DIVISION IN MODULES

SEBASTIANO TRONTO

Abstract. Motivated by applications in algebraic number theory, in this talk we will explore "division modules" and highlight the connection between divisibility and injectivity over an arbitrary ring. More precisely, if M is a submodule of a left R-module N and I is a right ideal we call *I-division module* of M (inside N) the submoudle of N consisting of those elements x such that Ix is contained in M. Using this classical concept we will then provide a generalization of injective modules which, among other things, extends the definition of p-divisibility for abelian groups. We will see how classical results, such as Baer's criterion and the exitence of an injective hull, extend seamlessly to this more general setting.

1. Motivation from Kummer theory

Let A be a finitely generated subgroup of the multiplicative group $\mathbb{Q}^\times$, for example $A = \langle 2, 3\rangle$. Fixing an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ we may consider for every positive integer n the group *(beware the additive notation)*:

$$n^{-1}A := \left\{x \in \overline{\mathbb{Q}} \mid x^n \in A\right\}$$

which contains A as well as the n-th roots of unity of $\overline{\mathbb{Q}}$. Clearly we have $n^{-1}A \subseteq m^{-1}A$ whenever n divides m. Understanding certain properties of these groups, in particular their *relative* automorphisms $\mathrm{Aut}_A(n^{-1}A)$, is an important step for studying *Kummer extensions* of $\mathbb{Q}$, that are extensions of $\mathbb{Q}$ of the form $\mathbb{Q}(n^{-1}A)$. Of great importance is also the union of these groups

$$\Gamma_A := \bigcup_{n>0} n^{-1}A = \left\{x \in \overline{\mathbb{Q}} \mid x^n \in A \text{ for some } n > 0\right\}.$$

The group Γ_A is *divisible*, that is for every $x \in \Gamma_A$ and every positive integer n there is $y \in \Gamma_A$ such that $y^n = x$.

Let now E be an elliptic curve over some number field K, and fix an algebraic closure $\overline{K}$ of K and a subgroup $A \subseteq E(K)$. We may consider the groups

$$n^{-1}A := \left\{x \in E(\overline{K}) \mid nx \in A\right\}$$

which contain A and $E(\overline{K})[n]$, and the extensions of K of the form $K(n^{-1}A)$. We call this *Kummer theory for elliptic curves*, but nothing prevents us from stating the problem more generally for any commutative algebraic group E.

As it turns out, it is more convenient to take A to be a module over the ring $R = \mathrm{End}_K(E)$ (which for elliptic curves can only be $\mathbb{Z}$ or an order in a quadratic imaginary field) and to use the R-module structure of the groups $n^{-1}A$ to our advantage. We are thus led to investigating the properties of *division modules* over arbitrary rings.

As an "extra", we might be interested in considering only those groups $n^{-1}A$ where n is a power of some prime p. In this case the group $\Gamma_A^{(p)} = \bigcup_{k\geqslant 0}(p^k)^{-1}A$ is *p-divisible*, that is for every $x \in \Gamma_A^{(p)}$ there is $y \in \Gamma_A^{(p)}$ such that $py = x$.

2. Division in modules

Fix for this and the following sections a unitary ring R.

Definition 2.1. If $M \subseteq N$ are left R-modules and I is a right ideal of R, we call the R-submodule of N

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

the *I-division module of M (inside N).*

Remark 2.2. Notice that:

- $(M :_N (0)) = N$ and $(M :_N (1)) = M$
- If $M \subseteq M'$ then $(M :_N I) \subseteq (M' :_N I)$
- If $I' \supseteq I$ then $(M :_N I') \subseteq (M :_N I)$

In general we might want to work with (possibly infinite) unions of division modules. For example if $R = \mathbb{Z}$ we are interested in working with infinite unions such as $\bigcup_{n \geqslant 1} (M :_N (n))$. So it makes sense to give the following definition.

Definition 2.3. An *ideal filter* of R is a non-empty set J of right ideals of R such that:

(1) If $I, I' \in J$ then $I \cap I' \in J$ and
(2) If $I \in J$ and I' is a right ideal of R that contains I, then $I' \in J$.

If J is an ideal filter of R and $M \subseteq N$ are R-modules, we let

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

which we call the J-division module of M in N, and

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

which we call the J-torsion submodule of N.

Remark 2.4. For an ideal filter J:

- *Maximal ideal filter:* If $(0) \in J$ then J contains every right ideal of R. In this case we denote J by 0. For every $M \subseteq N$ we have $(M :_N 0) = N$.
- *Minimal ideal filter:* We denote $J = \{R\}$ by 1. For every $M \subseteq N$ we have $(M :_N 1) = M$.
- *Principal ideal filter:* If I is a right ideal of R we let $\langle I \rangle$ be the set of all right ideals of R containing I, which is an ideal filter. For every $M \subseteq N$ we have $(M :_N \langle I \rangle) = (M :_N I)$.

