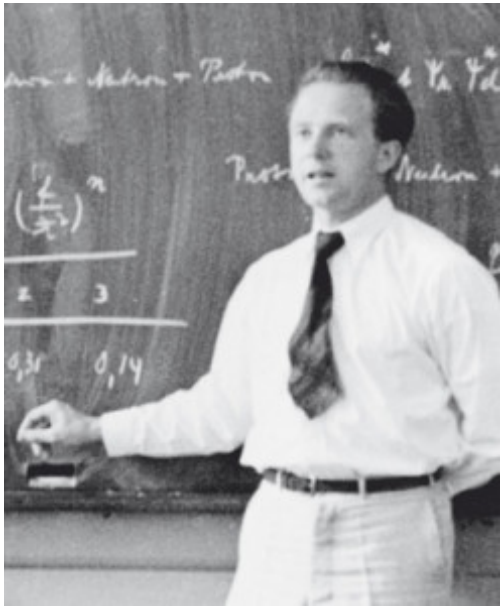
Heisenberg

Merkel (physique)

Leibniz (droit)

Möbius

Klein



Heisenberg

Merkel (physique)

Rostam

Qu'est-ce que le problème du logarithme discret ?

Qu'est-ce que le problème du logarithme discret ?

Trouver $\ell \in \mathbb{Z}$ dans l'équation :

$$y = x^{\ell}$$

pour $x, y \in G$.

Résolution générique

Soit G un groupe fini d'ordre N et soient $y \in \langle x \rangle$.

Résolution générique

Soit G un groupe fini d'ordre N et soient $y \in \langle x \rangle$.

- $1, x, x^2, \ldots$

Résolution générique

Soit G un groupe fini d'ordre N et soient $y \in \langle x \rangle$.

- $1, x, x^2, \ldots \rightarrow \mathcal{O}(N)$

Résolution générique

Soit G un groupe fini d'ordre N et soient $y \in \langle x \rangle$.

- $1, x, x^2, \ldots \rightarrow \mathcal{O}(N)$
- Algorithme « baby-step giant-step »

Résolution générique

Soit G un groupe fini d'ordre N et soient $y \in \langle x \rangle$.

- $1, x, x^2, \ldots \rightarrow \mathcal{O}(N)$
- Algorithme « baby-step giant-step »

Idée : $y = x^{\ell} = x^{nq+r}$ avec $n := \lceil \sqrt{N} \rceil$

Résolution générique

Soit G un groupe fini d'ordre N et soient $y \in \langle x \rangle$.

- $1, x, x^2, \ldots \rightarrow \mathcal{O}(N)$
- Algorithme « baby-step giant-step »

Idée : $y = x^{\ell} = x^{nq+r}$ avec $n := \lceil \sqrt{N} \rceil$

- $yx^{-a}, 0 \leqslant a < \sqrt{N}$

Résolution générique

Soit G un groupe fini d'ordre N et soient $y \in \langle x \rangle$.

- $1, x, x^2, \ldots \rightarrow \mathcal{O}(N)$
- Algorithme « baby-step giant-step »

  Idée : $y = x^{\ell} = x^{nq+r}$ avec $n := \lceil \sqrt{N} \rceil$
  - $yx^{-a}, 0 \leqslant a < \sqrt{N}$
  - $(x^n)^b, 0 \leqslant b < \sqrt{N}$

Résolution générique

Soit G un groupe fini d'ordre N et soient $y \in \langle x \rangle$.

- $1, x, x^2, \ldots \rightarrow \mathcal{O}(N)$
- Algorithme « baby-step giant-step »

  Idée : $y = x^{\ell} = x^{nq+r}$ avec $n := \lceil \sqrt{N} \rceil$
  - $yx^{-a}, 0 \leqslant a < \sqrt{N}$
  - $(x^n)^b, 0 \leqslant b < \sqrt{N}$

  $\rightarrow \widetilde{\mathcal{O}}(\sqrt{N})$

Résolution générique

Soit G un groupe fini d'ordre N et soient $y \in \langle x \rangle$.

- $1, x, x^2, \ldots \rightarrow \mathcal{O}(N)$
- Algorithme « baby-step giant-step »

  Idée : $y = x^{\ell} = x^{nq+r}$ avec $n := \lceil \sqrt{N} \rceil$
  - $yx^{-a}, 0 \leqslant a < \sqrt{N}$
  - $(x^n)^b, 0 \leqslant b < \sqrt{N}$

  $\rightarrow \widetilde{\mathcal{O}}(\sqrt{N})$

Remarque

Meilleure complexité connue pour un groupe *générique*.

Résolution générique

Soit G un groupe fini d'ordre N et soient $y \in \langle x \rangle$.

- $1, x, x^2, \ldots \rightarrow \mathcal{O}(N)$
- Algorithme « baby-step giant-step »

  Idée : $y = x^{\ell} = x^{nq+r}$ avec $n := \lceil \sqrt{N} \rceil$
  - $yx^{-a}, 0 \leqslant a < \sqrt{N}$
  - $(x^n)^b, 0 \leqslant b < \sqrt{N}$

  $\rightarrow \tilde{\mathcal{O}}(\sqrt{N})$

Remarque

Meilleure complexité connue pour un groupe *générique*. Pour $n \geqslant 2$ fixé et G le groupe des points $\mathbb{F}_{q^n}$-rationnels d'une courbe elliptique ($\#G \simeq q^n$)

Résolution générique

Soit G un groupe fini d'ordre N et soient $y \in \langle x \rangle$.

- $1, x, x^2, \ldots \rightarrow \mathcal{O}(N)$
- Algorithme « baby-step giant-step »

  Idée : $y = x^{\ell} = x^{nq+r}$ avec $n := \lceil \sqrt{N} \rceil$
  - $yx^{-a}, 0 \leqslant a < \sqrt{N}$
  - $(x^n)^b, 0 \leqslant b < \sqrt{N}$

  $\rightarrow \widetilde{\mathcal{O}}(\sqrt{N})$

Remarque

Meilleure complexité connue pour un groupe *générique*. Pour $n \geqslant 2$ fixé et G le groupe des points $\mathbb{F}_{q^n}$-rationnels d'une courbe elliptique $(\#G \simeq q^n) \rightarrow \widetilde{\mathcal{O}}(q^{2-\frac{2}{n}})$.

Corps de fonctions

Définition

Soit F une extension de corps de k.

Corps de fonctions

Définition

Soit F une extension de corps de k. On dit que $F|k$ est un *corps de fonctions algébrique en une variable*

Corps de fonctions

Définition

Soit F une extension de corps de k. On dit que $F|k$ est un *corps de fonctions algébrique en une variable* s'il existe $x \in F$ transcendant sur k tel que $F/k(x)$ est une extension finie.

