# Points rationnels et cycles algébriques

Chevaleret
Colloque

Henri Darmon
Université McGill
26 Juin, 2008

http://www.math.mcgill.ca/darmon/slides/slides.html

# Equations diophantiennes

$$f_1, \ldots, f_m \in \mathbf{Z}[x_1, \ldots, x_n],$$

$$X : \begin{cases} f_1(x_1, \ldots, x_n) = 0 \\ \vdots \qquad \vdots \qquad \vdots \\ f_m(x_1, \ldots, x_n) = 0. \end{cases}$$

Les équations diophantiennes motivent souvent l'étude d'objets mathématiques fondamentaux (corps cyclotomiques, groupes et corps de classe, représentations $\ell$-adiques, formes modulaires, variétés de Shimura...)

Elles peuvent aussi suggérer l'existence de structures mathématiques riches, encore mal comprises.

# Exemples

**Fermat, 1635**: L'équation de Pell $x^2 - ny^2 = 1$ possède une infinité de solutions *parce que* le groupe de classes d'équivalence de formes quadratiques binaires de discriminant $4n$ est *fini*.

**Kummer, 1847**: L'équation $x^n + y^n = z^n$ n'a pas de solutions non-triviales pour $2 < n < 37$ parce que tous les nombres premiers $p < 37$ sont *réguliers*.

**Mazur, Frey, Serre, Ribet, Wiles, Taylor, 1994**: L'équation de Fermat $x^n + y^n = z^n$ n'a pas de solutions non-triviales pour $n > 2$ parce que toutes les courbes elliptiques sont *modulaires*.

# Courbes Elliptiques

Une *courbe elliptique* est une equation de la forme

$$\boxed{E : y^2 = x^3 + ax + b,}$$

avec $\Delta := 4a^3 - 27b^2 \neq 0$.

