La méthode de Chabauty et Coleman

Nicolas Mascot

9 décembre 2010

Équations diophantiennes

Soit K un corps de nombres.

Équations diophantiennes

Soit K un corps de nombres.

Notre objectif est la résolution dans K^2 des équations de la forme

$$f(x, y) = 0,$$

où $f \in K[x, y]$.

Équations diophantiennes

Soit K un corps de nombres.

Notre objectif est la résolution dans K^2 des équations de la forme

$$f(x, y) = 0,$$

où $f \in K[x, y]$.

Ceci correspond à trouver les points à coordonnées dans K de la courbe plane d'équation $f(x, y) = 0$.

Table des matières

Table des matières

Table des matières

Table des matières

Variétés algébriques

Variétés algébriques affines

Soit K un corps parfait.

Variétés algébriques affines

Soit K un corps parfait.

Une *variété algébrique affine sur K* est le lieu des zéros communs de polynômes

$$f_i(x_1, \cdots, x_n) \in K[x_1, \cdots, x_n].$$

Variétés algébriques affines

Soit K un corps parfait.

Une *variété algébrique affine sur K* est le lieu des zéros communs de polynômes

$$f_i(x_1, \cdots, x_n) \in K[x_1, \cdots, x_n].$$

Son *anneau de fonctions régulières* est

$$K[x_1, \cdots, x_n]/(f_i).$$

Variétés algébriques affines

Soit K un corps parfait.

Une *variété algébrique affine sur K* est le lieu des zéros communs de polynômes

$$f_i(x_1, \cdots, x_n) \in K[x_1, \cdots, x_n].$$

Son *anneau de fonctions régulières* est

$$K[x_1, \cdots, x_n]/(f_i).$$

Les points de la variété correspondent aux idéaux maximaux de cet anneau.

Variétés algébriques projectives

On définit de même les variétés algébriques *projectives* comme lieu des zéros dans un espace projectif de polynômes homogènes. Elles sont recouvertes par des cartes affines.

Points rationnels

Soit X une variété sur K. Pour toute extension L de K, on note $X(L)$ les points de X à coordonnées dans L.

Points rationnels

Soit X une variété sur K. Pour toute extension L de K, on note $X(L)$ les points de X à coordonnées dans L.

Les éléments de $X(K)$ s'appellent *points rationnels*.

Points rationnels

Soit X une variété sur K. Pour toute extension L de K, on note $X(L)$ les points de X à coordonnées dans L.

Les éléments de $X(K)$ s'appellent *points rationnels*.

On notera X_L la variété définie sur L par les équations définissant X. Ainsi $X_L(L) = X(L)$.

Variétés irréductibles et réduites

Nous supposerons les f_i choisis de telle sorte que $K[x_1, \cdots, x_n]/(f_i)$ soit réduit.

Variétés irréductibles et réduites

Nous supposerons les f_i choisis de telle sorte que $K[x_1, \cdots, x_n]/(f_i)$ soit réduit.

On dit qu'une variété X est *irréductible* si on ne peut pas la décomposer non-trivialement en union de deux variétés.
Ceci est équivalent à ce que l'anneau de fonctions régulières soit intègre ; on appelle alors *corps des fractions rationnelles* son corps des fractions, et on le note $K(X)$.

Variétés irréductibles et réduites

Nous supposerons les f_i choisis de telle sorte que $K[x_1, \cdots, x_n]/(f_i)$ soit réduit.

On dit qu'une variété X est *irréductible* si on ne peut pas la décomposer non-trivialement en union de deux variétés. Ceci est équivalent à ce que l'anneau de fonctions régulières soit intègre ; on appelle alors *corps des fractions rationnelles* son corps des fractions, et on le note $K(X)$.

On dit que X est *absolument irréductible* si X_L est irréductible pour toute extension algébrique de K.

Réduction du problème

Dans le cas de la courbe d'équation $f(x, y) = 0$ qui nous intéresse, ceci se vérifie, et le cas échéant se corrige, en factorisant f dans $\overline{K}[x, y]$.

