Arithmetic Class Invariants and Semi-stable Elliptic Curves

Classical Kummer Theory

Suppose that :

- $n > 1$ is a natural integer.
- K is a number field containing the n-th roots of unity.
- x is an element of $K^\times$ such that $x \notin (K^\times)^d$ for all $d|n$, $d \neq 1$.

Then $F := K(\sqrt[n]{x})$ is an extension of K with Galois group $\Gamma := \mathbb{Z}/n\mathbb{Z}$. In 1962, A. Frohlich defined the "Kummer order" $\mathfrak{A}(x)$ to be the order generated over $\mathcal{O}_K$ by the integral radical elements of F.

In 1980, Martin Taylor determined the Galois module structure of $\mathfrak{A}(x)$.

Theorem 1. — $\mathfrak{A}(x)$ *and* $\mathcal{M}(K[\Gamma])$ *are isomorphic as* $\mathcal{M}(\mathbb{Q}[\Gamma])$*-modules.*

Here, $\mathcal{M}(C)$ denotes the (unique) maximal order in the algebra C.

Geometric Analogue of Kummer Theory

Let $\mathbf{G}_{\mathsf{m}}$ denote the multiplicative group scheme over $S := Spec(\mathcal{O}_K)$. Then we have an exact sequence of fppf sheaves

$$0 \longrightarrow \mu_n \longrightarrow \mathbf{G}_{\mathsf{m}} \xrightarrow{[n]} \mathbf{G}_{\mathsf{m}} \longrightarrow 0\,.$$

By applying the functor of sections on S, we get a coboundary map

$$\delta : \mathbf{G}_{\mathsf{m}}(S) = \mathcal{O}_K^{\times} \longrightarrow H^1(S, \mu_n)\,.$$

The group $H^1(S, \mu_n)$ is the set of μ_n-torsors over S. These torsors are spectra of $\mathcal{O}_K$-orders in Galois K-algebras with group $\mathbb{Z}/n\mathbb{Z}$. If x is congruent to 1 modulo a sufficiently large power of n, then $\delta(x) = Spec(\mathfrak{A}(x))$.

We say that $\delta(x)$ is obtained by dividing x by $[n]$ in the group scheme $\mathbf{G}_{\mathsf{m}}$.

The μ_n-torsors are spectra of Galois algebras. Now we want to study the Galois structure of these torsors.

Picard Invariants

This was done by W. Waterhouse in 1971.

Let G be a finite flat group scheme over S, and denote by G^D the Cartier dual of G. Then we have a homomorphism

$$\pi : H^1(S, G^D) \simeq \mathrm{Ext}^1(G, \mathbf{G}_\mathrm{m}) \longrightarrow \mathrm{Pic}(G)\,.$$

The isomorphism is given by the local-global spectral sequence for Ext^i, the other map is the natural one.

The group $\mathrm{Pic}(G)$ can be interpreted as the classgroup of the $\mathcal{O}_K$-order representing the affine scheme G. One can consider that π mesures the Galois structure of G^D-torsors. In the Kummer context, we have :

Theorem 2. — *Suppose that $G^D = \mu_n$. Then $\mathrm{Im}\,\delta$ is equal to $\ker\pi$.*

So, μ_n-torsors obtained by dividing points in $\mathbf{G}_\mathrm{m}$ have a trivial structure in $\mathrm{Pic}(\mathbb{Z}/n\mathbb{Z})$.

Abelian Varieties

We can replace the multiplicative group $\mathbf{G}_{\mathrm{m}}$ by other group schemes. Suppose that :

- A_K is an abelian variety defined over K.
- A_K^t is the dual abelian variety of A_K.
- $\mathcal{A}$ and $\mathcal{A}^t$ are the Néron models of A_K and A_K^t respectively.

Good Reduction Case

Moreover, suppose that A_K has everywhere good reduction. Then :

- $\mathcal{A}$ and $\mathcal{A}^t$ are abelian schemes, dual to each other.
- $\mathcal{A}[n]$ and $\mathcal{A}^t[n]$ are finite flat group schemes, Cartier dual to each other.
- we have an exact sequence of fppf sheaves

$$0 \longrightarrow \mathcal{A}^t[n] \longrightarrow \mathcal{A}^t \xrightarrow{[n]} \mathcal{A}^t \longrightarrow 0\,.$$

In 1988, M. Taylor defined a homomorphism ψ_n as the composition of the maps

$$\mathcal{A}^t(S) \longrightarrow H^1(S, \mathcal{A}^t[n]) \longrightarrow \mathrm{Pic}(\mathcal{A}[n])\,.$$

In other words ψ_n, the so-called *class invariant homomorphism*, mesures the Galois structure of torsors obtained by dividing points by $[n]$ in the group scheme $\mathcal{A}^t$.

Taylor, Srivastav, Agboola and Pappas (1990–1996) proved the following :

Theorem 3. — *Suppose that A_K is an elliptic curve, and that n is coprime to 6. Then $\mathcal{A}^t(S)_{\mathrm{Tors}}$ is contained in $\ker \psi_n$.*

This result implies the existence of Galois generators for certain rings of integers of abelian extensions of K.

General Case

We do not suppose any more that A_K has everywhere good reduction. Let us denote by $\mathcal{A}^\circ$ the identity component of $\mathcal{A}$, so that $\mathcal{A}^\circ$ has connected fibers.
The group $\mathcal{A}^\circ[n]$ is no longer necessarily finite, so we have to replace it by another group scheme.

Suppose that :
- G is a finite flat subgroup scheme of $\mathcal{A}^\circ$.
- $\mathcal{B}$ is the quotient $\mathcal{A}^\circ/G$.

