La multiplication complexe et le corps de classes de Hilbert

Martin Orr

17 mars 2010

Résumé

La théorie de la multiplication complexe relie l'arithmétique de certaines courbes elliptiques et les extensions abéliennes des corps quadratiques imaginaires. Cet exposé sera une introduction à cette jolie théorie, et je démontrerai que le corps de classe de Hilbert d'un corps quadratique imaginaire est engendré par le j-invariant d'une courbe elliptique associée. Une connaissance de base des courbes elliptiques serait utile, mais j'expliquerai les résultats nécessaires de la théorie du corps de classes, évitant les idèles.

Cet exposé suit largement l'approche de Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, chapitre 2. Je remercie Jon Nelson de m'avoir donné ses notes très claires d'un exposé semblable que j'ai fait à Cambridge. Je remercie aussi Javier Fresan pour plusieurs corrections linguistiques.

1 Introduction

1.1 Courbes elliptiques

On va se servir de deux définitions d'une *courbe elliptique* :

1. (valide sur un corps quelconque pas de caractéristique 2 ou 3)
   La clôture projective d'une courbe plane non-singulière $y^2 = x^3 + ax + b$.
   La courbe définie par une telle équation est singulière ssi $4a^3 + 27b^2 = 0$.
   On définit le *j-invariant* :
   $$j(E) = \frac{1728.4a^3}{4a^3 + 27b^2}$$
   Sur un corps algébriquement clos, deux courbes sont isomorphes ssi elles ont le même j-invariant.
2. (valide sur $\mathbb{C}$ seulement)
   Un quotient $\mathbb{C}/\Lambda$ pour un réseau $\Lambda \subseteq \mathbb{C}$.
   (Un *réseau* est un sous-groupe discret de $\mathbb{C}$ isomorphe en tant que groupe à $\mathbb{Z}^2$.)

Dans les deux cas, il y a une loi de groupe commutatif naturelle sur la courbe (évident pour la définition 2, pas si évident pour la définition 1).

Un *morphisme* de courbes elliptiques est un morphisme de variétés/de surfaces de Riemann qui est aussi un homomorphisme de groupes.

Fait 1.1. *Sur le corps $\mathbb{C}$, toute courbe vérifiant la définition 1 est isomorphe à une courbe vérifiant la définition 2, et vice versa.*

Sur un corps de caractéristique 0, l'anneau d'endomorphismes $\mathrm{End}(E)$ d'une courbe elliptique est isomorphe à :

1. $\mathbb{Z}$ (cas générique) ; ou
2. un sous-anneau de rang 2 de $\mathfrak{o}_K$, où K est un corps quadratique imaginaire $\mathbb{Q}(\sqrt{-d})$.

Le cas 2 est appelé le cas de la *multiplication complexe*.

1.2 Théorie du corps de classes

Il s'agit des extensions abéliennes des corps de nombres (extensions galoisiennes dont le groupe de Galois est abélien).

La théorie du corps de classes fournit une description abstraite de toutes les extensions abéliennes d'un corps fixé K.

Si $K = \mathbb{Q}$, le théorème de Kronecker-Weber permet d'expliciter la théorie :

Théorème 1.2. *Toute extension abélienne finie de $\mathbb{Q}$ est contenue dans $\mathbb{Q}(\mu_n)$, pour quelque $n \in \mathbb{N}$.*

Si $K = \mathbb{Q}(\sqrt{-d})$, la théorie de la multiplication complexe permet d'expliciter la théorie du corps de classe en termes des points de torsion et du j-invariant d'une courbe elliptique.

(Dans le théorème de Kronecker-Weber, on peut considerer les racines de l'unité comme points de torsion du cercle.)

Aujourd'hui je vais parler du *corps de classes de Hilbert H* :
l'extension abélienne non ramifiée (en tout premier) la plus grande de K.

Si $K = \mathbb{Q}$, il n'y a aucune extension non ramifiée non triviale donc $H = \mathbb{Q}$.

(Théorie du corps de classes : H existe, $\mathrm{Gal}(H/K) = \mathrm{Cl}_K$.)

Le but de l'exposé est de démontrer :

Théorème 1.3. *Si $K = \mathbb{Q}(\sqrt{-d})$ et E une courbe elliptique avec $\mathrm{End}(E) = \mathfrak{o}_K$, alos $H = K(j(E))$.*

2 Endomorphismes sur $\mathbb{C}$

Un morphisme de courbes elliptiques sur $\mathbb{C}$ se relève aux revêtements universels :

$$\begin{array}{ccc} \mathbb{C} & \xrightarrow{\times\alpha} & \mathbb{C} \\ \downarrow & & \downarrow \\ \mathbb{C}/\Lambda & \xrightarrow{\varphi} & \mathbb{C}/\Lambda' \end{array}$$

Par le théorème de Liouville appliqué à la dérivée, l'application $\mathbb{C} \to \mathbb{C}$ doit être multiplication par une constante $\alpha \in \mathbb{C}$. On a $\alpha\Lambda \subseteq \Lambda'$.

