A CATEGORY OF DIVISION MODULES

SEBASTIANO TRONTO

Abstract. Let G be a commutative algebraic group over a field K of characteristic zero. We are interested in studying the smallest field extension of K that contains the coordinates of all the points of G over some algebraic closure of K that have a multiple in $G(K)$, or other similar field extensions. In order to do so we first need to understand certain properties of G as a module over the ring of K-endomorphisms of G, and in particular its "division extensions". Using the theory of J-injective modules introduced in my previous talk we will construct a category that in a sense describes all such extensions.

1. Motivation

Let K be a field of characteristic 0 and fix an algebraic closure $\overline{K}$ of K. Let G be a commutative algebraic group over K, let R be a subring of $\mathrm{End}_K(G)$ and let J be a complete ideal filter of R (as defined in my previous talk). Let $M \subseteq G(K)$ be an R-submodule of $G(K)$. We are interested in studying the R-module

$$\Gamma := \left(M :_{G(\overline{K})} J\right)$$

from a purely algebraic point of view first, and from a number theoretical perspective (i.e. studying the tower of extensions $K \subseteq K(\Gamma[J]) \subseteq K(\Gamma)$) later.

If for example G is an abelian variety, $R = \mathbb{Z}$ and $J = p^\infty$ we have

$$\Gamma \cong \left(\mathbb{Z}[p^{-1}]\right)^{\mathrm{rk}_\mathbb{Z} M} \oplus G(\overline{K})[p^\infty]$$

where $\mathrm{rk}_\mathbb{Z} M$ is the rank of a free part of M, or if you prefer the dimension of the $\mathbb{Q}$-vector space $M \otimes_\mathbb{Z} \mathbb{Q}$. It is clear from this description that Γ depends in part on the R-module structure of M, but also on G: we know from last time that $\left(\mathbb{Z}[p^{-1}]\right)^{\mathrm{rk}_\mathbb{Z} M}$ is a J-*hull* of M, and as such it depends only on R, M and J; but there is no way to recover the torsion part $G(\overline{K})[p^\infty]$ from the data (R, M, J) without any information on G.

In order to continue our "purely algebraic" study of the R-module Γ we will fix a suitable R-module T and declare it to be our "maximal torsion" $G(\overline{K})[J]$. Under certain conditions, which hold for example when G is an elliptic curve, the module Γ is then determined by the data (R, M, J, T). However, in the general algebraic setting, the resulting algebraic theory bears interesting similiraties with Galois theory of field extensions.

2. The category of (J,T)-extensions

Fix for this section a unitary ring R, a complete ideal filter J of R and a J-torsion and J-injective left R-module T.

Definition 2.1. A *T-pointed R-module* is a pair (M,s), where M is a left R-module and $s : M[J] \hookrightarrow T$ is an injective homomorphism.

If (L,r) and (M,s) are two T-pointed R-modules, we call an R-module homomorphism $\varphi : L \to M$ a *homomorphism* or *map of T-pointed R-modules* if $s \circ \varphi|_{M[J]} = r$.

In the following we will sometimes omit the map s from the notation and simply refer to *the T-pointed R-module M* if clear from the context or if we don't need to refer to it explicitly.

Remark 2.2. A map $\varphi : (L,r) \to (M,s)$ of T-pointed R-modules is injective on $L[J]$. Indeed $s \circ \varphi|_{L[J]} = r$ is injective, so $\varphi|_{L[J]}$ must be injective as well.

Definition 2.3. Let (M,s) be a T-pointed R-module. A *(J,T)-extension* of (M,s) is a triple (N,i,t) such that (N,t) is a T-pointed R-module and $i : M \hookrightarrow N$ is a map of T-pointed R-modules and a J-extension.

If (N,i,t) and (P,j,u) are two (J,T)-extensions of (M,s) we call a homomorphism of T-pointed R-modules $\varphi : N \to P$ a *homomorphism* or *map of (J,T)-extensions* if $\varphi \circ i = j$.