Then we have an exact sequence of fppf sheaves

$$0 \longrightarrow G \longrightarrow \mathcal{A}^\circ \longrightarrow \mathcal{B} \longrightarrow 0\,.$$

We want to dualize this sequence. So we have to generalise the duality of abelian schemes.

Remember that, for an abelian scheme $\mathcal{Q}$, one defines the dual abelian scheme

$$\mathcal{Q}^* := \underline{\mathrm{Ext}}^1(\mathcal{Q}, \mathbf{G}_{\mathrm{m}})\,.$$

The dual properties of $\mathcal{Q}$ and $\mathcal{Q}^*$ then follow from the fact that $\underline{\mathrm{Hom}}(\mathcal{Q}, \mathbf{G}_{\mathrm{m}}) = 0$ in all the usual topologies.

Unfortunately, $\underline{\mathrm{Hom}}(\mathcal{A}^\circ, \mathbf{G}_{\mathrm{m}})$ is not zero in general (take any point $\mathfrak{p}$ of S where $\mathcal{A}^\circ$ has multiplicative reduction, and look at the sections on $Spec(k_{\mathfrak{p}})$).

In order to correct this, we use the *small fppf site* on S to which $Spec(k_{\mathfrak{p}}) \to S$ does not belong, namely the site of all flat S-schemes for the fppf topology. Then $\underline{\mathrm{Hom}}_S(\mathcal{A}^\circ, \mathbf{G}_{\mathrm{m}}) = 0$.

Now working in the small fppf site on S, we apply the functor $\underline{\mathrm{Hom}}_S(-, \mathbf{G}_{\mathrm{m}})$ to the first sequence and get a long exact sequence

$$0 = \underline{\mathrm{Hom}}_S(\mathcal{A}^\circ, \mathbf{G}_{\mathrm{m}}) \to \underline{\mathrm{Hom}}_S(G, \mathbf{G}_{\mathrm{m}}) \to$$

$$\underline{\mathrm{Ext}}^1_S(\mathcal{B}, \mathbf{G}_{\mathrm{m}}) \to \underline{\mathrm{Ext}}^1_S(\mathcal{A}^\circ, \mathbf{G}_{\mathrm{m}}) \to \underline{\mathrm{Ext}}^1_S(G, \mathbf{G}_{\mathrm{m}}) = 0$$

The last term vanishes by a well-known result of Waterhouse.

Hence

Theorem 4. — *We have an exact sequence*

$$0 \to G^D \to \underline{\mathsf{Ext}}^1_S(\mathcal{B}, \mathbf{G}_{\mathsf{m}}) \to \underline{\mathsf{Ext}}^1_S(\mathcal{A}^\circ, \mathbf{G}_{\mathsf{m}}) \to 0\,.$$

When we restrict all those sheaves to an open subscheme $U \subseteq S$ above which A_K has everywhere good reduction, we recover the usual duality for abelian schemes.

Now applying standard cohomology, we get a coboundary map

$$\delta : \mathsf{Ext}^1(\mathcal{A}^\circ, \mathbf{G}_{\mathsf{m}}) \longrightarrow H^1(S, G^D)\,.$$

On the other hand, Grothendieck's theory of biextensions allows us to define a map

$$\gamma : \mathcal{A}^t(S) \to \mathsf{Ext}^1(\mathcal{A}^\circ, \mathbf{G}_{\mathsf{m}})\,.$$

We then obtain our ψ by composing the arrows

$$\mathcal{A}^t(S) \to \mathrm{Ext}(\mathcal{A}^\circ, \mathbf{G}_{\mathrm{m}}) \to H^1(S, G^D) \to \mathrm{Pic}(G)\,.$$

Thus we obtain a generalisation of Taylor's construction.

Moreover, one can give an alternative description of ψ : the so-called *geometric description*. Given $x \in \mathcal{A}^t(S)$, we denote by $\mathcal{L}(x)$ the line bundle on $\mathcal{A}^\circ$ associated to $\gamma(x)$. We show :

Lemma 5. — *For all $x \in \mathcal{A}^t(S)$, the restriction of the line bundle $\mathcal{L}(x)$ to $G \subseteq \mathcal{A}^\circ$ is equal to $\psi(x)$ in the group* Pic(G)*.*

This generalises a similar result obtained by Agboola (1994) in the case of good reduction.

Using the theory of cubic torsors, and results of Moret-Bailly, one can show

Lemma 6. — *Suppose that A_K is an elliptic curve. Then there is an isomorphism*

$$\mathcal{A}(S) \xrightarrow{\sim} \mathrm{Pic}^0_r(\mathcal{A}^\circ)\,.$$

This generalizes the self-duality of elliptic curves, which is an essential argument in Pappas's proof. Assuming semi-stability of A_K, we extend the other arguments and show

Theorem 7. — *Suppose that A_K is a semi-stable elliptic curve, and that $\#G$ is coprime to 6. Then $\mathcal{A}^t(S)_{\mathrm{Tors}}$ is contained in $\ker\psi$.*

An Elliptic Example

Let E be the Néron model of the elliptic curve E_K defined over K by the equation

$$y^2 + y = x^3 - x^2 \, .$$

The curve E_K is semi-stable and $E_K(K)$ contains an element of order 5, which generates a subgroup G of E isomorphic to $(\mathbb{Z}/5\mathbb{Z})_S$. The quotient E_K/G_K is the elliptic curve F_K with equation

$$y^2 + y = x^3 - x^2 - 10x - 20 \, .$$

Let p in $E(S)_{\mathrm{Tors}}$. Our result states that $\psi(p)$ is a $\boldsymbol{\mu}_{5/S}$-torsor with trivial Galois structure.