Example 2.5. Let $R = \mathbb{Z}$ and $J = \langle (12) \rangle = \{(1), (2), (3), (4), (6), (12)\}$. We have

$$(\mathbb{Z} :_{\mathbb{Q}} J) = \bigcup_{d \,|\, 12} \{q \in \mathbb{Q} \mid dq \in \mathbb{Z}\} = \mathbb{Z} \cup \frac{1}{2}\mathbb{Z} \cup \frac{1}{3}\mathbb{Z} \cup \frac{1}{4}\mathbb{Z} \cup \frac{1}{6}\mathbb{Z} \cup \frac{1}{12}\mathbb{Z} = \frac{1}{12}\mathbb{Z}\,.$$

Ideal filters allow us to consider the possibly infinite unions of division modules mentioned in the introduction. We would also like to have a way to distinguish those ideal filters that describe a complete iteration of the division process, unlike the example above. We propose two definitions that might capture this concept, and we show that, under certain condition, one is stronger than the other.

Definition 2.6. We call an ideal filter J of R:

- *Complete* if for every $M \subseteq N$ we have $((M :_N J) :_N J) = (M :_N J)$.
- *Product-closed* if for any $I, I' \in J$ we have $II' \in J$.

Proposition 2.7 ([1, Proposition 2.8])**.** *Let R be a ring and let J be a product-closed ideal filter of R. If for every $I \in J$ the left ideal RI is finitely generated, then J is complete. In particular, every product-closed ideal filter over a left-Noetherian ring is complete.*

Example 2.8. For any unitary ring R, there are two interesting examples: the ideal filter generated by the powers of a given prime number p

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

and the one generated by all non-zero integers

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

Notice that some power of p is equal to 0 in R (respectively $n = 0$ for some $n \in \mathbb{N}_{n>0}$) then p^∞ (resp. ∞) is simply the set of all two-sided ideals of R.

Remark 2.9. It is easy to check that the ideal filters introduced in Example 2.8 are both product-closed. If, for example, R is Noetherian, then they are also complete.

On the other hand, the ideal filter $J = \langle(12)\rangle$ of $R = \mathbb{Z}$ is not complete, since $((M :_N J) :_N J) = \frac{1}{144}\mathbb{Z} \neq (M :_N J)$.

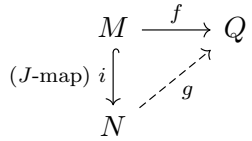
3. J-injective modules

Fix for this section a unitary ring R and a complete ideal filter J of R.

Definition 3.1. An R-module homomorphism $i : M \to N$ such that $(i(M) :_N J) = N$ is called a *J-map*.

We can finally give our definition of J-injective module. In words, one can say that an injective module is one that admits extensions of maps to it along any injective map. A J-injective module is one that admits extensions of maps into it along injective J-maps.

Definition 3.2. A left R-module Q is called J-injective if for every injective J-map $i : M \hookrightarrow N$ and every R-module homomorphism $f : M \to Q$ there exists a homomorphism $g : N \to Q$ such that $g \circ i = f$.



Remark 3.3. One may wonder if J-injective modules coincide with the injective objects in some category, for example the subcategory of J-maps between R-modules. This is at the moment an open question; the tricky part (that I was not able to solve so far) is determining that monomorphisms are in this category: are there monomorphisms that are not injective?

Remark 3.4.

- If $J = 0$ the definition of J-injective module coincides with that of injective module, because any injective homomorphism is a 0-map.
- If $J' \subseteq J$ then a J-injective module is also J'-injective, because every J'-map is also a J-map.

The following Proposition is an analogue of the well-known Baer's criterion in the classical case of injective modules, and the proof is almost identical to the classical case.

Proposition 3.5 ([1, Proposition 2.20])**.** *A left R-module Q is J-injective if and only if for every two-sided ideal $I \in J$ and every R-module homomorphism $f : I \to Q$ there is an R-module homomorphism $g : R \to Q$ that extends f.*

Remark 3.6. Let $J = 0$ be the maximal ideal filter of R and assume that $J' = J \setminus \{(0)\}$ is an ideal filter; this amounts to say that no two non-zero ideals of R have trivial intersection, which holds for example when R is an integral domain.

Using Proposition 3.5 one can easily show that an R-module Q is J-injective if and only if it is J'-injective. Indeed, one implication holds, as remarked above, because $J \supseteq J'$, and for the other it is enough to notice that the only map $0 \to Q$ can always be extended to the zero map on R.

One advantage of using J' instead of J is that the J'-torsion submodule may be different from $M[0] = M$. For example over $\mathbb{Z}$ we have $J' = \infty$ and $M[\infty] = M_{\text{tors}}$, the torsion subgroup.