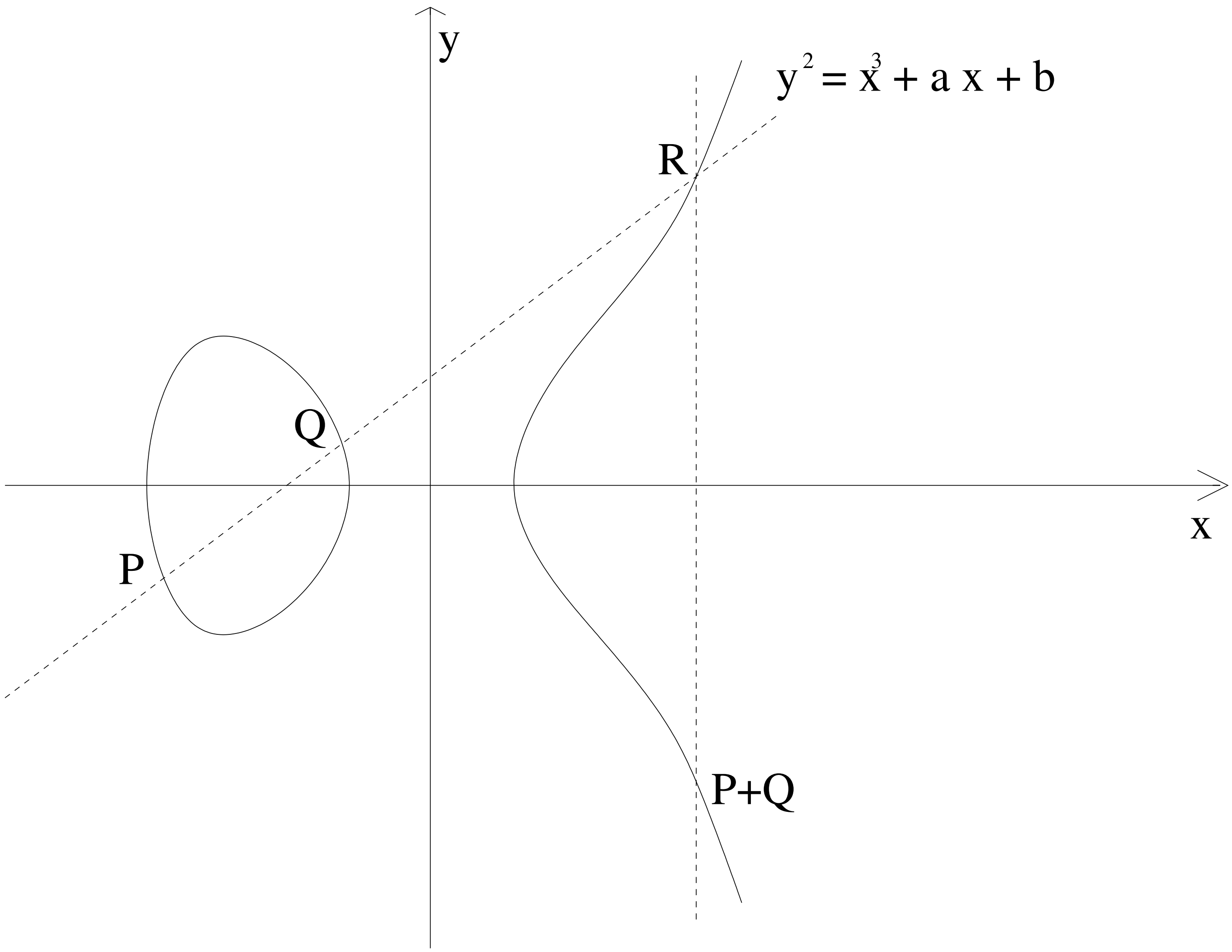
Si $F$ est un corps,

$E(F) :=$ Groupe de Mordell-Weil de $E$ sur $F$.

*Pourquoi les courbes elliptiques?*

# La loi d'addition

Les courbes elliptiques sont des *groupes algébriques*.




*Loi d'addition sur une courbe elliptique*

# Modularité

$N =$ *conducteur* de $E$.

$$a(p) := \begin{cases} p + 1 - \#E(\mathbf{Z}/p\mathbf{Z}) & \text{if } p \not| N; \\ 0, \pm 1 & \text{if } p | N. \end{cases}$$

$$a(mn) = a(m)a(n) \text{ si } \gcd(m,n) = 1,$$

$$a(p^n) = a(p)a(p^{n-1}) - pa(p^{n-2}), \text{ si } p \not| N.$$

**Série génératrice**:

$$f_E(z) = \sum_{n=1}^{\infty} a(n) e^{2\pi i n z}, \quad z \in \mathcal{H},$$

$\mathcal{H} :=$ Demi-plan de Poincaré

# Modularité

**Modularité**: Il s'agit d'une propriété d'invariance de la série $f_E(z)$ sous le groupe $\mathbf{SL}_2(\mathbf{Z})$.

$M_0(N) :=$ anneau des matrices $2 \times 2$, à coordonnées dans $\mathbf{Z}$, qui sont *triangulaires supérieures* modulo $N$.

$\Gamma_0(N) := M_0(N)_1^\times =$ unités de déterminant 1.

**Théorème**: La série $f_E$ est une *forme modulaire de poids* 2 *sur le groupe* $\Gamma_0(N)$.

$$f_E\left(\frac{az+b}{cz+d}\right) = (cz+d)^2 f_E(z).$$

Il en résulte que la forme différentielle $\omega_f := f_E(z)dz$ est définie sur le quotient

$$X := \Gamma_0(N)\backslash\mathcal{H}.$$

# Modularité et cycles spéciaux

La surface de Riemann $X$ est munie d'une collection (infinie) de *cycles* naturels. Ces cycles contiennent *énormément d'informations* sur l'arithmét de la courbe $E$.

Les cycles spéciaux vont être indexés par les sous-anneaux commutatifs de $M_0(N)$ (eg: le ordres dans un corps quadratique).

$\mathrm{Disc}(R) :=$ discriminant de $R$.

$\Sigma_D = \Gamma_0(N)\backslash\{R \subset M_0(N)$ with $\mathrm{Disc}(R) = D\}$.

