Kummer theory for commutative algebraic groups

Tronto, S.

Chapter 4

Division in modules and Kummer theory

by Sebastiano Tronto [Tro21]

1 Introduction

Let K be a number field and fix an algebraic closure $\overline{K}$ of K. If G is a connected commutative algebraic group over K and A is a subgroup of $G(K)$, we may consider for every positive integer n the field extension $K(n^{-1}A)$ of K inside $\overline{K}$ generated by all points $P \in G(\overline{K})$ such that $nP \in A$. This is a Galois extension of K containing the n-torsion field $K(G[n])$ of G.

If $G = \mathbb{G}_m$ is the multiplicative group, extensions of this kind are studied by classical Kummer theory. Explicit results for this case can be found for example in [PS19], [PST20b] and [PST20a]. The more general case of an extension of an abelian variety by a torus is treated in Ribet's foundational paper [Rib79]. Under certain assumptions, for example if G is the product of an abelian variety and a torus and A is free of rank r with a basis of points that are linearly independent over $\mathrm{End}_K(G)$, it is known that the ratio

$$\frac{n^{rs}}{[K\,(n^{-1}A) : K(G[n])]} \tag{1.1}$$

where s is the positive integer such that $G(\overline{K})[n] \cong (\mathbb{Z}/n\mathbb{Z})^s$ for all $n \geqslant 1$, is bounded independently of n (see also [Ber88, Théorème 5.2] and [Hin88, Lemme 14]).

In the case of elliptic curves, one may hope to obtain an explicit version of this result. Indeed the results of [Chapter 1] and [Chapter 3] provide such a statement under the assumption that $\mathrm{End}_K(G) = \mathbb{Z}$, and they show that an effective bound depends only on the abelian group structure of A and on the ℓ-adic Galois representations associated with the torsion of G for every prime ℓ.

It is clear from the above discussion that the existence of non-trivial endomorphisms defined over K plays an essential role in this theory. Without loss of generality we can take A to be an $\mathrm{End}_K(G)$-module, as done by Javan Peykar in his thesis [JP21]. This approach leads to an explicit "open image theorem" for Kummer extensions for CM elliptic curves, albeit under certain technical assuptions on $\mathrm{End}_K(G)$.

Motivated by [JP21] and by the author's previous results [Chapter 3], most of this paper is devoted to developing a general abstract framework for the study of certain *division modules* of a fixed R-module M, where R is any unitary ring. We strive to develop this theory in a way that is independent from the "ambient module" $G(\overline{K})$, taking inspiration from [Pal04] as well.

We introduce a natural generalization of the concept of injective modules, which to the author's knowledge is new. We also define a category of (J,T)-*extensions*, which shares many interesting properties with the category of field extensions. We believe that these topics are interesting in their own right.

At the end of the paper we prove the following result, which was previously known in this effective form only under certain restrictions on $\mathrm{End}_K(E)$:

Theorem. *Let E be an elliptic curve over a number field K, let $R = \mathrm{End}_K(E)$ and let M be an R-submodule of $E(K)$. There exists a positive integer c, depending only on the R-module structure of M and on the image of the Galois representations associated with the torsion of E, such that for every positive integer n*

$$\frac{n^{2\,\mathrm{rk}_R(M)}}{[K(n^{-1}M) : K(E[n])]} \qquad \textit{divides} \qquad c\,.$$

This result follows from Theorem 5.11, which is essentially an application of Theorem 5.4, which in turn is a generalization of [Chapter 3, Theorem 5.9]. The results on Galois representations needed to apply this general theorem are mostly taken from [Chapter 1], and it can be easily seen that the given bounds only depend on the ℓ-adic representations, so that the constant c of our main theorem is effectively computable.

1.1 Notation

In this paper, rings are assumed to be unitary, but not necessarily commutative; subrings always contain the multiplicative unit 1. Unless otherwise specified, by ideal of a ring we mean a right ideal and by module over a ring we mean a left module. If R is a ring and n is a positive integer, we will denote by $\mathrm{Mat}_{n\times n}(R)$ the ring of $n \times n$ matrices with coefficients in R.

We denote by $\mathbb{Z}$ the integers and by $\mathbb{Z}_{>0}$ the set of positive integers. If p is a prime number we denote by $\mathbb{Z}_p$ the completion of the ring $\mathbb{Z}$ at the ideal (p). We denote by $\widehat{\mathbb{Z}}$ the product of $\mathbb{Z}_p$ over all primes p, which we identify with $\varprojlim_{n\in\mathbb{Z}_{>0}} \mathbb{Z}/n\mathbb{Z}$.

1.2 Structure of the paper

In Section 2 we introduce the concept of *ideal filter* and of division module by an ideal filter. This provides us with a way to generalize the notion of injective module, and we are able to show the equivalent of Baer's criterion for injectivity and the existence of the analogue of injective hulls in this setting. At the end of Section 2 we prove a certain duality result for J-injective modules that will be applied in Section 5.

In Section 3 we construct the category of (J, T)-extensions, our abstraction for the modules of division points of an algebraic group. This category behaves similarly to that of field extensions of a given field. After studying an interesting pair of adjoint functors, we conclude this section by proving the existence of a *maximal* (J, T)-extension, in analogy with field theory.

Section 4 is devoted to the study of automorphism groups of (J, T)-extensions. The fundamental exact sequence of Theorem 4.10 gives us a framework to study the Galois groups of Kummer extensions associated with a commutative algebraic group, provided that some technical assumptions hold. This is what we do in Section 5, and we conclude by applying these results to elliptic curves.

Acknowledgements

I would like to thank my supervisors Antonella Perucca and Peter Bruin for their constant support. I would also like to thank Hendrik Lenstra and Peter Stevenhagen for the interesting discussion about the results of [JP21] which gave me the main ideas for this paper. Last but not least, I would like to thank Davide Lombardo for his comments on this paper, in particular for suggesting Remarks 5.1 and 5.12.

2 J-injectivity

2.1 Ideal filters and division in modules

In order to study division in modules over a general ring, we take inspiration from [JP21]. However, instead of using Steinitz ideals (that is, ideals of the completion of a ring), we use a more general concept that we now introduce.

Definition 2.1. Let R be a ring. We call a non-empty set J of right ideals of R an *ideal filter* if the following conditions hold:

1. If $I, I' \in J$ then $I \cap I' \in J$.
2. If $I \in J$ and I' is a right ideal containing I, then $I' \in J$.

The minimal ideal filter is $\{R\}$, while the maximal ideal filter contains all ideals (equivalently, it contains the zero ideal): we denote the former by 1 and the latter by 0.

For any ring R and any set S of right ideals of R we call the ideal filter *generated* by S the smallest ideal filter containing S: it consists of all ideals of R which contain a finite intersection of elements of S.

Example 2.2. We will be interested in the ideal filters generated by the powers of a given prime number p

$$p^\infty := \{I \text{ right ideal of } R \mid I \supseteq p^n R \text{ for some } n \in \mathbb{N}\}$$

and the one generated by all non-zero integers

$$\infty := \{I \text{ right ideal of } R \mid I \supseteq nR \text{ for some } n \in \mathbb{Z}_{>0}\} .$$

Notice that if $p^n = 0$ (resp. $n = 0$) for some $n \in \mathbb{Z}_{>0}$ then p^∞ (resp. ∞) is simply the maximal ideal filter 0. We will often consider such ideal filters in the case where R is a commutative integral domain of characteristic different from p (resp. characteristic 0).

Fix for the remainder of this section a ring R.

Definition 2.3. If $M \subseteq N$ are left R-modules, for any right ideal I of R we call

$$(M :_N I) := \{x \in N \mid Ix \subseteq M\}$$

the *I-division module of M in N*.

A similar concept for ideals of R is sometimes referred to as *quotient ideal*, but we deemed a change of terminology appropriate.

We can easily generalize this notion to ideal filters of R.

Definition 2.4. Let J be an ideal filter of R and let $M \subseteq N$ be left R-modules. We call

$$(M :_N J) := \bigcup_{I \in J} (M :_N I)$$

the *J-division module of M in N*. One can easily check that $(M :_N J)$ is an R-submodule of N.

Moreover, we call $N[J] := (0 :_N J)$ the *J-torsion submodule* of N. We call N a *J-torsion module* if $N = N[J]$.

Remark 2.5. If $J = 0$ then $(M :_N J) = N$ and $M[J] = M$. On the other hand, if $J = 1$ then $(M :_N J) = M$ and $M[J] = 0$.

Remark 2.6. Let $M \subseteq N$ be left R-modules and let J and J' be ideal filters of R with $J' \subseteq J$. If $M' \subseteq M$ and $N' \subseteq N$ are submodules with $M' \subseteq N'$, then it is clear from the definition of J-division module that $(M' :_{N'} J') \subseteq (M :_N J)$.

Definition 2.7. We say that an ideal filter J of R is *complete* if for every left R-module N and every submodule $M \subseteq N$ we have

$$((M :_N J) :_N J) = (M :_N J) \ .$$

We say that an ideal filter J is *product-closed* if for any $I, I' \in J$ we have $II' \in J$.

Proposition 2.8. *Let R be a ring and let J be a product-closed ideal filter of R. If for every $I \in J$ the left ideal RI is finitely generated, then J is complete. In particular, every product-closed ideal filter over a left-Noetherian ring is complete.*

Proof. Let J be a product-closed ideal filter of R and let $M \subseteq N$ be left R-modules. The inclusion $(M :_N J) \subseteq ((M :_N J) :_N J)$ is always true, so let us prove the other inclusion. Let $x \in N$ be such that there is $I \in J$ with $Ix \subseteq (M :_N J)$. Let $\{y_1, \dots y_n\}$ be a set of generators for the left ideal RI. Then for every $i = 1, \dots n$ there is $I_i \in J$ such that $I_i y_i x \subseteq M$. By definition of ideal filter we have $I' := \bigcap_{i=1}^n I_i \in J$ and since J is product-closed we have $I'I \in J$. Since $\{y_1, \dots, y_n\}$ is a set of generators of the left ideal RI and I' is a right ideal we have $I'Ix = I'(RI)x \subseteq M$, which shows that J is complete. □

Example 2.9. The ideal filters introduced in Example 2.2 are both product-closed. If, for example, R is Noetherian, then they are also complete.

We conclude this subsection with a list of properties of division modules.

Lemma 2.10. *Let $M \subseteq N \subseteq P$ and M' be left R-modules and let J and J' be ideal filters of R. Then the following properties hold:*

1. $(M :_N J) = (M :_P J) \cap N$.
2. $\left(M :_{(M:_N J)} J\right) = (M :_N J)$.
3. $(N/M)[J] = (M :_N J)/M$.
4. $(M :_N J) = N$ *if and only if* N/M *is* J*-torsion.*
5. $(M \oplus M')[J] = M[J] \oplus M'[J]$.

Proof.