Réduction du problème

Dans le cas de la courbe d'équation $f(x, y) = 0$ qui nous intéresse, ceci se vérifie, et le cas échéant se corrige, en factorisant f dans $\overline{K}[x, y]$.

Remarque : Si la courbe X est irréductible sur le corps de base K mais pas absolument irréductible, elle acquiert toute sa réductibilité sur la clôture algébrique de K dans $K(X)$, qui est une extension finie de K.

Variétés abéliennes

Une *variété abélienne* est une variété projective X munie d'une structure de groupe définie par des fonctions rationnelles. Les $X(L)$ sont alors des groupes.

Variétés abéliennes

Une *variété abélienne* est une variété projective X munie d'une structure de groupe définie par des fonctions rationnelles. Les $X(L)$ sont alors des groupes. Les groupes obtenus sont automatiquement abéliens.

Variétés abéliennes

Une *variété abélienne* est une variété projective X munie d'une structure de groupe définie par des fonctions rationnelles. Les $X(L)$ sont alors des groupes. Les groupes obtenus sont automatiquement abéliens.

Théorème (Mordell, Weil)

Soit X une variété abélienne sur un corps de nombres K. Le groupe abélien $X(K)$ est de type fini.

Variétés abéliennes

Une *variété abélienne* est une variété projective X munie d'une structure de groupe définie par des fonctions rationnelles. Les $X(L)$ sont alors des groupes. Les groupes obtenus sont automatiquement abéliens.

Théorème (Mordell, Weil)

Soit X une variété abélienne sur un corps de nombres K. Le groupe abélien $X(K)$ est de type fini , donc isomorphe à

$$\mathbb{Z}^r \times (\mathbb{Z}/n_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/n_i\mathbb{Z}).$$

L'entier r s'appelle le *rang* de X.

Variétés abéliennes

Une *variété abélienne* est une variété projective X munie d'une structure de groupe définie par des fonctions rationnelles. Les $X(L)$ sont alors des groupes. Les groupes obtenus sont automatiquement abéliens.

Théorème (Mordell, Weil)

Soit X une variété abélienne sur un corps de nombres K. Le groupe abélien $X(K)$ est de type fini , donc isomorphe à

$$\mathbb{Z}^r \times (\mathbb{Z}/n_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/n_i\mathbb{Z}).$$

L'entier r s'appelle le *rang* de X.

La structure de groupe aide grandement à calculer $X(K)$.

Dimension d'une variété

La *dimension* d'une variété est la borne supérieure de la longueur des chaînes strictement croissantes de sous-variétés irréductibles.

Genre d'une courbe et théorème de Riemann-Roch

De la nécessité d'un meilleur invariant que le degré

Les équations $y^2 = x^5 + x^4$ et $y^2 = x^5 + x$, bien qu'apparemment semblables, ont des comportements très différents puisque la première à une infinité de solutions dans $\mathbb{Q}^2$, tandis que la seconde n'a qu'on nombre fini de solutions sur n'importe quel corps de nombres.

Courbes non singulières

On dit qu'une courbe algébrique sur K est *non singulière* si son équation et le gradient de celle-ci ne s'annulent jamais simultanément sur $\overline{K}$.

Courbes non singulières

On dit qu'une courbe algébrique sur K est *non singulière* si son équation et le gradient de celle-ci ne s'annulent jamais simultanément sur $\overline{K}$.
Ceci est équivalent à dire que les anneaux locaux en les points fermés de la courbe sont des anneaux de valuation discrète.
On appelle *paramètre local en un point* tout élément de valuation 1 de l'anneau local en ce point.

Courbes non singulières

On dit qu'une courbe algébrique sur K est *non singulière* si son équation et le gradient de celle-ci ne s'annulent jamais simultanément sur $\overline{K}$.
Ceci est équivalent à dire que les anneaux locaux en les points fermés de la courbe sont des anneaux de valuation discrète.
On appelle *paramètre local en un point* tout élément de valuation 1 de l'anneau local en ce point.

Dans toute la suite, on ne considérera que des courbes projectives réduites absolument irréductibles non singulières sur K.