Corps de fonctions

Définition

Soit F une extension de corps de k. On dit que $F|k$ est un *corps de fonctions algébrique en une variable* s'il existe $x \in F$ transcendant sur k tel que $F/k(x)$ est une extension finie.

Remarque

On supposera toujours k parfait et algébriquement clos dans F.

Corps de fonctions

Définition

Soit F une extension de corps de k. On dit que $F|k$ est un *corps de fonctions algébrique en une variable* s'il existe $x \in F$ transcendant sur k tel que $F/k(x)$ est une extension finie.

Remarque

On supposera toujours k parfait et algébriquement clos dans F.

Exemple

Le corps des fractions rationnelles $k(X)|k$.

Anneau de valuation

Définition

Un *anneau de valuation* de $F|k$ est un sous-anneau $\mathcal{O}$ de F tel que :

Anneau de valuation

Définition

Un *anneau de valuation* de $F|k$ est un sous-anneau $\mathcal{O}$ de F tel que :

- $k \subsetneq \mathcal{O} \subsetneq F$;

Anneau de valuation

Définition

Un *anneau de valuation* de $F|k$ est un sous-anneau $\mathcal{O}$ de F tel que :

- $k \subsetneq \mathcal{O} \subsetneq F$;
- $\forall z \in F^*, z \in \mathcal{O}$ ou $z^{-1} \in \mathcal{O}$.

Anneau de valuation

Définition

Un *anneau de valuation* de $F|k$ est un sous-anneau $\mathcal{O}$ de F tel que :

- $k \subsetneq \mathcal{O} \subsetneq F$;
- $\forall z \in F^*, z \in \mathcal{O}$ ou $z^{-1} \in \mathcal{O}$.

Exemple

$F := k(X), \mathcal{O} := \{f \in F : \deg f \leqslant 0\}$.

Anneau de valuation

Définition

Un *anneau de valuation* de $F|k$ est un sous-anneau $\mathcal{O}$ de F tel que :

- $k \subsetneq \mathcal{O} \subsetneq F$;
- $\forall z \in F^*, z \in \mathcal{O}$ ou $z^{-1} \in \mathcal{O}$.

Exemple

$F := k(X), \mathcal{O} := \{f \in F : \deg f \leqslant 0\}$.

Propriété

Un anneau de valuation est un anneau *local*.

Place

Place

Définition

Une *place* de $F|k$ est l'unique idéal maximal d'un anneau de valuation de $F|k$.

Place

Définition

Une *place* de $F|k$ est l'unique idéal maximal d'un anneau de valuation de $F|k$.

Propriété

Pour $P \in \mathbb{P}_F$, il existe un unique anneau de valuation $\mathcal{O}_P$ d'(unique) idéal maximal P.

Place

Définition

Une *place* de $F|k$ est l'unique idéal maximal d'un anneau de valuation de $F|k$.

Propriété

Pour $P \in \mathbb{P}_F$, il existe un unique anneau de valuation $\mathcal{O}_P$ d'(unique) idéal maximal P.

Proposition

Soit $P \in \mathbb{P}_F$. Les idéaux non nuls de $\mathcal{O}_P$ sont de la forme P^n, $n \in \mathbb{N}$.

Groupe des diviseurs

Groupe des diviseurs

Définition

Un *diviseur* sur F est une somme formelle

$$D := \sum_{P \in \mathbb{P}_F} n_P P$$

Groupe des diviseurs

Définition

Un *diviseur* sur F est une somme formelle

$$D := \sum_{P \in \mathbb{P}_F} n_P P$$

avec $\mathrm{Supp}(D) := \{P \in \mathbb{P}_F : n_P \neq 0\}$ fini.

Groupe des diviseurs

Définition

Un *diviseur* sur F est une somme formelle

$$D := \sum_{P \in \mathbb{P}_F} n_P P$$

avec $\mathrm{Supp}(D) := \{P \in \mathbb{P}_F : n_P \neq 0\}$ fini.

Remarque

$\mathrm{Div}(F)$ est le groupe libre abélien engendré par les places de F.

Anneau de Dedekind

Anneau de Dedekind

Définition

Soit $\mathcal{O}$ un sous-anneau de F. On dit que $\mathcal{O}$ est un *anneau de Dedekind*

Anneau de Dedekind

Définition

Soit $\mathcal{O}$ un sous-anneau de F. On dit que $\mathcal{O}$ est un *anneau de Dedekind* si tout idéal propre non nul de $\mathcal{O}$ se décompose en un unique produit d'idéaux premiers,

Anneau de Dedekind

Définition

Soit $\mathcal{O}$ un sous-anneau de F. On dit que $\mathcal{O}$ est un *anneau de Dedekind* si tout idéal propre non nul de $\mathcal{O}$ se décompose en un unique produit d'idéaux premiers, à l'ordre des facteurs près.

Anneau de Dedekind

Définition

Soit $\mathcal{O}$ un sous-anneau de F. On dit que $\mathcal{O}$ est un *anneau de Dedekind* si tout idéal propre non nul de $\mathcal{O}$ se décompose en un unique produit d'idéaux premiers, à l'ordre des facteurs près.

Remarque

Si I est un idéal propre non nul de $\mathcal{O}$ anneau de Dedekind alors $I = \prod_{\mathfrak{p}} \mathfrak{p}^{\nu_{\mathfrak{p}}}$ avec $\nu_{\mathfrak{p}} \in \mathbb{N}$ presque tous nuls.

Idéal fractionnaire

Définition

Soit $\mathcal{O}$ un anneau de Dedekind.

Idéal fractionnaire

Définition

Soit $\mathcal{O}$ un anneau de Dedekind. L'ensemble $\mathfrak{J}_{\mathcal{O}}$ des *idéaux fractionnaires* de $\mathcal{O}$ est le groupe libre abélien engendré par les idéaux premiers non nuls de $\mathcal{O}$.

Idéal fractionnaire

Définition

Soit $\mathcal{O}$ un anneau de Dedekind. L'ensemble $\mathfrak{J}_{\mathcal{O}}$ des *idéaux fractionnaires* de $\mathcal{O}$ est le groupe libre abélien engendré par les idéaux premiers non nuls de $\mathcal{O}$.

Remarque

Un idéal fractionnaire s'écrit donc de manière unique $\prod_{\mathfrak{p}} \mathfrak{p}^{\nu_{\mathfrak{p}}}$ avec $\nu_{\mathfrak{p}} \in \mathbb{Z}$ presque tous nuls.