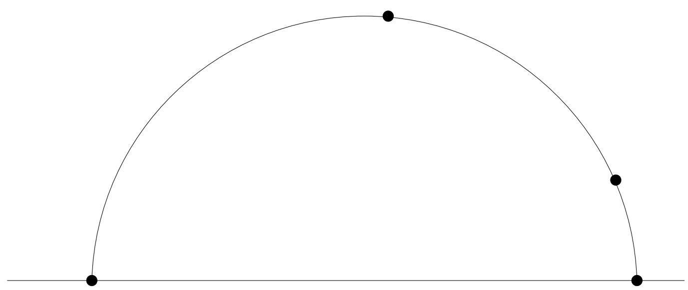
$G_D :=$ Classes d'équivalence de formes quadratiques binaires de discriminant $D$.

L'ensemble $\Sigma_D$, lorsqu'il est non-nul, est muni d'une action naturelle du groupe de classes $G_D$.

# Les cycles spéciaux $\gamma_R \subset X$

**Premier cas**. Disc$(R) > 0$. Alors, l'action de $(R \otimes \mathbf{Q})^\times$ sur $\mathbf{P}_1(\mathbf{C})$ a *deux points fixes* $\tau_R, \tau'_R \in \mathbf{R}$.

$\Upsilon_R :=$ chemin géodésique allant de $\tau_R$ à $\tau'_R$;

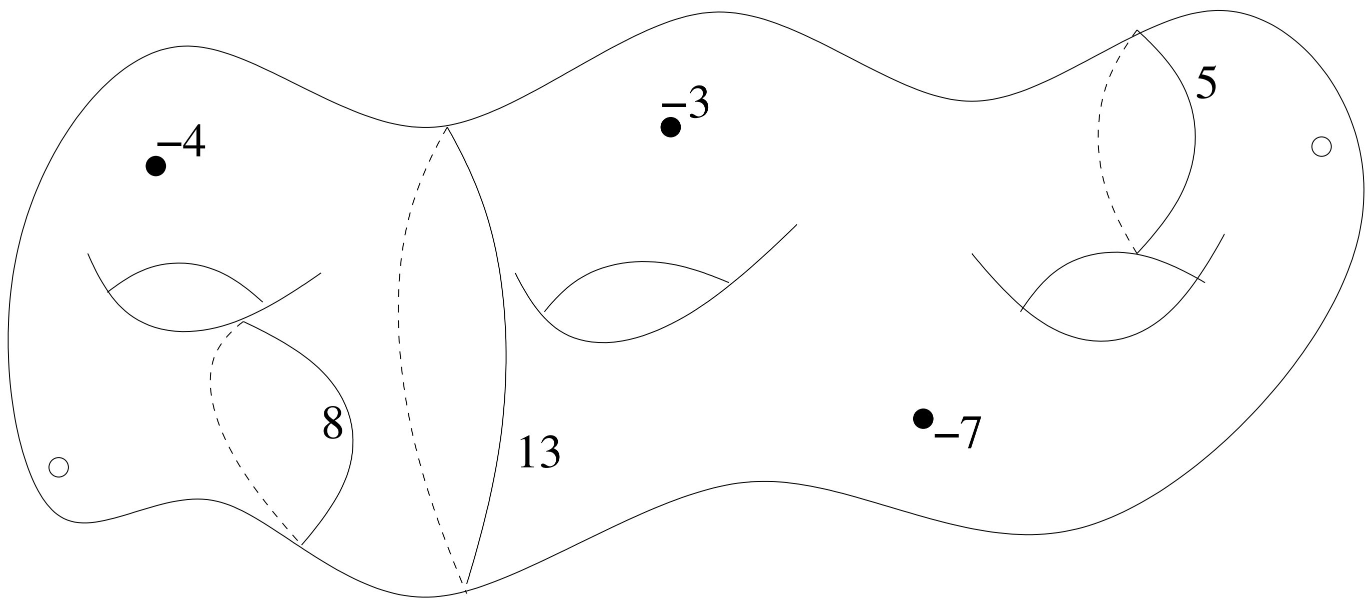


$$\boxed{\gamma_R := R_1^\times \backslash \Upsilon_R}$$

**Second cas**. Disc$(R) < 0$. L'action de $(R \otimes \mathbf{Q})^\times$ sur $\mathcal{H}$ a alors *un seul point fixe* $\tau_R \in \mathcal{H}$.

