JOURNAL de Théorie des Nombres de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Sebastiano TRONTO

Division in Modules and Kummer Theory

Tome 37, nº 2 (2025), p. 389-441.

https://doi.org/10.5802/jtnb.1326

Le Journal de Théorie des Nombres de Bordeaux *est membre du Centre Mersenne pour l'édition scientifique ouverte*
http://www.centre-mersenne.org/
e-ISSN : 2118-8572

Journal de Théorie des Nombres de Bordeaux **37** (2025), 389–441

Division in Modules and Kummer Theory

par Sebastiano TRONTO

Résumé. Dans ce travail, nous généralisons la notion de module injectif et développons une théorie de divisibilité pour les modules sur un anneau quelconque, ce qui fournit un cadre général et unifié pour l'étude des extensions de corps commutatifs de type Kummer provenant des groupes algébriques commutatifs. Avec ces outils, nous fournissons une borne effective pour le degré des extensions de corps commutatifs engendrées par des points de division des courbes elliptiques, en étendant les résultats précédents de Javan Peykar pour les courbes CM et de Lombardo et l'auteur pour le cas non-CM.

Abstract. In this work we generalize the concept of injective module and develop a theory of divisibility for modules over a general ring, which provides a general and unified framework to study Kummer-like field extensions arising from commutative algebraic groups. With these tools we provide an effective bound for the degree of the field extensions arising from division points of elliptic curves, extending previous results of Javan Peykar for CM curves and of Lombardo and the author for the non-CM case.

1. Introduction

Let K be a number field and fix an algebraic closure $\overline{K}$ of K. If G is a commutative connected 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 [15], [16] and [17]. The more general case of an extension of an abelian variety by a torus is treated in Ribet's foundational paper; see [20, Theorem 1.2]. 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

Manuscrit reçu le 21 janvier 2023, révisé le 24 mai 2025, accepté le 30 mai 2025.

2020 *Mathematics Subject Classification.* 13C11, 16D10, 16D90, 11F80, 11G05, 11G10.

Mots-clefs. Kummer theory, elliptic curves, abelian varieties, modules, injective modules, injectivity, Galois representations, open-image theorem.

points 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 unique 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 [7, Proposition 1]).

In the case of elliptic curves, one may hope to obtain an explicit version of this result. Indeed the results of [11] for the case $r = 1$ and [22, Theorem 1.2 and Theorem 1.3] for the general case 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 discussion above that the existence of non-trivial endomorphisms defined over K plays an essential role in this theory. In this paper we chose to follow the methods introduced by Javan Peykar in his thesis [8] and consider the $\mathrm{End}_K(G)$-module generated by A. This approach leads to an explicit "open image theorem" for Kummer extensions for CM elliptic curves, albeit under certain technical assumptions on $\mathrm{End}_K(G)$.

Motivated by [8] and by the author's previous results [22], 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 of the "ambient module" $G(\overline{K})$, taking inspiration from [12] as well.

We introduce a natural generalization of the concept of injective modules, which to the author's knowledge is novel. We also define a category of $(\mathcal{J}, T)$-*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 5.21, which is essentially an application of Theorem 5.7, which in turn is a generalization of [22, Theorem 5.9]. The results on Galois representations needed to apply this general theorem, which include Serre's fundamental Open Image Theorem [21, Section 4,

Théorème 3′], are mostly taken from [11], where they are used to prove the main theorems 1.1, 1.2 and 1.3; see for example [11, Section 3]. The given bounds only depend on the images of the ℓ-adic representations, so that the constant c of our main theorem is effectively computable. See Propositions 5.18, 5.19 and 5.20 and Example 5.22 for more details.

The main results of Section 5 are stated and proved here only for elliptic curves. However, the general formulation of the technical framework developed in Section 4 makes it possible to apply some of the results of this paper to higher-dimensional abelian varieties, or even to products of abelian varieties by tori. Indeed, some of our main results, such as Theorem 5.7 and Corollary 5.12, are stated in a general form, and they can be applied directly to different classes of algebraic groups, provided that one can prove suitable analogues of some preliminary lemmas, such as Lemma 5.2. See also Remark 5.23. Some work in this direction has been carried out by Perissinotto in [14].

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 the 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 $\mathcal{J}$-injective modules that will be applied in Section 5.

In Section 3 we construct the category of $(\mathcal{J}, T)$-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* $(\mathcal{J}, T)$-extension, in analogy with field theory.

Section 4 is devoted to the study of automorphism groups of $(\mathcal{J}, T)$-extensions. The fundamental exact sequence of Theorem 4.14 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 [8] which gave me the main ideas for this paper. Likewise, I would like to thank Davide Lombardo for his comments on this paper, in particular for suggesting Lemma 5.2

Finally, I am thankful to the anonymous referee who suggested many improvements to the structure of the paper as well as to multiple statements.

2. $\mathcal{J}$-injectivity

2.1. Ideal filters and division in modules. In order to study division in modules over a general ring, we take inspiration from [8]. 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 $\mathcal{J}$ of right ideals of R an *ideal filter* if the following conditions hold:

(1) If $I, I' \in \mathcal{J}$ then $I \cap I' \in \mathcal{J}$, and
(2) If $I \in \mathcal{J}$ and I' is a right ideal of R containing I, then $I' \in \mathcal{J}$.

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

Notice that the definition given above coincides with that of a filter in set theory, with the additional requirement that the sets are right ideals of R.

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

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

and the one generated by all non-zero integers

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

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. Recall that, for any right ideal I of R and any left R-module M, the submodule $M[I] = \{x \in M \mid Ix = 0\}$ is called the I-torsion of M. Analogously, we define the torsion with respect to an ideal filter.

Definition 2.3. Let $\mathcal{J}$ be an ideal filter of R and let M be a left R-module. We call

$$M[\mathcal{J}] := \bigcup_{I \in \mathcal{J}} M[I]$$

the *$\mathcal{J}$-torsion submodule* of M.

Example 2.4. Let M be an abelian group.

(1) If p is a prime and p^∞ is the ideal filter of $\mathbb{Z}$ introduced in Example 2.2, the subgroup $M[p^\infty]$ of M consists of all the p-power torsion points, that is

$$M[p^\infty] = \{x \in M \mid p^n x = 0 \text{ for some } n \in \mathbb{N}\} .$$

(2) If ∞ is the other ideal filter of $\mathbb{Z}$ introduced in Example 2.2, then $M[\infty]$ coincides with the torsion subgroup of M.

We can then extend this notion to what is one of the main new concepts of this section, generalizing *division modules* with respect to ideals.

Definition 2.5. 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 appropriate a change of terminology.

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

Definition 2.6. Let $\mathcal{J}$ be an ideal filter of R and let $M \subseteq N$ be left R-modules. We call

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

the *$\mathcal{J}$-division module of M in N*.

One can easily check that $(M :_N \mathcal{J})$ is an R-submodule of N and that $M[\mathcal{J}] = (0 :_M \mathcal{J})$.

Example 2.7. Let $M = \mathbb{Z}$ and $N = \mathbb{Q}$ as modules of the ring $\mathbb{Z}$.

(1) Let p be a prime and let p^∞ be the ideal filter introduced in Example 2.2. Then

$$(\mathbb{Z} :_{\mathbb{Q}} p^\infty) = \{x \in \mathbb{Q} \mid p^n x \in \mathbb{Z} \text{ for some } n \in \mathbb{N}\} = \mathbb{Z}[p^{-1}]\,.$$

(2) Let ∞ be the other ideal filter introduced in Example 2.2. Then

$$(\mathbb{Z} :_{\mathbb{Q}} \infty) = \{x \in \mathbb{Q} \mid nx \in \mathbb{Z} \text{ for some } n \in \mathbb{Z}_{\geqslant 0}\} = \mathbb{Q}\,.$$

Remark 2.8. If $\mathcal{J} = 0$ then $(M :_N \mathcal{J}) = N$ and $M[\mathcal{J}] = M$. On the other hand, if $\mathcal{J} = 1$ then $(M :_N \mathcal{J}) = M$ and $M[\mathcal{J}] = 0$.

Remark 2.9. Let $M \subseteq N$ be left R-modules and let $\mathcal{J}$ and $\mathcal{J}'$ be ideal filters of R with $\mathcal{J}' \subseteq \mathcal{J}$. If $M' \subseteq M$ and $N' \subseteq N$ are submodules with $M' \subseteq N'$ then it is clear from the definition of $\mathcal{J}$-division module that $(M' :_{N'} \mathcal{J}') \subseteq (M :_N \mathcal{J})$.

Definition 2.10. We say that an ideal filter $\mathcal{J}$ of R is *complete* if for every left R-module N and every submodule $M \subseteq N$ we have

$$((M :_N \mathcal{J}) :_N \mathcal{J}) = (M :_N \mathcal{J})\ .$$

The definition of complete ideal filter given above can be hard to test in practice. However, in some cases completeness is implied by product-closedness (see Definition 2.1). In order to prove this we are going to need the following Lemma:

Lemma 2.11. *Let R be a ring and let $\mathcal{J}$ be an ideal filter of R such that for every $I \in \mathcal{J}$ the left ideal RI is finitely generated. Then for every left R-module N and every submodule $M \subseteq N$ we have:*

$$((M :_N \mathcal{J}) :_N \mathcal{J}) \subseteq \bigcup_{I,I' \in \mathcal{J}} (M :_N I'I)$$

Proof. Let $\mathcal{J}$ be an ideal filter of R and let $M \subseteq N$ be left R-modules. Let $x \in N$ be such that there is $I \in \mathcal{J}$ with $Ix \subseteq (M :_N \mathcal{J})$. 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 $I_i \in \mathcal{J}$ such that $I_i y_i x \subseteq M$. By definition of ideal filter we have that $I' := \bigcap_{i=1}^n I_i$ is in $\mathcal{J}$. Since $\{y_1, \dots, y_n\}$ is a set of generators for the left ideal RI and I' is a right ideal we have $I'Ix = I'(RI)x \subseteq M$, which concludes our proof. □

Proposition 2.12. *Let R be a ring and let $\mathcal{J}$ be a product-closed ideal filter of R such that for every $I \in \mathcal{J}$ the left ideal RI is finitely generated. Then $\mathcal{J}$ is complete.*

In particular, every product-closed ideal filter over a left-Noetherian ring is complete.

Proof. Let $\mathcal{J}$ be a product-closed ideal filter of R and let $M \subseteq N$ be left R-modules. By Lemma 2.11 we have

$$((M :_N \mathcal{J}) :_N \mathcal{J}) \subseteq \bigcup_{I,I' \in \mathcal{J}} (M :_N I'I) \ .$$

Since $\mathcal{J}$ is product-closed, we have $I'I \in \mathcal{J}$ for every $I, I' \in \mathcal{J}$, therefore

$$\bigcup_{I,I' \in \mathcal{J}} (M :_N I'I) \subseteq \bigcup_{I'' \in \mathcal{J}} (M :_N I'') = (M :_N \mathcal{J}) \ .$$

This implies that $\mathcal{J}$ is complete. □

Example 2.13. The ideal filters introduced in Example 2.2 are 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 2.14. *Let $M \subseteq N \subseteq P$ and M' be left R-modules and let $\mathcal{J}$ and $\mathcal{J}'$ be ideal filters of R. Then the following properties hold:*

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

Proof.

(1) The inclusion $(M :_N \mathcal{J}) \subseteq (M :_P \mathcal{J}) \cap N$ is obvious; for the other inclusion it suffices to notice that if $n \in N$ is such that $In \subseteq M$ for some $I \in \mathcal{J}$ then by definition $n \in (M :_N \mathcal{J})$.
(2) Follows directly from (1).
(3) For every $I \in \mathcal{J}$ we have $(N/M)[I] = (M :_N I)/M$ by definition, and the conclusion follows by taking the union over $I \in \mathcal{J}$ on both sides of the equality.
(4) By (3) we have that $(N/M)[\mathcal{J}] = N/M$ if and only if $(M :_N \mathcal{J}) = N$.
(5) For any right ideal I of R 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

$$\begin{aligned}(M \oplus M')[\mathcal{J}] &= \bigcup_{I \in \mathcal{J}} (M \oplus M')[I] \\ &= \bigcup_{I \in \mathcal{J}} M[I] \oplus M'[I] \\ &= M[\mathcal{J}] \oplus M'[\mathcal{J}].\end{aligned}$$

□

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

Definition 2.15. Let M be a left R-module. An R-module homomorphism $\varphi : M \to N$ is called a *$\mathcal{J}$-map* if $(\varphi(M) :_N \mathcal{J}) = N$. If φ is injective we will call it a *$\mathcal{J}$-extension*, and we say that N is a $\mathcal{J}$-extension of M.

Remark 2.16. By Lemma 2.14(4) a homomorphism $\varphi : M \to N$ is a $\mathcal{J}$-map if and only if $N/\varphi(M)$ is $\mathcal{J}$-torsion. In particular, if $\mathcal{J} = 0$ then every homomorphism of R-modules is a $\mathcal{J}$-map, and if $\mathcal{J} = 1$ then a homomorphism is a $\mathcal{J}$-map if and only if it is surjective.

Example 2.17. If p is a prime and p^∞ is the ideal filter of $\mathbb{Z}$ introduced in Example 2.2, The standard inclusion $\mathbb{Z} \hookrightarrow \mathbb{Z}[p^{-1}]$ is a p^∞-extension of $\mathbb{Z}$-modules.

On the other hand, the inclusion $\mathbb{Z} \hookrightarrow \mathbb{Q}$ is an ∞-extension, but it is not a p^∞-map for any prime p.

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

The following Lemma, which strongly relies on the assumption that $\mathcal{J}$ is complete, shows moreover that R-modules and $\mathcal{J}$-maps form a subcategory of the category of R-modules.

Lemma 2.18. *Let $\mathcal{J}$ be a complete ideal filter of R. 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 $\mathcal{J}$-maps, then so is $\psi \circ \varphi$.*

Proof. Assume that $\varphi : M \to N$ and $\psi : N \to P$ are $\mathcal{J}$-maps. As $N/\varphi(M)$ is torsion, its image $\psi(N)/\psi(\varphi(M))$ also is. Since $\mathcal{J}$ is complete we have

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

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

Remark 2.19. Let $\varphi : M \to N$ be a homomorphism of R-modules.

(1) If N is $\mathcal{J}$-torsion, then φ is a $\mathcal{J}$-map.
(2) It follows from (1) that $\varphi|_{M[\mathcal{J}]} : M[\mathcal{J}] \to N[\mathcal{J}]$ is a $\mathcal{J}$-map for any R-modules M and N.

The following Lemma illustrates how certain properties of a $\mathcal{J}$-map largely depend on its restriction to the $\mathcal{J}$-torsion submodule. Recall that

an R-module homomorphism $f : M \hookrightarrow N$ is called an *essential extension* if it is injective and for every submodule $N' \subseteq N$ we have $N' \cap f(M) = 0 \implies N' = 0$, see for example [1, Section 5].