Rappels

Soit $x \in F|k$ un élément transcendant ; F est une extension finie de $k(x)$.

Rappels

Soit $x \in F|k$ un élément transcendant ; F est une extension finie de $k(x)$.

Définition

$f \in F$ est *entier* sur $k[x]$ si $\Pi_{k(x),f} \in k[x][T]$.

Rappels

Soit $x \in F|k$ un élément transcendant ; F est une extension finie de $k(x)$.

Définition

$f \in F$ est *entier* sur $k[x]$ si $\Pi_{k(x),f} \in k[x][T]$.

Définition

$A \subseteq F$, la *fermeture intégrale* de A dans F est

$$\overline{A}^F := \{z \in F : z \text{ est entier sur } A\}.$$

Idée de la correspondance

Soit $D := \sum n_P P$ un diviseur.

Idée de la correspondance

Soit $D := \sum n_P P$ un diviseur.

$$\forall P, P \subseteq \mathcal{O}_P$$

Idée de la correspondance

Soit $D := \sum n_P P$ un diviseur.

$$\forall P, P \subseteq \mathcal{O}_P$$
$$\forall P, \Phi(P) \subseteq \mathcal{O}$$

Idée de la correspondance

Soit $D := \sum n_P P$ un diviseur.

$$\forall P, P \subseteq \mathcal{O}_P$$
$$\forall P, \Phi(P) \subseteq \mathcal{O}$$
$$\prod \Phi(P)^{n_P} \in \mathfrak{J}_{\mathcal{O}}$$

Idée de la correspondance

Soit $D := \sum n_P P$ un diviseur.

$$\forall P, P \subseteq \mathcal{O}_P$$
$$\forall P, \Phi(P) \subseteq \mathcal{O}$$
$$\prod \Phi(P)^{n_P} \in \mathfrak{J}_{\mathcal{O}}$$
$$\mathcal{O} \stackrel{?}{:=} \langle \cup \mathcal{O}_P \rangle$$

Idée de la correspondance

Soit $D := \sum n_P P$ un diviseur.

$$\forall P, P \subseteq \mathcal{O}_P$$
$$\forall P, \Phi(P) \subseteq \mathcal{O}$$
$$\prod \Phi(P)^{n_P} \in \mathfrak{J}_{\mathcal{O}}$$
$$\mathcal{O} \stackrel{?}{:=} \langle \cup \mathcal{O}_P \rangle \rightsquigarrow \mathcal{O} = F$$

Idée de la correspondance

Soit $D := \sum n_P P$ un diviseur.

$$\forall P, P \subseteq \mathcal{O}_P$$
$$\forall P, \Phi(P) \subseteq \mathcal{O}$$
$$\prod \Phi(P)^{n_P} \in \mathfrak{J}_{\mathcal{O}}$$
$$\mathcal{O} \stackrel{?}{:=} \langle \cup \mathcal{O}_P \rangle \rightsquigarrow \mathcal{O} = F$$
$$\mathcal{O} \stackrel{?}{:=} \cap \mathcal{O}_P$$

Idée de la correspondance

Soit $D := \sum n_P P$ un diviseur.

$$\forall P, P \subseteq \mathcal{O}_P$$
$$\forall P, \Phi(P) \subseteq \mathcal{O}$$
$$\prod \Phi(P)^{n_P} \in \mathfrak{J}_{\mathcal{O}}$$
$$\mathcal{O} \stackrel{?}{:=} \langle \cup \mathcal{O}_P \rangle \rightsquigarrow \mathcal{O} = F$$
$$\mathcal{O} \stackrel{?}{:=} \cap \mathcal{O}_P \rightsquigarrow \text{Oui !}$$

Ordres maximaux

Soit $x \in F|k$ transcendant.

Ordres maximaux

Soit $x \in F|k$ transcendant.

Définition

On définit l'*ordre fini maximal* par :

Ordres maximaux

Soit $x \in F|k$ transcendant.

Définition

On définit l'*ordre fini maximal* par :

$$\mathcal{O}_F := \bigcap_{x \in \mathcal{O}_P} \mathcal{O}_P$$

Ordres maximaux

Soit $x \in F|k$ transcendant.

Définition

On définit l'*ordre fini maximal* par :

$$\mathcal{O}_F := \bigcap_{x \in \mathcal{O}_P} \mathcal{O}_P$$

ainsi que l'*ordre infini maximal* par :

Ordres maximaux

Soit $x \in F|k$ transcendant.

Définition

On définit l'*ordre fini maximal* par :

$$\mathcal{O}_F := \bigcap_{x \in \mathcal{O}_P} \mathcal{O}_P$$

ainsi que l'*ordre infini maximal* par :

$$\mathcal{O}_F^{\infty} = \bigcap_{x \notin \mathcal{O}_P} \mathcal{O}_P$$

Ordres maximaux

Soit $x \in F|k$ transcendant.

Définition

On définit l'*ordre fini maximal* par :

$$\mathcal{O}_F := \bigcap_{x \in \mathcal{O}_P} \mathcal{O}_P$$

ainsi que l'*ordre infini maximal* par :

$$\mathcal{O}_F^\infty = \bigcap_{x \notin \mathcal{O}_P} \mathcal{O}_P$$

Proposition

$\mathcal{O}_F$ et $\mathcal{O}_F^\infty$ sont des anneaux de Dedekind.

Ordres maximaux

Théorème

- $\mathcal{O}_F = \overline{k[x]}^F$
- $\mathcal{O}_F^\infty = \overline{k[\frac{1}{x}]_{\langle \frac{1}{x} \rangle}}^F$

Ordres maximaux

Théorème

- $\mathcal{O}_F = \overline{k[x]}^F$
- $\mathcal{O}_F^\infty = \overline{k[\frac{1}{x}]_{\langle \frac{1}{x} \rangle}}^F$

Remarque (corps de nombres)

Ordres maximaux

Théorème

- $\mathcal{O}_F = \overline{k[x]}^F$
- $\mathcal{O}_F^\infty = \overline{k[\frac{1}{x}]_{\langle \frac{1}{x} \rangle}}^F$

Remarque (corps de nombres)

- $K/\mathbb{Q}$ finie $\rightsquigarrow$ $F/k(x)$ finie

Ordres maximaux

Théorème

- $\mathcal{O}_F = \overline{k[x]}^F$
- $\mathcal{O}_F^\infty = \overline{k[\frac{1}{x}]_{\langle \frac{1}{x} \rangle}}^F$

Remarque (corps de nombres)