We denote by $\mathfrak{J}\mathfrak{T}(M,s)$ the category of (J,T)-extensions of (M,s).

In the following we will sometimes omit the maps i and t from the notation and simply refer to *the (J,T)-extension N of M* if clear from the context or if we don't need to refer to them explicitly.

We can immediately see some similarities between (J,T)-extensions and field extensions: every map is injective, and every surjective map is an isomorphism.

Lemma 2.4. *Every map of (J,T)-extensions is injective.*

Proof. Let (N,i,t) and (P,j,u) be (J,T)-extensions of the T-pointed R-module (M,s) and let $\varphi : N \to P$ be a map of (J,T)-extensions. Let $n \in \ker\varphi$. Since $i : M \hookrightarrow N$ is a J-extension there is $I \in J$ such that $In \subseteq i(M)$. But since $j : M \hookrightarrow P$ is injective and $\varphi(In) = 0$, we must have $In = 0$, hence n is J-torsion. But since φ is a map of T-pointed R-modules by remark 2.2 we have $n = 0$. □

Corollary 2.5. *Every surjective map of (J,T)-extensions is an isomorphism.*

Proof. Let (N,i,t) and (P,j,u) be (J,T)-extensions of the T-pointed R-module (M,s) and let $\varphi : N \to P$ be a map of (J,T)-extensions. In view of Lemma 2.4 it is enough to show that if φ is an isomorphism of R-modules, then its inverse $\varphi^{-1} : P \xrightarrow{\sim} N$ is also a map of (J,T)-extensions. But the fact that $\varphi^{-1} \circ j = i$ follows directly from $\varphi \circ i = j$ and $t = u \circ \varphi|_{P[J]}^{-1} = u$ follows from $u \circ \varphi|_{N[J]} = t$. □

Proposition 2.6. *Let (M,s) be a T-pointed R-module, let (N,i,t) be a (J,T)-extension of (M,s) and let (P,j,u) be a (J,T)-extension of (N,t). Then $(P, j\circ i, u)$ is a (J,T)-extension of (M,s).*

Proof. The $j \circ i$ is clearly a map of T-pointed R-modules, so we are left to check that it is a J-extension. Since J is complete (see my previous talk), and omitting the map i and j from the notation for simplicity, we have

$$(M :_P J) = ((M :_P J) :_P J) \supseteq ((M :_N J) :_P J) = (N :_P J) = P$$

so $(M :_P J) = P$, which shows that $j \circ i : M \hookrightarrow P$ is a (J,T)-extension. □

3. Pushout of T-pointed R-modules

Given a T-pointed R-module (M, s), there are two interesting T-pointed R-modules associated with it: its *torsion* $(M[J], s)$, which we will sometimes denote by $\mathfrak{tor}(M, s)$, and its *saturation* $\mathfrak{sat}(M, s)$, which can be defined as the pushout of R-modules

$$\begin{array}{ccc} M[J] & \xhookrightarrow{\mathfrak{t}_M} & M \\ \downarrow{\scriptstyle s} & & \downarrow{\scriptstyle \mathfrak{s}_M} \\ T & \longrightarrow & \mathfrak{sat}(M) \end{array}$$

It can be seen that the bottom map surjects onto $\mathfrak{sat}(M)[J]$, and its inverse $\mathfrak{sat}(s) : \mathfrak{sat}(M)[J] \to T$ is the structural map of the T-pointed R-module $\mathfrak{sat}(M)$. We will call any T-pointed R-module (M, s) such that $s : M[J] \to T$ is an isomorphism (or equivalently that is isomorphic to its saturation) *saturated*.

It would be interesting to relate the (J, T) extensions of a T-pointed R-module to those of its torsion and its saturation.

For the torsion, the process is relatively straightforward: we just need to consider the J-torsion submodule of an extension. This can be seen as a pullback operation.

For the saturation it seems natural that we make use of a pushout of some sorts along the map $M \hookrightarrow \mathfrak{sat}(M)$: after all, the saturation itself is a pushout construction. This is possible, but the construction of a pushout in the category of (J, T)-extensions requires some caution: as is the case in the category of field extensions, the pushout of two (J, T)-extensions does not always exist.