Lemma 2.20. *A $\mathcal{J}$-extension $\varphi : M \to N$ is essential if and only if $\varphi|_{M[\mathcal{J}]} : M[\mathcal{J}] \to N[\mathcal{J}]$ is.*

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

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

Since $\varphi : M \to N$ is a $\mathcal{J}$-map, there is $I \in \mathcal{J}$ such that $In \subseteq \varphi(M)$. In particular, since $0 \notin \mathcal{J}$ and n is not $\mathcal{J}$-torsion, there is $r \in I$ 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 2.21. *Let $\varphi : M \to N$ be a $\mathcal{J}$-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 $f(n) - g(n) \in P[\mathcal{J}]$.*

Proof. The statement is clearly true for $\mathcal{J} = 0$, so we may assume that $\mathcal{J} \neq 0$. Since $(\varphi(M) :_N \mathcal{J}) = N$ there is $I \in \mathcal{J}$ 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 $f(n) - g(n) \in P[\mathcal{J}]$. □

2.3. $\mathcal{J}$-injective modules and $\mathcal{J}$-hulls. We are going to introduce the notion of *$\mathcal{J}$-injective module*, which generalizes the classical notion of injectivity. For an overview of the classical theory of injective modules, see for example [3, Section 57].

Fix for this section a ring R and a complete ideal filter $\mathcal{J}$ of R.

Definition 2.22. A left R-module Q is called *$\mathcal{J}$-injective* if for every $\mathcal{J}$-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 2.23. Notice that in case $\mathcal{J} = 0$ the definition of $\mathcal{J}$-injective R-module coincides with that of injective module (see [3, Section 57.2]). Moreover, if $\mathcal{J}'$ is a complete ideal filter of R such that $\mathcal{J}' \subseteq \mathcal{J}$, then a $\mathcal{J}$-injective module is also $\mathcal{J}'$-injective.

In particular, every injective R-module is $\mathcal{J}$-injective for every complete ideal filter $\mathcal{J}$.

The following proposition shows the strong analogy that exists between the classical theory of injective modules and the theory developed here.

Proposition 2.24. *If Q is a $\mathcal{J}$-injective left R-module, then every short exact sequence*

$$0 \longrightarrow Q \xrightarrow{i} M \longrightarrow N \longrightarrow 0$$

where i is a $\mathcal{J}$-extension is split. In particular, M is isomorphic to the direct sum of Q with a $\mathcal{J}$-torsion left R-module.

Proof. The definition of $\mathcal{J}$-injectivity ensures the existence of an R-module homomorphism $f : M \to Q$ such that $f \circ i = \mathrm{id}_Q$, which implies that the sequence is split with $M = i(Q) \oplus \ker f$.

The last part of the Proposition follows from the fact that $N \cong M/Q$ is $\mathcal{J}$-torsion By Remark 2.16. □

Corollary 2.25. *Let M be a $\mathcal{J}$-injective R-module. If $f : M \hookrightarrow N$ is an essential $\mathcal{J}$-extension, then it is an isomorphism.*

Proof. By Proposition 2.24, the module N is the internal direct sum of $f(M)$ with a torsion submodule $N' \subseteq N$. But by definition of essential extension we must have $N' = 0$, hence f is an isomorphism. □

The converse of Proposition 2.24 is also true, but it relies on the fact that every left R-module admits a $\mathcal{J}$-extension into a $\mathcal{J}$-injective module, something that will be proved in Theorem 2.36. The proof of this converse is analogous to the classical case, which relies on the fact that every left R-module can be embedded in an injective module.

Example 2.26. 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 analogous to that of the well-known result that a $\mathbb{Z}$-module is injective if and only if it is divisible, see for example [3, Section 57.5].

In particular, the following $\mathbb{Z}$-modules are p^∞-injective:

(1) The localization $M[p^{-1}]$ of any abelian group M;
(2) The torsion module $\mathbb{Z}[p^{-1}]/\mathbb{Z}$;
(3) Any n-torsion module M, where n is a positive integer not divisible by p.

The following proposition is an analogue of the well-known Baer's criterion in the classical case of injective modules, see [3, Section 57.14].

Proposition 2.27. *A left R-module Q is $\mathcal{J}$-injective if and only if for every two-sided ideal $I \in \mathcal{J}$ 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 $\mathcal{J}$-extension if $I \in \mathcal{J}$. For the other implication, let $i : M \hookrightarrow N$ be a $\mathcal{J}$-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 $(i(M) :_N \mathcal{J}) = N$ there is $I' \in \mathcal{J}$ such that $I'x \subseteq N'$, which implies $I' \subseteq I$, so also $I \in \mathcal{J}$. 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 $I \cap \ker(h)$, the map h gives rise to a map $h' : Rx \to Q$ by sending $rx \in Rx$ to $h(r)$. Since by definition $N' \cap Rx \subseteq Ix$, 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 2.28. Let R be an integral domain and let $\mathcal{J}$ be the ideal filter 0 on R. Then the set of ideals $\mathcal{J}' = \mathcal{J} \setminus \{0\}$ is an ideal filter, which is complete if R is Noetherian.

Using Proposition 2.27 one can easily show that an R-module Q is $\mathcal{J}$-injective if and only if it is $\mathcal{J}'$-injective. Indeed, one implication holds by Remark 2.23 because $\mathcal{J} \subseteq \mathcal{J}'$, 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.

The completeness of $\mathcal{J}'$ follows from Proposition 2.12, because the fact that R is an integral domain implies that the product of any two non-zero ideals of R is non-zero.

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

Example 2.29. Let M be an abelian group, let p be a prime and let $\mathcal{J} = p^\infty$ be the ideal filter of $\mathbb{Z}$ introduced in Example 2.2. Then the localization $M[p^{-1}]$, being a p-divisible abelian group, is a $\mathcal{J}$-injective $\mathbb{Z}$-module (see Example 2.26).

To see this directly, let $i : N \hookrightarrow P$ be a $\mathcal{J}$-extension and let $f : N \to M[p^{-1}]$ be 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 then a well-defined group homomorphism such that $g \circ i = f$.

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 (see also [3, Section 57.10]). 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 [2], [4], [5] or [3, Sections 57.8 and 57.13].

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

Definition 2.30. Let M be a left R-module. A $\mathcal{J}$-extension $\iota : M \hookrightarrow \Omega$ is called a *$\mathcal{J}$-hull* of M if it is an essential extension and Ω is $\mathcal{J}$-injective.

Remark 2.31. If $\mathcal{J} = 0$ the definition of $\mathcal{J}$-hull coincides with that of injective hull.

Example 2.32. Let $R = \mathbb{Z}$ and $\mathcal{J} = p^\infty$ be the ideal filter introduced in Example 2.2.

(1) Let $M = \mathbb{Z}$. Then the natural inclusion $\mathbb{Z} \hookrightarrow \mathbb{Z}[p^{-1}]$ is a $\mathcal{J}$-hull. In fact it is an essential extension, and $\mathbb{Z}[p^{-1}]$ is $\mathcal{J}$-injective by Example 2.26.

(2) Let M be an abelian group such that $nM = 0$ for some positive integer n not divisible by p. Then $\mathrm{id}_M : M \to M$ is a $\mathcal{J}$-hull, again by Example 2.26.

(3) Let $M = \mathbb{Z}/p^e\mathbb{Z}$ for some positive integer e. Then the map

$$\begin{array}{rccc} \iota : & M & \longrightarrow & \mathbb{Z}[p^{-1}]/\mathbb{Z} \\ & s \bmod p^e & \longmapsto & \dfrac{s}{p^e} \bmod \mathbb{Z} \end{array}$$

is a $\mathcal{J}$-hull. Indeed, it is a $\mathcal{J}$-extension, because the Prüfer group $\mathbb{Z}[p^{-1}]/\mathbb{Z}$ is $\mathcal{J}$-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 $\frac{1}{p^{\min(e,d)}}\mathbb{Z}$.

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

Remark 2.33. If $f_i : M_i \hookrightarrow N_i$, for $i = 1, \dots, k$, are $\mathcal{J}$-hulls, then the finite sum

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

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

Example 2.34. Let $R = \mathbb{Z}$ and $\mathcal{J} = p^\infty$ be the ideal filter introduced in Example 2.2. Let M be a finitely generated abelian group and write it 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

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

It follows directly from Example 2.32 and Remark 2.33 that $\iota : M \to \Gamma$ is a $\mathcal{J}$-hull.

Lemma 2.35. *Let Q be a $\mathcal{J}$-injective R-module and let $P \subseteq Q$ be any submodule. Then $(P :_Q \mathcal{J})$ is $\mathcal{J}$-injective.*

Proof. Let $i : M \hookrightarrow N$ be a $\mathcal{J}$-extension and let $f : M \to (P :_Q \mathcal{J})$ be any R-module homomorphism. Denote by $j : (P :_Q \mathcal{J}) \hookrightarrow Q$ the inclusion. Since Q is $\mathcal{J}$-injective, there is a map $g : N \to Q$ such that $g \circ i = j \circ f$.

Since N/M is $\mathcal{J}$-torsion, $g(N)/(P :_Q \mathcal{J})$ also is, which implies that $g(N) \subseteq ((P :_Q \mathcal{J}) :_Q \mathcal{J})$. Since $\mathcal{J}$ is complete we have thus $g(N) \subseteq (P :_Q \mathcal{J})$. This shows that $(P :_Q \mathcal{J})$ is $\mathcal{J}$-injective. □

Theorem 2.36. *Every left R-module M admits a $\mathcal{J}$-hull. Moreover, the following holds for any $\mathcal{J}$-hull $\iota : M \hookrightarrow \Omega$ of M:*

(1) *For every essential $\mathcal{J}$-extension $i : M \hookrightarrow N$ there is a $\mathcal{J}$-hull $j : N \hookrightarrow \Omega$ with $j \circ i = \iota$.*
(2) *For every $\mathcal{J}$-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 $\Omega := (\iota(M) :_\Gamma \mathcal{J})$. Since $\iota : M \hookrightarrow \Gamma$ is an essential extension then also $\iota : M \hookrightarrow \Omega$ is, and by Lemma 2.14(2) we have $(\iota(M) :_\Omega \mathcal{J}) = \Omega$, so $\iota : M \hookrightarrow \Omega$ is a $\mathcal{J}$-extension of M. By Lemma 2.35 the R-module Ω is $\mathcal{J}$-injective, so it is a $\mathcal{J}$-hull of M.

For (1), since Ω is $\mathcal{J}$-injective there is a map $j : N \to \Omega$ such that $j \circ i = \iota$. This map is injective because $i : M \hookrightarrow N$ is an essential extension: indeed we have $\ker(j) \cap i(M) = i(\ker(\iota)) = 0$, hence $\ker(j) = 0$. Moreover, it is an essential extension, because $\iota : M \hookrightarrow \Omega$ is. So $j : N \hookrightarrow \Omega$ is a $\mathcal{J}$-hull.

For (2), let $\iota : M \hookrightarrow \Omega$ and $\iota' : M \hookrightarrow \Omega'$ be two $\mathcal{J}$-hulls. Since Ω' is $\mathcal{J}$-injective there is an R-module homomorphism $f : \Omega \to \Omega'$ such that

$f \circ \iota = \iota'$. Since ι is an essential extension, by the same reasoning used in (2) it follows that f is injective. But then, since $\mathrm{id}_\Omega : \Omega \hookrightarrow \Omega$ is a $\mathcal{J}$-hull by (2), 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. □

For the equivalent result in the classical setting, see [3, Section 57.13].

2.4. Duality. Fix again a ring R and a complete ideal filter $\mathcal{J}$ of R. Fix as well a left R-module M and a $\mathcal{J}$-injective and $\mathcal{J}$-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 5.6).

Definition 2.37. 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.

Definition 2.38. If M' is a submodule of M we will denote by $\pi_{M,M'}$ the quotient map $M \to M'$.

Moreover, we denote the set homomorphisms factoring through the quotient by

$$\pi_{M,M'}^{-1} \mathrm{Hom}_R(M/M', T) := \left\{ f \in \mathrm{Hom}_R(M, T) \,\middle|\, \ker(f) \supseteq M' \right\} .$$

Proposition 2.39. *If V is a finitely generated E-submodule of $\mathrm{Hom}_R(M, T)$ we have*

$$V = \pi_{M,\ker(V)}^{-1} \mathrm{Hom}_R(M/\ker(V), T) .$$

Remark 2.40. Proposition 2.39 is a generalization of the following fact from linear algebra: let V be a finite-dimensional vector space over a field K and let $f_1, \dots, f_n : V \to K$ 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 $f_1, \dots, f_n$.

Proof of Proposition 2.39. Notice that the inclusion

$$V \subseteq \pi_{M,\ker(V)}^{-1} \mathrm{Hom}_R(M/\ker(V), T)$$

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

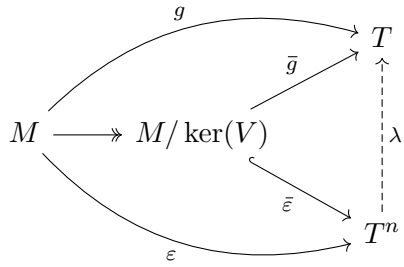
a map and let $\bar{g} := g \circ \pi_{M,M'}$. Let $\{f_1, \ldots, f_n\}$ be a set of generators for V as an E-module and let

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

We have $\ker(\varepsilon) = \ker(V)$, so that ε factors as an injective map

$$\bar{\varepsilon} : M/\ker(V) \longrightarrow T^n \,.$$

Since T is $\mathcal{J}$-torsion, so is T^n, hence $\bar{\varepsilon}$ is a $\mathcal{J}$-extension. Since T is $\mathcal{J}$-injective there is an R-linear map $\lambda : T^n \to T$ such that $\lambda \circ \bar{\varepsilon} = \bar{g}$, 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. □

In order to state the final result of this section we need to introduce the concept of *cogenerator* for a left R-module. For more details on this, see for example [1, Section 8].

Definition 2.41. 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 2.42. *Let R be a ring and let $\mathcal{J}$ be a complete ideal filter on R. Let T be a $\mathcal{J}$-injective and $\mathcal{J}$-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*

$$\begin{array}{ccc} \{R\text{-submodules of } M\} & \longrightarrow & \{\mathrm{End}_R(T)\text{-submodules of } \mathrm{Hom}_R(M,T)\} \\ M' & \longmapsto & \pi_{M,M'}^{-1}\,\mathrm{Hom}_R(M/M', T) \\ \ker(V) & \longleftarrow & V \end{array}$$

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 of all that the 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 $\mathrm{End}_R(T)$-submodule V is finitely generated, so from Proposition 2.39 we have $V = \pi^{-1}_{M,\ker(V)} \mathrm{Hom}(M/\ker(V), T)$.

For the other inclusion, for any submodule $M' \subseteq M$, we have that T is a cogenerator for M/M', which implies that

$$\ker(\pi^{-1}_{M,M'} \mathrm{Hom}_R(M/M', T)) = M. \qquad \square$$

Example 2.43. Let $R = \mathbb{Z}$, let $\mathcal{J} = \infty$ 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 $\mathcal{J}$-torsion and, since it is injective, it is in particular $\mathcal{J}$-injective.