1. The inclusion "$\subseteq$" is obvious; for the other inclusion it suffices to notice that if $n \in N$ is such that $In \subseteq M$ for some $I \in J$ then by definition $n \in (M :_N J)$.
2. Follows directly from (1).
3. We have
$$\begin{aligned}(N/M)[J] &= \bigcup_{I\in J}(N/M)[I] = \\ &= \bigcup_{I\in J}\{n+M \in N/M \mid I(n+M) = M\} = \\ &= \bigcup_{I\in J}\{n \in N \mid In \subseteq M\}/M = \\ &= \bigcup_{I\in J}(M :_N I)/M = \\ &= (M :_N J)/M\,.\end{aligned}$$
4. By (3) we have that $(N/M)[J] = N/M$ if and only if $(M :_N J) = N$.
5. For any right ideal I and any $(m, m') \in M \oplus M'$ we have that $I(m, m') = 0$ if and only if $Im = Im' = 0$. This implies that $(M \oplus M')[I] = M[I] \oplus M'[I]$, so we have
$$\begin{aligned}(M \oplus M')[J] &= \bigcup_{I\in J}(M \oplus M')[I] = \\ &= \bigcup_{I\in J} M[I] \oplus M'[I] = \\ &= M[J] \oplus M'[J].\end{aligned}$$

□

2.2 J-maps and J-extensions

Fix for this section a ring R and a complete ideal filter J of R. We introduce here some simple notions that will lead us closer to our definition of (J,T)-extensions.

Definition 2.11. Let M be a left R-module. An R-module homomorphism $\varphi : M \to N$ is called a *J-map* if $(\varphi(M) :_N J) = N$. If φ is injective we will call it a *J-extension*, and we say that N is a J-extension of M.

Remark 2.12. By Lemma 2.10(4) a homomorphism $\varphi : M \to N$ is a J-map if and only if $N/\varphi(M)$ is J-torsion. In particular, if $J = 0$, then every homomorphism of R-modules is a J-map.

It is clear from the definition that, if $\varphi : M \to N$ and $\psi : M \to P$ are two J-maps, then any R-module homomorphism $f : N \to P$ such that $f \circ \varphi = \psi$ is also a J-map.

The following lemma, which strongly relies on the assumption that J is complete, shows moreover that R-modules and J-maps form a subcategory of the category of R-modules.

Lemma 2.13. *Let M, N and P be R-modules and let $\varphi : M \to N$ and $\psi : N \to P$ be R-module homomorphisms. If φ and ψ are J-maps, then so is $\psi \circ \varphi$.*

Proof. Since J is complete we have

$$\begin{aligned} P &= (\psi(N) :_P J) = \\ &= \big((\psi\varphi(M) :_{\psi(N)} J) :_P J\big) \subseteq \\ &\subseteq ((\psi\varphi(M) :_P J) :_P J) = \\ &= (\psi\varphi(M) :_P J) \end{aligned}$$

hence $(\psi\varphi(M) :_P J) = P$ and $\psi \circ \varphi$ is a J-map. □

Remark 2.14. Any homomorphism of R-modules $\varphi : M \to N$ such that N is J-torsion is a J-map. In particular, the restriction of an R-module homomorphism to the J-torsion submodule is a J-map.

The following lemma illustrates how certain properties of a J-map largely depend on its restriction to the J-torsion submodule. Recall that an injective R-module homomorphism $f : M \hookrightarrow N$ is called an *essential extension* if for every submodule $N' \subseteq N$ we have $N' \cap f(M) = 0 \implies N' = 0$.

Lemma 2.15. *A J-map $\varphi : M \to N$ is essential if and only if $\varphi|_{M[J]} : M[J] \to N[J]$ is.*

Proof. Notice that the statement is trivially true in case $J = 0$, so we may assume that $J \neq 0$. If φ is essential then clearly so is $\varphi|_{M[J]}$, because any submodule N' of $N[J]$ such that $N' \cap \varphi(M[J]) = 0$ is in particular a submodule of N such that $N' \cap \varphi(M) = 0$.

Assume than that $\varphi|_{M[J]} : M[J] \to N[J]$ is essential. Let $N' \subseteq N$ be a non-trivial submodule and let $n \in N'$ be a non-zero element. If $n \in N[J]$ then $N' \cap N[J]$ is non-trivial, and since $\varphi|_{M[J]}$ is essential then $N' \cap \varphi(M)[J]$ is non-trivial as well. So we may assume that $n \notin N[J]$.

Since $\varphi : M \to N$ is a J-map, there is $I \in J$ such that $In \subseteq \varphi(M)$. In particular, since $0 \notin J$ and n is not J-torsion, there is $r \in R$ such that $0 \neq rn \in \varphi(M)$. Since N' is a submodule we have $rn \in N' \cap \varphi(M)$, so $\varphi : M \to N$ is an essential extension. □

Lemma 2.16. *Let $\varphi : M \to N$ be a J-map and let $f, g : N \to P$ be R-module homomorphisms such that $f \circ \varphi = g \circ \varphi$. Then for every $n \in N$ we have that $f(n) - g(n) \in P[J]$.*

Proof. The statement is clearly true for $J = 0$, so we may assume that $J \neq 0$. Since $(\varphi(M) :_N J) = N$ there is $I \in J$ such that $In \subseteq \varphi(M)$. In particular there is a non-zero $r \in I$ such that $rn \in \varphi(M)$, say $rn = \varphi(m)$ for some $m \in M$. This implies that

$$r(f(n) - g(n)) = f(\varphi(m)) - g(\varphi(m)) = 0$$

thus $f(n) - g(n) \in P[J]$. □

2.3 J-injective modules and J-hulls

Fix for this section a ring R and a complete ideal filter J of R. We introduce the notion of *J-injective module*, which generalizes the classical notion of injectivity.

Definition 2.17. A left R-module Q is called *J-injective* if for every J-extension $i : M \hookrightarrow N$ and every R-module homomorphism $f : M \to Q$ there exists a homomorphism $g : N \to Q$ such that $g \circ i = f$.

Remark 2.18. Notice that in case $J = 0$ the definition of J-injective R-module coincides with that of injective module. Moreover, if J' is a complete ideal filter of R such that $J' \subseteq J$, then a J-injective module is also J'-injective.

Example 2.19. A $\mathbb{Z}$-module is p^∞-injective if and only if it is p-divisible as an abelian group. The proof of this fact is completely analogous to that of the well-known result that a $\mathbb{Z}$-module is injective if and only if it is divisible.

The following proposition is an analogue of the well-known Baer's criterion in the classical case of injective modules.

Proposition 2.20. *A left R-module Q is J-injective if and only if for every two-sided ideal $I \in J$ and every R-module homomorphism $f : I \to Q$ there is an R-module homomorphism $g : R \to Q$ that extends f.*

Proof. The "only if" part is trivial, because any two-sided ideal of R is also a left R-module and $I \hookrightarrow R$ is a J-extension if $I \in J$. For the other implication, let $i : M \hookrightarrow N$ be a J-extension and let $f : M \to Q$ be any R-module homomorphism. By Zorn's Lemma there is a submodule N' of N and an extension $g' : N' \to Q$ of f to N' that is maximal in the sense that it cannot be extended to any larger submodule of N. If $N' = N$ we are done, so assume that $N' \neq N$ and let $x \in N \setminus N'$.

Let I be the two-sided ideal of R generated by $\{r \in R \mid rx \in N'\}$. Since $i(M) \subseteq N'$ and $(i(M) :_N J) = N$ there is $I' \in J$ such that $I'x \subseteq N'$, which implies $I' \subseteq I$, so also $I \in J$. By assumption the map $I \to Q$ that sends $y \in I$ to $g'(yx)$ extends to a map $h : R \to Q$. Since $\ker(R \to Rx)$ is contained in $\ker(h)$, the map h gives rise to a map $h' : Rx \to Q$ by sending $rx \in Rx$ to $h(r)$. By definition the restrictions of g' and h' to $N' \cap Rx$ coincide, so we can define a map $g'' : N' + Rx \to Q$ that extends both. This contradicts the maximality of g', so we conclude that $N' = N$. □

Remark 2.21. Let R be an integral domain and let J be the ideal filter 0 on R. Since R is an integral domain, the set of ideals $J' = J \setminus \{0\}$ is an ideal filter. Using Proposition 2.20 one can easily show that an R-module Q is J-injective if and only if it is J'-injective. Indeed, one implication holds, as remarked above, because $J \subseteq J'$, and for the other it is enough to notice that the unique map $0 \to Q$ can always be extended to the zero map on R.

One advantage of using J' instead of J is that the J'-torsion submodule may be different from the whole module.

Example 2.22. Let M be an abelian group, let p be a prime and let $J = p^\infty$ be the ideal filter of $\mathbb{Z}$ introduced in Example 2.2. Then the localization $M[p^{-1}]$ is a J-injective $\mathbb{Z}$-module. Indeed, if $i : N \hookrightarrow P$ is a J-extension and $f : N \to M[p^{-1}]$ is any homomorphism then for every $x \in P$ there is $k \in \mathbb{N}$ such that $p^k x \in i(N)$, and one can define $g(x) := \frac{f(p^k x)}{p^k}$. It is easy to check that g is a well-defined group homomorphism such that $g \circ i = f$.

Proposition 2.23. *Let M be a J-injective R-module. If $f : M \hookrightarrow N$ is an essential J-extension, then it is an isomorphism.*

Proof. By definition of J-injectivity there is a map $g : N \to M$ such that $g \circ f = \mathrm{id}_M$. Then g is surjective and since f is an essential extension g is also injective, so it is an isomorphism. □

Recall that an *injective hull* of an R-module M is an essential extension $i : M \hookrightarrow N$ such that N is injective as an R-module. It is well-known that every R-module M admits an injective hull and that any two injective hulls $i : M \hookrightarrow \Omega$ and $j : M \hookrightarrow \Gamma$ are isomorphic via a (not necessarily unique) isomorphism that commutes with i and j, see [Bae40], [ES53] or [Fle68].

Lemma 2.24. *Let R be a ring and let M be a left R-module. If $i : M \hookrightarrow \Omega$ is an injective hull and $j : M \hookrightarrow N$ is an essential extension, there is an injective R-module homomorphism $\varphi : N \hookrightarrow \Omega$ such that $\varphi \circ j = i$. Moreover, $\varphi : N \hookrightarrow \Omega$ is an injective hull.*

Proof. Since Ω is injective there exists an R-module homomorphism $\varphi : N \to \Omega$ such that $\varphi \circ j = i$. Since i is injective and j is an essential extension, then also φ is injective.

The last part follows from the fact that Ω is injective and $\varphi : N \hookrightarrow \Omega$ is an essential extension, since $i : M \hookrightarrow \Omega$ is. □

We conclude this section by proving that every R-module admits a *J-hull*, which is the generalization of an injective hull:

Definition 2.25. Let M be a left R-module. A J-extension $\iota : M \hookrightarrow \Omega$ is called a *J-hull* of M if it is an essential extension and Ω is J-injective.

Remark 2.26. If $J = 0$ the definition of J-hull coincides with that of injective hull.

Remark 2.27. If $f_i : M_i \hookrightarrow N_i$, for $i = 1, \ldots, k$, are J-hulls, then the finite sum

$$\oplus_i f_i : \bigoplus_{i=1}^{k} M_i \hookrightarrow \bigoplus_{i=1}^{k} N_i$$

is a J-hull. Indeed $\bigoplus_i N_i$ is J-injective because it is a finite direct sum of J-injective modules, and it is easy to see that it is also an essential J-extension of $\bigoplus_i M_i$.