Proposition 3.1. *Let (L, r), (M, s) and (N, t) be T-pointed R-modules and let $f : L \to M$ and $g : L \to N$ be maps of T-pointed R-modules. Assume that:*

(1) f is pure*, that is $(f(L) :_M J) = f(L) + M[J]$, and that*
(2) f is injective.

Then the pushout (P, i, j) of f along g exists in the category of T-pointed R-modules.

Moreover, the pushout map $i : M \to N$ is injective if g is injective, and the pushout map $j : M \to N$ is injective if f is injective.

Sketch of proof. The idea is to take the pushout of f along g as maps of R-modules and then further identify those torsion elements that map to the same element in T.

More explicitly, let P' be the pushout of f along g as maps of R-modules and write it as $(M \oplus N)/S$ where $S = \{(f(\lambda), -g(\lambda)) \mid \lambda \in L\}$. Let P be the quotient of P' by the submodule

$$K := \langle \{[(m, -n)] \mid \text{for all } m \in M[J],\, n \in N[J] \text{ such that } s(m) = t(n)\} \rangle \ .$$

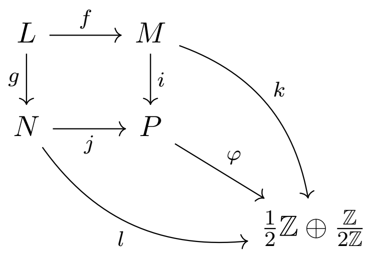
One key step for giving a map $P[J] \hookrightarrow T$ is showing that $P'[J]$ is generated by the images of $M[J]$ and $N[J]$, and it is in this step that the two assumptions on f are used. After doing so, it is relatively straightforward to show that P is the required pushout and that the injectivity of maps is preserved. □

Remark 3.2. It is easy to see that, in the situation of Proposition 3.1, if (N, i, t) is a (J, T)-extension of (L, r) then the pushout is a (J, T)-extension of (M, s).

The following example shows the necessity of the "purity" condition.

Example 3.3. Let $R = \mathbb{Z}$, $J = 2^\infty$, $T = \mathbb{Z}\left[\frac{1}{2}\right]/\mathbb{Z}$, $L = \mathbb{Z}$ and $M = N = \frac{1}{2}\mathbb{Z}$. The R-modules L, M and N are T-pointed via the zero map, since their J-torsion is trivial. Let $f : L \hookrightarrow M$ and $g : L \hookrightarrow N$ be the natural inclusions and notice that they are maps of T-pointed R-modules that are not pure. We claim that the pushout of f along g does not exist in the category of T-pointed R-modules.

To see this, assume by contradiction that (P, u) is the pushout of f along g and consider the T-pointed R-module $\left(\frac{1}{2}\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}, z\right)$, where $z : \mathbb{Z}/2\mathbb{Z} \to T$ is the only possible injective map. Consider the diagram

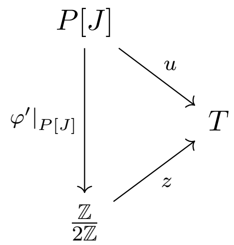


where the maps k and l are defined as

$$k : \begin{array}{ccc} \frac{1}{2}\mathbb{Z} & \to & \frac{1}{2}\mathbb{Z} \oplus \frac{\mathbb{Z}}{2\mathbb{Z}} \\ \frac{1}{2} & \mapsto & \left(\frac{1}{2}, 0\right) \end{array} \quad \text{and} \quad l : \begin{array}{ccc} \frac{1}{2}\mathbb{Z} & \to & \frac{1}{2}\mathbb{Z} \oplus \frac{\mathbb{Z}}{2\mathbb{Z}} \\ \frac{1}{2} & \mapsto & \left(\frac{1}{2}, 1\right) \end{array}$$

Notice that k and l are maps of T-pointed R-modules such that $k \circ f = l \circ g$. Then by assumption there exists a unique map of T-pointed R-moduels $\varphi : P \to \frac{1}{2}\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ that makes the diagram commute. In particular we have $\varphi(j(\frac{1}{2})) \neq \varphi(i(\frac{1}{2}))$, which implies that $j(\frac{1}{2}) \neq i(\frac{1}{2})$. But since $2j(\frac{1}{2}) = j(g(1)) = i(f(1)) = i(\frac{1}{2})$ we have that $t := j(\frac{1}{2}) - i(\frac{1}{2})$ is a 2-torsion element of P, and we must have $u(t) = \frac{1}{2}$.