$$\boxed{\gamma_R := \{\tau_R\}}$$

# La courbe modulaire




On peut donc associer à tout discriminant $D$ la quantité:

$$\gamma_D = \sum \gamma_R,$$

la somme étant prise sur une $G_D$-orbite complète dans $\Sigma_D$.

**Principe**: Les périodes de $\omega_f$ sur les cycles $\gamma_R$ et $\gamma_D$ sont liées, de facon profonde, à l'arithmetique de la courbe $E$ sur les extensions quadratiques associées.

# Périodes de $\omega_f$: le cas $D > 0$

**Théorème** (Eichler, Shimura) L'ensemble

$$\Lambda := \left\langle \int_{\gamma_R} \omega_f, \quad R \in \Sigma_{>0} \right\rangle \subset \mathbf{C}$$

est un réseau dans $\mathbf{C}$, commensurable avec le réseau de Weierstrass de $E$.

*Esqisse de démonstration*

1. **Courbes modulaires**: $X = Y_0(N)(\mathbf{C})$, où $Y_0(N)$ est une courbe algérique sur $\mathbf{Q}$, qui s'interprète comme une variété de modules de courbes elliptiques sur $\mathbf{Q}$.

2. **Eichler-Shimura**: Il existe une courbe elliptique $E_f$ et un morphisme

$$\Phi_f : Y_0(N) \longrightarrow E_f$$

de courbes algébriques sur $\mathbf{Q}$, tel que

$$\int_{\gamma_R} \omega_f = \int_{\Phi(\gamma_R)} \omega_{E_f} \in \Lambda_{E_f}.$$

Par conséquent, $\int_{\gamma_R} \omega_f$ est une *période* de $E_f$.

Les courbes elliptiques $E_f$ et $E$ sont liées par les relations:

$$a_n(E_f) = a_n(E) \text{ for all } n \geq 1.$$

3. **Théprème d'isogénie pour les courbes** (Faltings): Les courbes $E_f$ et $E$ sont isogènes sur $\mathbf{Q}$.

# Arithmétique des courbes elliptiques

**Conjecture** (BSD) Soit $D > 0$ un discriminant fondamental. Alors

$$J_D := \int_{\gamma_D} \omega_f \neq 0 \quad \text{ssi} \quad \#E(\mathbf{Q}(\sqrt{D})) < \infty.$$

"La position de $\gamma_D$ dans l'homologie $H_1(X, \mathbf{Z})$ présente une *obstruction* à la présence de points rationnels dans $E(\mathbf{Q}(\sqrt{D}))$. "

**Gross-Zagier, Kolyvagin**. Si $J_D \neq 0$, alors le groupe $E(\mathbf{Q}(\sqrt{D}))$ est fini.

# Périodes de $\omega_f$: le cas $D < 0$

Les cycles $\gamma_R$ sont alors des 0-cycles, et leur image dans $H_0(X, \mathbf{Z})$ est *constante* (indépendemment de $R$).

On peut donc produire, à partir des $\gamma_R$, beaucoup de 0-cycles *homologiquement triviaux* avec support dans $\Sigma_D$:

$$\Sigma_D^0 := \ker(\mathrm{Div}(\Sigma_D) \longrightarrow H_0(X, \mathbf{Z})).$$

On étend l'application $R \mapsto \gamma_R$ à $\Delta \in \Sigma_D^0$ par linéarité.