Lemma 2.28. *Let Q be a J-injective R-module and let $P \subseteq Q$ be any submodule. Then $(P :_Q J)$ is J-injective.*

Proof. Let $i : M \hookrightarrow N$ be a J-extension and let $f : M \to (P :_Q J)$ be any R-module homomorphism. Denote by $j : (P :_Q J) \hookrightarrow Q$ the inclusion. Since Q is J-injective, there is a map $g : N \to Q$ such that $g \circ i = j \circ f$. For every $x \in N$ there is some $I \in J$ such that $Ix \subseteq i(M)$ and thus $Ig(x) = g(Ix) \subseteq g(i(M)) = j(f(M))$, which means that the image of g is contained in $(P :_Q J)$. This shows that $(P :_Q J)$ is J-injective. □

Theorem 2.29. *Every left R-module M admits a J-hull. Moreover, the following holds for any J-hull $\iota : M \hookrightarrow \Omega$ of M:*

1. *For every J-extension $i : M \hookrightarrow N$ there is a J-hull $j : N \hookrightarrow \Omega$ with $j \circ i = \iota$.*
2. *For every J-hull $\iota' : M \hookrightarrow \Omega'$ there is an isomorphism $\varphi : \Omega \xrightarrow{\sim} \Omega'$ with $\varphi \circ \iota = \iota'$.*

Proof. Let $\iota : M \hookrightarrow \Gamma$ be an injective hull of M and let $\Omega := (\iota(M) :_\Gamma J)$. Since $\iota : M \hookrightarrow \Gamma$ is an essential extension then also $\iota : M \hookrightarrow \Omega$ is, and by Lemma 2.10(2) we have $(\iota(M) :_\Omega J) = \Omega$, so $\iota : M \hookrightarrow \Omega$ is a J-extension of M. By Lemma 2.28 the R-module Ω is J-injective, so it is a J-hull of M.

For (1), since Ω is J-injective there is a map $j : N \to \Omega$ such that $j \circ i = \iota$. Moreover since $\iota : M \hookrightarrow \Omega$ is an essential extension also $j : N \hookrightarrow \Omega$ is, so it is a J-hull.

For (2), let $\iota : M \hookrightarrow \Omega$ and $\iota' : M \hookrightarrow \Omega'$ be two J-hulls. Since Ω' is J-injective there is an R-module homomorphism $f : \Omega \to \Omega'$ such that $f \circ \iota = \iota'$, so since ι is an essential extension f is injective. But then, since $\mathrm{id}_\Omega : \Omega \hookrightarrow \Omega$ is a J-hull by (1), there is an R-module homomorphism $g : \Omega' \to \Omega$ such that $g \circ f = \mathrm{id}_\Omega$, so in particular g is surjective. But we also have $g \circ \iota' = \iota$, and since ι' is an essential extension then g must be injective too, hence it is an isomorphism. □

Example 2.30. Let M be a finitely generated abelian group, let p be a prime number and let $J = p^\infty$ be the ideal filter of $\mathbb{Z}$ introduced in Example 2.2. Write M as

$$M = \mathbb{Z}^r \oplus \bigoplus_{i=1}^{k} \mathbb{Z}/p^{e_i}\mathbb{Z} \oplus M[n]$$

where n is a positive integer coprime to p and the e_i's are suitable exponents. Let

$$\Gamma = (\mathbb{Z}[p^{-1}])^r \oplus (\mathbb{Z}[p^{-1}]/\mathbb{Z})^k \oplus M[n]$$

and

$$\begin{array}{rccc} \iota : & M & \to & \Gamma \\ & (z, (s_i \bmod p^{e_i})_i, t) & \mapsto & \left(\frac{z}{1}, \left(\frac{s}{p^{e_i}} \bmod \mathbb{Z}\right)_i, t\right) \end{array}$$

Then $\iota : M \to \Gamma$ is a J-hull. To see this it is enough to show that $f : \mathbb{Z}^r \hookrightarrow (\mathbb{Z}[p^{-1}])^r$ and $g_i : \mathbb{Z}/p^{e_i}\mathbb{Z} \hookrightarrow \mathbb{Z}[p^{-1}]/\mathbb{Z}$ for every $i = 1, \ldots, k$ are J-hulls, and that $M[n]$ is J-injective, being trivially an essential extension of itself. The assertions about f and $M[n]$ follow from Example 2.22, noticing that multiplication by p is an automorphism of $M[n]$ and that $\mathbb{Z}^r \hookrightarrow (\mathbb{Z}[p^{-1}])^r$ is an essential J-extension.

So we are left to show that for every positive integer e the map $g : \mathbb{Z}/p^e\mathbb{Z} \hookrightarrow \mathbb{Z}[p^{-1}]/\mathbb{Z}$ defined by $(s \bmod p^e) \mapsto (\frac{s}{p^e} \bmod \mathbb{Z})$ is a J-hull. It is a J-extension, because the Prüfer group $\mathbb{Z}[p^{-1}]/\mathbb{Z}$ itself is J-torsion, and it is also essential because every subgroup of $\mathbb{Z}[p^{-1}]/\mathbb{Z}$ is of the form $\frac{1}{p^d}\mathbb{Z}$, so it intersects the image of g in $\frac{1}{p^{\min(e,d)}}\mathbb{Z}$.

Finally, $\mathbb{Z}[p^{-1}]/\mathbb{Z}$ is divisible as an abelian group, so in particular it is J-injective, since in this case it is equivalent to being p-divisible.

2.4 Duality

Fix again a ring R and a complete ideal filter J of R. Fix as well a left R-module M and a J-injective and J-torsion left R-module T and let $E = \mathrm{End}_R(T)$.

In this section we prove an elementary duality result that will be key to the proof of our main Kummer-theoretic results (Theorem 5.3).

Definition 2.31. If V is a subset of $\mathrm{Hom}_R(M,T)$ we denote by $\ker(V)$ the submodule of M given by

$$\ker(V) := \bigcap_{f \in V} \ker(f)$$

and we call it the *joint kernel* of V.

If M' is a submodule of M we will identify $\mathrm{Hom}_R(M/M', T)$ with the submodule $\{f \in \mathrm{Hom}_R(M,T) \mid \ker(f) \supseteq M'\}$ of $\mathrm{Hom}_R(M,T)$.

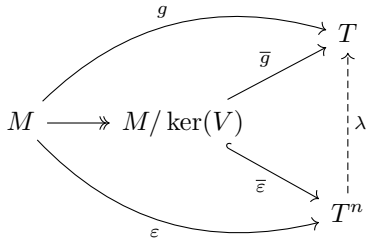
Proposition 2.32. *If V is a finitely generated E-submodule of $\mathrm{Hom}_R(M,T)$ we have $V = \mathrm{Hom}_R(M/\ker(V), T)$.*

Proof. Notice that the inclusion $V \subseteq \mathrm{Hom}_R(M/\ker(V), T)$ is obvious. For the other inclusion we want to show that every homomorphism $g : M \to T$ with $\ker(g) \supseteq \ker(V)$ belongs to V. Let then g be such a map and let $\overline{g} : M/\ker(V) \to T$ be its factorization through the quotient $M/\ker(V)$. Let $\{f_1, \ldots, f_n\}$ be a set of generators for V as an E-module and let

$$\begin{aligned} \varepsilon : M &\to T^n \\ x &\mapsto (f_1(x), \ldots, f_n(x)) \end{aligned}$$

We have $\ker(\varepsilon) = \ker(V)$, so that ε factors as an injective map $\overline{\varepsilon} : M/\ker(V) \to T^n$. Since T is J-torsion, so is T^n, hence $\overline{\varepsilon}$ is a J-extension. Since T is J-injective

there is an R-linear map $\lambda : T^n \to T$ such that $\lambda \circ \overline{\varepsilon} = \overline{g}$, or equivalently $\lambda \circ \varepsilon = g$.



Since $\mathrm{Hom}_R(T^n, T) \cong \bigoplus_{i=1}^n \mathrm{End}_R(T)$, there are elements $e_1, \ldots, e_n \in \mathrm{End}_R(T)$ such that $\lambda(t_1, \ldots, t_n) = e_1(t_1) + \cdots + e_n(t_n)$ for every $(t_1, \ldots, t_n) \in T^n$. Then for $x \in M$ we get

$$\begin{aligned} \lambda(\varepsilon(x)) &= \lambda(f_1(x), \ldots, f_n(x)) \\ &= e_1(f_1(x)) + \cdots + e_n(f_n(x)) \end{aligned}$$

which means that $g = e_1 \circ f_1 + \cdots + e_n \circ f_n \in V$ because V is an E-module. □

Remark 2.33. Proposition 2.32 is a generalization of the following fact from linear algebra: let V be a finite-dimensional vector space over a field K and let $f_1, \ldots, f_n : V \to K$ be linear functions. If $f : V \to K$ is a linear function such that $\ker(f) \supseteq \bigcap_{i=1}^n \ker(f_i)$, then f is a linear combination of $f_1, \ldots, f_n$.

Definition 2.34. Let N and Q be left R-modules. We say that Q is a *cogenerator* for N if $\ker(\mathrm{Hom}_R(N, Q)) = 0$.

Theorem 2.35. *Let R be a ring and let J be a complete ideal filter on R. Let T be a J-injective and J-torsion left R-module and let M be any left R-module. Assume that T is a cogenerator for every quotient of M and that* $\mathrm{Hom}_R(M, T)$ *is Noetherian as an* $\mathrm{End}_R(T)$*-module. The maps*

$$\begin{array}{ccc} \{R\text{-submodules of } M\} & \to & \{\mathrm{End}_R(T)\text{-submodules of } \mathrm{Hom}_R(M,T)\} \\ M' & \mapsto & \mathrm{Hom}_R(M/M', T) \\ \ker(V) & \leftarrow\!\shortmid & V \end{array}$$

define an inclusion-reversing bijection between the set of R-submodules of M and that of $\mathrm{End}_R(T)$*-submodules of* $\mathrm{Hom}_R(M, T)$.

Proof. Notice first the above maps are well-defined and they are both inclusion-reversing. Since $\mathrm{Hom}_R(M, T)$ is Noetherian as an $\mathrm{End}_R(T)$-module, every submodule is finitely generated, so we may apply Proposition 2.32. Since T is a cogenerator for every quotient of M we can conclude that the two given maps are inverse of each other. □

Example 2.36. Let $R = \mathbb{Z}$, let $J = \infty$ and let $T = (\mathbb{Q}/\mathbb{Z})^s$ for some positive integer s. Let M be a finitely generated abelian group. Notice that T is J-torsion and, since it is injective, it is in particular J-injective. Since $\mathbb{Q}/\mathbb{Z}$ is a cogenerator for every abelian group, so is T. We have $\mathrm{End}_R(T) = \mathrm{Mat}_{s\times s}(\widehat{\mathbb{Z}})$ and since M is finitely generated $\mathrm{Hom}_R(M,T)$ is Noetherian over $\mathrm{Mat}_{s\times s}(\widehat{\mathbb{Z}})$. We are then in the setting of Theorem 2.35.