Problèmes de Riemann-Roch

Soit X une courbe sur un corps parfait K.
Existe-t-il des fonctions régulières qui s'annulent à l'ordre au moins 2 au point A et à l'ordre au moins 3 au point B, et qui sont régulières partout, sauf peut-être en C où elles ont un pôle d'ordre au plus 7 ?

Diviseurs

Un *diviseur* sur la courbe est une somme formelle finie de points fermés de la courbe à coefficients dans $\mathbb{Z}$.

Exemple : $2A + 3B - 7C$.

Diviseurs

Un *diviseur* sur la courbe est une somme formelle finie de points fermés de la courbe à coefficients dans $\mathbb{Z}$.

Exemple : $2A + 3B - 7C$.

Les diviseurs forment un groupe abélien.

Degré d'un diviseur

Le *degré* d'un point P est le degré du corps engendré par ses coordonnées sur le corps de base K.

Degré d'un diviseur

Le *degré* d'un point P est le degré du corps engendré par ses coordonnées sur le corps de base K.

Le *degré* d'un diviseur

$$\sum_P n_P P$$

est

$$\sum_P n_P \deg(P).$$

Diviseurs principaux

Un diviseur est *principal* s'il est de forme

$$\mathrm{div}(\alpha) = \sum_P \mathrm{ord}_P(\alpha)\, P$$

pour une certaine fonction rationnelle $\alpha \neq 0$.

Les diviseurs principaux forment un sous-groupe du groupe des diviseurs.

Diviseurs principaux

Un diviseur est *principal* s'il est de forme

$$\mathrm{div}(\alpha) = \sum_P \mathrm{ord}_P(\alpha)\, P$$

pour une certaine fonction rationnelle $\alpha \neq 0$.

Les diviseurs principaux forment un sous-groupe du groupe des diviseurs.

Théorème

Une fonction rationnelle a autant de zéros que de pôles ; autrement dit, le degré d'un diviseur principal est nul.

Groupe de Picard

Le *groupe de Picard* d'une courbe X est le quotient

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

Groupe de Picard

Le *groupe de Picard* d'une courbe X est le quotient

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

On définit aussi le sous-groupe

$$\mathrm{Pic}^0(X) = \{\text{Diviseurs de degré } 0\} \,/\, \{\text{Diviseurs principaux}\}.$$

Groupe de Picard

Le *groupe de Picard* d'une courbe X est le quotient

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

On définit aussi le sous-groupe

$$\mathrm{Pic}^0(X) = \{\text{Diviseurs de degré } 0\} \,/\, \{\text{Diviseurs principaux}\}.$$

Le groupe de Picard est l'analogue du groupe des classes, il dit l'obstruction aux problèmes de Riemann-Roch.

Notations pour les problèmes de Riemann-Roch

Un diviseur

$$D = \sum_P n_P P$$

est dit *effectif* si les n_P sont tous positifs ou nuls.
On note alors $D \geqslant 0$.

Notations pour les problèmes de Riemann-Roch

Un diviseur

$$D = \sum_P n_P P$$

est dit *effectif* si les n_P sont tous positifs ou nuls.
On note alors $D \geqslant 0$.

Pour tout diviseur D, on pose

$$L_D = \{\alpha \in K(X)^* \mid \mathrm{div}(\alpha) + D \geqslant 0\} \cup \{0\}.$$

C'est un K-espace de dimension finie, on note $l(D)$ sa dimension.

La classe canonique et le genre

Si D et D' représentent la même classe dans $\mathrm{Pic}(X)$, mettons

$$D' = D + \mathrm{div}(\alpha),$$

alors la multiplication par α réalise un isomorphisme

$$L_{D'} \xrightarrow[\sim]{\times\alpha} L_D \ .$$

En particulier $\deg(D) = \deg(D')$ et $l(D) = l(D')$.

La classe canonique et le genre

Si D et D' représentent la même classe dans $\mathrm{Pic}(X)$, mettons

$$D' = D + \mathrm{div}(\alpha),$$

alors la multiplication par α réalise un isomorphisme

$$L_{D'} \xrightarrow[\sim]{\times\alpha} L_D \ .$$

En particulier $\deg(D) = \deg(D')$ et $l(D) = l(D')$.

