HOPF-GALOIS THEORY AND ELLIPTIC CURVES

JEAN GILLIBERT

Abstract. We first introduce the ideas of Hopf-Galois theory as an attempt to taming wild extensions with Hopf algebras, in connection with the problems of Galois module structure in arithmetic. Then, as in the works of M. Taylor and others, we explain how one obtains, from an elliptic curve having everywhere good reduction, a family of algebras with trivial Galois module structure.

Let $K/\mathbf{Q}$ be a finite Galois extension, G the Galois group of $K/\mathbf{Q}$, and $\mathcal{O}_K$ the ring of integers of K. It is well known that $\mathcal{O}_K$ is a free $\mathbf{Z}$-module of rank $[K : \mathbf{Q}] = \#G$. We can ask the following :

Question : Does there exists $\alpha \in \mathcal{O}_K$ such that $\{\sigma(\alpha) \mid \sigma \in G\}$ is a $\mathbf{Z}$-basis of $\mathcal{O}_K$?

In more algebraic terms, we are trying to understand the structure of $\mathcal{O}_K$ as $\mathbf{Z}[G]$-module. It is a fundamental problem of number theory to classify this structure.

The Noether criterion states that $\mathcal{O}_K$ is a locally free rank-one $\mathbf{Z}[G]$-module if and only if $K/\mathbf{Q}$ is tamely ramified. This condition is equivalent to the surjectivity of the trace map $\mathcal{O}_K \to \mathbf{Z}$.

In the wild case, this is no longer true. So we need to introduce another Galois structure, for which we want $\mathcal{O}_K$ to be locally free. The Hopf structure is an answer.

1. The Galois Theory Revisited

We will need some basic definitions. All our rings and algebras will be commutative with a unit element. We fix once for all a ring R. Unadorned tensors are over R. We say an R-algebra is finite if it is finitely generated and projective as an R-module.

If M is an R-module, we denote by $M^* = \mathrm{Hom}_R(M, R)$ the linear dual of M. Recall that the functor $\mathcal{D} : M \mapsto M^*$ defines a contravariant auto-equivalence of the category of finitely generated and projective R-modules. Moreover, $\mathcal{D}$ preserves the tensor product : if M and N are finitely generated and projective R-modules, then there is a canonical isomorphism between $(M \otimes N)^*$ and $M^* \otimes N^*$. This isomorphism will allow us an identification.

We now introduce the notion of Hopf algebra, a very rich algebraic structure which has strong links with algebraic geometry. We will use a Hopf algebra in place of the deficient $\mathbf{Z}[G]$.

1.1. **Hopf algebras.** An R-Hopf algebra is an R-algebra H together with R-algebra maps $\Delta : H \to H \otimes H$, $\varepsilon : H \to R$ and $\lambda : H \to H$, satisfying the following conditions :

(i) Coassociativity : the diagram

$$\begin{tikzcd}
H \arrow[r, "\Delta"] \arrow[d, "\Delta"'] & H \otimes H \arrow[d, "\Delta \otimes id_H"] \\
H \otimes H \arrow[r, "id_H \otimes \Delta"'] & H \otimes H \otimes H
\end{tikzcd}$$

is commutative.

(ii) Counitary : the diagram

$$\begin{tikzcd}
H \otimes H \arrow[d, "id_H \otimes \varepsilon"'] & H \arrow[l, "\Delta"'] \arrow[r, "\Delta"] \arrow[d, equal] & H \otimes H \arrow[d, "\varepsilon \otimes id_H"] \\
H \otimes R \arrow[r] & H & R \otimes H \arrow[l]
\end{tikzcd}$$

is commutative.

(iii) Antipode property : the diagram

$$\begin{tikzcd}
H \otimes H \arrow[d, "id_H \otimes \lambda"'] & H \arrow[l, "\Delta"'] \arrow[r, "\Delta"] \arrow[d, "\iota \circ \varepsilon"'] & H \otimes H \arrow[d, "\lambda \otimes id_H"] \\
H \otimes H \arrow[r, "\mu"] & H & H \otimes H \arrow[l, "\mu"']
\end{tikzcd}$$

is commutative, where $\mu : H \otimes H \to H$ and $\iota : R \to H$ are the multiplication and unit maps, respectively, of the algebra H.

The maps Δ, ε and λ are called comultiplication, counit and antipode, respectively, of the Hopf algebra H.