If A is any abelian group, for any $a \in A$ there exists a group homomorphism $f : A \to \mathbb{Q}/\mathbb{Z}$ such that $f(x) \neq 0$: indeed any torsion element of A can be mapped to an element of $\mathbb{Q}/Z$ with the same order. This implies that $\mathbb{Q}/\mathbb{Z}$ is a cogenerator for every abelian group.

Since M is finitely generated, the group $\mathrm{Hom}_R(M,T)$ is isomorphic to a submodule of $\mathrm{Hom}_R(\mathbb{Z}^r, T) \cong T^r$ for some $r \in \mathbb{N}$. Therefore, it is Noetherian as a module over $\mathrm{End}_R(T) = \mathrm{Mat}_{s\times s}(\widehat{\mathbb{Z}})$.

We conclude that in this situation Theorem 2.42 can be applied.

Remark 2.44. By [1, Section 18.19] there exists an injective R-module C that is a cogenerator for every R-module and it is minimal in the sense that every other injective R-module C' that is a cogenerator for every R-module a submodule isomorphic to C. By taking T to be such a minimal injective cogenerator, Theorem 2.42 can be interpreted as a duality result.

3. The category of $(\mathcal{J}, T)$-extensions

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

In this section we introduce $(\mathcal{J}, T)$-extensions, which are essentially $\mathcal{J}$-extensions whose $\mathcal{J}$-torsion is contained in an R-module T as above (see Definition 3.16). 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" $(\mathcal{J}, T)$-extension, analogous to an algebraic closure in field theory.

3.1. T-pointed R-modules.

In order to define $(\mathcal{J}, T)$-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 $s : M[\mathcal{J}] \hookrightarrow T$ 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 $s \circ \varphi|_{L[\mathcal{J}]} = r$.

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 $L[\mathcal{J}]$. Indeed $s \circ \varphi|_{L[\mathcal{J}]} = r$ is injective, so $\varphi|_{L[\mathcal{J}]}$ must be injective as well.

Definition 3.3. If (M, s) is a T-pointed R-module we denote the T-pointed R-module $(M[\mathcal{J}], s)$ 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 $\mathcal{J}$ 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 $(\frac{1}{6}, 0)$ and $(0, 1)$ to $(0, \frac{1}{2})$ 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 $\mathcal{J}$-map as possible".

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

Example 3.6. Let $\mathcal{J} = \infty$ be the ideal filter of $\mathbb{Z}$ introduced in Example 2.2.

(1) The map $\mathfrak{t}_M : \mathfrak{tor}(M) \hookrightarrow M$ introduced in Definition 3.3 is pure for every T-pointed R-module M, because $(M[\mathcal{J}] :_M \mathcal{J}) = M[\mathcal{J}]$.

(2) Let M and N be two abelian groups. Then the inclusion $M \hookrightarrow M \oplus N$ is always a pure map. Indeed we have

$$\begin{aligned}(f(L) :_M \infty) &= \{(m, n) \in M \oplus N \mid k(m, n) \in (M, 0) \text{ for some } k \in \mathbb{Z}_{\geqslant 1}\} \\ &= \{(m, n) \mid m \in M,\, n \in N_{\mathrm{tors}}\} \\ &= (M, 0) + (M \oplus N)_{\mathrm{tors}}\end{aligned}$$

(3) Let M be an abelian group and write it as $M \cong M' \oplus M_{\mathrm{tors}}$, where M' is torsion-free. Then the inclusion $M' \hookrightarrow M$ is at the same time a $\mathcal{J}$-extension and a pure map.

Remark 3.7. If $f : L \to M$ is an injective pure map of T-pointed R-modules, then the sequence

$$0 \longrightarrow L[\mathcal{J}] \xrightarrow{f} M[\mathcal{J}] \longrightarrow (M/f(L))[\mathcal{J}] \longrightarrow 0$$

is exact. Indeed, exactness at $M[\mathcal{J}]$ comes form the injectivity of f, and exactness at $(M/f(L))[\mathcal{J}]$ follows from the fact that f is pure: indeed we have $(M/f(L))[\mathcal{J}] = (f(L) :_M \mathcal{J})/f(L) = (f(L) + M[\mathcal{J}])/f(L)$.

Remark 3.8. For every T-pointed R-module (M, s), the map $\mathfrak{t}_M$ is pure and injective.

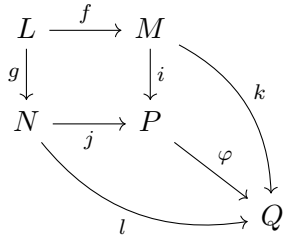
Proposition 3.9. *Let (L, r), (M, s) and (N, t) be T-pointed R-modules and let $f : L \to M$ and $g : L \to N$ be maps of T-pointed R-modules. Assume that f is injective and pure. Then the pushout $M \xrightarrow{i} P \xleftarrow{j} N$ of f along g exists in the category of T-pointed R-modules.*

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 $S = \{(f(\lambda), -g(\lambda)) \mid \lambda \in L\}$.

We claim that $P'[\mathcal{J}]$ is generated by $i'(M[\mathcal{J}])$ and $j'(N[\mathcal{J}])$. The claim is obviously true if $\mathcal{J} = 0$, so we may assume that $\mathcal{J} \neq 0$. To prove the claim, notice that by Lemma 2.14(3) we have $P'[\mathcal{J}] = (S :_{M\oplus N} \mathcal{J})/S$, so any element of $P'[\mathcal{J}]$ is represented by a pair (m, n) such that $I(m, n) \subseteq S$

for some $I \in \mathcal{J}$. Then since f is a pure map we have $m = f(\lambda) + t_m$ for some $\lambda \in L$ and some $t_m \in M[\mathcal{J}]$.

Let $I' \in \mathcal{J}$ be such that $I't_m = 0$. Then $I \cap I' \in \mathcal{J}$ and for any non-zero $h \in I \cap I'$ 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 $t_n \in N[\mathcal{J}]$. It follows that the class of (m, n) in $P'[\mathcal{J}]$ is the same as that of (t_m, t_n), which proves our claim.

Let $\pi : P' \to P$ be the quotient by the submodule

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

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

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

$$\begin{array}{rccc} u: & P[\mathcal{J}] & \longrightarrow & T \\ & [(m,n)] & \longmapsto & s(m) + t(n) \end{array}$$

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.

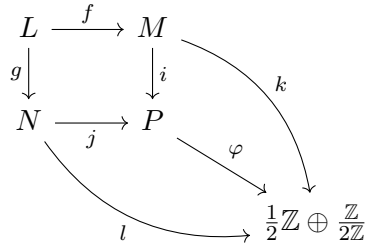
Let now (Q, v), k and l be as above. By the universal property of the pushout there is a unique R-module homomorphism $\varphi' : P' \to Q$ such that $\varphi' \circ i' = k$ and $\varphi' \circ j' = l$. Since k is a map of T-pointed R-modules, this implies that $v \circ \varphi' \circ i' = s$ and $v \circ \varphi' \circ j' = t$, 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 $m_0 \in m$, $m \in M[\mathcal{J}]$ and $n \in N[\mathcal{J}]$ 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 $\mathcal{J}$-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. The fact that the injectivity of f implies that of j is completely analogous. □

Remark 3.10. Let $R = \mathbb{Z}$, $\mathcal{J} = 2^\infty$, $T = \mathbb{Z}[\frac{1}{2}]/\mathbb{Z}$, $L = \mathbb{Z}$ and $M = N = \frac{1}{2}\mathbb{Z}$. The R-modules L, M and N are T-pointed via the zero map, since their $\mathcal{J}$-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 $(\frac{1}{2}\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}, z)$, where $z : \mathbb{Z}/2\mathbb{Z} \to T$ is the only possible

injective map. Consider the diagram

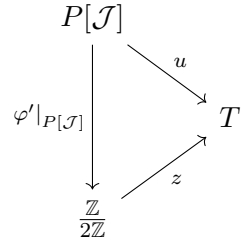


where the maps k and l are defined as

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

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-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 non-zero 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 $(\frac{1}{2}, 0)$, 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 $\varphi'(j(\frac{1}{2})) = (\frac{1}{2}, 0) = \varphi'(i(\frac{1}{2}))$. 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 3.11. Let (M, s) be a T-pointed R-module. We say that (M, s) is *saturated* if $s : M[\mathcal{J}] \hookrightarrow T$ is surjective (and hence an isomorphism).

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 3.12. Let (M, s) be a T-pointed R-module. Recall from Example 3.6(1) that the inclusion $\mathfrak{t}_M : M[\mathcal{J}] \hookrightarrow M$ of the $\mathcal{J}$-torsion of M into M is an injective pure map.

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

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

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

Example 3.13. Let $R = \mathbb{Z}$ and let $\mathcal{J} = p^\infty$ be the ideal filter of $\mathbb{Z}$ introduced in Example 2.2 for some prime p.

Let M be a finitely generated abelian group and write it 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.

Fix an integer $K \geqslant k$ and let $T = (\mathbb{Z}[p^{-1}])^K$. Fix an injective map $s : M[p^\infty] \hookrightarrow T$ so that (M, s) becomes a T-pointed R-module.

It is easy to check that the saturation of (M, s) is

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

and the map $\mathfrak{s}_M : M \hookrightarrow \mathfrak{sat}(M)$ is given by $\mathfrak{s}_M(z, u, t) = (z, s(u), t)$.

Remark 3.14. Notice that the pushout map $T \to P$ of Definition 3.12 is an isomorphism onto $P[\mathcal{J}]$. Indeed by definition of T-pointed R-module the following diagram commutes:

$$\begin{array}{ccc} T = T[\mathcal{J}] & & \\ \downarrow & \searrow^{\mathrm{id}_T} & \\ & & T \\ & \nearrow_{\mathfrak{sat}(s)} & \\ P[\mathcal{J}] & & \end{array}$$

where the vertical map on the left is the pushout map. It follows that $\mathfrak{sat}(s)$, which is injective by Proposition 3.9, 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.

Moreover, the saturation of a saturated T-pointed R-module is canonically isomorphic to itself. Indeed, let (M, s) be a saturated T-pointed R-module. Then the saturation of (M, s) is the pushout of the diagram:

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

and is easy to see that, since s is an isomorphism, $(M, \mathrm{id}_M, \mathfrak{t}_M \circ s^{-1})$ satisfies the universal property of the pushout.

Remark 3.15. In the setting of Definition 3.12, the map $\mathfrak{sat}(s)$ is injective by Proposition 3.9. Moreover, it is a pure map because P is generated by M and $P[\mathcal{J}]$.

3.2. $(\mathcal{J}, T)$-extensions. We can finally introduce the main object of study of this section.

Definition 3.16. Let (M, s) be a T-pointed R-module. A $(\mathcal{J}, T)$-*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 $\mathcal{J}$-extension.

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

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

Alternatively, one can think of a $(\mathcal{J}, T)$-extension as a $\mathcal{J}$-extension $M \hookrightarrow N$ where both M and N are endowed with the structure of a T-pointed R-module such that the diagram

$$\begin{array}{ccc} M[\mathcal{J}] & & \\ \downarrow & \searrow & \\ & & T \\ & \nearrow & \\ N[\mathcal{J}] & & \end{array}$$

commutes.

In the following we will sometimes omit the maps i and t from the notation and simply refer to *the* $(\mathcal{J}, T)$-*extension* N *of* M.

Example 3.17. Let $R = \mathbb{Z}$, let $\mathcal{J}$ 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 $(\frac{1}{2},0)$ and $(0,1)$ to $(0,\frac{1}{2})$ 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

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

define two different T-pointed R-module structures (N,t_1) and (N,t_2) on N. The component-wise 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 $(\mathcal{J},T)$-extensions and field extensions: every map is injective, and every surjective map is an isomorphism.

Lemma 3.18. *Every map of $(\mathcal{J},T)$-extensions is injective.*

Proof. Let (N,i,t) and (P,j,u) be $(\mathcal{J},T)$-extensions of the T-pointed R-module (M,s) and let $\varphi : N \to P$ be a map of $(\mathcal{J},T)$-extensions. Let $n \in \ker\varphi$. Since $i : M \hookrightarrow N$ is a $\mathcal{J}$-extension there is $I \in \mathcal{J}$ 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 $\mathcal{J}$-torsion. But since φ is a map of T-pointed R-modules it is injective on $M[\mathcal{J}]$ (see Remark 3.2) so $n = 0$. □

Remark 3.19. Let (N,i,t) and (P,j,u) be $(\mathcal{J},T)$-extensions of the T-pointed R-module (M,s) and let $\varphi : N \to P$ be a map of $(\mathcal{J},T)$-extensions. Then (P,φ,u) is a $(\mathcal{J},T)$-extension of (N,t). In fact we have

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

Corollary 3.20. *Every surjective map of $(\mathcal{J},T)$-extensions is an isomorphism.*

Proof. Let (N,i,t) and (P,j,u) be $(\mathcal{J},T)$-extensions of the T-pointed R-module (M,s) and let $\varphi : N \to P$ be a map of $(\mathcal{J},T)$-extensions. In view of Lemma 3.18 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 $(\mathcal{J},T)$-extensions. But the fact that $\varphi^{-1} \circ j = i$ follows directly from $\varphi \circ i = j$ while $t = u \circ \varphi|^{-1}_{P[\mathcal{J}]} = u$ follows from $u \circ \varphi|_{N[\mathcal{J}]} = t$. □

Proposition 3.21. *Let (M,s) be a T-pointed R-module, let (N,i,t) be a $(\mathcal{J},T)$-extension of (M,s) and let (P,j,u) be a $(\mathcal{J},T)$-extension of (N,t). Then $(P,j\circ i,u)$ is a $(\mathcal{J},T)$-extension of (M,s).*

Proof. The map $j\circ i$ is clearly a $\mathcal{J}$-injective map of T-pointed R-modules, and it is a $\mathcal{J}$-map by Lemma 2.18. □

Remark 3.22. Any $(\mathcal{J},T)$-extension of a saturated T-pointed R-module is saturated.