La *classe canonique* est la classe dans $\mathrm{Pic}(X)$ de n'importe quelle 1-forme différentielle.

La classe canonique et le genre

Si D et D' représentent la même classe dans $\mathrm{Pic}(X)$, mettons

$$D' = D + \mathrm{div}(\alpha),$$

alors la multiplication par α réalise un isomorphisme

$$L_{D'} \xrightarrow[\sim]{\times\alpha} L_D \ .$$

En particulier $\deg(D) = \deg(D')$ et $l(D) = l(D')$.

La *classe canonique* est la classe dans $\mathrm{Pic}(X)$ de n'importe quelle 1-forme différentielle.

Le *genre* de la courbe X est le l de sa classe canonique.

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. Choisissons un diviseur C représentant la classe canonique.

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. Choisissons un diviseur C représentant la classe canonique. Le degré de la classe canonique est

$$\deg(C) = 2g - 2.$$

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. Choisissons un diviseur C représentant la classe canonique. Le degré de la classe canonique est

$$\deg(C) = 2g - 2.$$

Pour tout diviseur D,

$$l(D) = \deg(D) + 1 - g + l(C - D).$$

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. Choisissons un diviseur C représentant la classe canonique. Le degré de la classe canonique est

$$\deg(C) = 2g - 2.$$

Pour tout diviseur D,

$$l(D) = \deg(D) + 1 - g + l(C - D).$$

Ceci se démontre avec de la cohomologie des faisceaux.

La méthode de Chabauty

Le théorème de Faltings

Théorème (Faltings, 1983)

Soit X une courbe de genre $\geqslant 2$ sur un corps de nombres K. Alors $X(K)$ est fini.

Le théorème de Faltings

Théorème (Faltings, 1983)

Soit X une courbe de genre $\geqslant 2$ sur un corps de nombres K. Alors $X(K)$ est fini.

Malheureusement, la preuve n'est pas du tout effective.

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 $j : X \hookrightarrow J_X$, défini sur K, et qui, étendu par linéarité au groupe des diviseurs de X, induit un isomorphisme entre $\mathrm{Pic}^0(X)$ et $J_X(K)$.

Stratégie (et échec)

$J_X(K)$ est bien plus facile à calculer que $X(K)$.

Stratégie (et échec)

$J_X(K)$ est bien plus facile à calculer que $X(K)$.

Prenons $K = \mathbb{Q}$. $\overline{J_X(\mathbb{R})}$ est un groupe de Lie analytique réel compact, dont $J_X(\mathbb{Q})$ est un sous-groupe de Lie. S'il est de dimension strictement inférieure, alors il est plausible qu'il ne rencontre la courbe $X(\mathbb{R})$ qu'en un nombre fini de points.

Stratégie (et échec)

$J_X(K)$ est bien plus facile à calculer que $X(K)$.

Prenons $K = \mathbb{Q}$. $J_X(\mathbb{R})$ est un groupe de Lie analytique réel compact, dont $\overline{J_X(\mathbb{Q})}$ est un sous-groupe de Lie. S'il est de dimension strictement inférieure, alors il est plausible qu'il ne rencontre la courbe $X(\mathbb{R})$ qu'en un nombre fini de points.

Malheureusement, le plus souvent,

$$\dim \overline{J_X(\mathbb{Q})} = \dim J_X(\mathbb{R}).$$

Il faut donc trouver autre chose.

Intégration de formes différentielles

Soit $\mathfrak{p}$ un idéal maximal de K, et soit $K_\mathfrak{p}$ la complétion $\mathfrak{p}$-adique de K. Nous allons remplacer $\mathbb{R}$ par $K_\mathfrak{p}$.

Intégration de formes différentielles

Soit $\mathfrak{p}$ un idéal maximal de K, et soit $K_\mathfrak{p}$ la complétion $\mathfrak{p}$-adique de K. Nous allons remplacer $\mathbb{R}$ par $K_\mathfrak{p}$.

Soit X une courbe algébrique non singulière de genre $g \geqslant 2$ sur un corps de nombres K. Notons $J = J_X$ sa jacobienne.