Example. The integral group ring $\mathbf{Z}[G]$ is a $\mathbf{Z}$-Hopf algebra, where Δ and ε are defined, for all $\sigma \in G$, by $\Delta(\sigma) = \sigma \otimes \sigma$ and $\varepsilon(\sigma) = 1$.

1.2. **Cartier duality.** If H is a finite R-Hopf algebra, then we can apply the functor $\mathcal{D}$, which gives us a structure of R-Hopf algebra on H^*. The comultiplication of H^* is ${}^t\mu$, the counit of H^* is ${}^t\iota$, etc. We say that H and H^* are Cartier dual to each other. For example, the Cartier dual of the integral group ring $\mathbf{Z}[G]$ is the algebra $Map(G, R)$. If we denote by $(f_g)_{g \in G}$ the canonical basis of $Map(G, R)$, then the comultiplication is given by $\Delta(f_g) = \sum_{h \in G} f_{gh^{-1}} \otimes f_h$, the counit is given by $\varepsilon(f_g) = \delta_{1,g}$.

1.3. **Comodules.** A left H-comodule is an R-module C together with an R-linear map $\rho : C \to H \otimes C$ such that the diagrams

$$\begin{tikzcd}
C \arrow[r, "\rho"] \arrow[d, "\rho"'] & H \otimes C \arrow[d, "\Delta\otimes id_C"] \\
H \otimes C \arrow[r, "id_H\otimes\rho"'] & H \otimes H \otimes C
\end{tikzcd}$$

and

$$\begin{tikzcd}
C \arrow[r, "\rho"] \arrow[d, equal] & H \otimes C \arrow[d, "\varepsilon\otimes id_C"] \\
C & R \otimes C \arrow[l]
\end{tikzcd}$$

are commutative. The map ρ is called the coaction associated to C.

Moreover, if C is endowed with the structure of an R-algebra, such that ρ is in addition an R-algebras morphism, then we say that C is an H-comodule algebra.

We denote by C^{coH} the set $\{m \in C \mid \rho(m) = 1_H \otimes m\}$. In the case when $H = Map(G, R)$, then C is a right G-module, and $C^{coH} = C^G$.

1.4. **Galois objects.** A left H-Galois object is a finite H-comodule algebra C, satisfying $C^{coH} = R$, and such that the map

$$\begin{array}{rcl}
\gamma_C : C \otimes C & \longrightarrow & H \otimes C \\
x \otimes y & \longrightarrow & \rho(x)(1_H \otimes y)
\end{array}$$

is a R-algebras isomorphism, where ρ denotes the coaction on C, the product being computed in the algebra $H \otimes C$.

Example. Let C be a finite R-algebra, with a right action of the finite group G on C. Following Chase and Harrison, C is a Galois extension of R with group G if $R = C^G$ and the map

$$r : C \otimes C \longrightarrow Map(G, C)$$

given by $r(x \otimes y) = \sum_{\sigma\in G} xy^\sigma f_\sigma$ is an isomorphism of left C-modules, where we let C act on $C \otimes C$ via the first factor. This is the same to say that C is a $Map(G, R)$-Galois object.

Example. Let $n > 0$ be an integer. We denote by ζ a 2^{n+1}-th root of unity. Then $K = \mathbf{Q}[\zeta]$ is an abelian Galois extension of $\mathbf{Q}$, with group $(\mathbf{Z}/2^{n+1}\mathbf{Z})^\times$. The ring $\mathcal{O}_K$ is equal to $\mathbf{Z}[\zeta]$, but $K/\mathbf{Q}$ is wild (because 2^{n+1} is not square-free !). So we introduce a group G, cyclic of order 2^n with generator σ, the algebra $H = \mathbf{Z}[G]$, and the coaction $\rho : \mathbf{Z}[\zeta] \to \mathbf{Z}[G] \otimes \mathbf{Z}[\zeta]$ defined by $\rho(\zeta^i) = \sigma^i \otimes \zeta^i$. Then the map γ satisfies $\gamma(\zeta^i \otimes \zeta^j) = \sigma^i \otimes \zeta^{i+j}$, so γ is an isomorphism (it changes a basis of $\mathbf{Z}[\zeta]\otimes\mathbf{Z}[\zeta]$ into a basis of $\mathbf{Z}[G]\otimes\mathbf{Z}[\zeta]$), and $\mathcal{O}_K$ is an H-Galois object. But G is not the Galois group of $K/\mathbf{Q}$.