3 The category of (J,T)-extensions

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

In this section we introduce (J,T)-extensions, which are essentially J-extensions whose J-torsion is contained in an R-module T as above (see Definition 3.12). These extensions of R-modules share many interesting properties with field extensions, and in fact at the end of this section we will be able to prove the existence of a "maximal" (J,T)-extension, analogous to an algebraic closure in field theory.

3.1 T-pointed R-modules

In order to define (J,T)-extensions we first introduce the more fundamental concept of T-pointed R-module.

Definition 3.1. 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 $s \circ \varphi|_{L[J]} = r$.

In the following we will sometimes omit the map s from the notation and simply refer to *the T-pointed R-module M*.

Remark 3.2. 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 3.3. If (M,s) is a T-pointed R-module we denote the T-pointed R-module $(M[J],s)$ by $\mathfrak{tor}(M,s)$, or simply by $\mathfrak{tor}(M)$. We will denote the natural inclusion $\mathfrak{tor}(M) \hookrightarrow M$ by $\mathfrak{t}_M$.

Example 3.4. Let $R = \mathbb{Z}$ and let J be the complete ideal filter ∞ on $\mathbb{Z}$. Let $T = (\mathbb{Q}/\mathbb{Z})^2$, which is ∞-injective and ∞-torsion. The abelian group $M = \mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ together with the map $s : \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ that sends $(1,0)$ to $\left(\frac{1}{6},0\right)$ and $(0,1)$ to $\left(0,\frac{1}{2}\right)$ is a T-pointed R-module.

As is the case with field extensions, pushouts do not always exist in our newly-defined category. However the pushout of two maps of T-pointed R-modules exists if at least one of the two is injective and "as little a J-map as possible".

Definition 3.5. We say that a map $f : L \to M$ of T-pointed R-modules is *pure* if $(f(L) :_M J) = f(L) + M[J]$.

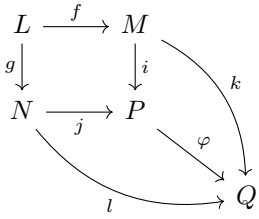
Proposition 3.6. *Let (L, r), (M, s) and (N, t) be T-pointed R-modules and let $f : L \to M$ and $g : L \to N$ be maps of T-pointed R-modules. Assume that f is injective and pure. Then the pushout $M \xrightarrow{i} P \xleftarrow{j} N$ of f along g exists in the category of T-pointed R-modules.*

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

Proof. We have to show that there is a T-pointed R-module (P, u) with maps $i : M \to P$ and $j : N \to P$ such that the diagram

$$\begin{array}{ccc} L & \xrightarrow{f} & M \\ {\scriptstyle g}\downarrow & & \downarrow{\scriptstyle i} \\ N & \xrightarrow[j]{} & P \end{array}$$

commutes and such that for every T-pointed R-module (Q, v) with maps $k : M \to Q$ and $l : N \to Q$ with $k \circ f = l \circ g$ there is a unique map $\varphi : L \to Q$ such that the diagram



commutes.

Let P' be the pushout of f along g as maps of R-modules, and let $i' : M \to P'$ and $j' : N \to P'$ be the pushout maps. Write P' as $(M \oplus N)/S$ where $S = \{(f(\lambda), -g(\lambda)) \mid \lambda \in L\}$. Let $\pi : P' \to P$ be the quotient by the submodule

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

and let $i = \pi \circ i'$ and $j = \pi \circ j'$. Notice that $i \circ f = j \circ g$.

We claim that $P'[J]$ is generated by $i'(M[J])$ and $j'(N[J])$. The claim is obviously true if $J = 0$, so we may assume that $J \neq 0$. To prove the claim, notice

that by Lemma 2.10(3) we have $P'[J] = (S :_{M\oplus N} J)/S$, so any element of $P'[J]$ is represented by a pair (m,n) such that $I(m,n) \subseteq S$ for some $I \in J$. Then since f is a pure map we have $m = f(\lambda) + t_m$ for some $\lambda \in L$ and some $t_m \in M[J]$.

Let $I' \in J$ be such that $I't_m = 0$. Then $I \cap I' \in J$ and for any nonzero $h \in I \cap I'$ we have $(f(h\lambda), hn) = h(m - t_m, n) = h(m,n) \in S$, which means that $hn = -g(h\lambda + z)$ for some $z \in \ker(f)$. Since f is injective we have that $n = -g(\lambda) + t_n$ for some $t_n \in N[J]$. It follows that the class of (m,n) in $P'[J]$ is the same as that of (t_m, t_n), which proves our claim.

Since $K \subseteq P'[J]$, it follows easily from our claim that $P[J] = P'[J]/K$ and thus that the map

$$\begin{aligned} u : P[J] &\to T \\ [(m,n)] &\mapsto s(m) + t(n) \end{aligned}$$

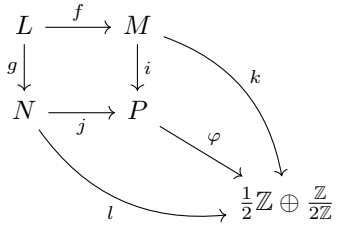
is well-defined and injective. This shows that (P,u) is a T-pointed R-module and that $i : M \to P$ and $j : N \to P$ are maps of T-pointed R-modules.

Let now (Q,v), k and l be as above. By the universal property of the pushout there is a unique R-module homomorphism $\varphi' : P' \to Q$ such that $\varphi' \circ i' = k$ and $\varphi' \circ j' = l$. Since k is a map of T-pointed R-modules, this implies that $v \circ \varphi' \circ i' = s$ and $v \circ \varphi' \circ j' = t$, so that φ' factors through P as a T-pointed R-module homomorphism $\varphi : P \to Q$.

For the last assertion we first notice that if g is injective, then so is the R-module pushout map i'. Then we claim that $i'(M) \cap K = 0$. Indeed if $[(m_0, 0)] = [(m, -n)]$ in P' for some $m_0 \in m$, $m \in M[J]$ and $n \in N[J]$ such that $s(m) = t(n)$, then there is some $\lambda \in L$ such that $m - m_0 = f(\lambda)$ and $n = g(\lambda)$. Since g is injective λ is J-torsion, and we have $r(\lambda) = s(m) - s(m_0) = t(n)$. But, since $s(m) = t(n)$, we must have $m_0 = 0$, and we conclude that $i'(M) \cap K = 0$. It follows that $i = \pi \circ i'$ is injective. Analogously, injectivity of f implies that of j. □

Remark 3.7. 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 inclusion 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.

Suppose instead that (P,u) is a 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



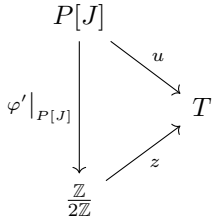
where the maps k and l are defined as

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

and

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-modules $\varphi : P \to \frac{1}{2}\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ 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. 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.

The class of T-pointed R-modules whose torsion submodule is isomorphic to T will be particularly important for us.

Definition 3.8. Let (M, s) be a T-pointed R-module. We say that (M, s) is *saturated* if $\mathfrak{t}_M : M[J] \hookrightarrow T$ is surjective (and hence an isomorphism).

Remark 3.9. The map $\mathfrak{t}_M$ is a pure and injective map.

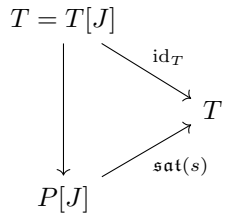
Every T-pointed R-module can be embedded in a saturated module, and the smallest saturated module containing a given one can be constructed as a pushout.

Definition 3.10. If (M, s) is a T-pointed R-module we call *saturation* of (M, s), denoted by $\mathfrak{sat}(M, s)$ or simply by $\mathfrak{sat}(M)$, the T-pointed R-module (P, u) which is the pushout (in the category of T-pointed R-modules) of the diagram

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

We will also denote by $\mathfrak{sat}(s)$ the map u and by $\mathfrak{s}_M$ the pushout map $M \to P$.

Remark 3.11. Notice that the pushout map $T \to P$ of Definition 3.10 is an isomorphism onto $P[J]$. Indeed by definition of T-pointed R-module the following diagram commutes:



where the vertical map on the left is the pushout map. It follows that $\mathfrak{sat}(s)$, which is injective by definition, is also surjective, hence an isomorphism, and the pushout map is its inverse. In other words, the saturation of a T-pointed R-module is saturated.

3.2 (J, T)-extensions

We can finally introduce the main object of study of this section.

Definition 3.12. 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 $\mathfrak{JT}(M, s)$ 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.

Remark 3.13. 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. Then (P,φ,u) is a (J,T)-extension of (N,t). In fact we have

$$(\varphi(N) :_P J) \supseteq (j(M) :_P J) = P\,.$$

Example 3.14. Let $R = \mathbb{Z}$, let J be the complete ideal filter 2^∞ of $\mathbb{Z}$ and let T be the 2^∞-torsion and 2^∞-injective $\mathbb{Z}$-module $\left(\mathbb{Z}\left[\frac{1}{2}\right]/\mathbb{Z}\right)^2$. If $M = \mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$ then the map $s : \mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z} \to T$ that sends $(1,0)$ to $\left(\frac{1}{2},0\right)$ and $(0,1)$ to $\left(0,\frac{1}{2}\right)$ turns (M,s) into a T-pointed R-module.

Let $N = \frac{1}{2}\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$. The maps

$$\begin{array}{rcl} t_1 : \mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z} & \to & T \\ (1,0) & \mapsto & \left(\frac{1}{4},0\right) \\ (0,1) & \mapsto & \left(0,\frac{1}{2}\right) \end{array} \quad \text{and} \quad \begin{array}{rcl} t_2 : \mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z} & \to & T \\ (1,0) & \mapsto & \left(0,\frac{1}{4}\right) \\ (0,1) & \mapsto & \left(\frac{1}{2},0\right) \end{array}$$

define two different T-pointed R-module structures (N,t_1) and (N,t_2) on N. The componentwise inclusion $f : M \hookrightarrow N$ is a 2^∞ extension. Since it is compatible with all the maps to T, both (N,f,t_1) and (N,f,t_2) are $(2^\infty,T)$-extensions of M. They are not isomorphic as $(2^\infty,T)$-extensions, because they are not isomorphic as T-pointed R-modules.

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 3.15. *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 it is injective on $M[J]$ (see Remark 3.2) so $n = 0$. □

Corollary 3.16. *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 3.15 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 $\varphi\circ i = j$ while $t = u\circ\varphi|^{-1}_{P[J]} = u$ follows from $u\circ\varphi|_{N[J]} = t$. □

Proposition 3.17. *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 map $j \circ i$ is clearly a J-injective map of T-pointed R-modules, and it is a J-map by Lemma 2.13. □

3.3 Pullback and pushforward

One can recover much information about the (J, T)-extensions of a certain T-pointed R-module by studying the extensions of its torsion submodule and of its saturation – see for example our construction of the maximal (J, T)-extension in Section 3.4. In order to study the relation between these categories, we introduce the more general pullback and pushforward functors which, interestingly, form an adjoint pair.