Donc $\mathbb{C}/\Lambda \cong \mathbb{C}/\Lambda'$ ssi $\Lambda' = \alpha\Lambda$ pour quelque $\alpha \in \mathbb{C}$.

$\mathrm{End}(E) \cong \{\alpha \in \mathbb{C} : \alpha\Lambda \subseteq \Lambda\}$ est un sous-anneau discret de $\mathbb{C}$, donc un des choix au-dessus.

Si $K = \mathbb{Q}(\sqrt{-d})$ et $\mathfrak{a}$ est un idéal fractionnaire de K, alors $\mathfrak{a}$ est un réseau dans $\mathbb{C}$ et $\mathbb{C}/\mathfrak{a}$ une courbe elliptique avec $\mathrm{End}(\mathbb{C}/\mathfrak{a}) = \mathfrak{o}_K$.

Toute courbe elliptique sur $\mathbb{C}$ avec $\mathrm{End}(E) \cong \mathfrak{o}_K$ est isomorphe à $\mathbb{C}/\mathfrak{a}$ pour quelque $\mathfrak{a} \in \mathfrak{o}_K$.

Donc $\mathcal{E}(\mathfrak{o}_K) := \{\text{courbes ell. } E/\mathbb{C} \text{ avec } \mathrm{End}(E) \cong \mathfrak{o}_K\}/(\text{isom sur } \mathbb{C})$ est en bijection avec Cl_K.

3 Actions des groupes sur $\mathcal{E}(\mathfrak{o}_K)$

3.1 Action du groupe des classes

I_K (le groupe des idéaux fractionnaires) agit sur $\mathcal{E}(\mathfrak{o}_K)$:
Si $E = \mathbb{C}/\Lambda \in \mathcal{E}(\mathfrak{o}_K)$, alors

$$\mathfrak{a} * E := \mathbb{C}/\mathfrak{a}^{-1}\Lambda \in \mathcal{E}(\mathfrak{o}_K)$$

Noyau de l'action : $\mathbb{C}/\mathfrak{a}^{-1}\Lambda \cong \mathbb{C}/\Lambda$ ssi $\mathfrak{a}$ principal.

Donc Cl_K agit librement sur $\mathcal{E}(\mathfrak{o}_K)$; l'action est transitive car Cl_K, $\mathcal{E}(\mathfrak{o}_K)$ sont finis de la même cardinalité.

3.2 Action du groupe de Galois

Revenons à la définition algébrique d'une courbe elliptique :

$$E : y^2 = x^3 + ax + b$$

Si $\sigma \in \mathrm{Aut}(\mathbb{C})$, on définit

$$E^\sigma : y^2 = x^3 + \sigma(a)x + \sigma(b)$$

Alors $j(E^\sigma) = \sigma(j(E))$, $\mathrm{End}(E^\sigma) \cong \mathrm{End}(E)$.

Donc si $E \in \mathcal{E}(\mathfrak{o}_K)$, alors $E^\sigma \in \mathcal{E}(\mathfrak{o}_K)$.

Il y a un nombre fini de possibilités pour $\sigma(j(E))$, donc $j(E)$ est algébrique.

Comme Cl_K agit librement et transitivement sur $\mathcal{E}(\mathfrak{o}_K)$, $E^\sigma \cong \mathfrak{a} * E$ pour une seule classe $\bar{\mathfrak{a}} \in \mathrm{Cl}_K$.

Donc on définit $F : \mathrm{Gal}(\bar{K}/K) \to \mathrm{Cl}_K$ par $E^\sigma \cong F(\sigma) * E$.

Fait 3.1. *L'application F ne dépend pas du choix de $E \in \mathcal{E}(\mathfrak{o}_K)$. F est un homomorphisme de groupes.*

4 Application d'Artin

4.1 Définition de l'application d'Artin

K un corps de nombres quelconque,
L/K une extension finie abélienne,
$\mathfrak{p}$ un premier de K, non ramifiée dans L,
$\mathfrak{P}$ un premier de L au-dessus de $\mathfrak{p}$.

Alors il y a un unique $\sigma \in \mathrm{Gal}(L/K)$ tel que :

(i) $\sigma(\mathfrak{P}) = \mathfrak{P}$; et
(ii) $\sigma(x) \equiv x^q \bmod \mathfrak{P}$ pour tout $x \in L$ (où $q = \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p})$).

A priori, σ dépend de $\mathfrak{P}$; mais il est déterminé par $\mathfrak{p}$ à conjugaison près. L/K est supposée abélienne, donc en fait $\sigma_{\mathfrak{p}} = \sigma$ ne dépend que de $\mathfrak{p}$.

Soit I'_K le groupe d'idéaux fractionnaires de K engendrés par les premiers non ramifiés dans L.

L'*application d'Artin* $(-, L/K) : I'_K \to \mathrm{Gal}(L/K)$ est définie sur les premiers par $(\mathfrak{p}, L/K) = \sigma_{\mathfrak{p}}$, puis on étend en un homomorphisme de groupes.