3.3. Pullback and pushforward. One can recover much information about the $(\mathcal{J},T)$-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 $(\mathcal{J},T)$-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 3.23. If $\varphi : L \to M$ is a map of T-pointed R-modules and (N,i,t) is a $(\mathcal{J},T)$-extension of M, we let

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

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

Lemma 3.24. *Let $\varphi : L \to M$ be a map of T-pointed R-modules and let (N,i,t) be a $(\mathcal{J},T)$-extension of M. Then $(\varphi^*N,\varphi^*i,\varphi^*t)$ is a $(\mathcal{J},T)$-extension of $\varphi(L)$.*

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

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

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

Moreover $(\varphi^*i(\varphi(L)) :_{\varphi^*N} \mathcal{J}) = \varphi^*N$ by definition and by Lemma 2.14, so that $(\varphi^*N,\varphi^*i,\varphi^*t)$ is a $\mathcal{J}$-extension. □

Example 3.25. Let $R=\mathbb{Z}$ and let $\mathcal{J}=p^\infty$ be the ideal filter of $\mathbb{Z}$ introduced in Example 2.2. Let $T=\mathbb{Z}[p^{-1}]/\mathbb{Z}$ and $M=\mathbb{Z}\oplus\mathbb{Z}/p^n\mathbb{Z}$ for some positive integer n. Let $L=M_{\mathrm{tors}}=\mathbb{Z}/p^n\mathbb{Z}$ and denote by $\varphi : L\hookrightarrow M$ the inclusion. The map

$$\begin{array}{rccc} s: & \mathbb{Z}/p^n\mathbb{Z} & \longrightarrow & \mathbb{Z}[p^{-1}]/\mathbb{Z} \\ & 1 \bmod p^n & \longmapsto & \dfrac{1}{p^e} \bmod \mathbb{Z} \end{array}$$

endows M and L with the structure of T-pointed R-modules.

Let (N, i, t) be any $(\mathcal{J}, T)$-extension of M. Then the pullback of N along φ is

$$\begin{aligned}\varphi^* N &= (i(\varphi(L)) :_N \mathcal{J}) \\ &= (M_{\text{tors}} :_N \mathcal{J}) \\ &= N_{\text{tors}}\end{aligned}$$

with the restriction of i to M_{tors} making it a $(\mathcal{J}, T)$-extension of L.

Definition 3.26. If $\varphi : L \to M$ is a map of T-pointed R-modules, N and P are $(\mathcal{J}, T)$-extensions of M and $f : N \to P$ is a map of $(\mathcal{J}, T)$-extensions, the map

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

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

Proposition 3.27. *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 3.24 we only need to check that φ^* behaves well with the respect to the composition of maps of $(\mathcal{J}, T)$-extensions. If

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

are maps of $(\mathcal{J}, T)$-extensions of (M, s), we have

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

Definition 3.28. We call the functor of Proposition 3.27 the *pullback along* φ, and we denote it by φ^*.

Definition 3.29. If $\varphi : L \to M$ is an injective and pure map of T-pointed R-modules and (N, i, t) is a $(\mathcal{J}, T)$-extension of L we denote by $\varphi_* i : M \to \varphi_* N$ the pushout of i along φ in the category of $(\mathcal{J}, T)$-extensions of L.

Example 3.30. Let $R = \mathbb{Z}$ and let $\mathcal{J} = \infty$ be the usual ideal filter. Let $T = \mathbb{Q}/\mathbb{Z}$ and let L be a torsion-free abelian group. The trivial map $L_{\text{tors}} \to T$ endows L with the structure of a T-pointed R-module.

Let $M = L \oplus T$, seen as a T-pointed R-module via the identity map on T. The inclusion $\varphi : L \hookrightarrow M$ is a pure map of T-pointed R-modules (see also Example 3.6).

Let now (N, i, t) be a $(\mathcal{J}, T)$-extension of L, and write N as $N' \oplus N_{\text{tors}}$ for some torsion-free abelian group N. Since L is torsion-free, we can also

choose N' so that the image of $i : L \hookrightarrow N$ is contained in N'. It is easy to see that $\varphi_* N \cong N' \oplus T$ and $\varphi_* i : M \to \varphi_* N$ is

$$\begin{array}{rccc} \varphi_* i : & L \oplus T & \longrightarrow & N' \oplus T \\ & (\ell, t) & \longmapsto & (i(\ell), t) \end{array}$$

It is easy to show that $(\varphi_* N, \varphi_* i, \mathrm{id}_T)$ is a $(\mathcal{J}, T)$-extension of M.

It is in general true that, just as in the case of the pullback, the pushout along a pure map is a functor between the categories of $(\mathcal{J}, T)$-extension of the given modules. However, proving this requires some technical work, which will be carried out in the next two lemmas.

Lemma 3.31. *Let $\varphi : L \to M$ be an injective and pure map of T-pointed R-modules and let (N, i, t) be a $(\mathcal{J}, T)$-extension of L. Then $(\varphi_* N, \varphi_* i, \varphi_* t)$ is a $(\mathcal{J}, T)$-extension of (M, s).*

Proof. By Proposition 3.9 we have that φ_* is injective. Since $i : L \to N$ is a $\mathcal{J}$-extension $\varphi_* N / (\varphi_* i)(M) \cong N / i(L)$ is $\mathcal{J}$-torsion, and this concludes the proof. □

Lemma 3.32. *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 $(\mathcal{J}, T)$-extensions of L and let $f : N \to P$ be a map of $(\mathcal{J}, T)$-extensions. Then there is a unique map of $(\mathcal{J}, T)$-extensions of M*

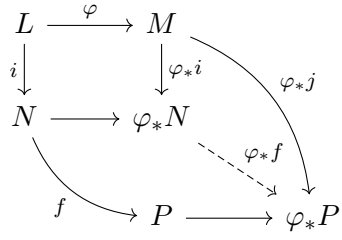
$$\varphi_* f : \varphi_* N \longrightarrow \varphi_* P$$

such that the diagram

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

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 $\mathcal{J}$-torsion. □

Proposition 3.33. *Let $\varphi : L \to M$ be an injective and pure map of T-pointed R-modules. The diagram*

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

with $\varphi_* f$ as in Lemma 3.32, defines a functor from $\mathfrak{JT}(L,r)$ to $\mathfrak{JT}(M,s)$.

Proof. In view of Lemmas 3.31 and 3.32 it is enough to show that φ_* behaves well with respect to the composition of maps of $(\mathcal{J},T)$-extensions. This is immediate from the construction in Lemma 3.32 and the uniqueness part of the universal property of the pushout. □

Definition 3.34. We call the functor of Proposition 3.33 the *pushforward along* φ, and we denote it by φ_*.

Theorem 3.35. *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 $(\mathcal{J},T)$-extension of L and let (P,j,u) be a $(\mathcal{J},T)$-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 $(\mathcal{J},T)$-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 $(\mathcal{J},T)$-extensions of M.

We define a map

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

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 $(\mathcal{J},T)$-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 $(\mathcal{J},T)$-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 $(\mathcal{J},T)$-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 $(\mathcal{J},T)$-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 3.36. 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 $(\mathcal{J},T)$-extensions of L and M respectively. We can give an explicit description of the counit

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

and the unit

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

of the adjunction.

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.

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

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

Definition 3.37. Let M be a T-pointed R-module and let $\mathfrak{t}_M : M[\mathcal{J}] \to M$ be the natural inclusion of its torsion submodule. We will call the pullback functor

$$\mathfrak{t}_M^* : \mathfrak{JT}(M,s) \longrightarrow \mathfrak{JT}(M[\mathcal{J}],s)$$

the *M-torsion* functor and we will denote it by $\mathfrak{tor}_M$.

If the module M is clear from the context, we may omit it from the notation and simply refer to the *torsion* functor $\mathfrak{tor}$.

Remark 3.38. Let (M,s) be a T-pointed R-module. For every $(\mathcal{J},T)$-extension (N,i,t) of (M,s) we have

$$\begin{aligned} \mathfrak{tor}_M(N) &= (i\,(\mathfrak{t}_M(M[\mathcal{J}])) :_N \mathcal{J}) \\ &= (i(M[\mathcal{J}]) :_N \mathcal{J}) \\ &= N[\mathcal{J}]\,. \end{aligned}$$

Remark 3.39. Let M be a T-pointed R-module. For every $(\mathcal{J},T)$-extension N of $M[\mathcal{J}]$ the unit map

$$\eta_N : ((\mathfrak{t}_M)_* N)[\mathcal{J}] \longrightarrow N$$

is an isomorphism.

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

Definition 3.40. 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

$$(\mathfrak{s}_M)_* : \mathfrak{JT}(M,s) \longrightarrow \mathfrak{JT}(\mathfrak{sat}(M), \mathfrak{sat}(s))$$

the *M-saturation* functor and we will denote it by $\mathfrak{sat}_M$.

If the module M is clear from the context, we may omit it from the notation and simply refer to the *saturation* functor $\mathfrak{sat}$.

Remark 3.41. Let M be a T-pointed R-module. For any $(\mathcal{J},T)$-extension P of $\mathfrak{sat}(M)$, the counit map

$$\varepsilon_P : P \longrightarrow \mathfrak{sat}(\mathfrak{s}_M^* P)$$

is an isomorphism. See also Remark 3.14.

3.4. Maximal $(\mathcal{J},T)$-extensions. Maximal $(\mathcal{J},T)$-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 $(\mathcal{J},T)$-extension for any T-pointed R-module, and we achieve this by first constructing such an extension for its torsion and its saturation.

Definition 3.42. A $(\mathcal{J},T)$-extension Γ of the T-pointed R-module M is called *maximal* if for every $(\mathcal{J},T)$-extension N of M there is a map of $(\mathcal{J},T)$-extensions $\varphi : N \hookrightarrow \Gamma$.

The definition of T-pointed R-module already provides a maximal $(\mathcal{J},T)$-extension for any $\mathcal{J}$-torsion module.

Lemma 3.43. *Let (M,s) be a T-pointed R-module. If M is $\mathcal{J}$-torsion, then (T,s,id_T) is a maximal $(\mathcal{J},T)$-extension of (M,s).*

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

$$\begin{aligned} N &= (i(M) :_N \mathcal{J}) \\ &= \Big(\big(0 :_{i(M)} \mathcal{J}\big) :_N \mathcal{J}\Big) \\ &\subseteq ((0 :_N \mathcal{J}) :_N \mathcal{J}) \\ &= (0 :_N \mathcal{J}) \\ &= N[\mathcal{J}] \end{aligned}$$

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

The existence of a maximal $(\mathcal{J}, T)$-extension of a saturated module comes from the existence of a $\mathcal{J}$-hull, and it requires only a little more technical work.

Lemma 3.44. *Let (M, s) be a saturated T-pointed R-module and let $\iota : M \hookrightarrow \Gamma$ be a $\mathcal{J}$-hull of M. Then*

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

Proof. For (1) notice that $\iota|_{M[\mathcal{J}]} : M[\mathcal{J}] \hookrightarrow \Gamma[\mathcal{J}]$ is an essential extension by Lemma 2.20, so it is an isomorphism by Corollary 2.25.

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

Finally we can construct a $(\mathcal{J}, T)$-extension of any T-pointed R-module.

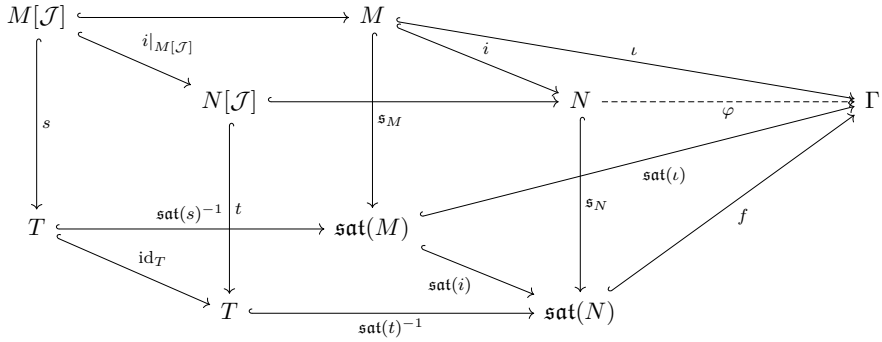
Proposition 3.45. *Let (Γ, ι, τ) be a $(\mathcal{J}, T)$-extension of the T-pointed R-module (M, s) such that Γ is saturated. Then Γ is a maximal $(\mathcal{J}, T)$-extension of M if and only if it is a maximal $(\mathcal{J}, T)$-extension of $\mathfrak{sat}(M)$.*

Proof. Notice first of all that Γ is canonically isomorphic to $\mathfrak{sat}(\Gamma)$ by Remark 3.14.

Assume first that Γ is a maximal $(\mathcal{J}, T)$-extension of M and let (N, i, t) be a $(\mathcal{J}, T)$-extension of $\mathfrak{sat}(M)$. Then there is a map $\varphi : \mathfrak{s}^*_M N \to \Gamma$ of $(\mathcal{J}, T)$-extensions of M, so there is a map $\mathfrak{sat}(\varphi) : \mathfrak{sat}(\mathfrak{s}^*_M N) \to \Gamma$ of $(\mathcal{J}, T)$-extensions of $\mathfrak{sat}(M)$. By Remark 3.41 we have $N \cong \mathfrak{sat}(\mathfrak{s}^*_M N)$, so there is also a map $N \to \Gamma$. This proves that Γ is a maximal $(\mathcal{J}, T)$-extension of $\mathfrak{sat}(M)$.

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

$\mathfrak{sat}(N) \to \Gamma$ completing the following diagram:



Defining $\varphi := f \circ \mathfrak{s}_N$ we have

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

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

Theorem 3.46. *Every T-pointed R-module M admits a maximal $(\mathcal{J}, T)$-extension. Moreover, for any maximal $(\mathcal{J}, T)$-extension Γ of M the following hold:*

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

Proof. Let $j : \mathfrak{sat}(M) \hookrightarrow \Gamma$ be a $\mathcal{J}$-hull of the saturation of M. By Lemma 3.44(1) we may define $\tau := \mathfrak{sat}(s) \circ j|^{-1}_{\mathfrak{sat}(M)[\mathcal{J}]}$, and we have that (Γ, j, τ) is a maximal $(\mathcal{J}, T)$-extension of $\mathfrak{sat}(M)$. By Remark 3.41 we have that $(\Gamma, \iota, \tau) = \mathfrak{s}^*_M(\Gamma, j, \tau)$ is a $(\mathcal{J}, T)$-extension of M such that $\mathfrak{sat}(\Gamma, \iota, \tau) \cong (\Gamma, j, \tau)$, so by Proposition 3.45 we conclude that it is a maximal $(\mathcal{J}, T)$-extension of M.

Let now (Γ', ι', τ') be another maximal $(\mathcal{J}, T)$-extension of (M, s). Then there is a map of $(\mathcal{J}, T)$-extensions $f : \Gamma \hookrightarrow \Gamma'$ which is an essential $\mathcal{J}$-extension by Lemma 2.20, as it is an isomorphism on the $\mathcal{J}$-torsion. Since Γ is $\mathcal{J}$-injective we have that f is an isomorphism by Corollary 2.25. This

shows that any maximal $(\mathcal{J},T)$-extension of M is isomorphic to Γ, which proves (1).

For (2), it is enough to prove that the Γ we constructed above is saturated. This comes from Lemma 3.44.

For (3), we once again have to prove that statement only for the Γ constructed above. This module is $\mathcal{J}$-injective because it is a $\mathcal{J}$-hull.

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

Example 3.47. As in Example 2.34 let $R=\mathbb{Z}$, $\mathcal{J}=p^\infty$ and let

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

be a finitely generated abelian group, where n is a positive integer coprime to p and the e_i's are suitable exponents.