Definition 3.18. If $\varphi : L \to M$ is a map of T-pointed R-modules and (N, i, t) is a (J, T)-extension of M, we let

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

and we call them the *pullback along* φ of N, i and t respectively.

Lemma 3.19. *Let $\varphi : L \to M$ be a map of T-pointed R-modules and let (N, i, t) be a (J, T)-extension of M. Then $(\varphi^* N, \varphi^* i, \varphi^* t)$ is a (J, T)-extension of $\varphi(L)$.*

Proof. Clearly $(\varphi^* N, \varphi^* t)$ is a T-pointed R-module and

$$\varphi^* t \circ \varphi^* i|_{\varphi(L)[J]} = t \circ i|_{\varphi(L)[J]} = s|_{\varphi(L)}$$

so $\varphi^* i : (\varphi(L), s|_{\varphi(L)}) \to (\varphi^* N, \varphi^* t)$ is an injective map of T-pointed R-modules.

Moreover $(\varphi^* i(\varphi(L)) :_{\varphi^* N} J) = \varphi^* N$ by definition and by Lemma 2.10(2), so that $(\varphi^* N, \varphi^* i, \varphi^* t)$ is a J-extension. □

Definition 3.20. If $\varphi : L \to M$ is a map of T-pointed R-modules, N and P are (J, T)-extensions of M and $f : N \to P$ is a map of (J, T)-extensions, the map

$$f|_{\varphi^* N} : \varphi^* N \to \varphi^* P$$

is a map of (J, T)-extensions of $\varphi(L)$, which we denote by $\varphi^* f$.

Proposition 3.21. *Let $\varphi : L \to M$ be a map of T-pointed R-modules. The diagram*

$$\begin{array}{ccc} (N,i,t) & \longmapsto & (\varphi^*N, \varphi^*i, \varphi^*t) \\ \downarrow f & & \downarrow \varphi^* f \\ (P,j,u) & \longmapsto & (\varphi^*P, \varphi^*j, \varphi^*u) \end{array}$$

defines a functor from $\mathfrak{JT}(M,s)$ *to* $\mathfrak{JT}(\varphi(L),\, s|_{\varphi(L)})$.

Proof. In view of Lemma 3.19 we only need to check that φ^* behaves well with the respect to the composition of maps of (J,T)-extensions. If

$$N \xrightarrow{f} P \xrightarrow{g} Q$$

are maps of (J,T)-extensions of (M,s), we have

$$\varphi^* g \circ \varphi^* f = g|_{\varphi^* P} \circ f|_{\varphi^* N} = (g \circ f)|_{\varphi^* N} = \varphi^*(g \circ f)\,.$$

□

Definition 3.22. We call the functor of Proposition 3.21 the *pullback along* φ, and we denote it by φ^*.

Definition 3.23. If $\varphi : L \to M$ is an injective and pure map of T-pointed R-modules and (N,i,t) is a (J,T)-extension of L we denote by $\varphi_* i : M \to \varphi_* N$ the pushout of i along φ.

Lemma 3.24. *Let* $\varphi : L \to M$ *be an injective and pure map of* T*-pointed* R*-modules and let* (N,i,t) *be a* (J,T)*-extension of* L*. Then* $(\varphi_* N, \varphi_* i, \varphi_* t)$ *is a* (J,T)*-extension of* (M,s).

Proof. This follows from the fact that $\varphi_* i$ is injective and $\varphi_* N/(\varphi_* i)(M) \cong N/i(L)$ is J-torsion, because $i : L \to N$ is a J-extension. □

Lemma 3.25. *Let* $\varphi : L \to M$ *be an injective and pure map of* T*-pointed* R*-modules, let* (N,i,t) *and* (P,j,u) *be* (J,T)*-extensions of* L *and let* $f : N \to P$ *be a map of* (J,T)*-extensions. Then there is a unique map of* (J,T)*-extensions of* M

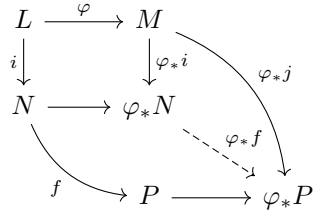
$$\varphi_* f : \varphi_* N \to \varphi_* P$$

such that the diagram

$$\begin{array}{ccc} N & \longrightarrow & \varphi_* N \\ \downarrow f & & \downarrow \varphi_* f \\ P & \longrightarrow & \varphi_* P \end{array}$$

commutes, where the horizontal maps are the pushout maps.

Proof. It is enough to apply the universal property of the pushout of $\varphi_* N$ to the diagram



Indeed the map $\varphi_* f : \varphi_* N \to \varphi_* P$, whose existence is ensured by the universal property, is such that $\varphi_* P / \varphi_* f(\varphi_* N) \cong P/f(N)$ is J-torsion. □

Proposition 3.26. *Let $\varphi : L \to M$ be an injective and pure map of T-pointed R-modules. The diagram*

$$\begin{array}{ccc} (N,i,t) & \longmapsto & (\varphi_* N, \varphi_* i, \varphi_* t) \\ \downarrow f & & \downarrow \varphi_* f \\ (P,j,u) & \longmapsto & (\varphi_* P, \varphi_* j, \varphi_* u) \end{array}$$

where $\varphi_* f$ is as in Lemma 3.25, defines a functor from $\mathfrak{JT}(L,r)$ to $\mathfrak{JT}(M,s)$.

Proof. In view of Lemmas 3.24 and 3.25 it is enough to show that φ_* behaves well with respect to the composition of maps of (J,T)-extensions. This is immediate from the construction in Lemma 3.25 and the uniqueness part of the universal property of the pushout. □

Definition 3.27. We call the functor of Proposition 3.26 the *pushforward along* φ, and we denote it by φ_*.

Theorem 3.28. *Let $\varphi : (L,r) \hookrightarrow (M,s)$ be an injective pure map of T-pointed R-modules. Then the functor φ_* is left adjoint to φ^*.*

Proof. Since φ is injective we will, for simplicity, denote $\varphi(L)$ by L.

Let (N,i,t) be a (J,T)-extension of L and let (P,j,u) be a (J,T)-extension of M. We want to show that we have

$$\mathrm{Hom}_{\mathfrak{JT}(L,r)}(N, \varphi^* P) \cong \mathrm{Hom}_{\mathfrak{JT}(M,s)}(\varphi_* N, P)$$

naturally in N and P.

Let $f : N \to \varphi^* P$ be a map of (J,T)-extensions of L; notice that in particular $f \circ i = \varphi^* j$. Composing f with the natural inclusion $\varphi^* P \hookrightarrow P$ we get a map of

T-pointed R-modules $f' : N \to P$ such that $f' \circ i = j \circ \varphi$, so by the universal property of the pushout there exists a unique map $g : \varphi_* N \to P$ that is a map of (J,T)-extensions of M.

We define a map

$$\Psi_{N,P} : \mathrm{Hom}_{\mathfrak{J}\mathfrak{T}(L,r)}(N, \varphi^* P) \to \mathrm{Hom}_{\mathfrak{J}\mathfrak{T}(M,s)}(\varphi_* N, P)$$

by letting $\Psi_{N,P}(f) := g$. The map Ψ is natural in N and P, since it is defined by means of a universal property. Indeed, if $h : N' \to N$ is a map of (J,T)-extensions of L and $f' = f \circ h$ then $\Psi_{N',P}(f')$ is by definition the unique map $\varphi_* N' \to P$ that makes the pushout diagram commute so it must coincide with $g \circ \varphi_* h$. Similarly if $k : P \to P'$ is a map of (J,T)-extensions of M then $\Psi_{N,P'}(\varphi^* k \circ f)$ must coincide with $k \circ g$.

To see that the map $\Psi_{N,P}$ is injective, let $f' : N \to \varphi^* P$ be another map and assume that $\Psi_{N,P}(f) = \Psi_{N,P}(f')$. But then the composition of $\Psi_{N,P}(f)$ with the pushout map $N \to \varphi_* N$ coincides with the composition of f and the natural inclusion $\varphi^* P \hookrightarrow P$, and analogously for f', so we conclude that $f = f'$.

To see that $\Psi_{N,P}$ is surjective, let $g' : \varphi_* N \to P$ be a map of (J,T)-extensions of M. Then by definition of pullback its composition with $N \to \varphi_* N$ factors through $\varphi^* P \hookrightarrow P$ as a map of (J,T)-extensions $f' : N \to \varphi^* P$, and again by the uniqueness of the map of the universal property of the pushout one can check that $\Psi_{N,P}(f') = g'$. □

Remark 3.29. Let $\varphi : L \hookrightarrow M$ be an injective and pure map of T-pointed R-modules and let (N, i, t) and (P, j, u) be (J,T)-extensions of L and M respectively. We can give an explicit description of the unit

$$\eta_N : N \to \varphi^* \varphi_* N$$

and the counit

$$\varepsilon_P : \varphi_* \varphi^* P \to P$$

of the adjunction.

Notice that the pushout map $N \to \varphi_* N$ is injective. Moreover, since N is a J-extension of L, the image of this map is contained in $\varphi^* \varphi_* N = (\varphi_* i(\varphi(L)) :_{\varphi_* N} J)$. The resulting inclusion $N \hookrightarrow \varphi^* \varphi_* N$ is the unit η_N.

By definition $\varphi^* P$ is contained in P, and the diagram

$$\begin{array}{ccc} L & \xhookrightarrow{\varphi} & M \\ \downarrow & & \downarrow j \\ \varphi^* P & \hookrightarrow & P \end{array}$$

commutes, so by the universal property of the pushout there exists a map $\varphi_* \varphi^* P \to P$. This map is the counit ε_P.

The following examples of pullback and pushforward functors are of particular importance to us, because they will be key to the construction of maximal (J,T)-extensions.

Definition 3.30. Let M be a T-pointed R-module and let $\mathfrak{t}_M : M[J] \to M$ be the natural inclusion of its torsion submodule. We will call the pullback functor $\mathfrak{t}_M^*$ the *torsion* functor and we will denote it by $\mathfrak{tor}$.

Remark 3.31. For every (J,T)-extension of $\mathfrak{tor}(M)$ the unit map

$$\eta_N : \mathfrak{tor}((\mathfrak{t}_M)_* N) \to N$$

is an isomorphism. Indeed, we have $\mathfrak{tor}((\mathfrak{t}_M)_* N) = ((\mathfrak{t}_M)_* N)[J] = N[J]$, and since N is a (J,T)-extension of a J-torsion module and J is complete then $N[J] = N$.

Notice that the inclusion $\mathfrak{s}_M$ of a T-pointed R-module into its saturation is injective and pure.

Definition 3.32. Let M be a T-pointed R-module and let $\mathfrak{s}_M : M \to \mathfrak{sat}(M)$ be the inclusion into its saturation. We will call the pushforward functor $(\mathfrak{s}_M)_*$ the *saturation* functor and we will denote it by $\mathfrak{sat}$.

Remark 3.33. The counit map $\varepsilon_P : P \to \mathfrak{sat}(\mathfrak{s}_M^* P)$ is an isomorphism. Indeed, one can see from the definition of pullback that $\mathfrak{s}_M^* P = P$ is saturated, hence it coincides with its own saturation.