Intégration de formes différentielles

Soit $\mathfrak{p}$ un idéal maximal de K, et soit $K_\mathfrak{p}$ la complétion $\mathfrak{p}$-adique de K. Nous allons remplacer $\mathbb{R}$ par $K_\mathfrak{p}$.

Soit X une courbe algébrique non singulière de genre $g \geqslant 2$ sur un corps de nombres K. Notons $J = J_X$ sa jacobienne. Soit $H^0(J_{K_\mathfrak{p}}, \Omega^1)$ l'espace des 1-formes différentielles sans pôles sur $J_{K_\mathfrak{p}}$, c'est un $K_\mathfrak{p}$-espace vectoriel de dimension g.

Intégration de formes différentielles

Soit $\mathfrak{p}$ un idéal maximal de K, et soit $K_\mathfrak{p}$ la complétion $\mathfrak{p}$-adique de K. Nous allons remplacer $\mathbb{R}$ par $K_\mathfrak{p}$.

Soit X une courbe algébrique non singulière de genre $g \geqslant 2$ sur un corps de nombres K. Notons $J = J_X$ sa jacobienne. Soit $H^0(J_{K_\mathfrak{p}}, \Omega^1)$ l'espace des 1-formes différentielles sans pôles sur $J_{K_\mathfrak{p}}$, c'est un $K_\mathfrak{p}$-espace vectoriel de dimension g.

Étant donnée une 1-forme ω, il est possible de l'intégrer :

$$\begin{array}{ccc} J_{K_\mathfrak{p}}(K_\mathfrak{p}) & \longrightarrow & K_\mathfrak{p} \\ P & \longmapsto & \displaystyle\int_0^P \omega \end{array},$$

Intégration de formes différentielles

Soit $\mathfrak{p}$ un idéal maximal de K, et soit $K_\mathfrak{p}$ la complétion $\mathfrak{p}$-adique de K. Nous allons remplacer $\mathbb{R}$ par $K_\mathfrak{p}$.

Soit X une courbe algébrique non singulière de genre $g \geqslant 2$ sur un corps de nombres K. Notons $J = J_X$ sa jacobienne. Soit $H^0(J_{K_\mathfrak{p}}, \Omega^1)$ l'espace des 1-formes différentielles sans pôles sur $J_{K_\mathfrak{p}}$, c'est un $K_\mathfrak{p}$-espace vectoriel de dimension g.

Étant donnée une 1-forme ω, il est possible de l'intégrer :

$$\begin{array}{ccc} J_{K_\mathfrak{p}}(K_\mathfrak{p}) & \longrightarrow & K_\mathfrak{p} \\ P & \longmapsto & \displaystyle\int_0^P \omega \end{array},$$

d'où un morphisme ϕ de $J_{K_\mathfrak{p}}(K_\mathfrak{p})$ dans $H^0(J_{K_\mathfrak{p}}, \Omega^1)^*$, qui est un difféomorphisme local.

La méthode de Chabauty

$J(K_\mathfrak{p})$ est un groupe de Lie p-adique. L'adhérence de $J(K)$ est un sous-groupe de Lie de celui-ci, et

$$\dim \overline{J(K)} = \dim \phi\big(\overline{J(K)}\big) = \dim \overline{\phi\big(J(K)\big)} = \dim \big(\mathbb{Z}_p \phi(J(K))\big)$$

$$= \mathrm{rg}_{\mathbb{Z}_p} \big(\mathbb{Z}_p \phi\big(J(K)\big)\big) \leqslant \mathrm{rg}_{\mathbb{Z}}\, \phi\big(J(K)\big) \leqslant \mathrm{rg}_{\mathbb{Z}}\, J(K).$$

La méthode de Chabauty

$J(K_\mathfrak{p})$ est un groupe de Lie p-adique. L'adhérence de $J(K)$ est un sous-groupe de Lie de celui-ci, et

$$\dim \overline{J(K)} = \dim \phi\big(\overline{J(K)}\big) = \dim \overline{\phi\big(J(K)\big)} = \dim \big(\mathbb{Z}_p \phi(J(K))\big)$$

$$= \mathrm{rg}_{\mathbb{Z}_p} \big(\mathbb{Z}_p \phi\big(J(K)\big)\big) \leqslant \mathrm{rg}_{\mathbb{Z}} \, \phi\big(J(K)\big) \leqslant \mathrm{rg}_{\mathbb{Z}} \, J(K).$$

Théorème (Chabauty, 1941)

Si le rang de J est strictement inférieur au genre de X, alors $X(K)$ est fini.