Fix an integer $K \geqslant k$ and let $T = (\mathbb{Z}[p^{-1}]/\mathbb{Z})^K$ and an injective map $s : M[p^\infty] \hookrightarrow T$, so that (M,s) becomes a T-pointed R-module.

By Example 3.13 the saturation of M is

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

and the injective hull of $\mathfrak{sat}(M)$ is

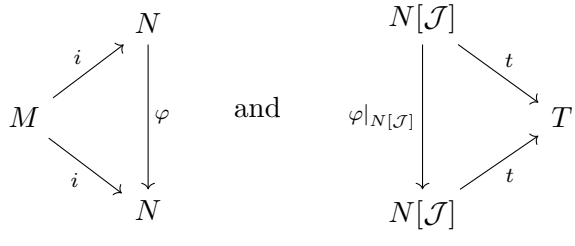
$$\Gamma = (\mathbb{Z}[p^{-1}])^r \oplus (\mathbb{Z}[p^{-1}]/\mathbb{Z})^K \oplus M[n]\,.$$

With the obvious map $M \hookrightarrow \Gamma$, the module Γ is a maximal $(\mathcal{J},T)$-extension of M.

4. Automorphisms of $(\mathcal{J},T)$-extensions

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

For any $(\mathcal{J},T)$-extension (N,i,t) of (M,s) we will denote by $\mathrm{Aut}_M(N)$ the group of automorphisms of (N,i,t) as a $(\mathcal{J},T)$-extension of (M,s). More precisely, an automorphism of the $(\mathcal{J},T)$-extension (N,i,t) is an R-module automorphism $\varphi : N \to N$ such that the diagrams



commute.

4.1. Normal extensions. We define normal extensions in analogy with field theory.

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

Notice that we are considering all injective $\mathcal{J}$-maps that respect $\iota : M \hookrightarrow \Gamma$, even if they are not maps of $(\mathcal{J},T)$-extensions, that is even if they do not respect the embeddings of the torsion submodules into T. Restricting to maps of $(\mathcal{J},T)$-extensions would make the concept of normality too broad; see Example 4.2 (3) below.

Example 4.2. Let $R = \mathbb{Z}$ and let p^∞ be the usual ideal filter. Let $T = (\mathbb{Z}[p^{-1}]/\mathbb{Z})^2$ and let $M = \mathbb{Z}$, with the trivial map $M_{\mathrm{tors}} \to T$ making it a T-pointed R-module. By Example 3.47 we have that $\Gamma = \mathbb{Z}[p^{-1}] \oplus (\mathbb{Z}[p^{-1}]/\mathbb{Z})^2$ be a maximal $(\mathcal{J},T)$-extension of M; we denote by ι the inclusion map of M in Γ.

(1) Let $N = \mathbb{Z} \oplus (\mathbb{Z}/p\mathbb{Z})^2$. With the inclusion $i : M \hookrightarrow N$ and the map

$$\begin{array}{rccc} t: & (\mathbb{Z}/p\mathbb{Z})^2 & \longrightarrow & (\mathbb{Z}[p^{-1}]/\mathbb{Z})^2 \\ & (1 \bmod p\mathbb{Z}, 0) & \longmapsto & \left(\dfrac{1}{p} \bmod \mathbb{Z}, 0\right) \\ & (0, 1 \bmod p\mathbb{Z}) & \longmapsto & \left(0, \dfrac{1}{p} \bmod \mathbb{Z}\right) \end{array}$$

we have that (N,i,t) is a $(\mathcal{J},T)$-extension of M.

We claim that this $(\mathcal{J},T)$-extension is normal. To see this, let $f : N \hookrightarrow \Gamma$ be an injective $\mathcal{J}$-map such that $f \circ i = \iota$. The last condition implies that the non-torsion part $\mathbb{Z}$ of N maps isomorphically onto $\iota(M)$. The two elements $(1 \bmod p\mathbb{Z}, 0)$ and $(0, 1 \bmod p\mathbb{Z})$ of N must map via f to p-torsion elements of Γ. Since the $\Gamma[p] \cong (\mathbb{Z}/p\mathbb{Z})^2$ and f is injective, we deduce that $f(N) = \iota(M) \oplus \Gamma[p]$.

Since the choice of f was arbitrary, we conclude that N is normal.

(2) Let $N = \mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p^2\mathbb{Z}$. With the inclusion $i : M \hookrightarrow N$ and the map

$$\begin{array}{rccc} t: & \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p^2\mathbb{Z} & \longrightarrow & (\mathbb{Z}[p^{-1}]/\mathbb{Z})^2 \\ & (1 \bmod p\mathbb{Z}, 0) & \longmapsto & \left(\dfrac{1}{p} \bmod \mathbb{Z}, 0\right) \\ & (0, 1 \bmod p^2\mathbb{Z}) & \longmapsto & \left(0, \dfrac{1}{p^2} \bmod \mathbb{Z}\right) \end{array}$$

we have that (N,i,t) is a $(\mathcal{J},T)$-extension of M.

We claim that this $(\mathcal{J},T)$-extension is not normal. To see this, it is enough to check that the maps

$$\begin{array}{rccc} f_1: & \mathbb{Z}\oplus\mathbb{Z}/p\mathbb{Z}\oplus\mathbb{Z}/p^2\mathbb{Z} & \longrightarrow & \mathbb{Z}[p^{-1}]\oplus\mathbb{Z}[p^{-1}]/\mathbb{Z}\oplus\mathbb{Z}[p^{-1}]/\mathbb{Z} \\ & (1,0,0) & \longmapsto & (1,0,0) \\ & (0,1 \bmod p\mathbb{Z},0) & \longmapsto & \left(0,\frac{1}{p},0\right) \\ & (0,0,1 \bmod p^2\mathbb{Z}) & \longmapsto & \left(0,0,\frac{1}{p^2}\right) \end{array}$$

and

$$\begin{array}{rccc} f_1: & \mathbb{Z}\oplus\mathbb{Z}/p\mathbb{Z}\oplus\mathbb{Z}/p^2\mathbb{Z} & \longrightarrow & \mathbb{Z}[p^{-1}]\oplus\mathbb{Z}[p^{-1}]/\mathbb{Z}\oplus\mathbb{Z}[p^{-1}]/\mathbb{Z} \\ & (1,0,0) & \longmapsto & (1,0,0) \\ & (0,1 \bmod p\mathbb{Z},0) & \longmapsto & \left(0,0,\frac{1}{p}\right) \\ & (0,0,1 \bmod p^2\mathbb{Z}) & \longmapsto & \left(0,\frac{1}{p^2},0\right) \end{array}$$

are both injective and such that $f_i\circ i=\iota$, but they have a different image in Γ. Indeed we have

$$f_1(N)=\mathbb{Z}\oplus\frac{1}{p}\mathbb{Z}/\mathbb{Z}\oplus\frac{1}{p^2}\mathbb{Z}/\mathbb{Z}$$

and

$$f_1(N)=\mathbb{Z}\oplus\frac{1}{p^2}\mathbb{Z}/\mathbb{Z}\oplus\frac{1}{p}\mathbb{Z}/\mathbb{Z}\,.$$

(3) Let $N=\mathbb{Z}\oplus\mathbb{Z}/p\mathbb{Z}\oplus\mathbb{Z}/p^2\mathbb{Z}$ as in (2). Even though N is not a normal $(\mathcal{J},T)$-extension of M, it is clear that every injective map of $(\mathcal{J},T)$-extensions $N\hookrightarrow\Gamma$ has the same image, because there is only one such map.

To see that there are less trivial examples of normal $(\mathcal{J},T)$-extensions such that every map of $(\mathcal{J},T)$-extensions into Γ has the same image, let $N'=\frac{1}{p}\mathbb{Z}\oplus\mathbb{Z}/p\mathbb{Z}\oplus\mathbb{Z}/p^2\mathbb{Z}$ with i and t defined as in (2). Similarly to what we did in (2), one can prove that N' is not a normal $(\mathcal{J},T)$-extension of M.

Let now $f,f':N'\hookrightarrow\Gamma$ be any two maps of $(\mathcal{J},T)$-extensions. Since we can identify T with $\Gamma[\mathcal{J}]$, we have that $f|_{N[\mathcal{J}]}=t$. Let $n\in N'$ and write it as $n=\frac{z}{p}+\tau$ with $z\in\mathbb{Z}$ and $\tau\in N[\mathcal{J}]$. Since $f(\frac{z}{p}+\tau)=zf(\frac{1}{p})+t(\tau)$, we have that the image of f is completely determined by $f(\frac{1}{p})$. Similarly, the same holds for f'. But $p(f(\frac{1}{p})-f'(\frac{1}{p}))=f(1)-f'(1)=0$, which means that $f(\frac{1}{p})-f'(\frac{1}{p})$ is a p-torsion element of Γ. Since the p-torsion of Γ is contained in both the image of f and that of f', we conclude that $f(N')=f'(N')$.

Remark 4.3. 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 $(\mathcal{J},T)$-extensions is indeed an opposite Galois category with fundamental functor $\mathrm{Emb}_M(-,\Gamma)$. Unfortunately, the fact that in general pushouts of $(\mathcal{J},T)$-extensions do not exist (see Remark 3.10) implies that this is not the case, as Galois categories require the existence of finite limits. This is not unlike the case of field extensions, where one has to consider the more general category of *étale algebras* over a field exactly for this reason.

As a further analogy, to prove the existence of pushouts we restricted ourselves to pure maps of $(\mathcal{J},T)$-extensions, which happen to be epimorphisms in this category. Epimorphisms in the category of field extensions are purely inseparable extensions, and indeed the pushout along such an extension is a field.

One may wonder if allowing modules whose $\mathcal{J}$-torsion embeds in some power of T could provide a suitable generalization. But this turns out not to be the case. Consider for example the case of $R=\mathbb{Z}$ and $\mathcal{J}=2^\infty$, with T some power of $\mathbb{Z}/2\mathbb{Z}$. If the map $f:\mathbb{Z}\hookrightarrow\frac{1}{2}\mathbb{Z}$ admitted a pushout with itself, then the difference of the two images of 1 via the two canonical maps would be a torsion point. But if $T=(\mathbb{Z}/2\mathbb{Z})^n$ for some $n\geqslant 2$, then there would be many non-equivalent choices for this torsion point, which implies the non-canonicity of this "pushout" object.

All of this suggests that the rigidity of $(\mathcal{J},T)$-extensions due to having a fixed structural map into T is too restrictive to see them as a Galois category. It is then natural to refine our question as follows: does the category of $(\mathcal{J},T)$-extensions embed as the subcategory of connected objects of some Galois category?

In order to show that a certain class of $(\mathcal{J},T)$-extensions is normal, we need to introduce a new concept.

Definition 4.4. We say that an R-module T is *admissible* if every injective R-module homomorphism $T\hookrightarrow T$ is surjective.

Proposition 4.5. *Assume that T is admissible. Then every saturated $(\mathcal{J},T)$-extension is normal.*

Remark 4.6. Notice that the converse is not true: Example 4.2 (1) shows that a normal $(\mathcal{J},T)$-extension need not be saturated.

Proof of Proposition 4.5. Let $i:M\hookrightarrow N$ be a saturated $(\mathcal{J},T)$-extension of a T-pointed R-module M. Let $f,g:N\hookrightarrow\Gamma$ be injective $\mathcal{J}$-maps with

$f \circ i = g \circ i = \iota$. Let $n \in N$ and $t = f(n) - g(n)$. By Lemma 2.21 we have $t \in \Gamma[\mathcal{J}]$. Since N is saturated and g is injective, the restriction of g to $N[\mathcal{J}] \cong T$ is an injective map $T \to T$, and thus it is surjective by hypothesis. So we have $t \in g(N)$, thus $f(n) = g(n) + t \in g(N)$. This means that $f(N) \subseteq g(N)$, and in the same way one can show that $g(N) \subseteq f(N)$. Thus $f(N) = g(N)$, so N is normal. □

Remark 4.7. The condition on injective endomorphisms of T being surjective is necessary for the normality of saturated extensions. Indeed, let $R = \mathbb{Z}$, let $\mathcal{J} = \infty$ be the ideal filter introduced in Example 2.2 and let and $T = (\mathbb{Q}/\mathbb{Z})^{\mathbb{N}}$. In other words, T is the set of functions $\mathbb{N} \to \mathbb{Q}/\mathbb{Z}$ with abelian group operations defined point-wise.

Consider the T-pointed R-module $M = 0$ and the saturated $(\mathcal{J}, T)$-extension $N = T$, with structural map given by the identity of T. The map

$$\begin{array}{rccc} \varphi: & (\mathbb{Q}/\mathbb{Z})^{\mathbb{N}} & \longrightarrow & (\mathbb{Q}/\mathbb{Z})^{\mathbb{N}} \\ & f & \longmapsto & g : n \mapsto \begin{cases} 0 & \text{if } n = 0 \\ f(n-1) & \text{otherwise} \end{cases} \end{array}$$

is injective, but it is not surjective. Therefore T does not satisfy the conditions of Proposition 4.5. The existence of this map also shows directly that N is not a normal $(\mathcal{J}, T)$-extension of M.

Corollary 4.8. *Assume that T is an admissible R-module such that every injective homomorphism $T \to T$ is surjective. Then every maximal $(\mathcal{J}, T)$-extension is normal.*

4.2. A fundamental exact sequence.

Proposition 4.9. *Let (N, i, t) be a normal $(\mathcal{J}, T)$-extension of (M, s) and let $\mathrm{Aut}_{M+N[\mathcal{J}]}(N)$ 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 $N[\mathcal{J}]$. Then the restriction map along $\mathfrak{s}_N : N \to \mathfrak{sat}(N)$*

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

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 $(\mathcal{J}, T)$-extensions of $\mathfrak{sat}(M)$, which is necessarily also a map of $(\mathcal{J}, T)$-extensions of M. Since $\mathfrak{sat}(s)$ is an isomorphism, also $f \circ \sigma$ is a map of $(\mathcal{J}, T)$-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 identity on $N[\mathcal{J}]$.

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

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

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

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

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

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

so by the universal property of the pushout there is a map of $(\mathcal{J},T)$-extensions

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

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 4.10. *Let (N,i,t) be a $(\mathcal{J},T)$-extension of (M,s). Then the map*

$$\begin{array}{rccc} \varphi: & \mathrm{Aut}_{M+N[\mathcal{J}]}(N) & \longrightarrow & \mathrm{Hom}\left(\dfrac{N}{i(M)+N[\mathcal{J}]}, N[\mathcal{J}]\right) \\ & \sigma & \longmapsto & (\varphi_\sigma : [n] \mapsto \sigma(n)-n) \end{array}$$

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 $N/(i(M)+N[\mathcal{J}])$. Notice that for any $\sigma \in \mathrm{Aut}_{M+N[\mathcal{J}]}(N)$ we have $\sigma(n)-n \in N[\mathcal{J}]$ by Lemma 2.21, and φ_σ is a homomorphism of R-modules. To see that $\sigma \mapsto \varphi_\sigma$ is a group homomorphism, let $\sigma' \in \mathrm{Aut}_{M+N[\mathcal{J}]}(N)$. Then, since σ is the identity on $N[\mathcal{J}]$ and $\sigma'(n)-n \in N[\mathcal{J}]$, 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 $\varphi_\sigma(n)=0$ then σ must be the identity.