3.4 Maximal (J,T)-extensions

Maximal (J,T)-extensions are the analogue of algebraic closures in field theory. The main result of this section is the proof of the existence 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 3.34. 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 definition of T-pointed R-module already provides a maximal (J,T)-extension for any J-torsion module.

Lemma 3.35. *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

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

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, and it requires only a little more technical work.

Lemma 3.36. *Let (M,s) be a saturated T-pointed R-module and let $\iota : M \hookrightarrow \Gamma$ be a J-hull of M. Then*

1. *$\iota|_{M[J]} : M[J] \hookrightarrow \Gamma[J]$ is an isomorphism.*

2. *(Γ, ι, τ) is a maximal (J,T)-extension of (M,s), where $\tau := s \circ \iota|^{-1}_{M[J]}$.*

Proof. For (1) notice that $\iota|_{M[J]} : M[J] \hookrightarrow \Gamma[J]$ is an essential extension by Lemma 2.15, so it is an isomorphism by Proposition 2.23.

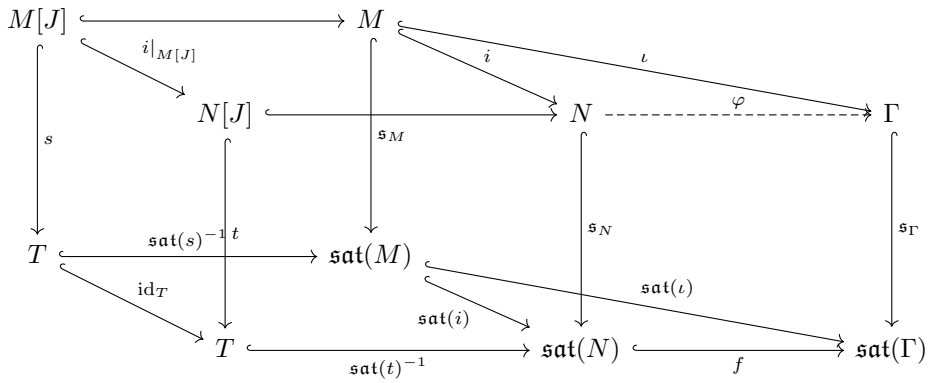
For (2) we have that Γ is a (J,T)-extension of M, because it is a J-extension and $\tau \circ \iota|_{M[J]} = s$. Let (N,i,t) be any (J,T)-extension of M. Since $i : M \hookrightarrow N$ is a J-extension, there is a homomorphism $\varphi : N \to \Gamma$ such that $\varphi \circ i = \iota$. Moreover, since $t \circ i|_{M[J]} = s$ and $\tau \circ (\varphi \circ i)|_{M[J]} = \tau \circ \iota|_{[M[J]} = s$, we have $\tau \circ \varphi|_{N[J]} = t$, so φ is a map of (J,T)-extensions. It follows that Γ is a maximal (J,T)-extension of M. □

Finally we can construct a (J,T)-extension of any T-pointed R-module.

Proposition 3.37. *Let (Γ, ι, τ) be a (J,T)-extension of the T-pointed R-module (M,s) such that Γ is saturated. Then Γ is a maximal (J,T)-extension of M if and only if $\mathfrak{sat}(\Gamma)$ is a maximal (J,T)-extension of $\mathfrak{sat}(M)$.*

Proof. Assume first that Γ is a maximal (J,T)-extension of M and let (N,i,t) be a (J,T)-extension of $\mathfrak{sat}(M)$. Then there is a map $\varphi : \mathfrak{s}^*_M N \to \Gamma$ of (J,T)-extensions of M, so there is a map $\mathfrak{sat}(\varphi) : \mathfrak{sat}(\mathfrak{s}^*_M N) \to \mathfrak{sat}(\Gamma)$ of (J,T)-extensions of $\mathfrak{sat}(M)$. By Remark 3.33 we have $N \cong \mathfrak{sat}(\mathfrak{s}^*_M N)$, so there is also a map $N \to \mathfrak{sat}(\Gamma)$. This proves that $\mathfrak{sat}(\Gamma, \iota, \tau)$ is a maximal (J,T)-extension of $\mathfrak{sat}(M)$.

Assume now that $\mathfrak{sat}(\Gamma)$ is a maximal (J,T)-extension of $\mathfrak{sat}(M)$. Let (N,i,t) be a (J,T)-extension of M. Then there is a map of (J,T)-extensions $f : \mathfrak{sat}(N) \to \mathfrak{sat}(\Gamma)$ completing the following diagram:



Notice that since Γ is saturated the map $\mathfrak{s}_\Gamma : \Gamma \hookrightarrow \mathfrak{sat}(\Gamma)$ is an isomorphism. So we can define $\varphi := \mathfrak{s}_\Gamma^{-1} \circ f \circ \mathfrak{s}_N : N \to \Gamma$ and we have

$$\mathfrak{s}_\Gamma \circ \varphi \circ i = f \circ \mathfrak{s}_N \circ i = f \circ \mathfrak{sat}(i) \circ \mathfrak{s}_M = \mathfrak{sat}(\iota) \circ \mathfrak{s}_s = \mathfrak{s}_\Gamma \circ \iota$$

hence $\varphi \circ i = \iota$. Moreover, since $\mathfrak{sat}(\tau) \circ \mathfrak{s}_\Gamma = \tau$, we have

$$\begin{aligned} \tau \circ \varphi|_{N[J]} &= \tau \circ \mathfrak{s}_\Gamma^{-1} \circ f \circ \mathfrak{s}_N|_{N[J]} = \\ &= \tau \circ \mathfrak{s}_\Gamma^{-1} \circ f \circ \mathfrak{sat}(t)^{-1} \circ t = \\ &= \tau \circ \mathfrak{s}_\Gamma^{-1} \circ \mathfrak{sat}(\tau)^{-1} \circ t = \\ &= t \end{aligned}$$

so φ is a map of (J,T)-extensions. Hence Γ is a maximal (J,T)-extension of M. □

Theorem 3.38. *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. *If Γ' is another maximal (J,T)-extension of M, then $\Gamma \cong \Gamma'$ as (J,T)-extensions;*
2. *The module Γ is saturated;*
3. *The module Γ is J-injective;*
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).*

Proof. Let $j : \mathfrak{sat}(M) \hookrightarrow \Gamma$ be a J-hull of the saturation of M and let $\tau := \mathfrak{sat}(s) \circ j|^{-1}_{\mathfrak{sat}(M)[J]}$. By Lemma 3.36 we have that (Γ, j, τ) is a maximal (J,T)-extension of $\mathfrak{sat}(M)$. By Remark 3.33 we have that $(\Gamma, \iota, \tau) = \mathfrak{t}^*_M(\Gamma, j, \tau)$ is a (J,T)-extension of M such that $\mathfrak{sat}(\Gamma, \iota, \tau) \cong (\Gamma, j, \tau)$, so by Proposition 3.37 we conclude that it is a maximal (J,T)-extension of M.

Let now (Γ', ι', τ') be another maximal (J,T)-extension of (M,s). Then there is a map of (J,T)-extensions $f : \Gamma \hookrightarrow \Gamma'$ which is an essential J-extension by Lemma 2.15, as it is an isomorphism on the J-torsion. Since Γ is J-injective we have that f is an isomorphism by Proposition 2.23. This shows that any maximal (J,T)-extension of M is isomorphic to Γ, which proves (1), (2) and (3) at once.

For (4) it is enough to notice that if $j : \mathfrak{sat}(M) \hookrightarrow \Gamma$ is a J-hull, then so is $\mathfrak{sat}(\varphi)$, thus by the same argument as above Γ is a maximal (J,T)-extension of N. □

4 Automorphisms of (J,T)-extensions

Fix for this section a ring R, a complete ideal filter J of R and a J-torsion and J-injective left R-module T. Fix moreover a T-pointed R-module (M,s) and a maximal (J,T)-extension (Γ, ι, τ) of (M,s).

4.1 Normal extensions

We define normal extensions in analogy with field theory.

Definition 4.1. A (J,T)-extension $i : M \hookrightarrow N$ is called *normal* if every injective J-map $f : N \hookrightarrow \Gamma$ such that $f \circ i = \iota$ has the same image.

Notice that we are considering all injective J-maps that respect $\iota : M \hookrightarrow \Gamma$, even if they are not maps of (J,T)-extensions, that is even if they do not respect the embeddings of the torsion submodules into T.

Remark 4.2. Although we will not make use of it, it interesting to notice that the group $\mathrm{Aut}_M(N)$ acts on $\mathrm{Emb}_M(N,\Gamma)$ by composition on the right. It is then easy to see that N is normal if and only if this action is transitive.

This is reminiscent of Galois theory *à la Grothendieck*. One might wonder if, assuming the necessary finiteness conditions on automorphism groups hold, the category of (J,T)-extensions is indeed a Galois category with fundamental functor $\mathrm{Emb}_M(-,\Gamma)$. Unfortunately, the fact that in general pushouts of (J,T)-extensions do not exist (see Remark 3.7) implies that this is not the case.

We may refine this question as follows: does the category of (J,T)-extensions embed as the subcategory of connected objects of some Galois category?

Proposition 4.3. *Every saturated (J,T)-extension of M is normal.*

Proof. Assume that M is saturated, let $i : M \hookrightarrow N$ be a (J,T)-extension and let $f, g : N \hookrightarrow \Gamma$ be injective J-maps with $f \circ i = g \circ i = \iota$. If $f(N) \neq g(N)$, we may assume without loss of generality that there is $n \in N$ with $f(n) \notin g(N)$. Then $t := f(n) - g(n) \in \Gamma[J]$ by Lemma 2.16. Since N is saturated and g is injective we have $t \in g(N)$, thus $f(n) = g(n) + t \in g(N)$, a contradiction. We deduce that $f(N) = g(N)$, so N is normal. □

Corollary 4.4. *Every maximal (J,T)-extension is normal.*

4.2 A fundamental exact sequence

Proposition 4.5. *Let (N, i, t) be a normal (J,T)-extension of (M, s) and let $\mathrm{Aut}_{M+N[J]}(N)$ denote the subgroup of $\mathrm{Aut}_M(N)$ consisting of those automorphisms that restrict to the identity on the submodule of N generated by $i(M)$ and $N[J]$. Then the restriction map along $\mathfrak{s}_N : N \to \mathfrak{sat}(N)$*

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

is a well-defined group isomorphism.

Proof. Let us identify for simplicity N with its image $\mathfrak{s}_N(N)$ in $\mathfrak{sat}(N)$, and let $\sigma \in \mathrm{Aut}_{\mathfrak{sat}(M)}(\mathfrak{sat}(N))$. To see that the image of $\sigma|_N$ is contained in N, let $f : \mathfrak{sat}(N) \hookrightarrow \Gamma$ be a map of (J,T)-extensions of $\mathfrak{sat}(M)$, which is necessarily also a map of (J,T)-extensions of M. Since $\mathfrak{sat}(s)$ is an isomorphism, also $f \circ \sigma$ is a map of (J,T)-extensions of $\mathfrak{sat}(M)$, and since N is normal we have that the image of N in Γ under f and under $f \circ \sigma$ are the same, which shows that $\sigma(N) = N$. Since this holds for both σ and its inverse, we have that $\sigma|_N \in \mathrm{Aut}_M(N)$, and clearly σ is the indentity on $N[J]$.