Soit $\gamma_\Delta^\#$ := une 1-chaine (différentiable par morceaux) ayant $\gamma_\Delta$ comme frontière.

$$P_\Delta := \int_{\gamma_\Delta^\sharp} \omega_f \in \mathbf{C}/\Lambda_f \simeq E(\mathbf{C}).$$

# Points CM

**Théorème des points CM:** Pour tout $\Delta \in \Sigma_D^0$, le point $P_\Delta$ appartient à $E(H_D) \otimes \mathbf{Q}$, où $H_D$ est le corps de classe de Hilbert de $\mathbf{Q}(\sqrt{D})$.

*Esquisse de démonstration*:

1. **Multiplication complexe**: Pour tout $R \in \Sigma_D$, le 0-cycle $\gamma_R$ est un point de $Y_0(N)(\mathbf{C})$ qui correspond à une courbe elliptique avec multiplication compexe par le corps $\mathbf{Q}(\sqrt{D})$. Par conséquent, ce cycle est défini sur le corps de classe $H_D$.

2. **Formule explicite pour** $\Phi$: $\Phi(\gamma_\Delta) = P_\Delta$.

La collection de points algébriques fournie par les $P_\Delta$ constitue une structure arithmétique très riche ("système d'Euler").

**Théorème de Gross-Zagier-Kolyvagin**: Si $D > 0$ et $J_D \neq 0$, alors $E(\mathbf{Q}(\sqrt{D}))$ est fini.

# Généralisations?

**Principe de fonctorialité**: la modularité se présente sous diverses incarnations.

Un exemple illustratif: **Le changement de base quadratique.**

Soit $F$ un corps **quadratique réel**. On considère $E$ comme une courbe elliptique définie sur ce corps.

**Notation**: $(v_1, v_2) : F \longrightarrow \mathbf{R} \oplus \mathbf{R}, \quad x \mapsto (x_1, x_2)$.

**Hypothèses (pour simplifier)**: $h^+(F) = 1$, $N = 1$.

Le comptage des points modulo $\mathfrak{p}$ donne une fonction $\mathfrak{n} \mapsto a(\mathfrak{n}) \in \mathbf{Z}$, sur les idéaux de $\mathcal{O}_F$.

On peut alors réunir ces coefficients dans une *série génératrice modulaire.*

# Modularité

**Série génératrice**

$$G(z_1, z_2) := \sum_{n>>0} a((n)) e^{2\pi i \left(\frac{n_1}{d_1} z_1 + \frac{n_2}{d_2} z_2\right)},$$

où $d$ := générateur totalement positif de la différente de $F$.

**Théorème**: (Doi-Naganuma, Shintani).

$G(\gamma_1 z_1, \gamma_2 z_2) = (c_1 z_1 + d_2)^2 (c_2 z_2 + d_2)^2 G(z_1, z_2)$,

pour tout

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}_2(\mathcal{O}_F).$$

# Formulation géométrique:

La forme différentielle

$$\alpha_G := G(z_1, z_2) dz_1 dz_2$$

est une 2-forme *holomorphe* (et donc; fermée) sur le quotient analytique

$$X_F := \mathbf{SL}_2(\mathcal{O}_F) \backslash (\mathcal{H} \times \mathcal{H}).$$

Pour la suite, il sera plus pratique de considerer la 2-forme harmonique:

$$\omega_G := G(z_1, z_2) dz_1 dz_2 + G(\epsilon_1 z_1, \epsilon_2 \bar{z}_2) dz_1 d\bar{z}_2,$$

où $\epsilon \in \mathcal{O}_F^\times$ satisfait $\epsilon_1 > 0$, $\epsilon_2 < 0$.

$\omega_G$ est une 2-forme fermée sur la variété différentiable $X_F$ de dimension 4.

**Enoncés désirés**: Les périodes de $\omega_G$ sur divers cycles naturels de $X_F$ "en savent long" sur l'arithmétique de $E$ sur $F$.

# Cycles sur la variété $X_F$

Les cycles naturels sur la variété $X_F$ sont maintenant indexés par les sous-$\mathcal{O}_F$-algèbres commutatives de $M_2(\mathcal{O}_F)$, c'est-à-dire, essentiellement, par les sous-$\mathcal{O}_F$-ordres dans des extensions quadratiques de $F$.

