Division in modules and Kummer theory

Sebastiano Tronto
sebastiano.tronto@uni.lu
University of Luxembourg / Universiteit Leiden

2022-02-22

Links

- These slides:
  https://sebastiano.tronto.net/research/division-groningen.pdf
- My paper *Division in modules and Kummer theory*:
  https://arxiv.org/abs/2111.14363
- Notes for a similar talk, part 1:
  https://sebastiano.tronto.net/research/notes-injectivity.pdf
- Notes for a similar talk, part 2:
  https://sebastiano.tronto.net/research/notes-division-modules.pdf

Kummer theory

Fix (just for the introduction):

- A number field K with algebraic closure $\overline{K}$
- An elliptic curve E over K
- A non-torsion point $\alpha \in E(K)$

(But one could take more generally a commutative algebraic group E and a finitely generated subgroup of $E(K)$)

Kummer theory

For $n \geq 1$ consider

$$n^{-1}\alpha := \{P \in E(\overline{K}) \mid nP = \alpha\}$$

and the extension of K generated by these points

$$K(n^{-1}\alpha)$$

which is Galois over K and abelian over $K(E[n])$

Kummer theory

Known results:

- Classical: $cn^2 \leq [K(n^{-1}\alpha) : K(E[n])] \leq n^2$ [Rib79]
- Effective $c = c(E, K, \alpha)$ in the non-CM case [LT21a]
- Explicit absolute c for $K = \mathbb{Q}$ [LT21b]
- CM case treated in [JP21]
- Other relevant papers: [Ber88, Hin88, JR10]

Groups (modules) of division points

Let $A = \langle \alpha \rangle$ and $n^{-1}A = \{P \in E(\overline{K}) \mid nP \in A\}$

- We need to study "algebraic" properties of $n^{-1}A$, in particular $\mathrm{Aut}_A(n^{-1}A)$
- No CM: consider $n^{-1}A$ an abelian group [Tro20]
- CM by $\mathcal{O}$: consider it an $\mathcal{O}$-module [JP21]

Goals

- Define "division modules" over any ring and determine certain properties of their automorphism groups
- Unify and generalize the results of [Tro20] and [JP21]
- Possibly extend to higher-dimensional abelian varieties

Division in modules

Fix a ring R (associative, with unit).

Definition

If I is a right ideal of R and $M \subseteq N$ are left R-modules, we call the R-submodule of N

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

the **I-division module of M in N**. For $M = 0$ we call

$$N[I] := (0 :_N I)$$

the **I-torsion submodule** of N.

Division in modules

Facts

- $(M :_N 0) = N$ *and* $(M :_N R) = M$
- *If* $M \subseteq M'$ *we have* $(M :_N I) \subseteq (M' :_N I)$
  - *In particular* $N[I] \subseteq (M :_N I)$ *for every* M
- *If* $I \subseteq I'$ *we have* $(M :_N I) \supseteq (M :_N I')$

But in general we want to work with **infinite unions** of division modules, like $\bigcup_{n \geq 1} n^{-1}A$.

Ideal filters

Definition

An **ideal filter** J on R is a set of right ideals such that:

1. If I and I' are in J, then $I \cap I' \in J$
2. If $I \in J$ and I' is a right ideal of R such that $I' \supseteq I$, then $I' \in J$

We let

$$(M :_N J) = \bigcup_{I \in J} (M :_N I) \qquad \text{and} \qquad N[J] = (0 :_N J)$$

Example

Let $R = \mathbb{Z}$

- $J = \langle (1), (2), (3), (4), (6), (12) \rangle$ is an ideal filter
- We have

$$(\mathbb{Z} :_{\mathbb{Q}} J) = \bigcup_{d \mid 12} \{q \in \mathbb{Q} \mid dq \in \mathbb{Z}\} =$$

$$= \mathbb{Z} \cup \frac{1}{2}\mathbb{Z} \cup \frac{1}{3}\mathbb{Z} \cup \frac{1}{4}\mathbb{Z} \cup \frac{1}{6}\mathbb{Z} \cup \frac{1}{12}\mathbb{Z} =$$

$$= \frac{1}{12}\mathbb{Z}$$

Ideal filters

Examples

- *Maximal ideal filter* $0 := \{$*all right ideals of* $R\}$
- *Minimal ideal filter* $1 := \{R\}$
- *Principal ideal filter: if* I *is a right ideal then*

$$\langle I \rangle := \{I' \subseteq R \text{ right ideal with } I \subseteq I'\}$$

is an ideal filter, and

$$(M :_N \langle I \rangle) = (M :_N I)$$

Ideal filters

Definition

An ideal filter J is called **complete** if $((M :_N J) :_N J) = (M :_N J)$ for every $M \subseteq N$.