La borne de Coleman

Bonne ou mauvaise réduction

On peut supposer que l'équation définissant X est à coefficients entiers (algébriques).

Bonne ou mauvaise réduction

On peut supposer que l'équation définissant X est à coefficients entiers (algébriques).

Soit $\mathfrak{p}$ un idéal maximal de K, posons

$$\mathbb{F}_{\mathfrak{p}} = \mathcal{O}_K/\mathfrak{p}.$$

Bonne ou mauvaise réduction

On peut supposer que l'équation définissant X est à coefficients entiers (algébriques).

Soit $\mathfrak{p}$ un idéal maximal de K, posons

$$\mathbb{F}_{\mathfrak{p}} = \mathcal{O}_K/\mathfrak{p}.$$

On dit que X a *bonne réduction en* $\mathfrak{p}$ si $X_{\mathbb{F}_{\mathfrak{p}}}$ est encore irréductible, réduite, et non singulière.

Bonne ou mauvaise réduction

On peut supposer que l'équation définissant X est à coefficients entiers (algébriques).

Soit $\mathfrak{p}$ un idéal maximal de K, posons

$$\mathbb{F}_{\mathfrak{p}} = \mathcal{O}_K/\mathfrak{p}.$$

On dit que X a *bonne réduction en* $\mathfrak{p}$ si $X_{\mathbb{F}_{\mathfrak{p}}}$ est encore irréductible, réduite, et non singulière.

Fixons un tel $\mathfrak{p}$ une bonne fois pour toutes, et notons p le nombre premier en-dessous de $\mathfrak{p}$.

Intégration le long de la courbe X

Si ω est une 1-forme sans pôles sur $J_{K_\mathfrak{p}}$, posons, pour tous P, $Q \in X(K_\mathfrak{p})$,

$$\int_P^Q \omega = \int_0^{Q-P} \omega.$$

Intégration le long de la courbe X

Si ω est une 1-forme sans pôles sur $J_{K_\mathfrak{p}}$, posons, pour tous P, $Q \in X(K_\mathfrak{p})$,

$$\int_P^Q \omega = \int_0^{Q-P} \omega.$$

Si Q est assez proche de P, plus précisement si $Q \equiv P \bmod \mathfrak{p}$, alors ceci peut se calculer en intégrant terme-à-terme le développement en série entière de ω par rapport à un paramètre local en P.

Une fonction qui s'annule sur $\overline{J(K)}$

Supposons comme précédemment que $\operatorname{rg} J < g$. Alors $\phi\big(\overline{J(K)}\big)$ est un sous-espace strict de $H^0(J_{K_\mathfrak{p}}, \Omega^1)^*$, donc il existe donc une forme linéaire non nulle qui s'annule sur ce sous-espace, autrement dit, une 1-forme $\omega \neq 0$ telle que

$$\sum_i \int_{P_i}^{Q_i} \omega = 0 \quad \text{si} \quad \sum_i (Q_i - P_i) \in \overline{J(K)}.$$

Une fonction qui s'annule sur $\overline{J(K)}$

Supposons comme précédemment que $\operatorname{rg} J < g$. Alors $\phi\big(\overline{J(K)}\big)$ est un sous-espace strict de $H^0(J_{K_\mathfrak{p}}, \Omega^1)^*$, donc il existe donc une forme linéaire non nulle qui s'annule sur ce sous-espace, autrement dit, une 1-forme $\omega \neq 0$ telle que

$$\sum_i \int_{P_i}^{Q_i} \omega = 0 \quad \text{si} \ \sum_i (Q_i - P_i) \in \overline{J(K)}.$$

Quitte à multiplier ω par un scalaire, on peut supposer que ω se réduit modulo $\mathfrak{p}$ en une 1-forme non nulle $\widetilde{\omega}$.