To show that the restriction to N is an isomorphism, we construct an inverse. Let now $\sigma \in \mathrm{Aut}_{M+N[J]}(N)$, and recall that we can see it as a map of (J,T)-extensions of (M, s)

$$\sigma : (N, t) \to (N, t \circ \sigma|_{N[J]}) .$$

Composing it with $\mathfrak{s}_N$ we get a map

$$\mathfrak{s}_N \circ \sigma : (N, t) \to (\mathfrak{sat}(N), (\mathfrak{s}_N)_*(t \circ \sigma|_{N[J]})) .$$

Moreover, the map $\mathfrak{sat}(i)$ is also a map of (J,T)-extensions

$$\mathfrak{sat}(i) : (\mathfrak{sat}(M), (\mathfrak{s}_M)_* s) \to (\mathfrak{sat}(N), (\mathfrak{s}_N)_*(t \circ \sigma|_{N[J]}))$$

so by the universal property of the pushout there is a map of (J,T)-extensions

$$\sigma' : (\mathfrak{sat}(N), (\mathfrak{s}_N)_* t), (\mathfrak{sat}(N), (\mathfrak{s}_N)_*(t \circ \sigma|_{N[J]})) .$$

It is straightforward to check that $\sigma \mapsto \sigma'$ provides an inverse for the restriction map $\mathrm{Aut}_{\mathfrak{sat}(M)}(\mathfrak{sat}(N)) \to \mathrm{Aut}_M(N)$, which is then an isomorphism. □

Proposition 4.6. *Let (N,i,t) be a (J,T)-extension of (M,s). Then the map*

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

is an isomorphism of groups. In particular, $\mathrm{Aut}_{\mathfrak{sat}(M)}(\mathfrak{sat}(N))$ is abelian.

Proof. We will denote by $[n]$ the class of an element $n \in N$ in $N/(i(M)+N[J])$. Notice that for any $\sigma \in \mathrm{Aut}_{M+N[J]}(N)$ we have $\sigma(n)-n \in N[J]$ by Lemma 2.16, and φ_σ is a homomorphism of R-modules. To see that $\sigma \mapsto \varphi_\sigma$ is a group homomorphism, let $\sigma' \in \mathrm{Aut}_{M+N[J]}(N)$. Then, since σ is the identity on $N[J]$ and $\sigma'(n) - n \in N[J]$, we have

$$\begin{aligned}\sigma(\sigma'(n)) - n &= \sigma(\sigma'(n)) - n + \sigma'(n) - n - \sigma(\sigma'(n) - n)\\ &= \sigma(n) - n + \sigma'(n) - n\end{aligned}$$

which shows that φ is a group homomorphism. It is also clearly injective, because if $\varphi_\sigma(n) = n$ then σ must be the identity.

To prove surjectivity it is enough to show that for any R-module homomorphism $h : N/(i(M)+N[J]) \to N[J]$ the map

$$\begin{aligned}\sigma_h : N &\to N\\ n &\mapsto n + h([n])\end{aligned}$$

which is clearly the identity on $i(M)+N[J]$, is an automorphism of N. It is injective, because if $n = -h([n])$ then in particular n is torsion and thus $[n] = 0$. It is also surjective, because for any $n \in N$ we have

$$\begin{aligned}\sigma_h(n - h([n])) &= n - h([n]) + h([n - h([n])])\\ &= n - h([n] - [n + h([n])])\\ &= n\end{aligned}$$

□

Corollary 4.7. *Let (N,i,t) be a normal (J,T)-extension of M. Denoting for simplicity by $\mathfrak{sat}(M)$ the image of $\mathfrak{sat}(M)$ inside $\mathfrak{sat}(N)$ we have*

$$\mathrm{Aut}_{\mathfrak{sat}(M)}(\mathfrak{sat}(N)) \cong \mathrm{Hom}\left(\frac{\mathfrak{sat}(N)}{\mathfrak{sat}(M)}, \mathfrak{tor}(N)\right).$$

Proof. The claim follows from the two propositions above and the fact that

$$\frac{N}{i(M)+N[J]} \cong \frac{\mathfrak{sat}(N)}{\mathfrak{sat}(M)}.$$

To see that the two quotients are isomorphic, consider the following map:

$$\begin{aligned} N &\to \mathfrak{sat}(N)/\mathfrak{sat}(M) \\ n &\mapsto \mathfrak{s}_N(n) + \mathfrak{sat}(M) \end{aligned}$$

Its kernel is $i(M) + N[J]$ and it is surjective because $\mathfrak{sat}(N)$ is generated by the images of N and T. □

Remark 4.8. Let N be a (J,T)-extension of M and let $\sigma \in \mathrm{Aut}_M(N)$. The restriction of σ to $N[J]$ is an element of $\mathrm{Aut}_{M[J]}(N[J])$. Indeed, the image of a J-torsion element under a map of (J,T)-extensions is again a J-torsion element; since this is true for both σ and σ^{-1} we can conclude that $\sigma|_{N[J]} : N[J] \to N[J]$ is an automorphism.

Lemma 4.9. *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 exact sequence appearing in the following theorem has been studied, in some particular cases, in [JP21], [Pal14] and [Chapter 3].

Theorem 4.10. *Let M be a T-pointed R-module and let N be a normal (J,T)-extension of M. Then there is an exact sequence of groups*

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

Moreover $\mathrm{Aut}_{\mathfrak{tor}(M)}(\mathfrak{tor}(N))$ *acts on* $\mathrm{Hom}(\mathfrak{sat}(N)/\mathfrak{sat}(M), \mathfrak{tor}(N))$ *by composition.*

Proof. By Lemma 4.9 the map $\mathrm{Aut}_M(N) \to \mathrm{Aut}_{\mathfrak{tor}(M)}(\mathfrak{tor}(N))$ is surjective and its kernel is $\mathrm{Aut}_{i(M)+N[J]}(N)$ by definition. By Proposition 4.5 this group is

isomorphic to $\mathrm{Aut}_{\mathfrak{sat}(M)}(\mathfrak{sat}(N))$ via the restriction under $\mathfrak{s}_N : N \to \mathfrak{sat}(N)$. Combining this with Corollary 4.7 we get the desired exact sequence.

The fact that $\mathrm{Aut}_{\mathfrak{tor}(M)}(\mathfrak{tor}(N))$ acts on $\mathrm{Aut}_{i(M)+N[J]}$ by conjugation is a standard result on short exact sequences with abelian kernel, and one can trace this action under the isomorphisms described above to check that on $\mathrm{Hom}(\mathfrak{sat}(N)/\mathfrak{sat}(M), \mathfrak{tor}(N))$ this action is indeed the composition of maps, similarly to [Chapter 3, Proposition 3.12]. □

5 Kummer theory for algebraic groups

5.1 General theory

Let K be a field and fix a separable closure K_s of K. Let G be a commutative algebraic group over K, let $R \subseteq \mathrm{End}_K(G)$ be a subring of the ring of K-endomorphisms of G and let $M \subseteq G(K)$ be an R-submodule. Let J be a complete ideal filter of R, let $T := G(\overline{K})[J]$ and let $\Gamma := \left(M :_{G(\overline{K})} J\right)$.

We are interested in studying the field extension $K(\Gamma)$ of K, that is the fixed field of the subgroup of $\mathrm{Gal}(K_s \mid K)$ that acts trivially on Γ, and we want to do so using the theory of (J,T)-extensions introduced in the previous section. A necesary and sufficient condition in order to proceed this way is that $T = G(\overline{K})[J]$ be J-injective: indeed in this case Γ is a saturated, and thus normal, (J,T)-extension of M.

Remark 5.1. The condition that T is J-injective for some, and in fact for all, ideal filters J, holds for example if G is a simple abelian variety with R a maximal order in the division algebra $\mathrm{End}_{\overline{K}}(G) \otimes \mathbb{Q}$. Indeed in this case every non-zero element r of R is surjective on $G(\overline{K})$, which implies that T is divisible: if an element $u \in G(\overline{K})$ is such that $ru = t \in T$ and $I \in J$ is such that $It = 0$, then since I is a right ideal we have $Iu = 0$, so $u \in T$; hence $r : T \to T$ is surjective and T is divisible.

It follows that T is injective: this is a well-known statement if R is a Dedekind domain, but the proof can be adapted to the non-commutative case as follows. Let I be a left ideal of R and let $f : I \to T$ be a map that we wish to extend to a map $\tilde{f} : R \to T$. By [Rei75, Theorem 22.7] there is a right *fractional* ideal J of R such that $IJ = R$ and $1 \in JI \subseteq R$. In particular there are non-zero elements $b_1, \ldots, b_n \in J$ and $a_1, \ldots, a_n \in I$ such that $\sum_{i=1}^n b_i a_i = 1$, and since T is divisible there are $x_1, \ldots, x_n \in T$ such that $a_i x_i = f(a_i)$. It follows that for every $y \in I$ we have

$$f(y) = f\left(y \sum_{i=1}^n b_i a_i\right) = \sum_{i=1}^n (y b_i) f(a_i) = y \sum_{i=1}^n (b_i a_i) x_i$$

and we can let $\tilde{f}(r) = r\sum_{i=1}^{n}(b_i a_i)x_i$ for every $r \in R$.

Let us then assume that $T = G(\overline{K})[J]$ is J-injective, so that Γ is a saturated, therefore normal, (J,T)-extension of M. Then the standard exact sequence of groups coming from the tower of Galois extensions $K \subseteq K(T) \subseteq K(\Gamma)$ maps into the exact sequence 4.10 via the Galois action on the points of G, and we obtain the following commutative diagram of groups with exact rows:

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

Notice that the action of $\mathrm{Aut}_{M[J]}(T)$ on $\mathrm{Hom}(\Gamma/(M+T), T)$ restricts to an action of $\mathrm{Im}(\tau)$ on $\mathrm{Im}(\kappa)$.

Definition 5.2. In the situation described above we will call the maps κ, τ and ρ the *Kummer representation*, the *torsion representation* and the *torsion-Kummer representation*, respectively.

As in Section 2.4, if N and P are R-modules and S is a subset of $\mathrm{Hom}_R(N,P)$ we let $\ker(S) = \bigcap_{f\in S}\ker(f)$.