Consider now the map $k' : M \to \frac{1}{2}\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ mapping $\frac{1}{2}$ to $\left(\frac{1}{2}, 0\right)$, just as l does. This is again a map of T-pointed R-modules such that $k' \circ f = l \circ g$, so there must be a map of T-pointed R-modules $\varphi' : P \to \frac{1}{2}\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ that makes this new diagram commute. But such a map φ' must map t to 0, because $\varphi'(j(\frac{1}{2})) = \left(\frac{1}{2}, 0\right) = \varphi'(i(\frac{1}{2}))$. But then the diagram of structural maps into T



would not commute, which is a contradiction. This proves our claim.

Open question 1. Is there a larger category, analogous to that of finite algebras over a field, in which all pushouts of (J, T)-extensions exist?

4. Pullback and pushforward functors

As stated at the beginning of the section, our goal is to relate the (J,T)-extensions of a T-pointed R-module M to those of its torsion $\mathfrak{tor}(M)$ and its saturation $\mathfrak{sat}(M)$. It is however interesting to study two more general contructions, namely the *pullback* and *pushforward* functors.

Let $\varphi : (L,r) \to (M,s)$ be a map of T-pointed R-module. For any (J,T)-extension (N,i,t) of (M,s) we can define the *pullback*

$$(\varphi^* N, \quad \varphi^* i, \quad \varphi^* t) := \Big((i(\varphi(L)) :_N J) \,, \quad i|_{\varphi(L)} \,, \quad t|_{(\varphi^* N)[J]} \Big)$$

which, as one can easily see, is a (J,T)-extension of (L,r). One can define the pullback $\varphi^* f$ of a map $f : N \to P$ of (J,T)-extensions of (M,s) simply by restricting it to $\varphi^* N$, which is a submodule of N. In this way φ^* becomes a functor

$$\varphi^* : \mathfrak{JT}(M,s) \to \mathfrak{JT}(L,r)$$

which we call the *pullback along* φ.

If φ is pure and injective we can moreover define, for every (J,T)-extension (N,i,t) of (L,r), the *pushforward* $(\varphi_* N, \varphi_* i, \varphi_* t)$ via the pushout diagram

$$\begin{array}{ccc} (L,r) & \xrightarrow{\varphi} & (M,s) \\ \big\downarrow i & & \big\downarrow \varphi_* i \\ (N,t) & \longrightarrow & (\varphi_* N, \varphi_* t) \end{array}$$

One can easily see that $(\varphi_* N, \varphi_* i, \varphi_* t)$ is a (J,T)-extension of (M,s), and using the universal property of the pushout one can define a map of (J,T)-extensions $\varphi_* f : \varphi_* N \to \varphi_* P$ for every map of (J,T)-extensions $f : N \to P$. In this way we get a functor

$$\varphi_* : \mathfrak{JT}(L,r) \to \mathfrak{JT}(M,s)$$

which we call the *pushforward along* φ.

Theorem 4.1. *Let $\varphi : (L,r) \hookrightarrow (M,s)$ be an injective and pure map of T-pointed R-modules. Then the functor φ_* is left adjoint to φ^*.*

Now we can finally talk about the two particular cases that are most interesting for us. Let M be a T-pointed R-module. Denoting by

$$\mathfrak{t}_M : M[J] \hookrightarrow M$$

the inclusion map, we call the pullback along this map $\mathfrak{t}_M^*$ the *torsion* functor, and we denote it by $\mathfrak{tor}$.