If H and C are both finitely generated and projective R-modules, then the following data are equivalent :

(1) a structure of left H-comodule on C.
(2) a structure of left H^*-module on C^*.
(3) a structure of right H^*-module on C.

Let C be an H-Galois object. We say that C has a normal basis if C is isomorphic to H as an H^*-module, or, equivalently, if C^* is a free rank-one H^*-module.

We now introduce a kind of dual version of the tensor product. Let C_1 be a right H-comodule, and C_2 a left H-comodule. Let ρ_1 and ρ_2 denote the corresponding coactions. We define the cotensor product of C_1 and C_2 to be the kernel of the map

$$\rho_1\otimes id_{C_2}-id_{C_1}\otimes\rho_2 : C_1\otimes C_2 \longrightarrow C_1\otimes H\otimes C_2$$

we denote by $C_1\Box_H C_2$ this cotensor product. Of course, when H is cocommutative, there is no difference to make between left and right H-comodules, and the cotensor product of two H-comodules (provided that they are flat as R-modules) is again an H-comodule.

If H is finite and cocommutative, then the set of isomorphism classes of H-Galois objects is a group, the composition law being given by the cotensor product. The inverse of the H-comodule algebra C is the same algebra C with coaction $(\lambda\otimes id_C)\circ\rho$, where ρ denotes the coaction associated to C. We will denote this group by $Gal(H)$.

On the other hand, if A is any (commutative) ring, the Picard group of A is the set of isomorphism classes of invertible A-modules, the law being given by the tensor product over A. Recall that an A-module M is said invertible iff there exists an A-module N such that $M\otimes_A N\simeq A$. In this case, N is isomorphic to $\mathrm{Hom}_A(M,A)$.

Using the functor $\mathcal{D}$, the cotensor product $C_1\Box_H C_2$ of H-comodules C_1 and C_2 is changed into the tensor product $C_1^*\otimes_{H^*}C_2^*$. Moreover, the map sending the class of the H-Galois object C to the class of the H^*-module C^* is a group homomorphism

$$\pi : Gal(H) \longrightarrow \mathrm{Pic}(H^*)$$

which is known as the Picard-invariant map. The kernel of this map is the set of H-Galois objects having a normal basis. The image is the set of realizable classes.

Remark. The ring H^* being commutative, an invertible H^*-module is the same than a locally free rank-one H^*-module. So we could replace the group $\mathrm{Pic}(H^*)$ by the class-group $Cl(H^*)$, which is the kernel of the rank map $\mathrm{rk} : K_0(H^*) \to \mathbf{Z}$. Here, the composition law is induced by the direct sum.

2. Geometry and Torsors

The algebraic geometry associates to any (commutative) ring R a geometric space, namely the spectrum of R, which we will denote by $Spec(R)$. Our algebraic structures can then be interpreted geometrically as follows :

(1) H is an R-Hopf algebra $\Longleftrightarrow$ $Spec(H)$ is a $Spec(R)$-group scheme.
(2) C is an H-comodule algebra $\Longleftrightarrow$ the group scheme $Spec(H)$ acts on the scheme $Spec(C)$.
(3) C is an H-Galois object $\Longleftrightarrow$ $Spec(C)$ is a $Spec(H)$-torsor (or $Spec(H)$-principal homogeneous space).

Let $S = Spec(R)$, and $\underline{G} = Spec(H)$. If H is cocommutative, then $\underline{G}$ is a commutative S-group scheme. We can then introduce the contracted product. If Y_1 and Y_2 are two $\underline{G}$-torsors (over S), then $\underline{G}$ acts on $Y_1 \times_S Y_2$ by $g.(y_1, y_2) = (g.y_1, g^{-1}.y_2)$. We define $Y_1 \wedge^{\underline{G}} Y_2$ to be the quotient of $Y_1 \times_S Y_2$ by this action (also called the scheme of orbits of $Y_1 \times_S Y_2$ under the action of $\underline{G}$). This operation turns the set of isomorphism classes of $\underline{G}$-torsors into an abelian group, which we denote by $H^1(S, \underline{G})$. Moreover, if C_1 and C_2 are two H-Galois objects, then $Spec(C_1) \wedge^{\underline{G}} Spec(C_2)$ is isomorphic to $Spec(C_1 \square_H C_2)$. This shows that $Gal(H)$ is isomorphic to the first cohomology group $H^1(S, \underline{G})$.