$D :=$ Disc$(R)$ := discriminant relatif de $R$ sur $F$.

On distingue maintenant *trois cas*.

1. $D_1, D_2 > 0$: le cas totalement réel.

2. $D_1, D_2 < 0$: le cas CM.

3. $D_1 < 0, D_2 > 0$: le cas "à peu près totalement réel" ("almost totally real"—ATR).

# Les cycles $\gamma_R \subset X_F$

**Premier cas**. Disc($R$) $>> 0$. Alors, pour $j = 1, 2$,

$(R \otimes_{v_j} \mathbf{R})^\times$ a *deux points fixes* $\tau_j, \tau_j' \in \mathbf{R}$.

Soit $\Upsilon_j :=$ le chemin géodésique allant de $\tau_j$ à $\tau_j'$;

$$\boxed{\gamma_R := R_1^\times \backslash (\Upsilon_1 \times \Upsilon_2)}$$

**Case 2**. Disc($R$) $<< 0$. Alors, pour $j = 1, 2$,

$(R \otimes_{v_j} \mathbf{R})^\times$ a *un seul point fixe* $\tau_j \in \mathcal{H}$.

$$\boxed{\gamma_R := \{(\tau_1, \tau_2)\}}$$

# Le cas ATR

**Troisième cas**. $D_1 < 0, D_2 > 0$. Alors

$(R \otimes_{v_1} \mathbf{R})^\times$ a un unique point fixe $\tau_1 \in \mathcal{H}$.

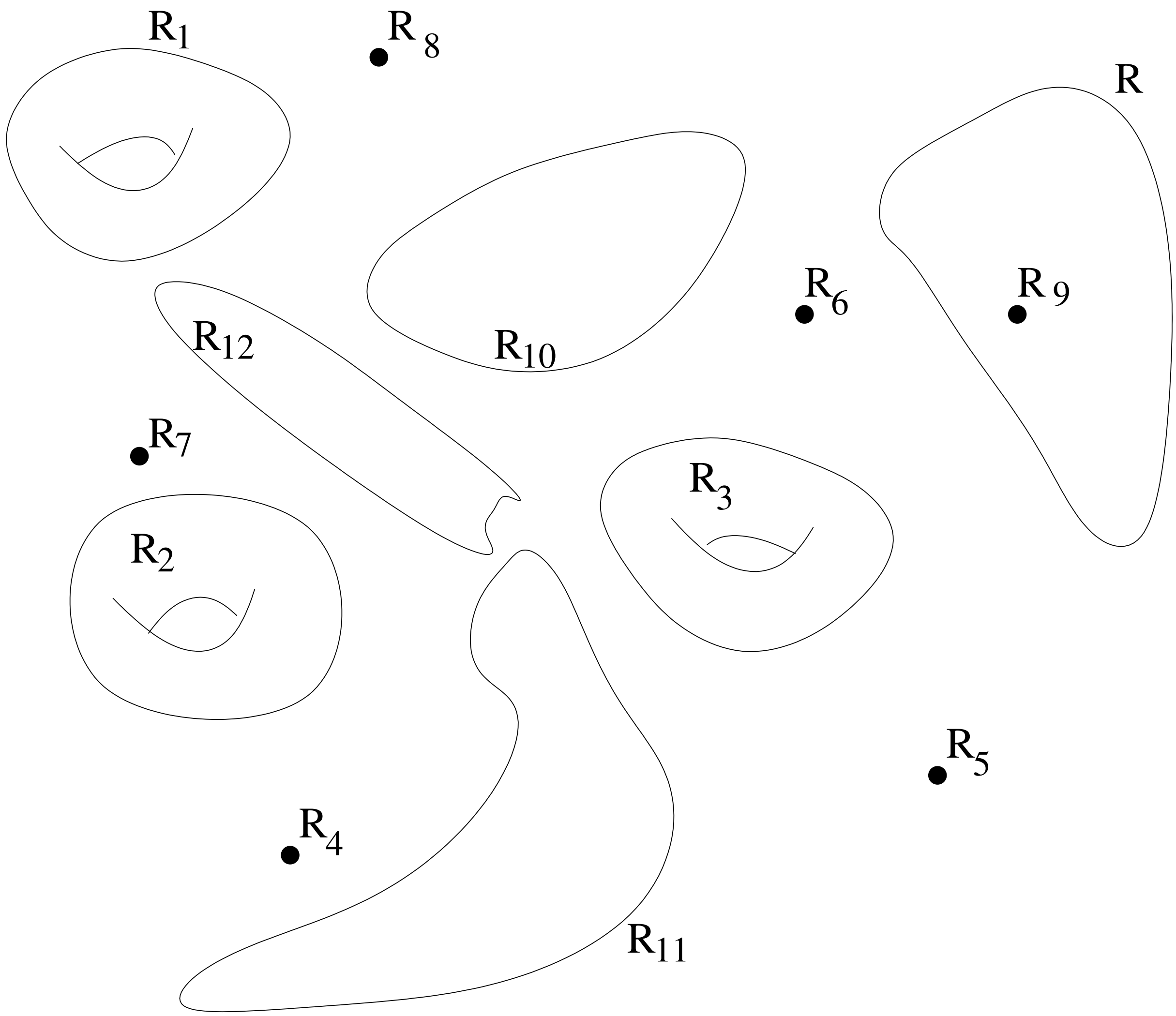
$(R \otimes_{v_2} \mathbf{R})^\times$ a deux points fixes $\tau_2, \tau_2' \in \mathbf{R}$.