The inclusion of M into its saturation

$$\mathfrak{s}_M : M \hookrightarrow \mathfrak{sat}(M)$$

is injective and pure, thus we may consider the pushforward $(\mathfrak{s}_M)_*$. We call this functor the *saturation* functor, and we denote it by $\mathfrak{sat}$.

5. Maximal (J,T)-extensions

Maximal (J,T)-extensions are the analogue of the algebraic (or separable) closure in field theory. The main result of this section is the construction of a maximal (J,T)-extension for any T-pointed R-module, and we achieve this by first constructing such an extension for its torsion and its saturation.

Definition 5.1. A (J,T)-extension Γ of the T-pointed R-module M is called *maximal* if for every (J,T)-extension N of M there is a map of (J,T)-extensions $\varphi : N \hookrightarrow \Gamma$.

The very definition of T-pointed R-module already provides a maximal (J,T)-extension for any J-torsion module.

Lemma 5.2. *Let (M,s) be a T-pointed R-module. If M is J-torsion, then (T,s,id_T) is a maximal (J,T)-extension of (M,s).*

Proof. If (N,i,t) is a (J,T)-extension of M, then in particular we have

$$N = (i(M) :_N J) = \left((0 :_{i(M)} J\right) :_N J) \subseteq ((0 :_N J) :_N J) = (0 :_N J) = N[J]$$

so N is J-torsion. Then $t : N \hookrightarrow T$ satisfies $t \circ i = s$ and $\mathrm{id}_T \circ t = t$, so it is a map of (J,T)-extensions. ☐

The existence of a maximal (J,T)-extension of a saturated module comes from the existence of a J-hull.

Lemma 5.3. *Let (M,s) be a saturated T-pointed R-module and let $\iota : M \hookrightarrow \Gamma$ be a J-hull of M. Then (Γ, ι, τ), where $\tau = s \circ \iota|_{M[J]}^{-1}$, is a maximal (J,T)-extension of (M,s).*

Finally we can construct a (J,T)-extension of any T-pointed R-module using the last two results.

Theorem 5.4. *Every T-pointed R-module M admits a maximal (J,T)-extension. Moreover, for any maximal (J,T)-extension Γ of M the following hold:*

1. *(1) If Γ' is another (J,T)-extension of M, then $\Gamma \cong \Gamma'$ as (J,T)-extensions.*
2. *(2) Γ is saturated.*
3. *(3) Γ is J-injective.*
4. *(4) If (N,i,t) is a (J,T)-extension of M and $\varphi : N \to \Gamma$ is a map of (J,T)-extensions, then (Γ, φ, τ) is a maximal (J,T)-extension of (N,t).*

Idea of proof. Let Γ be a maximal (J,T)-extension of the saturation of M. ☐

6. A glimpse of Galois theory

Fix a T-pointed R-module (M, s) and a maximal (J, T)-extension (Γ, ι, τ) of (M, s).

If (N, i, t) is a (J, T)-extension of (M, s), we will denote by $\mathrm{Aut}_M(N)$ the group of R-module automorphisms σ of N such that $\sigma \circ i = i$. Notice that these are not automorphisms of the (J, T)-extension (N, i, t), because **we do not require that** $t \circ \sigma|_{M[J]} = s$.

In a similar way we let $\mathrm{Emb}_M(N, \Gamma)$ denote the set of injective R-module maps $f : N \hookrightarrow \Gamma$ such that $f \circ i = \iota$. Again, these are not necessarily maps of (J, T)-extensions, but one can see that given $f \in \mathrm{Emb}_M(N, \Gamma)$ the map $z := \tau \circ f|_{N[J]} : N[J] \hookrightarrow T$ is such that (N, i, z) is a (J, T)-extension of (M, s) and $f : (N, i, z) \to (\Gamma, \iota, \tau)$ is a map of (J, T)-extensions.

Definition 6.1. A (J, T)-extension $i : M \hookrightarrow N$ *normal* if every element of $\mathrm{Emb}_M(N, \Gamma)$ has the same image.