Fait 4.1 (conséquence de la théorie du corps de classes)**.** *$L = H$ ssi le noyau de l'application d'Artin est $P_K \cap I'_K$. (P_K = idéaux principaux.)*

4.2 Application à la multiplication complexe

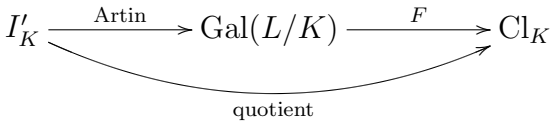
Soit $K = \mathbb{Q}(\sqrt{-d})$, $L = K(j(E))$.
Si $\sigma \in \mathrm{Gal}(\bar{K}/K)$, alors

$$\sigma \text{ fixe } L \;\Leftrightarrow\; \sigma(j(E)) = j(E) \;\Leftrightarrow\; E^\sigma \cong E \;\Leftrightarrow\; F(\sigma) = 1 \in \mathrm{Cl}_K.$$

Donc $\mathrm{Gal}(\bar{K}/L)$ est distingué dans $\mathrm{Gal}(\bar{K}/K)$, et L/K est galoisienne.

De plus F se factorise à travers une injection $\mathrm{Gal}(L/K) \hookrightarrow \mathrm{Cl}_K$, donc L/K est abélienne.

On a un diagramme :



On va montrer que ce diagramme commute. Ensuite on pourra déduire que $H = K(j(E))$.

Preuve du théorème 1.2. $F : \mathrm{Gal}(L/K) \to \mathrm{Cl}_K$ est injective, donc le noyau de l'application quotient est égale au noyau de l'application d'Artin.

Or le noyau de l'application quotient est $P_K \cap I'_K$, et on peut appliquer le Fait 4.1. □

4.3 Démonstration de la commutativité du diagramme

Lemme 4.2. *Si* $\mathfrak{a} \in I'_K$, *alors* $F((\mathfrak{a}, L/K)) = \bar{\mathfrak{a}}$.

Démonstration. On élarge L en M de sorte que :

(i) il y a des représentants $E_1, \ldots, E_h$ de tous classes de $\mathcal{E}(\mathfrak{o}_K)$ définis sur M ;
(ii) tous morphismes $E_i \to E_{i'}$ sont définis sur M ;
(iii) M/K est galoisienne finie.

(Il existe une extension finie vérifiant (ii) car $\mathrm{Hom}(E_i, E_{i'})$ est un $\mathbb{Z}$-module de type fini pour chaque i, i'.)

D'abord on va supposer que : $\mathfrak{a} = \mathfrak{p}$ est premier dans K de degré 1 et

(i) $\mathfrak{p}$ est non ramifié dans M ;
(ii) tout E_i a bonne réduction en tout premier $\mathfrak{P}$ de M au-dessus de $\mathfrak{p}$;
(iii) $\mathfrak{P}$ ne divise pas $j(E_i) - j(E_{i'})$ pour tout i, i' et tout premier $\mathfrak{P}$ de M au-dessus de $\mathfrak{p}$.

(L'importance des conditions (i) et (ii) est évident. On verra l'importance de la condition (iii) à la fin de la preuve. Les trois conditions n'excluent qu'un nombre fini des premiers.)

Soit $E = E_1 \cong \mathbb{C}/\Lambda$, E' un des E_i isomorphe à $\mathfrak{p} * E$.

$\mathfrak{p}^{-1}\Lambda \supseteq \Lambda$ donc on a une application quotient $\mathbb{C}/\Lambda \to \mathbb{C}/\mathfrak{p}^{-1}\Lambda$, de degré $\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}) = p$.

Elle correspond à $\varphi : E \to E'$.

On réduit modulo $\mathfrak{P}$, un premier de M au-dessus de $\mathfrak{p}$: $\tilde{\varphi} : \tilde{E} \to \tilde{E}'$.

Un argument astucieux (utilisant une différentielle sur E) montre que $\tilde{\varphi}$ est non séparable, donc elle se factorise par le morphisme de Frobenius :

$$\tilde{E} \xrightarrow[\deg p]{\text{Frob}} \tilde{E}^p \longrightarrow \tilde{E}', \qquad \tilde{E} \xrightarrow[\tilde{\varphi} \quad \deg p]{} \tilde{E}'$$

Donc $\tilde{E}^p \to \tilde{E}'$ est de degré 1, i.e. un isomorphisme.

Donc $j(\tilde{E}') = j(\tilde{E}^p) = j(\tilde{E})^p$ dans $\mathbb{F}_{\mathfrak{P}}$.

Donc $j(E') \equiv j(E)^p \equiv \sigma_{\mathfrak{p}}(j(E)) \equiv j(E^{\sigma_{\mathfrak{p}}}) \bmod \mathfrak{P}$.

Condition (iii) sur $\mathfrak{p}$ implique que $E' \cong E^{\sigma_{\mathfrak{p}}}$, c'est-à-dire $\mathfrak{p} * E \cong F(\sigma_{\mathfrak{p}}) * E$.

Enfin pour $\mathfrak{a} \in I'_K$ général, on peut se ramener au cas précédent en appliquant le théorème de Chebotarev. □