- $K/\mathbb{Q}$ finie $\rightsquigarrow$ $F/k(x)$ finie
- $\mathbb{Q} = \mathrm{Frac}(\mathbb{Z}) \rightsquigarrow k(x) = \mathrm{Frac}(k[x])$

Ordres maximaux

Théorème

- $\mathcal{O}_F = \overline{k[x]}^F$
- $\mathcal{O}_F^\infty = \overline{k[\frac{1}{x}]_{\langle \frac{1}{x} \rangle}}^F$

Remarque (corps de nombres)

- $K/\mathbb{Q}$ finie $\rightsquigarrow$ $F/k(x)$ finie
- $\mathbb{Q} = \mathrm{Frac}(\mathbb{Z}) \rightsquigarrow k(x) = \mathrm{Frac}(k[x])$
- $\mathcal{O}_K = \overline{\mathbb{Z}}^K \rightsquigarrow \mathcal{O}_F = \overline{k[x]}^F$

Bijections fondamentales

$$D := \sum n_P P \mapsto \prod \Phi(P)^{n_P}$$

Bijections fondamentales

$$D := \sum n_P P \mapsto \prod \Phi(P)^{n_P}$$

Théorème

$$\{P \in \mathbb{P}_F : x \in \mathcal{O}_P\} \simeq \{\langle 0 \rangle \subsetneq \mathfrak{p} \subseteq \mathcal{O}_F\}$$

Bijections fondamentales

$$D := \sum n_P P \mapsto \prod \Phi(P)^{n_P}$$

Théorème

$$\{P \in \mathbb{P}_F : x \in \mathcal{O}_P\} \simeq \{\langle 0 \rangle \subsetneq \mathfrak{p} \subseteq \mathcal{O}_F\}$$
$$P \mapsto P \cap \mathcal{O}_F$$

Bijections fondamentales

$$D := \sum n_P P \mapsto \prod \Phi(P)^{n_P}$$

Théorème

$$\{P \in \mathbb{P}_F : x \in \mathcal{O}_P\} \simeq \{\langle 0 \rangle \subsetneq \mathfrak{p} \subseteq \mathcal{O}_F\}$$
$$P \mapsto P \cap \mathcal{O}_F$$

Théorème

$$\{P \in \mathbb{P}_F : x \notin \mathcal{O}_P\} \simeq \{\langle 0 \rangle \subsetneq \mathfrak{p} \subseteq \mathcal{O}_F^\infty\}$$
$$P \mapsto P \cap \mathcal{O}_F^\infty$$

Correspondance

Définition

Soit $D := \sum n_P P \in \mathrm{Div}(F)$.

Correspondance

Définition

Soit $D := \sum n_P P \in \mathrm{Div}(F)$. On définit la *partie finie* de D par :

Correspondance

Définition

Soit $D := \sum n_P P \in \mathrm{Div}(F)$. On définit la *partie finie* de D par :

$$D_0 := \prod_{x \in \mathcal{O}_P} (P \cap \mathcal{O}_F)^{n_P} \in \mathfrak{J}_{\mathcal{O}_F}$$

Définition

Soit $D := \sum n_P P \in \mathrm{Div}(F)$. On définit la *partie finie* de D par :

$$D_0 := \prod_{x \in \mathcal{O}_P} (P \cap \mathcal{O}_F)^{n_P} \in \mathfrak{J}_{\mathcal{O}_F}$$

ainsi que la *partie infinie* de D par :

$$D_\infty := \prod_{x \notin \mathcal{O}_P} (P \cap \mathcal{O}_F^\infty)^{n_P} \in \mathfrak{J}_{\mathcal{O}_F^\infty}.$$

Correspondance

Définition

Soit $D := \sum n_P P \in \mathrm{Div}(F)$. On définit la *partie finie* de D par :

$$D_0 := \prod_{x \in \mathcal{O}_P} (P \cap \mathcal{O}_F)^{n_P} \in \mathfrak{J}_{\mathcal{O}_F}$$

ainsi que la *partie infinie* de D par :

$$D_\infty := \prod_{x \notin \mathcal{O}_P} (P \cap \mathcal{O}_F^\infty)^{n_P} \in \mathfrak{J}_{\mathcal{O}_F^\infty}.$$

Théorème de correspondance

$(\mathfrak{D}_F)^{-1} : D \mapsto (D_0, D_\infty)$ est un isomorphisme.

Définition

$F'|k'$ est une *extension finie* de $F|k$ si :

Définition

$F'|k'$ est une *extension finie* de $F|k$ si :

- $k \subseteq k'$ et $F \subseteq F'$;

Définition

$F'|k'$ est une *extension finie* de $F|k$ si :

- $k \subseteq k'$ et $F \subseteq F'$;
- $[k' : k] < \infty$.

Définition

$F'|k'$ est une *extension finie* de $F|k$ si :

- $k \subseteq k'$ et $F \subseteq F'$;
- $[k' : k] < \infty$.

Remarque

On a automatiquement $[F' : F] < \infty$.

Places

Définition

$P' \in \mathbb{P}_{F'}$ *divise* $P \in \mathbb{P}_F$ si $P' \supseteq P$.

Places

Définition

$P' \in \mathbb{P}_{F'}$ *divise* $P \in \mathbb{P}_F$ si $P' \supseteq P$.

Définition

- $e_{P'|P} := \max\{e \in \mathbb{N}^* : P'^e \supseteq P\}$ est l'*indice de ramification*.

Places

Définition

$P' \in \mathbb{P}_{F'}$ *divise* $P \in \mathbb{P}_F$ si $P' \supseteq P$.

Définition

- $e_{P'|P} := \max\{e \in \mathbb{N}^* : P'^e \supseteq P\}$ est l'*indice de ramification*.
- $f_{P'|P} := [\mathcal{O}_{P'}/P' : \mathcal{O}_P/P]$ est le *degré relatif*.

Places

Définition

$P' \in \mathbb{P}_{F'}$ *divise* $P \in \mathbb{P}_F$ si $P' \supseteq P$.

Définition

- $e_{P'|P} := \max\{e \in \mathbb{N}^* : P'^e \supseteq P\}$ est l'*indice de ramification*.
- $f_{P'|P} := [\mathcal{O}_{P'}/P' : \mathcal{O}_P/P]$ est le *degré relatif*.

Théorème

Soit $P \in \mathbb{P}_F$.

Places

Définition

$P' \in \mathbb{P}_{F'}$ *divise* $P \in \mathbb{P}_F$ si $P' \supseteq P$.