Example 3.7. For modules over $\mathbb{Z}$:

- Divisible (as an abelian group) $\iff$ injective $\iff$ ∞-injective
- p-divisible (as an abelian group) $\iff$ p^∞-injective

See the appendix for proofs.

Example 3.8. Let M be an abelian group, let p be a prime and let $J = p^\infty$ be the ideal filter of $\mathbb{Z}$ introduced in Example 2.8. Then the localization $M[p^{-1}]$ is a J-injective $\mathbb{Z}$-module. Indeed if $i : N \hookrightarrow P$ is an injective J-map and $f : N \to M[p^{-1}]$ is any homomorphism then for every $x \in P$ there is $k \in \mathbb{N}$ such that $p^k x \in N$, 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 $g \circ i = f$.

4. Injective hulls

Definition 4.1. A map of R-modules $i : M \hookrightarrow N$ is called an *essential extension* if for every nonzero submodule P of N we have $P \cap i(M) \neq 0$.

It is a well-known fact of commutative algebra that every R-module M admits an injective hull $\iota : M \hookrightarrow \Gamma$, which is an essential extension such that Γ is injective. Such an extension, which is unique up to a not-necessarily-unique isomorphism that is the identity on M, may be as well characterized by either of the following two properties:

(1) It is the largest essential extension of M, that is to say if $i : M \hookrightarrow N$ is an essential extension then there is an (injective) R-module homomorphism $j : N \hookrightarrow \Gamma$ such that $\iota \circ i = j$ (the injectivity of j follows from the injectivity of ι and the fact that $i : M \hookrightarrow N$ is an essential extension).
(2) It is the smallest injective extension of M, that is to say if $i : M \hookrightarrow N$ is an injective R-module homomorphism and N is injective, then there is an *injective* R-module homomorphism $j : \Gamma \hookrightarrow N$ such that $j \circ \iota = i$ (the existence of a map $\Gamma \to N$ that commutes with i follows from the injectivity of N, but the fact that this map is injective does not).

As an example, the standard map $\mathbb{Z}^n \hookrightarrow \mathbb{Q}^n$ is an injective hull of the $\mathbb{Z}$-module $\mathbb{Z}^n$.

We can draw an interesting parallel between the J-hull of an R-module M and the algebraic closure $\overline{k}$ of a field k. Indeed $\overline{k}$ is at the same time the smallest *algebraically closed* extension and the largest *algebraic* extension of k. Similarly to J-hulls, an algebraic closure is unique up to a not-necessarily-unique isomorphism that fixes the base field.

There is an analogue construction for J-injectivity.

Definition 4.2. Let J be a complete ideal filter of R and let M be a left R-module. An injective J-map $\iota : M \hookrightarrow \Gamma$ is called a *J-hull* of M if it is an essential extension and Γ is J-injective.

The following theorem is not a replacement for the classical one, since it relies on it.

Theorem 4.3. *Every left R-module M admits a J-hull, which is unique up to a not-necessarily-unique isomorphism that is the identity on M.*

Sketch of proof. Let $\iota : M \hookrightarrow \Omega$ be an injective hull of M and let $\Gamma := (\iota(M) :_\Omega J)$. One can show that ι maps M into Γ and $\iota : M \hookrightarrow \Gamma$ is indeed a J-hull of M, and that for any other J-hull $\iota' : M \hookrightarrow \Gamma'$ there is an isomorphism $j : \Gamma \xrightarrow{\sim} \Gamma'$ such that $j \circ \iota = \iota'$. □

Example 4.4. Let M be an abelian group, let p be a prime and let $J = p^\infty$ be the ideal filter of $\mathbb{Z}$ introduced in Example 2.8. Write M as

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

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

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

and

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

Then $\iota : M \to \Gamma$ is a J-hull. To see this it is enough to show that $f : \mathbb{Z}^r \hookrightarrow (\mathbb{Z}[p^{-1}])^r$ and $g_i : \mathbb{Z}/p^{e_i}\mathbb{Z} \hookrightarrow \mathbb{Z}[p^{-1}]/\mathbb{Z}$ for every $i = 1, \dots, k$ are J-hulls, and that $M[n]$ is J-injective, being trivially an essential extension of itself. The assertions about f and $M[n]$ follow from Example 3.8, noticing that multiplication by p is an automorphism of $M[n]$ and that $\mathbb{Z}^r \hookrightarrow (\mathbb{Z}[p^{-1}])^r$ is an essential extension and a J-map.

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

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

Appendix A. Divisible and injectivity for $\mathbb{Z}$-modules

Definition A.1. An abelian group A is called *divisible* if for every $x \in A$ and every positive integer n there is $y \in A$ such that $ny = x$.