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

$$\begin{array}{rccc} \sigma_h: & N & \longrightarrow & N \\ & n & \longmapsto & n+h([n]) \end{array}$$

which is clearly the identity on $i(M) + N[\mathcal{J}]$, 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 4.11. *Let (N, i, t) be a normal $(\mathcal{J}, T)$-extension of M. Denoting for simplicity by $\mathfrak{sat}(M)$ the image of $\mathfrak{sat}(M)$ inside $\mathfrak{sat}(N)$ we have*

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

Proof. By Proposition 4.9 we have

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

and by Proposition 4.10 we have

$$\mathrm{Aut}_{M+N[\mathcal{J}]}(N) \cong \mathrm{Hom}\left(\frac{N}{i(M) + N[\mathcal{J}]}, N[\mathcal{J}]\right)\,.$$

The claim then follows from the fact that

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

To see that the two quotients are isomorphic, consider the map $N \to \mathfrak{sat}(N)/\mathfrak{sat}(M)$ given by $n \mapsto \mathfrak{s}_N(n) + \mathfrak{sat}(M)$: its kernel is $\mathfrak{s}_N^{-1}(\mathfrak{sat}(M)) = i(M) + N[\mathcal{J}]$ and it is surjective because $\mathfrak{sat}(N)$ is generated by the images of N and T. □

Remark 4.12. Let N be a $(\mathcal{J}, T)$-extension of M and let $\sigma \in \mathrm{Aut}_M(N)$. The restriction of σ to $N[\mathcal{J}]$ is an element of $\mathrm{Aut}_{M[\mathcal{J}]}(N[\mathcal{J}])$. Indeed, the image of a $\mathcal{J}$-torsion element under a map of $(\mathcal{J}, T)$-extensions is again a $\mathcal{J}$-torsion element; since this is true for both σ and σ^{-1} we can conclude that $\sigma|_{N[\mathcal{J}]} : N[\mathcal{J}] \to N[\mathcal{J}]$ is an automorphism.

Lemma 4.13. *If (N, i, t) is a normal $(\mathcal{J}, T)$-extension of (M, s), the restriction map*

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

is surjective.

Proof. Let $\sigma \in \mathrm{Aut}_{M[\mathcal{J}]}(N[\mathcal{J}])$. Notice that $(N, i, t \circ \sigma)$ is also a $(\mathcal{J}, T)$-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 $(\mathcal{J}, T)$-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 [8], [13] and [22].

Theorem 4.14. *Let M be a T-pointed R-module and let N be a normal $(\mathcal{J},T)$-extension of M. Then there is an exact sequence of groups*

$$1 \longrightarrow \mathrm{Hom}\left(\frac{\mathfrak{sat}(N)}{\mathfrak{sat}(M)}, N[\mathcal{J}]\right) \longrightarrow \mathrm{Aut}_M(N) \longrightarrow \mathrm{Aut}_{M[\mathcal{J}]}(N[\mathcal{J}]) \longrightarrow 1 \tag{4.1}$$

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

Proof. By Lemma 4.13 the map $\mathrm{Aut}_M(N) \to \mathrm{Aut}_{M[\mathcal{J}]}(N[\mathcal{J}])$ is surjective and its kernel is $\mathrm{Aut}_{i(M)+N[\mathcal{J}]}(N)$ by definition. By Proposition 4.9 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 4.11 we get the desired exact sequence.

The fact that $\mathrm{Aut}_{M[\mathcal{J}]}(N[\mathcal{J}])$ acts on $\mathrm{Aut}_{i(M)+N[\mathcal{J}]}(N)$ 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 $\mathrm{Hom}(\mathfrak{sat}(N)/\mathfrak{sat}(M), N[\mathcal{J}])$ this action is indeed the composition of maps, similarly to [22, Proposition 3.12]. □

Remark 4.15. It is worth remarking how Theorem 4.14 relates to other known results.

(1) Let $R = \mathbb{Z}$, let $\mathcal{J} = \infty$ be the ideal filter introduced in Example 2.2 and let $T = (\mathbb{Q}/\mathbb{Z})^s$ for some positive integer s. It is clear that any $(\mathcal{J},T)$-extension N of a T-pointed R-module M is an *s-extension* in the sense of [22, Definition 3.1].

In this setting, Theorem 4.14 is a generalization of [22, Proposition 3.12].

(2) Assume that R is a Dedekind domain. As defined in [8, Definition 3.5], a *Steinitz ideal* of R is a closed ideal of the profinite completion $\widehat{R} = \varprojlim_I R/I$. We can identify a Steinitz ideal $\mathcal{I}$ with the ideal filter $\mathcal{J}$ consisting of those ideals I of R such that $I\widehat{R} \supseteq \mathcal{I}$. Since R is a Dedekind domain, this ideal filter $\mathcal{J}$ is product-closed and hence complete by Proposition 2.12.

This shows that the theory developed in [8, Chapter 3] can be framed in terms of $(\mathcal{J},T)$-extensions as defined in this paper. In particular, the exact sequence of Theorem 4.14 is a generalization of those that appear on [8, p. 92] with $M = W$ and $N = E$.

(3) An exact sequence analogous to this one also appears in [13, Lemma 3.7 and Corollaries 3.12, 3.17 and 3.18].

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 $\mathcal{J}$ be a complete ideal filter of R, let $T := G(K_s)[\mathcal{J}]$ and let $\Gamma := (M :_{G(K_s)} \mathcal{J})$.

We are interested in studying the field extension $K(\Gamma)$ of K, that is the fixed field of the subgroup of $\mathrm{Gal}(K_s \,|\, K)$ that acts trivially on Γ, and we want to do so using the theory of $(\mathcal{J}, T)$-extensions introduced in the previous section. In order to proceed this way it is necessary that $T = G(K_s)[\mathcal{J}]$ be $\mathcal{J}$-injective. Moreover, we need to assume that T is admissible, that is that every injective R-module endomorphism of T is surjective: indeed in this case, by Proposition 4.5, Γ is a saturated, and thus normal, $(\mathcal{J}, T)$-extension of M.

Example 5.1. Let $K = \mathbb{Q}$, let A be an abelian variety of dimension d over $\mathbb{Q}$, let $R = \mathbb{Z}$ viewed as a subring of $\mathrm{End}_{\mathbb{Q}}(A)$ and assume that A has a non-torsion rational point $a \in A(\mathbb{Q})$. Let $M = \mathbb{Z}a$ be the subgroup of $A(\mathbb{Q})$ consisting of all integer multiples of a.

(1) Let p be a prime and let $\mathcal{J} = p^\infty$ be the usual ideal filter of $\mathbb{Z}$. We then have

$$T = A(\overline{\mathbb{Q}})[p^\infty] \cong (\mathbb{Z}[p^{-1}]/\mathbb{Z})^{2d}$$

In particular, T is p^∞-injective because it is p-divisible (Example 2.26). Moreover, every injective group homomorphism $T \hookrightarrow T$ is surjective, because every proper subgroup of the Prüfer group $\mathbb{Z}[p^{-1}]/\mathbb{Z}$ is finite cyclic.

Since T is not only p-divisible, but also divisible, the short exact sequence

$$0 \longrightarrow T \longrightarrow \Gamma \longrightarrow \Gamma/T \longrightarrow 0$$

splits, so that $\Gamma \cong T \oplus \Gamma/T$.

Moreover, we have

$$\begin{aligned}\Gamma/T &= \left(M :_{A(\overline{\mathbb{Q}})} p^\infty\right)/A(\overline{\mathbb{Q}})[p^\infty] \\ &= \left\{b \in A(\overline{\mathbb{Q}}) \mid p^n b \in \mathbb{Z}a \text{ for some } n \in \mathbb{N}\right\}/A(\overline{\mathbb{Q}})[p^\infty] \\ &\cong \mathbb{Z}[p^{-1}].\end{aligned}$$

So we can conclude that there is a non-canonical isomorphism $\Gamma \cong \mathbb{Z}[p^{-1}] \oplus (\mathbb{Z}[p^{-1}]/\mathbb{Z})^{2d}$.

(2) $\mathcal{J} = \infty$ be the other ideal filter of $\mathbb{Z}$ introduced in Example 2.2 usual ideal filter of $\mathbb{Z}$; in other words, ∞ is the collection of all non-zero ideals of $\mathbb{Z}$. We then have

$$T = A(\overline{\mathbb{Q}})[\infty] \cong (\mathbb{Q}/\mathbb{Z})^{2d}$$

In particular, T is ∞-injective because it is divisible (Example 2.26) and every injective homomorphism $T \hookrightarrow T$ is surjective, since $\mathbb{Q}/\mathbb{Z} \cong \bigoplus_{p \text{ prime}}(\mathbb{Z}[p^{-1}]/\mathbb{Z})$. As in (1), we can conclude that there is a non-canonical isomorphism $\Gamma \cong Q \oplus (\mathbb{Q}/\mathbb{Z})^{2d}$.

The following Lemma gives us a sufficient condition for T to be $\mathcal{J}$-injective.

Lemma 5.2. *Let K be a field with separable closure K_s, let A be an abelian variety over K, let $R \subseteq \mathrm{End}_K(A)$ be a subring, let $\mathcal{J}$ be a complete ideal filter on R and let $T = A(K_s)[\mathcal{J}]$.*

If A is simple and R is a maximal order in $\mathrm{End}_{K_s}(A) \otimes \mathbb{Q}$, then T is $\mathcal{J}$-injective.

Proof. We first show that T is divisible. Since R is a maximal order in the division algebra $\mathrm{End}_{K_s}(A) \otimes \mathbb{Q}$, every non-zero element r of R is surjective on $A(K_s)$. Then if an element $u \in A(K_s)$ is such that $ru = t \in T$ and $I \in \mathcal{J}$ is such that $It = 0$, 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 $\widetilde{f} : R \to T$. By [18, Theorem 22.7] there is a right *fractional* ideal L of R such that $IL = R$ and $1 \in LI \subseteq R$. In particular there are non-zero elements $b_1, \dots, b_n \in L$ and $a_1, \dots, a_n \in I$ such that $\sum_{i=1}^n b_i a_i = 1$, and since T is divisible there are $x_1, \dots, x_n \in T$ 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 $\widetilde{f}(r) = r \sum_{i=1}^n (b_i a_i) x_i$ for every $r \in R$.

Since T is injective, it is also $\mathcal{J}$-injective (see Remark 2.23). □

Let us assume that $T = G(K_s)[\mathcal{J}]$ is $\mathcal{J}$-injective and admissible, so that Γ is a normal $(\mathcal{J}, T)$-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 (4.1) via the Galois action on the points of G, and we obtain the following commutative diagram of groups with exact rows:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathrm{Gal}(K(\Gamma) \mid K(T)) & \longrightarrow & \mathrm{Gal}(K(\Gamma) \mid K) & \longrightarrow & \mathrm{Gal}(K(T) \mid K) & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \kappa} & & \downarrow{\scriptstyle \rho} & & \downarrow{\scriptstyle \tau} & & \\ 1 & \longrightarrow & \mathrm{Hom}\left(\frac{\Gamma}{\mathfrak{sat}(M)}, T\right) & \longrightarrow & \mathrm{Aut}_M(\Gamma) & \longrightarrow & \mathrm{Aut}_{M[\mathcal{J}]}(T) & \longrightarrow & 1 \end{array} \tag{5.1}$$

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

Remark 5.3. The commutative diagram (5.1) generalizes those that can be found in [8, p. 92] for the case of elliptic curves with complex multiplication and in [22, p. 11] for the non-CM case.

Definition 5.4. 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.

Example 5.5. Using the setting and notation of Example 5.1, we have:

(1) For $\mathcal{J} = \infty$, after choosing an isomorphism $\Gamma \cong Q \oplus (\mathbb{Q}/\mathbb{Z})^{2d}$, the bottom row of the diagram (5.1) becomes

$$1 \longrightarrow \mathrm{Hom}\Big(\mathbb{Q}/\mathbb{Z}, (\mathbb{Q}/\mathbb{Z})^{2d}\Big) \longrightarrow \mathrm{Aut}_{(\mathbb{Z},0)}\Big(\mathbb{Q} \oplus (\mathbb{Q}/\mathbb{Z})^{2d}\Big) \longrightarrow \mathrm{Aut}\Big((\mathbb{Q}/\mathbb{Z})^{2d}\Big) \longrightarrow 1 \tag{5.2}$$

By standard properties of limits and colimits (for example following [22, Example 2.2]), we have

$$\mathrm{Hom}\left(\mathbb{Q}/\mathbb{Z}, (\mathbb{Q}/\mathbb{Z})^{2d}\right) \cong \widehat{\mathbb{Z}}^{2d} \quad \text{and} \quad \mathrm{Aut}\left((\mathbb{Q}/\mathbb{Z})^{2d}\right) \cong \mathrm{GL}_{2d}(\widehat{\mathbb{Z}})\,.$$

Moreover, we may identify the group $\mathrm{Aut}_{(\mathbb{Z},0)}\left(\mathbb{Q} \oplus (\mathbb{Q}/\mathbb{Z})^{2d}\right)$ with the subgroup of $\mathrm{GL}_{1+2d}(\widehat{\mathbb{Z}})$

$$G := \begin{pmatrix} 1 & 0 \\ \widehat{\mathbb{Z}}^{2d} & \mathrm{GL}_{2d}(\widehat{\mathbb{Z}}) \end{pmatrix}$$

that is, the group of matrices whose first row is zero except for the first entry, which is 1. To see this, consider the injective ring homomorphism

$$\varphi : \mathrm{End}\left(\mathbb{Q} \oplus (\mathbb{Q}/\mathbb{Z})^{2d}\right) \longrightarrow \begin{pmatrix} \mathrm{End}\,(\mathbb{Q}) & \mathrm{Hom}\left((\mathbb{Q}/\mathbb{Z})^{2d}, \mathbb{Q}\right) \\ \mathrm{Hom}\left(\mathbb{Q}, (\mathbb{Q}/\mathbb{Z})^{2d}\right) & \mathrm{End}\left((\mathbb{Q}/\mathbb{Z})^{2d}\right) \end{pmatrix} =: \mathcal{R}$$

which maps $(x, y) \mapsto (a(x) + b(y), c(x) + d(y))$ into its components

$$a \in \mathrm{End}\,(\mathbb{Q})\,, \qquad b \in \mathrm{Hom}\left((\mathbb{Q}/\mathbb{Z})^{2d}, \mathbb{Q}\right)$$
$$c \in \mathrm{Hom}\left(\mathbb{Q}, (\mathbb{Q}/\mathbb{Z})^{2d}\right), \quad d \in \mathrm{End}\left((\mathbb{Q}/\mathbb{Z})^{2d}\right).$$

Since $\mathbb{Q}$ is torsion-free and $(\mathbb{Q}/\mathbb{Z})^{2d}$ is torsion we have

$$\mathrm{Hom}((\mathbb{Q}/\mathbb{Z})^{2d}, \mathbb{Q}) = 0,$$

and using the same properties of limits mentioned above we can rewrite the ring $\mathcal{R}$ as

$$\mathcal{R} = \begin{pmatrix} \mathrm{End}(\mathbb{Q}) & 0 \\ \widehat{\mathbb{Z}}^{2d} & \mathrm{Mat}_{2d\times 2d}(\widehat{\mathbb{Z}}) \end{pmatrix}.$$

Consider now the restriction of φ to $\mathrm{Aut}_{(\mathbb{Z},0)}(\mathbb{Q}\oplus(\mathbb{Q}/\mathbb{Z})^{2d})$ as a group homomorphism $\varphi^{\times}$. Since these automorphism are the identity on $(\mathbb{Z},0)$, they must be the identity on $(\mathbb{Q},0)$ as well. Moreover, since they are invertible, their restriction to $(0,(\mathbb{Q}/\mathbb{Z})^{2d})$, which is well-defined because $\mathrm{Hom}((\mathbb{Q}/\mathbb{Z})^{2d},\mathbb{Q})=0$, must be invertible as well. this means that the image of $\varphi^{\times}$ coincides with G.