Définition

- $e_{P'|P} := \max\{e \in \mathbb{N}^* : P'^e \supseteq P\}$ est l'*indice de ramification*.
- $f_{P'|P} := [\mathcal{O}_{P'}/P' : \mathcal{O}_P/P]$ est le *degré relatif*.

Théorème

Soit $P \in \mathbb{P}_F$. Alors $\sum_{P'|P} e_{P'|P} f_{P'|P} = [F' : F]$.

$F'|k'$ extension finie de $F|k$.

Définition

Soit $\mathfrak{p}$ un idéal premier non nul de $\mathcal{O}_F$.

$F'|k'$ extension finie de $F|k$.

Définition

Soit $\mathfrak{p}$ un idéal premier non nul de $\mathcal{O}_F$.

$$\langle \mathfrak{p} \rangle_{\mathcal{O}_{F'}} =: \prod \mathfrak{p}'^{e_{\mathfrak{p}'|\mathfrak{p}}}$$

$F'|k'$ extension finie de $F|k$.

Définition

Soit $\mathfrak{p}$ un idéal premier non nul de $\mathcal{O}_F$.

$$\langle \mathfrak{p} \rangle_{\mathcal{O}_{F'}} =: \prod \mathfrak{p}'^{e_{\mathfrak{p}'|\mathfrak{p}}}$$

$$f_{\mathfrak{p}'|\mathfrak{p}} := [\mathcal{O}_{F'}/\mathfrak{p}' : \mathcal{O}_F/\mathfrak{p}]$$

$F'|k'$ extension finie de $F|k$.

Définition

Soit $\mathfrak{p}$ un idéal premier non nul de $\mathcal{O}_F$.

$$\langle \mathfrak{p} \rangle_{\mathcal{O}_{F'}} =: \prod \mathfrak{p}'^{e_{\mathfrak{p}'|\mathfrak{p}}}$$

$$f_{\mathfrak{p}'|\mathfrak{p}} := [\mathcal{O}_{F'}/\mathfrak{p}' : \mathcal{O}_F/\mathfrak{p}]$$

Théorème

Si F'/F est séparable alors $\sum_{\mathfrak{p}'} e_{\mathfrak{p}'|\mathfrak{p}} f_{\mathfrak{p}'|\mathfrak{p}} = [F' : F]$.

Plus loin dans la correspondance

$F'|k'$ extension finie de $F|k$, $P \in \mathbb{P}_F$ et $P' \in \mathbb{P}_{F'}$ (telles que $x \in \mathcal{O}_P, \mathcal{O}_{P'}$).

Plus loin dans la correspondance

$F'|k'$ extension finie de $F|k$, $P \in \mathbb{P}_F$ et $P' \in \mathbb{P}_{F'}$ (telles que $x \in \mathcal{O}_P, \mathcal{O}_{P'}$). $\mathfrak{p} := P \cap \mathcal{O}_F, \mathfrak{p}' := P' \cap \mathcal{O}_{F'}$.

Plus loin dans la correspondance

$F'|k'$ extension finie de $F|k$, $P \in \mathbb{P}_F$ et $P' \in \mathbb{P}_{F'}$ (telles que $x \in \mathcal{O}_P, \mathcal{O}_{P'}$). $\mathfrak{p} := P \cap \mathcal{O}_F, \mathfrak{p}' := P' \cap \mathcal{O}_{F'}$.

Proposition

$P'|P$ $\underline{\text{ssi}}$ $\mathfrak{p}'|\mathfrak{p}$.

Plus loin dans la correspondance

$F'|k'$ extension finie de $F|k$, $P \in \mathbb{P}_F$ et $P' \in \mathbb{P}_{F'}$ (telles que $x \in \mathcal{O}_P, \mathcal{O}_{P'}$). $\mathfrak{p} := P \cap \mathcal{O}_F, \mathfrak{p}' := P' \cap \mathcal{O}_{F'}$.

Proposition

$P'|P$ $\underline{\text{ssi}}$ $\mathfrak{p}'|\mathfrak{p}$.

Théorème

On suppose que $P'|P$:

Plus loin dans la correspondance

$F'|k'$ extension finie de $F|k$, $P \in \mathbb{P}_F$ et $P' \in \mathbb{P}_{F'}$ (telles que $x \in \mathcal{O}_P, \mathcal{O}_{P'}$). $\mathfrak{p} := P \cap \mathcal{O}_F, \mathfrak{p}' := P' \cap \mathcal{O}_{F'}$.

Proposition

$P'|P$ $\underline{\text{ssi}}$ $\mathfrak{p}'|\mathfrak{p}$.

Théorème

On suppose que $P'|P$:

- $f_{P'|P} = f_{\mathfrak{p}'|\mathfrak{p}}$;

Plus loin dans la correspondance

$F'|k'$ extension finie de $F|k$, $P \in \mathbb{P}_F$ et $P' \in \mathbb{P}_{F'}$ (telles que $x \in \mathcal{O}_P, \mathcal{O}_{P'}$). $\mathfrak{p} := P \cap \mathcal{O}_F, \mathfrak{p}' := P' \cap \mathcal{O}_{F'}$.

Proposition

$P'|P$ $\underline{\text{ssi}}$ $\mathfrak{p}'|\mathfrak{p}$.

Théorème

On suppose que $P'|P$:

- $f_{P'|P} = f_{\mathfrak{p}'|\mathfrak{p}}$;
- si F'/F est séparable alors $e_{P'|P} = e_{\mathfrak{p}'|\mathfrak{p}}$.

Norme

Définition

$$\mathrm{N}_{F'/F}(\mathfrak{p}') := \mathfrak{p}^{f_{\mathfrak{p}'|\mathfrak{p}}}$$

Norme

Définition

$$\mathrm{N}_{F'/F}(\mathfrak{p}') := \mathfrak{p}^{f_{\mathfrak{p}'|\mathfrak{p}}} \rightsquigarrow \mathfrak{J}\mathcal{O}_{F'} \to \mathfrak{J}\mathcal{O}_F$$

Norme

Définition

$$\mathrm{N}_{F'/F}(\mathfrak{p}') := \mathfrak{p}^{f_{\mathfrak{p}'|\mathfrak{p}}} \rightsquigarrow \mathfrak{J}\mathcal{O}_{F'} \to \mathfrak{J}\mathcal{O}_F$$

$$\mathrm{N}_{F'/F}(P') := f_{P'|P} P$$

Norme

Définition

$$\mathrm{N}_{F'/F}(\mathfrak{p}') := \mathfrak{p}^{f_{\mathfrak{p}'|\mathfrak{p}}} \rightsquigarrow \mathfrak{J}\mathcal{O}_{F'} \to \mathfrak{J}\mathcal{O}_F$$

$$\mathrm{N}_{F'/F}(P') := f_{P'|P} P \rightsquigarrow \mathrm{Div}(F') \to \mathrm{Div}(F)$$

Norme

Définition

$$\mathrm{N}_{F'/F}(\mathfrak{p}') := \mathfrak{p}^{f_{\mathfrak{p}'|\mathfrak{p}}} \rightsquigarrow \mathfrak{J}\mathcal{O}_{F'} \to \mathfrak{J}\mathcal{O}_F$$

$$\mathrm{N}_{F'/F}(P') := f_{P'|P} P \rightsquigarrow \mathrm{Div}(F') \to \mathrm{Div}(F)$$

Remarques

- $\mathfrak{p} = \mathfrak{p}' \cap \mathcal{O}_F$ et $P = P' \cap F$.