Examples

- $p^\infty := \{I \subseteq R \mid I \supseteq p^n R \textit{ for some } n \in \mathbb{Z}_{\geq 0}\}$
- $\infty := \{I \subseteq R \mid I \supseteq nR \textit{ for some } n \in \mathbb{Z}_{\geq 1}\}$

Example (cont.)

Let $R = \mathbb{Z}$ and $J = \langle(12)\rangle$

- We have

$$(\mathbb{Z} :_{\mathbb{Q}} J) = \frac{1}{12}\mathbb{Z}$$

- J is **not** complete:

$$\left(\frac{1}{12}\mathbb{Z} :_{\mathbb{Q}} J\right) = \frac{1}{144}\mathbb{Z}$$

Divisible groups

Definition

An abelian group A is called **divisible** if for every $x \in A$ and $n \in \mathbb{Z} \setminus \{0\}$ there is $y \in A$ such that $ny = x$.

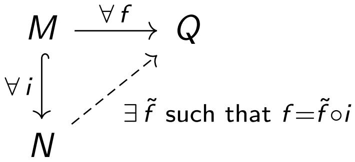
Examples:

- $\mathbb{Q}$, $\mathbb{Q}^n$, $\mathbb{Q}/\mathbb{Z}$...
- $\bigcup_{n \geq 1} n^{-1}A \cong \mathbb{Q}^{\mathrm{rk}_{\mathbb{Z}} A} \oplus (\mathbb{Q}/\mathbb{Z})^2$

Injective modules

Definition

A module Q over a ring R is called **injective** if every R-linear map to Q can be extended along injective maps:



Proposition

A $\mathbb{Z}$-module is injective if and only if it is divisible.

J-injective modules

Let J be a **complete** ideal filter

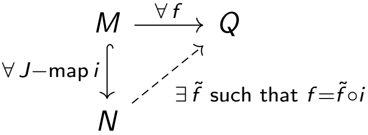
Definition

A map of left R-modules $f : M \to N$ is called a J-**map** if

$$(f(M) :_N J) = N$$

Definition

A left R-module Q is called J-**injective** if every R-linear map to Q can be extended along injective J-maps:



J-injectivity

Question

Is being J-injective equivalent to being injective in the category of J-maps?

Maybe. Tricky: are all monomorphisms injective J-maps?

J-injectivity

- Injective $\iff$ 0-injective (by definition)
- J-injective $\implies$ J'-injective for $J' \subseteq J$ (by definition)
- Baer's criterion (consider two-sided ideals in J)
- Assume R is an integral domain. Then

$$J = \{\text{all nonzero ideals}\}$$

  is an ideal filter and J-injective $\iff$ injective.
  But in general $M[J] \neq M = M[0]$.

Examples

Over $\mathbb{Z}$:

- Divisible $\iff$ injective $\iff$ ∞-injective
- p-divisible $\iff$ p^∞-injective
- $M[\infty] = M_{\text{tors}}$ and $M[p^\infty] = \bigcup_{n\geq 1} M[p^n]$

Injective hulls

Definition

A module N containing M is called an **essential extension** if for every submodule M' of M we have

$$M' \cap N = 0 \implies M' = 0$$

Definition

A module Ω containing M is called an **injective hull** of M if it is injective and an essential extension.

Injective hulls

- Ω is the largest essential extension of M
- Ω is the smallest injective module containing M
- Every module admits an injective hull, unique up to (non-unique) M-isomorphism

Compare with **algebraic closure**: largest algebraic extension and smallest algebraically closed extension

J-hulls

Let J be a **complete** ideal filter

Definition

A module Γ containing M is called a J-**hull** of M if it is J-injective and an essential extension.

Theorem

Every module admits a J-hull, unique up to isomorphism.

Idea: Take $\Gamma = (M :_\Omega J)$, where Ω is an injective hull.