In conclusion, we can rewrite the exact sequence (5.2) as

$$1 \longrightarrow \widehat{\mathbb{Z}}^{2d} \longrightarrow \begin{pmatrix} 1 & 0 \\ \widehat{\mathbb{Z}}^{2d} & \mathrm{GL}_{2d}(\widehat{\mathbb{Z}}) \end{pmatrix} \longrightarrow \mathrm{GL}_{2d}(\widehat{\mathbb{Z}}) \longrightarrow 1$$

with maps sending a vector $v\in\widehat{\mathbb{Z}}^{2d}$ to

$$\begin{pmatrix} 1 & 0 \\ v & \mathrm{Id}_{2d} \end{pmatrix}$$

and a matrix

$$\begin{pmatrix} 1 & 0 \\ v & M \end{pmatrix} \in \begin{pmatrix} 1 & 0 \\ \widehat{\mathbb{Z}}^{2d} & \mathrm{GL}_{2d}(\widehat{\mathbb{Z}}) \end{pmatrix}$$

to $M\,\mathrm{GL}_{2d}(\widehat{\mathbb{Z}})$.

(2) For p prime and $\mathcal{J}=p^{\infty}$, after choosing an isomorphism $\Gamma\cong\mathbb{Z}[p^{-1}]\oplus(\mathbb{Z}[p^{-1}]/\mathbb{Z})^{2d}$, the bottom row of the commutative diagram (5.1) above becomes

$$\begin{aligned} 1 \longrightarrow\ & \mathrm{Hom}\Big(\mathbb{Z}[p^{-1}]/\mathbb{Z},(\mathbb{Z}[p^{-1}]/\mathbb{Z})^{2d}\Big) \\ & \longrightarrow \mathrm{Aut}_{(\mathbb{Z},0)}\Big(\mathbb{Z}[p^{-1}]\oplus(\mathbb{Z}[p^{-1}]/\mathbb{Z})^{2d}\Big) \longrightarrow \mathrm{Aut}\Big((\mathbb{Z}[p^{-1}]/\mathbb{Z})^{2d}\Big) \longrightarrow 1 \end{aligned}$$

which, reasoning as in (1), we can rewrite as

$$1 \longrightarrow \mathbb{Z}_p^{2d} \longrightarrow \begin{pmatrix} 1 & 0 \\ \mathbb{Z}_p^{2d} & \mathrm{GL}_{2d}(\mathbb{Z}_p) \end{pmatrix} \longrightarrow \mathrm{GL}_{2d}(\mathbb{Z}_p) \longrightarrow 1$$

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 5.6. *There is an exact sequence of abelian groups*

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

which can be rewritten as

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

Proof. By Lemma 2.21 for any $b \in \Gamma \cap G(K(T))$ we may define a map

$$\begin{array}{rccc} \varphi_b : & \mathrm{Im}(\tau) & \longrightarrow & T \\ & \sigma & \longmapsto & \sigma(b) - b \end{array}$$

which is a cocycle. It follows that the map

$$\begin{array}{rccc} \varphi : & \Gamma \cap G(K(T)) & \longrightarrow & H^1(\mathrm{Im}(\tau), T) \\ & b & \longmapsto & \varphi_b \end{array}$$

is a group homomorphism. Moreover its kernel is

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

so that we have an exact sequence

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

and restricting the second term to its intersection with Γ we get

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

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

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

Which proves the first part of the Theorem.

To prove that the two exact sequences in the statement of the Theorem are indeed the same, it is enough to rewrite $M + T = \mathfrak{sat}(M)$ and $G(K) + T = \mathfrak{sat}(G(K))$, and to notice that by 2.14(1)

$$\begin{aligned} \Gamma \cap \mathfrak{sat}(G(K)) &= \left(M :_{G(K_s)} \mathcal{J}\right) \cap \mathfrak{sat}(G(K)) \\ &= \left(\mathfrak{sat}(M) :_{\mathfrak{sat}(G(K))} \mathcal{J}\right) \end{aligned}$$

and that

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

This concludes the proof. □

The below Theorem 5.7 extends [22, Theorem 5.9] in two ways:

- Theorem 5.7 works for submodules over any subring of the endomorphism ring, and the module need not be torsion-free.
- Theorem 5.7 works for any ideal filter $\mathcal{J}$, while [22, Theorem 5.9] is only stated for the case $\mathcal{J} = \infty$.

Theorem 5.7. *Assume that the* $\mathrm{End}(T)$*-submodule of* $\mathrm{Hom}(\Gamma/\mathfrak{sat}(M), T)$ *generated by* $\mathrm{Im}(\kappa)$ *is finitely generated. If the following three conditions hold*

(1) *There is a positive integer* d *such that*

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

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

Remark 5.8. The integer d of Theorem 5.7(1) is called a *divisibility parameter* in [22], see [22, Definition 5.1].

Proof of Theorem 5.7. 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 $\ker(V) = \ker(\mathrm{Im}\,\kappa) \subseteq X[dn]$ by Theorem 5.6. Since V is finitely generated as an $\mathrm{End}(T)$-module, by Proposition 2.39 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 a $\mathbb{Z}[\mathrm{Im}(\tau)]$-module, we have

$$\begin{aligned}\mathrm{Im}(\kappa) &= \mathbb{Z}[\mathrm{Im}(\tau)] \cdot \mathrm{Im}(\kappa)\\ &\supseteq m \cdot \mathrm{End}(T) \cdot \mathrm{Im}(\kappa)\\ &= m \cdot V\\ &\supseteq dnm \cdot \mathrm{Hom}(X, T)\end{aligned}$$

and we conclude. □

5.2. Finite quotients. Keep for this section the setting of Section 5.1, namely:

K	a field
K_s	a separable closure of K
G	a commutative algebraic group over K
R	a subring of $\mathrm{End}_K G$
M	an R-submodule of $G(K)$
$\mathcal{J}$	a complete ideal filter of R
T	the R-module $G(K_s)[\mathcal{J}]$, assumed to be $\mathcal{J}$-injective and admissible
Γ	the R-module $(M :_{G(K_s)} \mathcal{J})$

Before applying the results of Section 5.1, it is worth discussing how we can use them to obtain bounds on the degree of the finite subextensions of $K(\Gamma) \mid K$.

For every $I \in \mathcal{J}$ let $\Gamma_I := (M :_{G(K_s)} I)$ and $T_I := G(K_s)[I]$. By definition, we have $\Gamma_I \subseteq \Gamma$. We are interested in studying the tower of field extensions

$$K(\Gamma_I) \mid K(T_I) \mid K$$

Notice that these extensions do not necessarily have finite degree.

Example 5.9. Let $G = \mathbb{G}_m$ be the multiplicative group over $K = \mathbb{Q}$, that is the algebraic group whose L-points are $\mathbb{G}_m(L) = L^\times$ for every field extension L of $\mathbb{Q}$. Let $R = \mathbb{Z}$ and $\mathcal{J} = 2^\infty$, defined as usual, and let $I = 2\mathbb{Z}$.

- Let M be the submodule of $\mathbb{Q}^\times$ defined by $M = \{3^z \mid z \in \mathbb{Z}\}$. Then Γ contains all 2-power roots of 3, so the degree of $\mathbb{Q}(\Gamma)$ over $\mathbb{Q}$ is infinite. On the other hand, it is easy to see that $\Gamma_I = \{\sqrt{3}^z \mid z \in \mathbb{Z}\}$, so that $\mathbb{Q}(\Gamma_I) = \mathbb{Q}(\sqrt{3})$ is a finite extension of $\mathbb{Q}$.
- Let $M = \mathbb{Q}^\times$. In this setting, the module Γ contains all 2-power roots of every rational number. The module Γ_I contains the square roots of every rational number, so clearly the field extension $\mathbb{Q}(\Gamma_I) \mid \mathbb{Q}$ cannot have finite degree.

Lemma 5.10. *The $(\mathcal{J}, T)$-extension Γ_I of M is normal.*

Proof. Let $f : \Gamma_I \hookrightarrow \Gamma$ be any injective $\mathcal{J}$-map such that the diagram

$$\begin{array}{ccc} \Gamma_I & \xhookrightarrow{f} & \Gamma \\ {\scriptstyle i}\uparrow & \nearrow_{\iota} & \\ M & & \end{array}$$

commutes. Let $x \in \Gamma_I$. Since $Ix \subseteq i(M)$ we must have $If(x) \subseteq \iota(M)$, which means that $f(x) \in \Gamma_I$ by definition of Γ_I as a submodule of Γ. This shows that $f(\Gamma_I) \subseteq \Gamma_I$.

To show the other inclusion, notice that since Γ is $\mathcal{J}$-injective, the map f can be extended to a $\mathcal{J}$-map $f' : \Gamma \to \Gamma$. Moreover, since $T = \Gamma[\mathcal{J}]$ is admissible, the restriction of f' to T is surjective. Consider now $t := x - f(x)$, which by the previous part is in Γ_I. By Lemma 2.21 we have $t \in \Gamma_I[\mathcal{J}] \subseteq \Gamma[\mathcal{J}]$. By the above discussion there is $u \in \Gamma[\mathcal{J}]$ such that $f'(u) = t$, and since f' is an isomorphism on $\Gamma[\mathcal{J}]$ we must have $u \in \Gamma_I$. Therefore

$$x = f(x) + f(u) = f(x + u) \in f(\Gamma_I).$$

This shows that $\Gamma_I \subseteq f(\Gamma_I)$, concluding the proof. □

By the same reasoning as in Section 5.1, we have a commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathrm{Gal}(K(\Gamma_I) \mid K(T_I)) & \longrightarrow & \mathrm{Gal}(K(\Gamma_I) \mid K) & \longrightarrow & \mathrm{Gal}(K(T_I) \mid K) & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \kappa_I} & & \downarrow{\scriptstyle \rho_I} & & \downarrow{\scriptstyle \tau_I} & & \\ 1 & \longrightarrow & \mathrm{Hom}\left(\frac{\mathfrak{sat}(\Gamma_I)}{\mathfrak{sat}(M)}, T\right) & \longrightarrow & \mathrm{Aut}_M(\Gamma_I) & \longrightarrow & \mathrm{Aut}_{M[\mathcal{J}]}(T_I) & \longrightarrow & 1 \end{array} \tag{5.3}$$

where the bottom row is exact by Proposition 4.14.

Consider now the tower of extensions

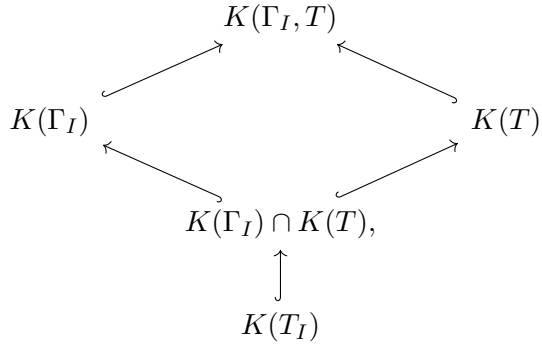
$$K(\mathfrak{sat}(\Gamma_I)) = K(\Gamma_I, T) \mid K(T) \mid K$$

Since $\mathfrak{sat}(\Gamma_I)$ is saturated and T is admissible, $\mathfrak{sat}(\Gamma_I)$ is a normal $(\mathcal{J}, T)$-extension of $\mathfrak{sat}(M)$. Thus by the same reasoning as above we have a commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathrm{Gal}(K(\Gamma_I, T) \mid K(T)) & \longrightarrow & \mathrm{Gal}(K(\Gamma_I, T) \mid K) & \longrightarrow & \mathrm{Gal}(K(T) \mid K) & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \kappa'_I} & & \downarrow{\scriptstyle \rho'_I} & & \downarrow{\scriptstyle \tau} & & \\ 1 & \longrightarrow & \mathrm{Hom}\left(\frac{\mathfrak{sat}(\Gamma_I)}{\mathfrak{sat}(M)}, T\right) & \longrightarrow & \mathrm{Aut}_M(\mathfrak{sat}(\Gamma_I)) & \longrightarrow & \mathrm{Aut}_{M[\mathcal{J}]}(T) & \longrightarrow & 1 \end{array} \tag{5.4}$$

where once again the bottom row is exact by Proposition 4.14.

Since the maps κ_I and κ'_I arise from the same Galois action, and considering the lattice of field extensions



we see that the κ_I' factors via κ_I, that is that there is an injective homomorphism $h : \mathrm{Gal}(K(\Gamma_I, T) \mid K(T)) \to \mathrm{Gal}(K(\Gamma_I) \mid K(T_I))$ such that $\kappa_I \circ h = \kappa_I'$, that is

$$\mathrm{Gal}(K(\Gamma_I, T) \mid K(T)) \hookrightarrow \mathrm{Gal}(K(\Gamma_I) \mid K(T_I)) \hookrightarrow \mathrm{Hom}\left(\frac{\mathfrak{sat}(\Gamma_I)}{\mathfrak{sat}(M)}, T\right) \tag{5.5}$$

In other words, $\mathrm{Gal}(K(\Gamma_I, T) \mid K(T))$ is a subgroup of $\mathrm{Gal}(K(\Gamma_I) \mid K(T_I))$ when viewing both as subgroups of $\mathrm{Hom}\left(\frac{\mathfrak{sat}(\Gamma_I)}{\mathfrak{sat}(M)}, T\right)$ via their Kummer representations.