Norme

Définition

$$\mathrm{N}_{F'/F}(\mathfrak{p}') := \mathfrak{p}^{f_{\mathfrak{p}'|\mathfrak{p}}} \rightsquigarrow \mathfrak{J}\mathcal{O}_{F'} \to \mathfrak{J}\mathcal{O}_F$$

$$\mathrm{N}_{F'/F}(P') := f_{P'|P} P \rightsquigarrow \mathrm{Div}(F') \to \mathrm{Div}(F)$$

Remarques

- $\mathfrak{p} = \mathfrak{p}' \cap \mathcal{O}_F$ et $P = P' \cap F$.
- Le degré relatif apparaît naturellement.

Commutativité

Théorème

$$\forall D' \in \mathrm{Div}(F'), \mathrm{N}_{F'/F}(D') = \mathfrak{D}_F(\mathrm{N}_{F'/F}(D'_0), \mathrm{N}_{F'/F}(D'_\infty)).$$

Commutativité

Théorème

$$\forall D' \in \mathrm{Div}(F'), \mathrm{N}_{F'/F}(D') = \mathfrak{D}_F(\mathrm{N}_{F'/F}(D'_0), \mathrm{N}_{F'/F}(D'_\infty)).$$

Illustration

$$\begin{array}{ccc} \mathrm{Div}(F') & & \\ \Big\downarrow{\scriptstyle \mathrm{N}_{F'/F}} & & \\ \mathrm{Div}(F) & & \end{array}$$

Commutativité

Théorème

$$\forall D' \in \mathrm{Div}(F'), \mathrm{N}_{F'/F}(D') = \mathfrak{D}_F(\mathrm{N}_{F'/F}(D'_0), \mathrm{N}_{F'/F}(D'_\infty)).$$

Illustration

$$\begin{array}{ccc} \mathrm{Div}(F') & \xrightarrow{(\mathfrak{D}_{F'})^{-1}} & \mathfrak{J}_{\mathcal{O}_{F'}} \times \mathfrak{J}_{\mathcal{O}_{F'}^\infty} \\ \Big\downarrow{\scriptstyle \mathrm{N}_{F'/F}} & & \\ \mathrm{Div}(F) & & \end{array}$$

Commutativité

Théorème

$$\forall D' \in \mathrm{Div}(F'), \mathrm{N}_{F'/F}(D') = \mathfrak{D}_F(\mathrm{N}_{F'/F}(D'_0), \mathrm{N}_{F'/F}(D'_\infty)).$$

Illustration

$$\begin{array}{ccc} \mathrm{Div}(F') & \xrightarrow{(\mathfrak{D}_{F'})^{-1}} & \mathfrak{J}\mathcal{O}_{F'} \times \mathfrak{J}\mathcal{O}_{F'}^{\infty} \\ \Big\downarrow{\scriptstyle \mathrm{N}_{F'/F}} & & \Big\downarrow{\scriptstyle \mathrm{N}_{F'/F} \times \mathrm{N}_{F'/F}} \\ \mathrm{Div}(F) & & \mathfrak{J}\mathcal{O}_F \times \mathfrak{J}\mathcal{O}_F^{\infty} \end{array}$$

Commutativité

Théorème

$$\forall D' \in \mathrm{Div}(F'), \mathrm{N}_{F'/F}(D') = \mathfrak{D}_F(\mathrm{N}_{F'/F}(D'_0), \mathrm{N}_{F'/F}(D'_\infty)).$$

Illustration

$$\begin{array}{ccc} \mathrm{Div}(F') & \xrightarrow{(\mathfrak{D}_{F'})^{-1}} & \mathfrak{J}\mathcal{O}_{F'} \times \mathfrak{J}\mathcal{O}_{F'}^{\infty} \\ \Big\downarrow{\scriptstyle \mathrm{N}_{F'/F}} & & \Big\downarrow{\scriptstyle \mathrm{N}_{F'/F} \times \mathrm{N}_{F'/F}} \\ \mathrm{Div}(F) & \xleftarrow[\mathfrak{D}_F]{} & \mathfrak{J}\mathcal{O}_F \times \mathfrak{J}\mathcal{O}_F^{\infty} \end{array}$$

Conorme

$F'|k'$ extension finie de $F|k$.

Conorme

$F'|k'$ extension finie de $F|k$.

Définition

$$\mathrm{Con}_{F'/F}(\mathfrak{p}) := \langle \mathfrak{p} \rangle_{\mathcal{O}_{F'}} = \prod_{\mathfrak{p}'|\mathfrak{p}} \mathfrak{p}'^{e_{\mathfrak{p}'|\mathfrak{p}}}$$

Conorme

$F'|k'$ extension finie de $F|k$.

Définition

$$\mathrm{Con}_{F'/F}(\mathfrak{p}) := \langle \mathfrak{p} \rangle_{\mathcal{O}_{F'}} = \prod_{\mathfrak{p}'|\mathfrak{p}} \mathfrak{p}'^{e_{\mathfrak{p}'|\mathfrak{p}}} \rightsquigarrow \mathfrak{J}\mathcal{O}_F \to \mathfrak{J}\mathcal{O}_{F'}$$

Conorme

$F'|k'$ extension finie de $F|k$.

Définition

$$\mathrm{Con}_{F'/F}(\mathfrak{p}) := \langle \mathfrak{p} \rangle_{\mathcal{O}_{F'}} = \prod_{\mathfrak{p}'|\mathfrak{p}} \mathfrak{p}'^{e_{\mathfrak{p}'|\mathfrak{p}}} \rightsquigarrow \mathfrak{J}\mathcal{O}_F \to \mathfrak{J}\mathcal{O}_{F'}$$

$$\mathrm{Con}_{F'/F}(P) := \sum_{P'|P} e_{P'|P} P'$$

Conorme

$F'|k'$ extension finie de $F|k$.