2.1. **Class-invariant homomorphism.**

Let K be a number field, E an elliptic curve defined over K, having everywhere good reduction, and $\mathcal{E}$ the Néron model of E. Remember that $\mathcal{E}$ is an abelian scheme over $S = Spec(\mathcal{O}_K)$. Moreover, for every integer $n > 1$, the group scheme $\mathcal{E}[n]$ is finite and locally free on S, so there exists a finite $\mathcal{O}_K$-Hopf algebra H such that $\mathcal{E}[n] = Spec(H)$, and we have an exact sequence

$$0 \longrightarrow \mathcal{E}[n] \longrightarrow \mathcal{E} \xrightarrow{[n]} \mathcal{E} \longrightarrow 0$$

so $[n] : \mathcal{E} \to \mathcal{E}$ is an $\mathcal{E}[n]$-torsor. By pullback, we can associate to every point $p \in \mathcal{E}(S)$ an $\mathcal{E}[n]$-torsor over S, which we denote by $[n]^{-1}p$. We obtain a map

$$\delta_n : \mathcal{E}(S) \longrightarrow H^1(S, \mathcal{E}[n])$$

which is a group homomorphism. Now we can compose δ_n with π, we obtain a homomorphism :

$$E(K) = \mathcal{E}(S) \xrightarrow{\delta_n} H^1(S, \mathcal{E}[n]) \xrightarrow{\pi} \mathrm{Pic}(H^*)$$

denoted by ψ_n, which is Taylor's class-invariant homomorphism [T].

2.2. **Geometric description.** In geometric language, an invertible A-module is a line bundle on $Spec(A)$. Remember the duality of elliptic curves : points of E are in one-to-one correspondance with line bundles on the dual elliptic curve E^*. The hypothesis of good reduction allow us to do the same with the abelian scheme $\mathcal{E}$. We can resume the situation by the following diagram

$$\begin{tikzcd}
\mathcal{E}(S) \arrow[r] \arrow[d, equal] & \mathrm{Pic}^0_r(\mathcal{E}^*) \arrow[r, "\mathrm{res}"] & \mathrm{Pic}(\mathcal{E}^*[n]) \arrow[d, equal] \\
E(K) \arrow[r, "\delta_n"] & H^1(S, \mathcal{E}[n]) \arrow[r, "\pi"] & \mathrm{Pic}(H^*)
\end{tikzcd}$$

Then, arguments given by Agboola in [A1] show that this diagram commutes. This gives us a geometric description of ψ_n.

The main interest of ψ_n is to build H-Galois objects which have a normal basis. We have the following :

Theorem 2.1. *Suppose n is coprime to 6, and let $p \in E(K)$ be a torsion point. Then $p \in \ker \psi_n$.*

This theorem was established first by Srivastav and Taylor in [S-T] (when E is a CM elliptic curve, and n is a power of some prime $l > 3$), then (without the CM hypothesis) by Agboola in [A2]. The general proof was given by Pappas in [P1].

References

[A1] A. Agboola, *A geometric description of the class invariant homomorphism*, J. Théor. Nombres Bordeaux **6** (1994), 273–280.

[A2] ———, *Torsion points on elliptic curves and Galois module structure*, Inventiones Mathematicae **123** (1996), 105–122.

[C-S] S.U. Chase and M.E. Sweedler, *Hopf algebras and Galois theory*, Lecture Notes in Mathematics **97** (1969), Springer-Verlag.

[P1] ———, *On torsion line bundles and torsion points on abelian varieties*, Inventiones Mathematicae **133** (1998), 193–225.

[P2] G. Pappas, *Galois modules and the theorem of the cube*, Duke Mathematical Journal **91** (1998), 215–224.

[S-T] A. Srivastav and M.J. Taylor, *Elliptic curves with complex multiplication and Galois module structure*, Inventiones Mathematicae **99** (1990), 165–184.

[T] M.J. Taylor, *Mordell-Weil groups and the Galois module structure of rings of integers*, Illinois J. of Mathematics **32** (1988), 428–452.

[W] W.C. Waterhouse, *Principal homogeneous spaces and group scheme extensions*, Transactions of the A.M.S. **153** (1971), 181–189.