Proposition A.2. *A $\mathbb{Z}$-module is injective if and only if it is divisible as an abelian group.*

Proof. Let A be an abelian group and assume that it is injective as a $\mathbb{Z}$-module. Let $x \in A$ and $n \in \mathbb{Z} \setminus \{0\}$. Consider the inclusion $i : n\mathbb{Z} \hookrightarrow \mathbb{Z}$ and the map $f : n\mathbb{Z} \to A$ which sends n to x. Then since A is injective f extends to a map $g : \mathbb{Z} \to A$ which sends n to x, so letting $y = g(1)$ we have $ny = x$, as required.

Assume now that A is divisible and let $j : M \hookrightarrow N$ be an injective homomorphism of abelian groups and $f : M \to A$ any homomorphism. In order to extend f to a map $g : N \to A$ we will use Zorn's Lemma. Let S be the set of pairs (N', φ) with N' a sugroup

of N containing M and φ a homomorphism $N' \to A$ that extends f. The set S admits a partial order

$$(N', \varphi) \leqslant (N'', \psi) \iff N' \subseteq N'' \text{ and } \psi|_{N'} = \varphi$$

Every chain in S has an upper bound. Namely, if $C \subseteq S$ is a chain, i.e. a totally ordered subset of S, then we can take $\mathcal{N}'$ to be the union of all N' for $(N', \varphi) \in C$ and we let

$$\begin{array}{rccl} \Phi : \mathcal{N}' & \to & & A \\ x & \mapsto & \varphi(x), \text{ if there is any } (N', \varphi) \in C \text{ with } x \in N' & \end{array}$$

which is well-defined because C is totally ordered (which means that if x belongs to N' and to N'' for $(N', \varphi) \in C$ and $(N'', \psi) \in C$, then either $(N', \varphi) \leqslant (N''\psi)$ or $(N'', \psi) \leqslant (N', \psi)$, and in any case φ and ψ are compatible on x).

By Zorn's lemma there is then a maximal element $(N', \varphi) \in S$, and we want to show that $N' = N$, so that f extends to the whole N. Assume that $N' \neq N$ and let $x \in N \setminus N'$; if we manage to extend φ to $\varphi_+ : N' + \langle x \rangle \to A$ this will yield a contradiction with the maximality of (N', φ), and thus we would be able to conclude that indeed $N' = N$.

If $\langle x \rangle \cap N' = 0$, we may simply define $\varphi_+(x) = 0$. Otherwise $\langle x \rangle \cap N'$ contains some $nx \neq 0$ for some positive integer n which we may assume minimal with respect to this property. Since A is divisible there is $y \in A$ such that $ny = \varphi(nx)$, and one easily checks that defining φ_+ as $\varphi_+(x) = y$ is compatible with φ. As explained above, this concludes the proof. □

Definition A.3. Let p be a prime. An abelian group A is called *p-divisible* if for every $x \in A$ there is $y \in A$ such that $py = x$.

Proposition A.4. *A $\mathbb{Z}$-module is p^∞-injective if and only if it is p-divisible as an abelian group.*

Proof. Let A be an abelian group and assume that it is p^∞-injective as a $\mathbb{Z}$-module. Let $x \in A$ and consider the inclusion $i : p\mathbb{Z} \hookrightarrow \mathbb{Z}$ and the map $f : p\mathbb{Z} \to A$ which sends p to x. Then since A is p^∞-injective and i is a p^∞-map, f extends to a map $g : \mathbb{Z} \to A$ which sends p to x, so letting $y = g(1)$ we have $py = x$, as required.

Assume now that A is p-divisible and let $j : M \hookrightarrow N$ be an injective p^∞-map and $f : M \to A$ any homomorphism. as in the proof of Proposition A.2 we want to extend f to a map $g : N \to A$ using Zorn's Lemma. Proceding as before we may assume that $\varphi : N' \to A$ extends f to some $N' \subsetneq N$, take $x \in N \setminus N'$ ans show that we can extend φ to $\varphi_+ : N' + \langle x \rangle \to A$.

If $\langle x \rangle \cap N' = 0$ we may once again let $\varphi_+(x) = 0$. Otherwise $\langle x \rangle \cap N'$ contains some $nx \neq 0$ for n minimal. We claim that n is a power of p: indeed, write it as $dm = n$ for some positive integers d and m with $p \nmid d$. Since $mx \in N$ and j is a J-map we have $p^k mx \in M \subseteq N'$. It follows that $mx = \gcd(d, p^k)mx \in N'$, but we assumed n minimal so $d = 1$ and n must be a power of p, say p^c. Now since A is p-divisible there must be $y \in A$ such that $p^c y = \varphi(p^c x)$, and we just have to let $\varphi_+(x) = y$. □

References

[1] Tronto, S. Division in modules and Kummer theory. *arXiv preprint arXiv:2111.14363* (2021). Submitted for publication.

Email address: sebastiano.tronto@uni.lu