Soit $\Upsilon_2 :=$ chemin géodésique allant de $\tau_2$ à $\tau_2'$;

$$\boxed{\gamma_R := R_1^\times \backslash (\{\tau_1\} \times \Upsilon_2)}$$

Le cycle $\gamma_R$ est un cycle fermé de dimension 1 dans $X_F$.

On l'appelle un *cycle ATR*.




*Cycles sur* $X_F$

## Périodes de $\omega_G$: le cas $D >> 0$

**Théorème/conjecture** (Oda) L'ensemble

$$\Lambda_G := \left\langle \int_{\gamma_R} \omega_G, \quad R \in \Sigma_{>>0} \right\rangle \subset \mathbf{C}$$

est un réseau dans $\mathbf{C}$ qui est commensurabe avec le réseau de Weierstrass de $E$.

**Conjecture** (BSD) Soit $D :=$ Disc$(K/F) >>$ 0. Alors

$$J_D := \int_{\gamma_D} \omega_G \neq 0 \quad \text{ssi} \quad \#E(K) < \infty.$$

"La position de $\gamma_D$ dans $H_2(X_F, \mathbf{Z})$ présente une *obstruction* à la presence de points rationnels sur $E(F(\sqrt{D}))$. "

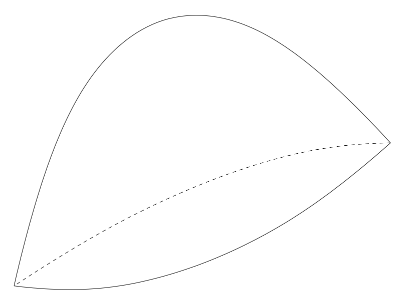
# Périodes de $\omega_G$: le cas ATR

**Theorem**: Les cycles $\gamma_R$ sont *homologiquement triviaux* (après tensorisation par $\mathbf{Q}$).

C'est parce que $H_1(X_F, \mathbf{Q}) = 0$.

Etant donné $R \in \Sigma_D$, soit

$\gamma_R^{\#}$ := une 2-chaine sur $X_F$ ayant $\gamma_R$ comme frontière.



$$P_R := \int_{\gamma_R^{\sharp}} \omega_G \in \mathbf{C}/\Lambda_G \simeq E(\mathbf{C}).$$

# La conjecture sur les points ATR

On suppose que $D_1 < 0$, $D_2 > 0$.