Consider now the tower of Galois extensions $K(\Gamma) \mid K(\Gamma_I, T) \mid K(T)$. The Galois quotient map extends to a commutative diagram with Kummer representations as vertical maps

$$\begin{array}{ccc} \mathrm{Gal}(K(\Gamma) \mid K(T)) & \twoheadrightarrow & \mathrm{Gal}(K(\Gamma_I, T) \mid K(T)) \\ \downarrow{\scriptstyle \kappa} & & \downarrow{\scriptstyle \kappa_I'} \\ \mathrm{Hom}\left(\frac{\Gamma}{\mathfrak{sat}(M)}, T\right) & \xrightarrow{\quad q \quad} & \mathrm{Hom}\left(\frac{\mathfrak{sat}(\Gamma_I)}{\mathfrak{sat}(M)}, T\right) \end{array} \tag{5.6}$$

The map q above maps a homomorphism $f : \frac{\Gamma}{\mathfrak{sat}(M)} \to T$ to its restriction to $\frac{\mathfrak{sat}(\Gamma_I)}{\mathfrak{sat}(M)}$, and it is surjective.

Lemma 5.11. *The homomorphism*

$$\begin{array}{rccc} q : \mathrm{Hom}\left(\dfrac{\Gamma}{\mathfrak{sat}(M)}, T\right) & \longrightarrow & \mathrm{Hom}\left(\dfrac{\mathfrak{sat}(\Gamma_I)}{\mathfrak{sat}(M)}, T\right) \\ f & \longmapsto & f|_{\mathfrak{sat}(\Gamma_I)/\mathfrak{sat}(M)} \end{array}$$

is surjective.

Proof. Let $g : \frac{\mathfrak{sat}(\Gamma_I)}{\mathfrak{sat}(M)} \to T$ be a group homomorphism and lift it to a homomorphism $\bar{g} : \mathfrak{sat}(\Gamma_I) \to T$. Since T is torsion, $\bar{g}$ is a $\mathcal{J}$-map. Since T is $\mathcal{J}$-injective, and $i : \mathfrak{sat}(\Gamma_I) \hookrightarrow \Gamma$ is a $\mathcal{J}$-extension, there is a $\mathcal{J}$-map $\overline{h} : \Gamma \to T$ such that $\overline{h} \circ i = \bar{g}$. In particular $\overline{h}(\mathfrak{sat}(M)) = 0$, so that it factors through the quotient as a map $h : \frac{\Gamma}{\mathfrak{sat}(M)} \to T$ whose restriction to $\frac{\mathfrak{sat}(\Gamma_I)}{\mathfrak{sat}(M)}$ coincides with g. This concludes the proof. □

Putting it all together, we have shown the following result.

Corollary 5.12 (of Theorem 5.7)**.** *Assume that the conditions of Theorem 5.7 hold for some positive integers d, n, and m. Then for every $I \in \mathcal{J}$ we have*

$$\kappa_I'(\mathrm{Gal}(K(\Gamma_I) \mid K(T_I))) \supseteq dnm \cdot \mathrm{Hom}(\mathfrak{sat}(\Gamma_I)/\mathfrak{sat}(M), T)\,.$$

Proof. This follows directly from the chain of inclusions (5.5) and the existence of the commutative diagram with surjective rows (5.6). □

Example 5.13. As in Example 5.1, let $K = \mathbb{Q}$, let A be an abelian variety of dimension d over $\mathbb{Q}$ and let $R = \mathbb{Z}$ viewed as a subring of $\mathrm{End}_{\mathbb{Q}}(A)$ and assume that A has a non-torsion rational point $a \in A(\mathbb{Q})$. Let $M = \mathbb{Z}a$ be the subgroup of $A(\mathbb{Q})$ consisting of all integer multiples of A.

(1) Assume that $\mathcal{J} = p^\infty$ for some prime p. If $I = p^n\mathbb{Z}$ for some positive integer n, then

$$\begin{aligned}\mathrm{Hom}\left(\frac{\mathfrak{sat}(\Gamma_I)}{\mathfrak{sat}(M)}, T\right) &\cong \mathrm{Hom}\left(\frac{p^{-n}\mathbb{Z}}{\mathbb{Z}}, \left(\frac{\mathbb{Z}[p^{-1}]}{\mathbb{Z}}\right)^{2d}\right)\\ &\cong \mathrm{Hom}\left(\frac{p^{-n}\mathbb{Z}}{\mathbb{Z}}, \left(\frac{p^{-n}\mathbb{Z}}{\mathbb{Z}}\right)^{2d}\right)\\ &\cong \left(\frac{\mathbb{Z}}{p^n\mathbb{Z}}\right)^{2d}\end{aligned}$$

(2) Assume that $\mathcal{J} = \infty$. If $I = n\mathbb{Z}$ for some positive integer n, then

$$\begin{aligned}\mathrm{Hom}\left(\frac{\mathfrak{sat}(\Gamma_I)}{\mathfrak{sat}(M)}, T\right) &\cong \mathrm{Hom}\left(\frac{\frac{1}{n}\mathbb{Z}}{\mathbb{Z}}, \left(\frac{\mathbb{Q}}{\mathbb{Z}}\right)^{2d}\right)\\ &\cong \mathrm{Hom}\left(\frac{\frac{1}{n}\mathbb{Z}}{\mathbb{Z}}, \left(\frac{\frac{1}{n}\mathbb{Z}}{\mathbb{Z}}\right)^{2d}\right)\\ &\cong \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^{2d}\end{aligned}$$

5.3. 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 $T = E(\overline{K})[\mathcal{J}]$ is contained in $E(\overline{K})_{\mathrm{tors}}$: indeed, if $x \in T$ then there is $I \in \mathcal{J}$ 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 5.14. *The R-module $E(\overline{K})[\mathcal{J}]$ is $\mathcal{J}$-injective.*

Proof. By [9, Proposition 5.1] the R-module $E(\overline{K})_{\mathrm{tors}}$ is injective, thus in particular $\mathcal{J}$-injective. Since $E(\overline{K})[\mathcal{J}] = (0 :_{E(\overline{K})_{\mathrm{tors}}} \mathcal{J})$ it follows from Lemma 2.35 that $E(\overline{K})[\mathcal{J}]$ is $\mathcal{J}$-injective. □

Proposition 5.15. *The R-module $E(\overline{K})[\mathcal{J}]$ is admissible.*

Proof. Since $E(\overline{K})_{\mathrm{tors}}$ is injective by [9, Proposition 5.1], every injective map $f : E(\overline{K})[\mathcal{J}] \to E(\overline{K})[\mathcal{J}]$ extends to an injective homomorphism g

of $E(\overline{K})_{\mathrm{tors}} \cong (\mathbb{Q}/\mathbb{Z})^2$. In particular, g is surjective as explained in Example 5.1.

Let now $x \in E(\overline{K})_{\mathrm{tors}}$ be such that $g(x) \in E(\overline{K})[\mathcal{J}]$. This means that $Ig(x) = 0$ for some $I \in \mathcal{J}$. But since g is injective, this means that $Ix = 0$, that is $x \in E(\overline{K})[\mathcal{J}]$. This shows that f is surjective, and therefore $E(\overline{K})[\mathcal{J}]$ is admissible. □

Remark 5.16. Although not necessary for our applications, it is interesting to notice that in this setting Γ is a maximal $(\mathcal{J}, T)$-extension of M.

Indeed since $E(\overline{K})_{\mathrm{tors}}$ is injective by [9, Proposition 5.1], the short exact sequence of R-modules

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

splits. Moreover $E(\overline{K})/E(\overline{K})_{\mathrm{tors}}$ is a torsion-free divisible module over the commutative integral domain R, so it is injective. It follows that $E(\overline{K})$ is direct sum of injective modules over a Noetherian ring, so it is injective. As in the above Proposition we may conclude that Γ is $\mathcal{J}$-injective, thus it is a maximal $(\mathcal{J}, T)$-extension of M.

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

Remark 5.17. Notice that in case $\mathcal{J} = \infty$ we have $T = E(\overline{K})_{\mathrm{tors}}$ and

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

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

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

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 5.18. *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*

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

Proof. First of all notice that $\mathfrak{sat}(M) = M + T$ and $\mathfrak{sat}(E(K)) = E(K) + T$ seen as subgroups of $E(\overline{K})$. We conclude thanks to the considerations of [22, Section 6.1]. □

Proposition 5.19. *There exists an effectively computable positive integer n such that*

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

Proof. This follows from [22, Proposition 6.3] and [22, Corollary 6.8] in the non-CM case and from [22, Proposition 6.12] in the CM case. □

Proposition 5.20. *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. In the case $R = \mathbb{Z}$, using the terminology of [22], the Proposition claims the existence of an *adelic bound* for the torsion representation, see [22, Definition 6.2]. The result then follows from [22, Corollary 6.8].

In the CM case, the result follows from [10, Theorem 1.5]. □

Theorem 5.21. *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. Moreover, for every $I \in \mathcal{J}$ the index of $\mathrm{Im}(\kappa_I)$ in $\mathrm{Hom}(\mathfrak{sat}(\Gamma_I)/\mathfrak{sat}(M), T)$ divides c.*

Proof. This is a direct consequence of Theorem 5.7 and the three propositions above. The last statement follows from Corollary 5.12. □

Example 5.22. Let $\mathcal{J} = \infty$ and assume that $a \in E(K)$ is a non-torsion point and let $M = \mathbb{Z}a$. For any positive integer n let $I = n\mathbb{Z}$ and denote by K_n the field $K\big((M :_{E(\overline{K})} I)\big)$.

Combining Theorem 5.21 with Example 5.13 it follows that there is a constant c such that for any positive integer n:

$$\frac{n^2}{\Big[K_n : K\big(E(\overline{K})[n]\big)\Big]} \qquad \text{divides} \qquad c$$

This can easily be generalized to groups M of any rank, thus obtaining [22, Theorem 1.2].

Remark 5.23. Since Theorem 5.7 is stated in a fairly general form, one might wonder if it can be applied to obtain a version of Theorem 5.21 for higher-dimensional abelian varieties.

Let $\mathcal{A}$ be an abelian variety over a number field K. Proving such a result would require the following steps:

- Proving that $T = \mathcal{A}[\infty]$ is an injective module over $R = \mathrm{End}_K(\mathcal{A})$, so that it is $\mathcal{J}$-injective for any complete ideal filter $\mathcal{J}$. We already know that this is the case, for example, for simple abelian varieties whose endomorphism ring is a maximal order in a division algebra, see Lemma 5.2.

  In case such a statement is too general to hold true for the considered class of abelian varieties, one could restrict to suitable subrings of R and specific ideal filters $\mathcal{J}$ to achieve similar results.
- Prove that T is admissible. This is unlikely to be true for any choice of ring R, but it holds true at least in case R is an integral domain, following Proposition 5.15. In other cases, while not true in general, it could still hold that T is admissible at least for some choices of ideal filter $\mathcal{J}$.
- Use the Mordell–Weil theorem to compute the group structure of the K-points of $\mathcal{A}$ and find a divisibility parameter for $\mathcal{A}$ (see Remark 5.8).
- Finding a bound for the integer n of Theorem 5.7, which seems like a harder problem to tackle. But an application of Sah's Lemma (see for example [22, Proposition 6.3]) shows that such a bound can be obtained by finding explicit homotheties in $\mathrm{Im}(\tau)$, and one can hope to reduce to finding homotheties in the images of the ℓ-adic representations, as done in [11, 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 [6].
- Finding a bound for the integer m of Theorem 5.7. The results of [19, Théorème 1.5(2)] provide some effective bounds that can help achieve this goal.

References

[1] F. ANDERSON & K. FULLER, *Rings and Categories of Modules*, Graduate Texts in Mathematics, vol. 13, Springer, 2012.

[2] R. BAER, "Abelian groups that are direct summands of every containing abelian group", *Bull. Am. Math. Soc.* **46** (1940), no. 10, p. 800-806.

[3] C. W. CURTIS & I. REINER, *Representation Theory of Finite Groups and Associative Algebras*, Pure and Applied Mathematics, vol. 11, John Wiley & Sons, 1962, xiv+685 pages.

[4] B. ECKMANN & A. SCHOPF, "Über injektive Moduln", *Arch. Math.* **4** (1953), no. 2, p. 75-78.

[5] I. FLEISCHER, "A new construction of the injective hull", *Can. Math. Bull.* **11** (1968), p. 19-21.

[6] A. Galateau & C. Martínez, "Homothéties explicites des représentations ℓ-adiques", *J. Théor. Nombres Bordeaux* **35** (2023), no. 2, p. 567-590.
[7] M. Hindry, "Autour d'une conjecture de Serge Lang", *Invent. Math.* **94** (1988), no. 3, p. 575-603.
[8] A. Javan Peykar, "Division points in arithmetic", PhD Thesis, Leiden University, 2021, https://hdl.handle.net/1887/138941.
[9] Jr. Lenstra, Hendrik W., "Complex multiplication structure of elliptic curves", *J. Number Theory* **56** (1996), no. 2, p. 227-241.
[10] D. Lombardo, "Galois representations attached to abelian varieties of CM type", *Bull. Soc. Math. Fr.* **145** (2017), no. 3, p. 469-501.
[11] D. Lombardo & S. Tronto, "Effective Kummer Theory for Elliptic Curves", *Int. Math. Res. Not.* **2022** (2022), no. 22, p. 17662-17712.
[12] W. J. Palenstijn, "Galois action on division points", Master's thesis, Leiden University, 2004, https://hdl.handle.net/1887/3597578.
[13] ———, "Radicals in arithmetic", PhD Thesis, Leiden University, 2014, https://hdl.handle.net/1887/25833.
[14] F. Perissinotto, "Kummer theory for abelian varieties", https://hdl.handle.net/10993/61819, 2024.
[15] A. Perucca & P. Sgobba, "Kummer theory for number fields and the reductions of algebraic numbers", *Int. J. Number Theory* **15** (2019), no. 8, p. 1617-1633.
[16] A. Perucca, P. Sgobba & S. Tronto, "Explicit Kummer theory for the rational numbers", *Int. J. Number Theory* **16** (2020), no. 10, p. 2213-2231.
[17] ———, "The degree of Kummer extensions of number fields", *Int. J. Number Theory* **17** (2021), no. 5, p. 1091-1110.
[18] I. Reiner, *Maximal orders*, London Mathematical Society Monographs, vol. 5, Academic Press Inc., 1975, xii+395 pages.
[19] G. Rémond & E. Gaudron, "Nouveaux théorèmes d'isogénies", preprint, 2020.
[20] K. A. Ribet, "Kummer theory on extensions of abelian varieties by tori", *Duke Math. J.* **46** (1979), p. 745-761.
[21] J.-P. Serre, "Propriétés galoisiennes des points d'ordre fini des courbes elliptiques", *Invent. Math.* **15** (1972), p. 259-331.
[22] S. Tronto, "Radical entanglement for elliptic curves", submitted for publication, 2020, https://arxiv.org/abs/2009.08298v1.

Sebastiano Tronto
E-mail: sebastiano@tronto.net
URL: https://sebastiano.tronto.net