Une fonction qui s'annule sur $\overline{J(K)}$

Supposons comme précédemment que $\operatorname{rg} J < g$. Alors $\phi\big(\overline{J(K)}\big)$ est un sous-espace strict de $H^0(J_{K_\mathfrak{p}}, \Omega^1)^*$, donc il existe donc une forme linéaire non nulle qui s'annule sur ce sous-espace, autrement dit, une 1-forme $\omega \neq 0$ telle que

$$\sum_i \int_{P_i}^{Q_i} \omega = 0 \quad \text{si} \ \sum_i (Q_i - P_i) \in \overline{J(K)}.$$

Quitte à multiplier ω par un scalaire, on peut supposer que ω se réduit modulo $\mathfrak{p}$ en une 1-forme non nulle $\widetilde{\omega}$.

Notons aussi $\widetilde{P} \in X_{\mathbb{F}_\mathfrak{p}}(\mathbb{F}_\mathfrak{p})$ la réduction d'un $P \in X(K_\mathfrak{p})$, et $m_{\widetilde{P}}$ l'ordre d'annulation de $\widetilde{\omega}$ en $\widetilde{P}$.

Polygones de Newton

Le procédé dit des *polygones de Newton* permet d'estimer le nombre et l'emplacement des zéros d'une série entière sur un corps p-adique par un simple examen de ses coefficients.

Polygones de Newton

Le procédé dit des *polygones de Newton* permet d'estimer le nombre et l'emplacement des zéros d'une série entière sur un corps p-adique par un simple examen de ses coefficients.

En l'appliquant à notre intégrale, on trouve que si $m_{\widetilde{P}} < p-2$, alors $\displaystyle\int_P^Q \omega$ a au plus $m_{\widetilde{P}} + 1$ zéros parmi les $Q \equiv P \bmod \mathfrak{p}$.

Polygones de Newton

Le procédé dit des *polygones de Newton* permet d'estimer le nombre et l'emplacement des zéros d'une série entière sur un corps p-adique par un simple examen de ses coefficients.

En l'appliquant à notre intégrale, on trouve que si $m_{\widetilde{P}} < p-2$, alors $\displaystyle\int_P^Q \omega$ a au plus $m_{\widetilde{P}} + 1$ zéros parmi les $Q \equiv P \bmod \mathfrak{p}$.

Ainsi, si $m_{\widetilde{P}} < p-2$, il existe au plus $m_{\widetilde{P}} + 1$ points de $\overline{J(K)}$ qui se réduisent à $\widetilde{P}$.

La borne de Coleman

D'après le théorème de Riemann-Roch appliqué à $X_{\mathbb{F}_\mathfrak{p}}$, $\widetilde{\omega}$ a exactement $2g-2$ zéros (comptés avec multiplicité) sur $X_{\mathbb{F}_\mathfrak{p}}(\overline{\mathbb{F}_\mathfrak{p}})$. En particulier, si $p > 2g$, alors la condition $m_{\widetilde{P}} < p-2$ est vérifiée.

La borne de Coleman

D'après le théorème de Riemann-Roch appliqué à $X_{\mathbb{F}_\mathfrak{p}}$, $\widetilde{\omega}$ a exactement $2g-2$ zéros (comptés avec multiplicité) sur $X_{\mathbb{F}_\mathfrak{p}}(\overline{\mathbb{F}_\mathfrak{p}})$. En particulier, si $p > 2g$, alors la condition $m_{\widetilde{P}} < p-2$ est vérifiée.

En sommant sur $\widetilde{P} \in X_{\mathbb{F}_\mathfrak{p}}(\mathbb{F}_\mathfrak{p})$, on trouve

$$|X(K)| \leqslant \sum_{\widetilde{P} \in X_{\mathbb{F}_\mathfrak{p}}(\mathbb{F}_\mathfrak{p})} (m_{\widetilde{P}} + 1) \leqslant |X_{\mathbb{F}_\mathfrak{p}}(\mathbb{F}_\mathfrak{p})| + 2g - 2.$$

La borne de Coleman

D'après le théorème de Riemann-Roch appliqué à $X_{\mathbb{F}_\mathfrak{p}}$, $\widetilde{\omega}$ a exactement $2g-2$ zéros (comptés avec multiplicité) sur $X_{\mathbb{F}_\mathfrak{p}}(\overline{\mathbb{F}_\mathfrak{p}})$. En particulier, si $p > 2g$, alors la condition $m_{\widetilde{P}} < p-2$ est vérifiée.