Using the fact that for any two $f, g \in \mathrm{Emb}_M(N, \Gamma)$ and any $n \in N$ we have $f(n) - g(n) \in \Gamma[J]$, one can show that every saturated extension is normal. In particular, every maximal (J, T)-extension is normal.

We can define a (right) action of $\mathrm{Aut}_M(N)$ on $\mathrm{Emb}_M(N, \Gamma)$ by composition: if $\sigma \in \mathrm{Aut}_M(N)$ and $f \in \mathrm{Emb}_M(N, \Gamma)$ then $f \circ \sigma$ is again an elment of $\mathrm{Emb}_M(N, \Gamma)$. This action is clearly free, that is if for $\sigma, \sigma' \in \mathrm{Aut}_M(N)$ and $(z, f) \in \mathrm{Emb}_M(N, \Gamma)$ we have $(z, f) \cdot \sigma = (z, f) \cdot \sigma'$, then $\sigma = \sigma'$, because f is injective.

Proposition 6.2. *A (J, T)-extension N of M is normal if and only if the action of $\mathrm{Aut}_M(N)$ on $\mathrm{Emb}_M(N, \Gamma)$ is transitive.*

Proof. Assume that N is normal and let $f, g \in \mathrm{Emb}_M(N, \Gamma)$. Since f and g both factor through the inclusion $f(N) \hookrightarrow \Gamma$, we can consider the automorphism of N given by $f^{-1} \circ g$, which is in $\mathrm{Aut}_M(N)$. Then clearly $f \circ (f^{-1} \circ g) = g$, and since $\tau \circ g|_{N[J]} = w$ and $\tau \circ f|_{N[J]} = z$ we have $z \circ (f^{-1} \circ g)\big|_{N[J]} = w$, showing that the action is transitive.

If the action is transitive and fix $f \in \mathrm{Emb}_M(N, \Gamma)$, every other element g of $\mathrm{Emb}_M(N, \Gamma)$ is of the form $f \circ \sigma$ for some $\sigma \in \mathrm{Aut}_M(N)$, so it has the same image as f. □

Open question 2. How close can we actually get to a "Galois theory" of (J, T)-extensions? Related to the previous first open question, can we find a Galois category whose subcategory of connected objects is exactly our category of (J, T)-extensions?

7. An important exact sequence

The key property of normal extensions for us is the following:

Lemma 7.1. *If* (N,i,t) *is a normal* (J,T)*-extension of* (M,s)*, the restriction map*

$$\mathrm{Aut}_M(N) \to \mathrm{Aut}_{M[J]}(N[J])$$

is surjective.

Proof. Let $\sigma \in \mathrm{Aut}_{M[J]}(N[J])$. Notice that $(N,i,t\circ\sigma)$ is also a (J,T)-extension of M, and let $f:(N,i,t)\hookrightarrow(\Gamma,\iota,\tau)$ and $g:(N,i,t\circ\sigma)\hookrightarrow(\Gamma,\iota,\tau)$ be maps of (J,T)-extensions. Since N is normal we have $f(N)=g(N)$, thus $f^{-1}\circ g$ is an automorphism of N that restricts to σ. □

The kernel of the surjective map above consists exactly of those automorphisms of N that restrict to the identity on $i(M)+N[J]$, and with a slight abuse of notation we may denote it by $\mathrm{Aut}_{M+N[J]}(N)$. One can see that the restriction along the map $\mathfrak{s}_N : N \hookrightarrow \mathfrak{sat}(N)$ induces an isomorphism

$$\mathrm{Aut}_{\mathfrak{sat}(M)}(\mathfrak{sat}(N)) \xrightarrow{\sim} \mathrm{Aut}_{M+N[J]}(N)$$

and so for every normal (J,T)-extension N of M we have an exact sequence

$$1 \to \mathrm{Aut}_{\mathfrak{sat}(M)}(\mathfrak{sat}(N)) \to \mathrm{Aut}_M(N) \to \mathrm{Aut}_{\mathfrak{tor}(M}(\mathfrak{tor}(N)) \to 1$$

Which relates the autormism group of N with that of its torsion and its saturation.