**Conjecture sur les points ATR**. *Si $R$ appartient à $\Sigma_D$, alors le point $P_R$ appartient à $E(H_D) \otimes \mathbf{Q}$, où $H_D$ est le corps de classe de Hilbert de $F(\sqrt{D})$.*

On voudrait mieux comprendre pourquoi les images des cycles ATR sur $X_F$ (qui ne sont *pas algébriques*) par des applications de style "Abel-Jacobi" sont des *points algébriques*.

Applications potentielles:

a) Constructions nouvelles de points algébriques et de systèmes d'Euler.

b) Constructions "explicites" de corps de classe.

# Conjectures de Stark

1. (Charollois, D). Après avoir remplacé “formes modulaires de Hilbert cuspidales” par “séries d’Eisenstein sur le groupe modulaire de Hilbert”, on récupère des versions plus fines (et à consonance plus nettement géométriques) des conjectures de Stark pour les extensions abéliennes de corps ATR.

(Ce colloquium doit beaucoup au point de vue présenté pour la première fois dans

P. Charollois et H. Darmon, *Arguments des unités de Stark et périodes des séries d’Eisenstein,*

http://www.math.mcgill.ca/darmon/pub/pub.html

**Variantes ($p$-adiques, et/ou non ATR)**.

En introduisant des méthodes $p$-adiques, ou en remplacant $\mathbf{GL}_2(F)$ par des goupes associés à des algèbres de quaternions, on peut traiter des cas où $K$ n'est pas ATR, et même où $F$ n'est pas totalement réel.

(Travaux de Matthew Greenberg et Mak Trifkovic; thèse en cours de Jérôme Gärtner).

# Cycles algébriques

Idée de base: remplacer les "cycles ATR sur les surfaces modulaires de Hilbert $X_F$" par des *cycles algébriques* sur des *variétés modulaires*.

**Exemple prototype** (Bertolini, Prasanna, D):

Soitt $K = \mathbf{Q}(\sqrt{-7})$, $E = \mathbf{C}/\mathcal{O}_K$,

$W =$ courbe elliptique universelle sur $X_1(7)$,

$X = W \times E$ (une "variété de Calabi-Yau de dimension trois".)

$$\mathrm{CH}^2(X)_0 = \left\{ \begin{array}{l} \text{cycles algébriques sur } X \\ \text{homologiquement triviaux} \\ \text{de codimension deux} \end{array} \right\} / \simeq .$$

La conjecture de Tate prédit l'existence d'une *correspondance algébrique* $X \longrightarrow E$, qui induit une "paramétrisation modulaire exotique":

$$\Phi : \mathrm{CH}^2(X)_0(F) \longrightarrow E(F),$$

pour tout corps $F$.

**Théorème** (Bertolini, Prasanna, D). Le groupe $\Phi(\mathrm{CH}_2(X)_0(K^{\mathrm{ab}}))$ est un sous-groupe de $E(K^{\mathrm{ab}})$ de *rang infini*, et donne lieu à un *système d'Euler* de points algébriques sur $E$ au sens de Kolyvagin.

Les points de $E(K^{\mathrm{ab}})$ sont le reflet d'une riche structure géométrique: une collection infinie de courbes algébriquement triviales sur une variété de Calabi-Yau de dimension 3.

## **Question pour clore**.

**Définition informelle**: Un point $P \in E(\bar{\mathbf{Q}})$ est dit *modulaire* s'il existe une variété modulaire $X$, une paramétrisation modulaire exotique

$$\Phi : \mathrm{CH}^r(X)_0 \longrightarrow E,$$

et un cycle modulaire $\Delta \in \mathrm{CH}^r(X)$, tel que

$$P = \lambda\Phi(\Delta), \qquad \text{pour } \lambda \in \mathbf{Q}.$$

**Question**. Étant donné $E$, quels points de $E(\bar{\mathbf{Q}})$ sont modulaires?

*Très optimiste*: Tous les points algébriques de $E$ sont modulaires.

*Optimiste*: Tous les points algébriques satisfaisant une "une condition de multiplicité un" sont modulaires.

*Question légitime*: Trouver une caractérisation simple des points modulaires de $E$.