Définition

$$\mathrm{Con}_{F'/F}(\mathfrak{p}) := \langle \mathfrak{p} \rangle_{\mathcal{O}_{F'}} = \prod_{\mathfrak{p}'|\mathfrak{p}} \mathfrak{p}'^{e_{\mathfrak{p}'|\mathfrak{p}}} \rightsquigarrow \mathfrak{J}\mathcal{O}_F \to \mathfrak{J}\mathcal{O}_{F'}$$

$$\mathrm{Con}_{F'/F}(P) := \sum_{P'|P} e_{P'|P} P' \rightsquigarrow \mathrm{Div}(F) \to \mathrm{Div}(F')$$

Conorme

$F'|k'$ extension finie de $F|k$.

Définition

$$\mathrm{Con}_{F'/F}(\mathfrak{p}) := \langle \mathfrak{p} \rangle_{\mathcal{O}_{F'}} = \prod_{\mathfrak{p}'|\mathfrak{p}} \mathfrak{p}'^{e_{\mathfrak{p}'|\mathfrak{p}}} \rightsquigarrow \mathfrak{J}_{\mathcal{O}_F} \to \mathfrak{J}_{\mathcal{O}_{F'}}$$

$$\mathrm{Con}_{F'/F}(P) := \sum_{P'|P} e_{P'|P} P' \rightsquigarrow \mathrm{Div}(F) \to \mathrm{Div}(F')$$

Remarque

Pour $I \in \mathfrak{J}_{\mathcal{O}_F}$, $\mathrm{Con}_{F'/F}(I) = \langle I \rangle_{\mathcal{O}_{F'}}$.

Commutativité

Théorème

Si F'/F est séparable alors :

$$\forall D \in \mathrm{Div}(F), \mathrm{Con}_{F'/F}(D) = \mathfrak{D}_{F'}(\mathrm{Con}_{F'/F}(D_0), \mathrm{Con}_{F'/F}(D_\infty)).$$

Commutativité

Théorème

Si F'/F est séparable alors :

$$\forall D \in \mathrm{Div}(F), \mathrm{Con}_{F'/F}(D) = \mathfrak{D}_{F'}(\mathrm{Con}_{F'/F}(D_0), \mathrm{Con}_{F'/F}(D_\infty)).$$

Illustration

$$\begin{array}{ccc} \mathrm{Div}(F') & \xleftarrow{\mathfrak{D}_{F'}} & \mathfrak{J}_{\mathcal{O}_{F'}} \times \mathfrak{J}_{\mathcal{O}_{F'}^\infty} \\ \uparrow{\scriptstyle \mathrm{Con}_{F'/F}} & & \uparrow{\scriptstyle \mathrm{Con}_{F'/F} \times \mathrm{Con}_{F'/F}} \\ \mathrm{Div}(F) & \xrightarrow[(\mathfrak{D}_F)^{-1}]{} & \mathfrak{J}_{\mathcal{O}_F} \times \mathfrak{J}_{\mathcal{O}_F^\infty} \end{array}$$

Le morphisme de conorme–norme

q puissance d'un nombre premier impair, $n \in \mathbb{N}^*$, $f \in \mathbb{F}_{q^n}[x]$ polynôme de degré 3 sans facteur carré.

Le morphisme de conorme–norme

q puissance d'un nombre premier impair, $n \in \mathbb{N}^*$, $f \in \mathbb{F}_{q^n}[x]$ polynôme de degré 3 sans facteur carré.

Définition

$E := \{(a, b) \in \mathbb{F}_{q^n}^2 : b^2 = f(a)\}$ est une *courbe elliptique*.

Le morphisme de conorme–norme

q puissance d'un nombre premier impair, $n \in \mathbb{N}^*$, $f \in \mathbb{F}_{q^n}[x]$ polynôme de degré 3 sans facteur carré.

Définition

$E := \{(a, b) \in \mathbb{F}_{q^n}^2 : b^2 = f(a)\}$ est une *courbe elliptique*.

- $\mathbb{F}_{q^n}(E) := \mathbb{F}_{q^n}(x)[y]/\langle y^2 - f(x)\rangle$ corps de fonctions de $E/\mathbb{F}_{q^n}$

Le morphisme de conorme–norme

q puissance d'un nombre premier impair, $n \in \mathbb{N}^*$, $f \in \mathbb{F}_{q^n}[x]$ polynôme de degré 3 sans facteur carré.

Définition

$E := \{(a, b) \in \mathbb{F}_{q^n}^2 : b^2 = f(a)\}$ est une *courbe elliptique*.

- $\mathbb{F}_{q^n}(E) := \mathbb{F}_{q^n}(x)[y]/\langle y^2 - f(x)\rangle$ corps de fonctions de $E/\mathbb{F}_{q^n}$
- F' une clôture galoisienne de $\mathbb{F}_{q^n}(E)/\mathbb{F}_{q^n}(x)$

Le morphisme de conorme–norme

q puissance d'un nombre premier impair, $n \in \mathbb{N}^*$, $f \in \mathbb{F}_{q^n}[x]$ polynôme de degré 3 sans facteur carré.

Définition

$E := \{(a, b) \in \mathbb{F}_{q^n}^2 : b^2 = f(a)\}$ est une *courbe elliptique*.

- $\mathbb{F}_{q^n}(E) := \mathbb{F}_{q^n}(x)[y]/\langle y^2 - f(x)\rangle$ corps de fonctions de $E/\mathbb{F}_{q^n}$
- F' une clôture galoisienne de $\mathbb{F}_{q^n}(E)/\mathbb{F}_{q^n}(x)$
- $F|\mathbb{F}_q$ qui vérifie $F\mathbb{F}_{q^n} = F'$

Le morphisme de conorme–norme

q puissance d'un nombre premier impair, $n \in \mathbb{N}^*$, $f \in \mathbb{F}_{q^n}[x]$ polynôme de degré 3 sans facteur carré.

Définition

$E := \{(a, b) \in \mathbb{F}_{q^n}^2 : b^2 = f(a)\}$ est une *courbe elliptique*.