Theorem 5.3. *There is an exact sequence of abelian groups*

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

Proof. By Lemma 2.16 for any $b \in G(K(T))$ we may define a map

$$\begin{aligned} \varphi_b : \mathrm{Im}(\kappa) &\to T \\ \sigma &\mapsto \sigma(b) - b \end{aligned}$$

which is a cocycle. It follows that the map

$$\begin{aligned} \varphi : G(K(T)) &\to H^1(\mathrm{Im}(\tau), T) \\ b &\mapsto \varphi_b \end{aligned}$$

is a group homomorphism. Moreover its kernel is

$$\begin{aligned} \ker(\varphi) &= \{b \in G(K(T)) \mid \varphi_b \text{ is a coboundary}\} \\ &= \{b \in G(K(T)) \mid \exists\, t \in T \text{ such that } \sigma(b) - b = \sigma(t) - t \,\forall\, \sigma \in \mathrm{Im}(\kappa)\} \\ &= \{b \in G(K(T)) \mid \exists\, t \in T \text{ such that } \sigma(b - t) = b - t \,\forall\, \sigma \in \mathrm{Im}(\kappa)\} \\ &= G(K) + T \end{aligned}$$

so that we have an exact sequence

$$0 \to G(K) + T \to G(K(T)) \to H^1(\mathrm{Im}(\tau), T)$$

and considering the intersection of the first two terms with Γ we get

$$0 \to \Gamma \cap (G(K) + T) \to \Gamma \cap G(K(T)) \to H^1(\mathrm{Im}(\tau), T)\,.$$

Since $M + T \subseteq \Gamma \cap (G(K) + T)$ we also have

$$0 \to \frac{\Gamma \cap (G(K) + T)}{M + T} \to \frac{\Gamma \cap G(K(T))}{M + T} \to H^1(\mathrm{Im}(\tau), T)\,.$$

Rewriting $M + T = \mathfrak{sat}(M)$ and $G(K) + T = \mathfrak{sat}(G(K))$, noticing that

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

and that

$$\begin{aligned}\ker(\mathrm{Im}(\kappa)) &= \left\{ x \in \frac{\Gamma}{M+T} \mid f(x) = 0 \,\forall\, f \in \mathrm{Im}(\kappa) \right\} \\ &= \frac{\{\tilde{x} \in \Gamma \mid \sigma(\tilde{x}) = \tilde{x} \,\forall\, \sigma \in \mathrm{Im}(\kappa)\}}{M+T} \\ &= \frac{\Gamma \cap G(K(T))}{M+T}\end{aligned}$$

we get the desired exact sequence. □

The following theorem generalizes [Chapter 3, Theorem 5.9].

Theorem 5.4. *Assume that the* $\mathrm{End}(T)$*-submodule of* $\mathrm{Hom}(\Gamma/\mathfrak{sat}(M), T)$ *generated by* $\mathrm{Im}(\kappa)$ *is finitely generated. Suppose that the following three conditions hold*

1. *There is a positive integer* d *such that*

$$d \cdot \left(\mathfrak{sat}(M) :_{\mathfrak{sat}(G(K))} J\right) \subseteq \mathfrak{sat}(M)\,.$$

2. *There is a positive integer* n *such that*

$$n \cdot H^1(\mathrm{Im}(\tau), T) = 0\,.$$

3. *There is a positive integer* m *such that the subring of* $\mathrm{End}(T)$ *generated by* $\mathrm{Im}(\tau)$ *contains*

$$m \cdot \mathrm{End}(T)\,.$$

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

Proof. Let V be the $\mathrm{End}(T)$-submodule of $\mathrm{Hom}(\Gamma/\mathfrak{sat}(M), T)$ generated by $\mathrm{Im}(\kappa)$ and let $X = \Gamma/\mathfrak{sat}(M)$. From (1) and (2) it follows that $\ker(V) = \ker(\mathrm{Im}\,\kappa) \subseteq X[dn]$. Since V is finitely generated as an $\mathrm{End}(T)$-module, by Proposition 2.32 we have

$$V = \mathrm{Hom}\left(\frac{X}{\ker(V)}, T\right) \supseteq \mathrm{Hom}\left(\frac{X}{X[dn]}, T\right) \supseteq dn \cdot \mathrm{Hom}(X, T)\,.$$

Since $\mathrm{Im}(\kappa)$ is an $\mathrm{Im}(\tau)$-module, we have

$$\mathrm{Im}(\kappa) = \mathrm{Im}(\tau) \cdot \mathrm{Im}(\kappa) \supseteq m \cdot \mathrm{End}(T) \cdot \mathrm{Im}(\kappa) = m \cdot V \supseteq dnm \cdot \mathrm{Hom}(X, T)$$

and we conclude. □

5.2 Elliptic curves over number fields

We keep the notation of the previous section and we further assume that K is a number field, that $G = E$ is an elliptic curve and that $R = \mathrm{End}_K(E)$. In particular we have that $K_s = \overline{K}$ and that R is either $\mathbb{Z}$ or an order in an imaginary quadratic number field. Up to replacing K by an extension of degree 2 we may assume that $\mathrm{End}_K(E) = \mathrm{End}_{\overline{K}}(E)$.

Notice that $T = E(\overline{K})[J]$ is contained in $E(\overline{K})_{\mathrm{tors}}$: indeed, if $x \in T$ then there is $I \in J$ such that $Ix = 0$. Since R is an order in a number field there is some non-zero integer $n \in I$, so $nx = 0$ and x is torsion.

Proposition 5.5. *The* R*-module* $E(\overline{K})[J]$ *is* J*-injective.*

Proof. By [LJ96, Proposition 5.1] the R-module $E(\overline{K})_{\mathrm{tors}}$ is injective, thus in particular J-injective. Since $E(\overline{K})[J] = \left(0 :_{E(\overline{K})_{\mathrm{tors}}} J\right)$ it follows from Lemma 2.28 that $E(\overline{K})[J]$ is J-injective. □

Remark 5.6. Although not necessary for our applications, it is interesting to notice that in this setting Γ is a maximal (J, T)-extension of M. Indeed $E(\overline{K})/E(\overline{K})_{\mathrm{tors}}$ is a torsion-free module over the commutative integral domain R, so it is injective. Then the short exact sequence of R-modules

$$0 \to E(\overline{K})_{\mathrm{tors}} \to E(\overline{K}) \to E(\overline{K})/E(\overline{K})_{\mathrm{tors}} \to 0$$

splits, so that $E(\overline{K}) \cong E(\overline{K})/T \oplus T$ as R-modules and since R is Noetherian it follows that $E(\overline{K})$ is injective. As in the above proposition we may conclude that Γ is J-injective, thus it is a maximal (J, T)-extension of M.

We now specialize to the case $J = \infty$.

Remark 5.7. Notice that in case $J = \infty$ we have $T = G(\overline{K})_{\mathrm{tors}}$ and

$$\Gamma = \left\{ x \in E(\overline{K}) \mid nx \in M \text{ for some } n \in \mathbb{Z}_{>0} \right\} .$$

If $R = \mathbb{Z}$ then $\mathrm{End}_R(T)$ is isomorphic, after fixing an isomorphism $T \cong (\mathbb{Q}/\mathbb{Z})^2$, to $\mathrm{Mat}_{2\times 2}(\widehat{\mathbb{Z}})$. If R is instead an order in an imaginary quadratic field then $\mathrm{End}_R(T) \cong R \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}}$. Indeed, fix for every prime p a $\mathbb{Z}_p$-basis for $R_p := R \otimes_{\mathbb{Z}} \mathbb{Z}_p$ and consider the $\widehat{\mathbb{Z}}$-subalgebra $C = \prod_p C_p$ of $\mathrm{Mat}_{2\times 2}(\widehat{\mathbb{Z}}) = \prod_p \mathrm{Mat}_{2\times 2}(\mathbb{Z}_p)$, where C_p is the image of the embedding of R_p into $\mathrm{Mat}_{2\times 2}(\mathbb{Z}_p)$ given by its multiplication action on the $\mathbb{Z}_p$-module $\mathbb{Z}_p^2 \cong R_p$. Then $R \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}} \cong C$ is a $\widehat{\mathbb{Z}}$-algebra free of rank 2 as a $\widehat{\mathbb{Z}}$-module, since every C_p is a $\mathbb{Z}_p$-algebra of rank 2. Then for a suitable choice of an isomorphism $T \cong (\mathbb{Q}/\mathbb{Z})^2$ we have

$$\begin{aligned} \mathrm{End}_R(T) &= \{\varphi \in \mathrm{End}_{\mathbb{Z}}(T) \mid f(r(t)) = r(f(t)) \, \forall r \in R,\, t \in T\} \\ &= \left\{ \varphi \in \mathrm{Mat}_{2\times 2}(\widehat{\mathbb{Z}}) \mid fc = cf \, \forall c \in C \right\} \\ &= C \end{aligned}$$

where the last equality follows by applying the Centralizer Theorem to the central simple $\mathbb{Q}_p$-subalgebra $R \otimes_{\mathbb{Z}} \mathbb{Q}_p$ of $\mathrm{Mat}_{2\times 2}(\mathbb{Q}_p)$ and then restricting the coefficients to $\mathbb{Z}_p$.

In both cases, the map τ coincides with the usual Galois representation associated with the torsion of E.

Proposition 5.8. *Assume that the abelian group structure of $E(K)$ is known and that M is given in terms of set of generators for $E(K)$. Then there exists an effectively computable positive integer d such that*

$$d \cdot \left(\mathfrak{sat}(M) :_{\mathfrak{sat}(G(K))} \infty \right) \subseteq \mathfrak{sat}(M) .$$

Proof. First of all notice that $\mathfrak{sat}(M) = M + T$ and $\mathfrak{sat}(G(K)) = G(K) + T$ seen as subgroups of $E(\overline{K})$. We conclude thanks to the considerations of [Chapter 3, Section 6.1]. □

Proposition 5.9. *There exists an effectively computable positive integer n such that*

$$n \cdot H^1(\mathrm{Im}(\tau), T) = 0 .$$

Proof. This follows from [Chapter 3, Proposition 6.3] and [Chapter 3, Corollary 6.8] in the non-CM case and from [Chapter 3, Proposition 6.12] in the CM case. □

Proposition 5.10. *There exists an effectively computable positive integer m such that the subring of $\mathrm{End}_R(T)$ generated by $\mathrm{Im}(\tau)$ contains $m \cdot \mathrm{End}_R(T)$.*

Proof. This follows again from [Chapter 3, Corollary 6.8] in the case $R = \mathbb{Z}$ and from [Lom17, Theorem 1.5] in the CM case. □

Theorem 5.11. *Assume that the abelian group structures of $E(K)$ and M are effectively computable. Then there exists an effectively computable positive constant c such that the index of $\mathrm{Im}(\kappa)$ in $\mathrm{Hom}(\Gamma/\mathfrak{sat}(M), T)$ divides c.*

Proof. This is a direct consequence of Theorem 5.4 and the three propositions above. □

Remark 5.12. Since Theorem 5.4 is stated in a fairly general form, one might wonder if it can be applied to obtain a version of Theorem 5.11 for higer-dimensional abelian varieties.

Provided that one is in, or can reduce to, a case in which T is a J-injective R-module (for example if the abelian variety is simple and its endomorphism ring is a maximal order in a division algebra, see Remark 5.1), the key steps are finding effective bounds for the integers n and m of Theorem 5.4. Effective bounds for m are known, see for example [RG20, Théorème 1.5(2)].

It is also known (see [Chapter 1]) that a bound for n can be obtained by finding explicit homotheties in $\mathrm{Im}(\tau)$. This seems a harder problem to tackle, but one can hope to reduce to finding homotheties in the images of the ℓ-adic representations, as done in [Chapter 1, Section 7]. Explicit results on the existence of homotheties in the image of ℓ-adic representations attached to abelian varieties are obtained for example in [GM20].