Example: ∞

Let $R = \mathbb{Z}$ and $J = \infty$.
Let A be a finitely generated abelian group, write it as

$$\mathbb{Z}^r \oplus \bigoplus_{i=1}^{s} \mathbb{Z}/a_i\mathbb{Z}$$

with a_i dividing a_{i+1}. Then A J-hull for A is

$$\begin{array}{ccc} A & \hookrightarrow & \mathbb{Q}^r \oplus (\mathbb{Q}/\mathbb{Z})^s \\ (z, (t_i \bmod a_i)_i) & \mapsto & \left(\frac{z}{1}, \left(\frac{t_i}{a_i} \bmod \mathbb{Z}\right)_i\right) \end{array}$$

Example: p^∞

Let $R = \mathbb{Z}$ and $J = p^\infty$.
Let A be a finitely generated abelian group, write it as

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

with $p \nmid n$. Then A J-hull for A is

$$\begin{array}{ccc} A & \hookrightarrow & (\mathbb{Z}[p^{-1}])^r \oplus (\mathbb{Z}[p^{-1}]/\mathbb{Z})^s \oplus A[n] \\ (z, (t_i \bmod p^{e_i})_i, u) & \mapsto & \left(\frac{z}{1}, \left(\frac{t_i}{p^{e_i}} \bmod \mathbb{Z}\right)_i, u\right) \end{array}$$

Kummer theory

Let E be an elliptic curve over a number field K,
$R = \mathrm{End}_K(E)$, $J = \infty$ and M an R-submodule of $E(K)$.

The module

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

is a J-hull "with some extra torsion".

Question: How do we make $E(\overline{K})_{\mathrm{tors}}$ appear?

(J, T)-extensions

Let R be a ring and J a complete ideal filter.
Let T be a J-injective module with $T[J] = T$.

Definition

- A T-**pointed** R-**module** is a pair (M, s) with M a module and s an injective map $s : M[J] \hookrightarrow T$
- A (J, T)-**extension** of (M, s) is an injective J-map $f : (M, s) \hookrightarrow (N, t)$ compatible with s and t
- Maps of (J, T)-extensions $(N, t) \to (L, r)$ are the identity on M and compatible t and r

Galois theory of (J, T)-extensions

(J, T)-extensions of (M, φ) behave like field extensions:

- Maps are injective, surjective maps are isomorphisms
- Maximal (J, T)-extension Γ: a J-hull of $M +_s T$
- All (J, T)-extensions embed into Γ and one can define normal extensions

Open question: are (J, T)-extensions the connected objects of some Galois category?

A fundamental exact sequence

There is an exact sequence

$$1 \to \mathrm{Aut}_{M+_s T}(\Gamma) \to \mathrm{Aut}_M(\Gamma) \to \mathrm{Aut}_{M[J]}(T) \to 1$$

and $\mathrm{Aut}_{M+_s T}(\Gamma) \cong \mathrm{Hom}\left(\frac{\Gamma}{M+_s T}, T\right)$ is abelian.

Remark: $\mathrm{Aut}_M(\Gamma) = \{\text{Aut. of } R\text{-module, fixing } M\}$.

Kummer theory

Back to E/K, $M \subseteq E(K)$, $R = \mathrm{End}_K(E)$, $T = E(\overline{K})_{\mathrm{tors}}$.

A maximal (J, T)-extension of M is $\Gamma = \left(M :_{E(\overline{K})_{\mathrm{tors}}}\right)$

We have a "representation"

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

Thank you for your attention!

[Ber88] Daniel Bertrand.
Galois representations and transcendental numbers.
In *New advances in transcendence theory (Durham, 1986)*, pages 37–55. Cambridge University Press, Cambridge, 1988.

[Hin88] Marc Hindry.
Autour d'une conjecture de Serge Lang.
Inventiones Mathematicae, 94(3):575–603, 1988.

[JP21] Abtien Javan Peykar.
Division points in arithmetic.
PhD thesis, Leiden University, 2021.

[JR10] Rafe Jones and Jeremy Rouse.
Galois theory of iterated endomorphisms.
Proceedings of the London Mathematical Society, 100(3):763–794, 2010.

[LT21a] Davide Lombardo and Sebastiano Tronto.
Effective Kummer Theory for Elliptic Curves.
International Mathematics Research Notices, 08 2021.

[LT21b] Davide Lombardo and Sebastiano Tronto.
Some uniform bounds for elliptic curves over $\mathbb{Q}$.
arXiv preprint arXiv:2106.09950, 2021.
Submitted for publication.

[Rib79] Kenneth A. Ribet.
Kummer theory on extensions of abelian varieties by tori.
Duke Mathematical Journal, 46(4):745–761, 1979.

[Tro20] Sebastiano Tronto.
Radical entanglement for elliptic curves.
arXiv preprint arXiv:2009.08298, 2020.
Submitted for publication.