- $\mathbb{F}_{q^n}(E) := \mathbb{F}_{q^n}(x)[y]/\langle y^2 - f(x)\rangle$ corps de fonctions de $E/\mathbb{F}_{q^n}$
- F' une clôture galoisienne de $\mathbb{F}_{q^n}(E)/\mathbb{F}_{q^n}(x)$
- $F|\mathbb{F}_q$ qui vérifie $F\mathbb{F}_{q^n} = F'$

$$\mathbb{F}_{q^n}(E)|\mathbb{F}_{q^n}$$

Le morphisme de conorme–norme

q puissance d'un nombre premier impair, $n \in \mathbb{N}^*$, $f \in \mathbb{F}_{q^n}[x]$ polynôme de degré 3 sans facteur carré.

Définition

$E := \{(a, b) \in \mathbb{F}_{q^n}^2 : b^2 = f(a)\}$ est une *courbe elliptique*.

- $\mathbb{F}_{q^n}(E) := \mathbb{F}_{q^n}(x)[y]/\langle y^2 - f(x)\rangle$ corps de fonctions de $E/\mathbb{F}_{q^n}$
- F' une clôture galoisienne de $\mathbb{F}_{q^n}(E)/\mathbb{F}_{q^n}(x)$
- $F|\mathbb{F}_q$ qui vérifie $F\mathbb{F}_{q^n} = F'$

$$\mathbb{F}_{q^n}(E)|\mathbb{F}_{q^n} \xrightarrow{\text{Con}} F'|\mathbb{F}_{q^n}$$

Le morphisme de conorme–norme

q puissance d'un nombre premier impair, $n \in \mathbb{N}^*$, $f \in \mathbb{F}_{q^n}[x]$ polynôme de degré 3 sans facteur carré.

Définition

$E := \{(a, b) \in \mathbb{F}_{q^n}^2 : b^2 = f(a)\}$ est une *courbe elliptique*.

- $\mathbb{F}_{q^n}(E) := \mathbb{F}_{q^n}(x)[y]/\langle y^2 - f(x)\rangle$ corps de fonctions de $E/\mathbb{F}_{q^n}$
- F' une clôture galoisienne de $\mathbb{F}_{q^n}(E)/\mathbb{F}_{q^n}(x)$
- $F|\mathbb{F}_q$ qui vérifie $F\mathbb{F}_{q^n} = F'$

$$\mathbb{F}_{q^n}(E)|\mathbb{F}_{q^n} \xrightarrow{\text{Con}} F'|\mathbb{F}_{q^n} \xrightarrow{\text{N}} F|\mathbb{F}_q$$

Le morphisme de conorme–norme

q puissance d'un nombre premier impair, $n \in \mathbb{N}^*$, $f \in \mathbb{F}_{q^n}[x]$ polynôme de degré 3 sans facteur carré.

Définition

$E := \{(a, b) \in \mathbb{F}_{q^n}^2 : b^2 = f(a)\}$ est une *courbe elliptique*.

- $\mathbb{F}_{q^n}(E) := \mathbb{F}_{q^n}(x)[y]/\langle y^2 - f(x)\rangle$ corps de fonctions de $E/\mathbb{F}_{q^n}$
- F' une clôture galoisienne de $\mathbb{F}_{q^n}(E)/\mathbb{F}_{q^n}(x)$
- $F|\mathbb{F}_q$ qui vérifie $F\mathbb{F}_{q^n} = F'$

$$\mathbb{F}_{q^n}(E)|\mathbb{F}_{q^n} \xrightarrow{\text{Con}} F'|\mathbb{F}_{q^n} \xrightarrow{\text{N}} F|\mathbb{F}_q$$

Idée

On sait résoudre le PLD plus rapidement avec $F|\mathbb{F}_q$ qu'avec $\mathbb{F}_{q^n}(E)|\mathbb{F}_{q^n}$.

Références


M. Deuring, *Lectures on the Theory of Algebraic Functions of One Variable*. Springer, 1973.


C. Diem, *The GHS Attack in odd Characteristic*. J. Ramanujan Math. Soc. 18, No.1, 1–32, 2003.


J. Neukirch, *Algebraic Number Theory*. Springer, 1999.


J.H. Silverman, *The Arithmetic of Elliptic Curves* (second edition). Springer, 2009.


H. Stichtenoth, *Algebraic Function Fields and Codes* (second edition). Springer, 2009.

Degré

Définition

Le *degré* d'une place $P \in \mathbb{P}_{F|k}$ est :

$$\deg P := \left[\frac{\mathcal{O}_P}{P} : k\right].$$

On prolonge deg en un morphisme $\mathrm{Div}(F) \to \mathbb{Z}$.

Degré

Définition

Le *degré* d'une place $P \in \mathbb{P}_{F|k}$ est :

$$\deg P := \left[\frac{\mathcal{O}_P}{P} : k\right].$$

On prolonge deg en un morphisme $\mathrm{Div}(F) \to \mathbb{Z}$.

Définition

$$\mathrm{Div}^0(F) := \{D \in \mathrm{Div}(F) : \deg D = 0\}$$

Diviseur principal

Définition

Soit $f \in F^*$; on définit le *diviseur principal associé à* f par

$$\mathrm{div}(f) := \sum_{P \in \mathbb{P}_F} \mathrm{ord}_P(f) P.$$

Diviseur principal

Définition

Soit $f \in F^*$; on définit le *diviseur principal associé à* f par

$$\operatorname{div}(f) := \sum_{P \in \mathbb{P}_F} \operatorname{ord}_P(f) P.$$

Théorème

$$\forall f \in F^*, \deg \operatorname{div}(f) = 0$$

Diviseur principal

Définition

Soit $f \in F^*$; on définit le *diviseur principal associé à* f par

$$\operatorname{div}(f) := \sum_{P \in \mathbb{P}_F} \operatorname{ord}_P(f) P.$$

Théorème

$$\forall f \in F^*, \deg \operatorname{div}(f) = 0$$

Définition

$$\mathrm{Cl}^0(F) := \frac{\mathrm{Div}^0(F)}{\mathrm{Princ}(F)}$$

Genre

Définition

L'*espace de Riemann–Roch* associé à $D \in \mathrm{Div}(F)$ est

$$\mathcal{L}(D) := \{x \in F^* : (x) + D \geqslant 0\} \cup \{0\}.$$

On définit la *dimension* de D par $\ell(D) := \dim_k \mathcal{L}(D)$.

Définition

Le *genre* de $F|k$ est :

$$g(F) := \max\{\deg D - \ell(D) + 1 : D \in \mathrm{Div}(F)\} \in \mathbb{N}.$$

Proposition

Si $F|\mathbb{F}_q$ est de genre g, on a l'encadrement suivant :

$$(\sqrt{q} - 1)^{2g} \leqslant \#\mathrm{Cl}^0(F) \leqslant (\sqrt{q} + 1)^{2g}.$$