Moreover, one can show that the map

$$\varphi : \mathrm{Aut}_{M+N[J]}(N) \to \mathrm{Hom}\left(\frac{N}{i(M)+N[J]}, N[J]\right)$$
$$\sigma \mapsto (\varphi_\sigma : [n] \mapsto \sigma(n)-n)$$

is a group isomorphism, and that

$$\mathrm{Hom}\left(\frac{N}{i(M)+N[J]}, N[J]\right) \cong \mathrm{Hom}\left(\frac{\mathfrak{sat}(N)}{\mathfrak{sat}(M)}, \mathfrak{tor}(N)\right)$$

which highlights the commutativity of $\mathrm{Aut}_{\mathfrak{sat}(M)}(\mathfrak{sat}(N))$. It is an elementary fact from group theory that, whenever we have we have an exact sequence of groups $1\to A\to G\to Q\to 1$ with A abelian, the quotient Q acts of A by conjugation. Tracking down this action along the isomorphisms described above, one sees that in our case

$$1 \to \mathrm{Hom}\left(\frac{\mathfrak{sat}(N)}{\mathfrak{sat}(M)}, \mathfrak{tor}(N)\right) \to \mathrm{Aut}_M(N) \to \mathrm{Aut}_{\mathfrak{tor}(M)}(\mathfrak{tor}(N)) \to 1$$

the action of $\mathrm{Aut}_{\mathfrak{tor}(M)}(\mathfrak{tor}(N))$ on $\mathrm{Hom}(\mathfrak{sat}(N)/\mathfrak{sat}(M), \mathfrak{tor}(N))$ is just composition on the left.

Example 7.2. Let $R=\mathbb{Z}$, $J=p^\infty$, $T=(\mathbb{Z}[p^{-1}]/\mathbb{Z})^2$, $M=\mathbb{Z}^3$ and $N=\Gamma=(\mathbb{Z}[p^{-1}])^3\oplus T$ (i.e. a maximal (J,T)-extension of M, hence normal). Notice that $\mathfrak{tor}(M)=0$, $\mathfrak{sat}(M)=M\oplus T$, $\mathfrak{tor}(\Gamma)=T$ and $\mathfrak{sat}(\Gamma)=\Gamma$. Then

$$\mathrm{Hom}\left(\tfrac{\mathfrak{sat}(N)}{\mathfrak{sat}(M)}, \mathfrak{tor}(N)\right) \cong \mathrm{Mat}_{2\times 3}(\mathbb{Z}_p) \quad \text{and} \quad \mathrm{Aut}_{\mathfrak{tor}(M)}(\mathfrak{tor}(N)) \cong \mathrm{GL}_2(\mathbb{Z}_p)$$

and the action described above is just matrix multiplication on the left.

8. Kummer theory for elliptic curves

Let E be an elliptic curve over a number field K, with fixed algebraic closure $\overline{K}$. Let $R = \mathrm{End}_K(E)$ be the ring of K-endomorphisms of E and let J be the ideal filter

$$\infty := \{I \triangleleft R \mid n \in I \text{ for some } n \in \mathbb{Z}_{>0}\}$$

that we called $\widehat{n}$ last time (just a change of notation).

Let $T := E(\overline{K})[\infty] = E(\overline{K})_{\mathrm{tors}}$ be the "absolute torsion" of E, which is isomorphic to $(\mathbb{Q}/\mathbb{Z})^2$ as an abelian group. A theorem of Lenstra [2] states that $E(\overline{K})$ and T are injective R-modules; thus in particular they are J-injective for any ideal filter J of R, so we can talk about the theory of (J,T)-extensions of any R-submodule M of $E(K)$. It is not hard to see that

$$\Gamma := \left(M :_{E(\overline{K})} J\right)$$

is a maximal (J,T)-extension of M.