En sommant sur $\widetilde{P} \in X_{\mathbb{F}_\mathfrak{p}}(\mathbb{F}_\mathfrak{p})$, on trouve

$$|X(K)| \leqslant \sum_{\widetilde{P} \in X_{\mathbb{F}_\mathfrak{p}}(\mathbb{F}_\mathfrak{p})} (m_{\widetilde{P}} + 1) \leqslant |X_{\mathbb{F}_\mathfrak{p}}(\mathbb{F}_\mathfrak{p})| + 2g - 2.$$

Théorème (Coleman, 1985)

Si $\operatorname{rg} J < g$ et $p > 2g$, alors $|X(K)| \leqslant |X_{\mathbb{F}_\mathfrak{p}}(\mathbb{F}_\mathfrak{p})| + 2g - 2$.

Un exemple pour finir

Prenons $K = \mathbb{Q}$, et soit X la courbe définie par l'équation

$$y^2 = x(x-1)(x-2)(x-5)(x-6).$$

Un exemple pour finir

Prenons $K = \mathbb{Q}$, et soit X la courbe définie par l'équation

$$y^2 = x(x-1)(x-2)(x-5)(x-6).$$

X est de genre 2 et a bonne réduction modulo 7, de plus sa Jacobienne est de rang 1.

Un exemple pour finir

Prenons $K = \mathbb{Q}$, et soit X la courbe définie par l'équation

$$y^2 = x(x-1)(x-2)(x-5)(x-6).$$

X est de genre 2 et a bonne réduction modulo 7, de plus sa Jacobienne est de rang 1.
$X_{\mathbb{F}_7}$ a huit points rationnels

$$(0,0),\ (1,0),\ (2,0),\ (5,0),\ (6,0),\ (3,1),\ (3,6) \text{ et } \infty,$$

donc

$$|X(\mathbb{Q})| \leqslant 8 + 2 \times 2 - 2 = 10.$$

Un exemple pour finir

Prenons $K = \mathbb{Q}$, et soit X la courbe définie par l'équation

$$y^2 = x(x-1)(x-2)(x-5)(x-6).$$

X est de genre 2 et a bonne réduction modulo 7, de plus sa Jacobienne est de rang 1.
$X_{\mathbb{F}_7}$ a huit points rationnels

$$(0,0),\ (1,0),\ (2,0),\ (5,0),\ (6,0),\ (3,1),\ (3,6) \text{ et } \infty,$$

donc

$$|X(\mathbb{Q})| \leqslant 8 + 2 \times 2 - 2 = 10.$$

Une recherche naïve donne rapidement dix points rationnels de X :

$$(0,0),\ (1,0),\ (2,0),\ (5,0),\ (6,0),\ (3,\pm 6),\ (10,\pm 120) \text{ et } \infty.$$

Un exemple pour finir

Prenons $K = \mathbb{Q}$, et soit X la courbe définie par l'équation

$$y^2 = x(x-1)(x-2)(x-5)(x-6).$$

X est de genre 2 et a bonne réduction modulo 7, de plus sa Jacobienne est de rang 1.
$X_{\mathbb{F}_7}$ a huit points rationnels

$$(0,0),\ (1,0),\ (2,0),\ (5,0),\ (6,0),\ (3,1),\ (3,6) \text{ et } \infty,$$

donc

$$|X(\mathbb{Q})| \leqslant 8 + 2 \times 2 - 2 = 10.$$

Une recherche naïve donne rapidement dix points rationnels de X :

$$(0,0),\ (1,0),\ (2,0),\ (5,0),\ (6,0),\ (3,\pm 6),\ (10,\pm 120) \text{ et } \infty.$$

Ainsi, la borne de Coleman est optimale, et la recherche naïve a bien trouvé tous les points rationnels.