We want to study the tower of field extensions $K \subseteq K(T) \subseteq K(\Gamma)$. The classical exact sequence of Galois groups embed into the "important exact sequence" discussed in the previous section via its action on the points of Γ:

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mathrm{Gal}(K(\Gamma) \mid K(T)) & \longrightarrow & \mathrm{Gal}(K(\Gamma) \mid K) & \longrightarrow & \mathrm{Gal}(K(T) \mid K) & \longrightarrow & 1 \\
 & & \Big\downarrow{\scriptstyle\kappa} & & \Big\downarrow{\scriptstyle\rho} & & \Big\downarrow{\scriptstyle\tau} & & \\
1 & \longrightarrow & \mathrm{Hom}\left(\frac{\Gamma}{M+T}, T\right) & \longrightarrow & \mathrm{Aut}_M(\Gamma) & \longrightarrow & \mathrm{Aut}_{M[\infty]}(T) & \longrightarrow & 1
\end{array}$$

and we can use this to study our field extensions. Notice that the action of $\mathrm{Aut}_{M[\infty]}(T)$ on $\mathrm{Hom}(\Gamma/(M+T),T)$ restricts to an action of $\mathrm{Im}(\tau)$ on $\mathrm{Im}(\kappa)$.

It turns out that there is an exact sequence of abelian groups

$$0 \to \frac{\left(\mathfrak{sat}(M) :_{\mathfrak{sat}(E(K))} J\right)}{\mathfrak{sat}(M)} \to \bigcap_{f \in \mathrm{Im}(\kappa)} \ker(f) \to H^1(\mathrm{Im}(\tau), T)\,.$$

One can combine this with a duality theorem that you can find in the notes for my previous talk (but that I did not have time to discuss last time) to obtain the following:

Theorem 8.1. *Suppose that*

1. *The group* $\left(\mathfrak{sat}(M) :_{\mathfrak{sat}(E(K))} J\right)/\mathfrak{sat}(M)$ *has finite exponent* d*;*
2. *The group* $H^1(\mathrm{Im}(\tau), T)$ *has finite exponent* n*;*
3. *The subring of* $\mathrm{End}(T)$ *generated by* $\mathrm{Im}(\tau)$ *contains* $m \cdot \mathrm{End}(T)$*.*

Then $\mathrm{Im}(\kappa)$ *contains* $dnm \cdot \mathrm{Hom}(\Gamma/(M+T), T)$*.*

Idea of proof. It follows from (1) and (2) that $\bigcup_{f \in \mathrm{Im}(\kappa)} \ker(f)$ has finite exponent. If $\mathrm{Im}(\kappa)$ was a module over $\mathrm{End}(T)$ (with its natural action by composition on the left), this fact together with the aforementioned duality result would imply that $dn \cdot \mathrm{Hom}(\Gamma/(M+T),T) \subseteq \mathrm{Im}(\kappa)$. In general this is not the case, but $\mathrm{Im}(\kappa)$ is at least an $\mathrm{Im}(\tau)$-module, and by linear extension it is also a module over the subring of $\mathrm{End}(T)$ generated by $\mathrm{Im}(\tau)$. If this subring is "close to" the whole $\mathrm{End}(T)$, then $\mathrm{Im}(\kappa)$ is "close to" being an $\mathrm{End}(T)$-module, and we can get a similar conclusion. □

Integers d, m and n as above always exist. This result was previously known only in some cases, namely if $R = \mathbb{Z}$ ([3] or [4]) or R is a Dedekind domain [1].

References

[1] Javan Peykar, A. *Division points in arithmetic*. PhD thesis, Leiden University, 2021.

[2] Lenstra Jr, H. W. Complex multiplication structure of elliptic curves. *journal of number theory 56*, 2 (1996), 227–241.

[3] Lombardo, D., and Tronto, S. Explicit kummer theory for elliptic curves. *arXiv e-prints* (2019), arXiv:1909.05376.

[4] Tronto, S. Radical entanglement for elliptic curves, 2020.

Department of Mathematics, University of Luxembourg, 6 av. de la Fonte, 4364 Esch-sur-Alzette, Luxembourg

Email address: `sebastiano.tronto@uni.lu`