Internship Report

Formalization of ideals in commutative algebra

Nazila Sharifi Amina

Remy Seassau

September 2021

Summary

We would first like to thank Mr. Pierre-Yves Strub for offering us this opportunity. This internship was entirely organized by him and were are both very grateful to have been able do it with him. We (Nazila Sharifi Amina and Remy Seassau) conducted this internship jointly with Mr. Strub at Ecole Polytechnique's Computer Science Laboratory, LIX. We discussed this internship after the conclusion of our CSE203 class on logic and formalization which was taught in part by Mr. Strub. We decided to work on formalizing some mathematics that would be necessary to one of Mr. Strub's larger projects.

The work we had decided undertake would be done using the Coq Proof Assistant, a tool for formalization that we had discovered during the CSE203 class. It would deal with a branch of mathematics called commutative algebra. In order to prepare us for the task at hand, we were first instructed with finishing a Coq online school and reading a mathematics textbook. This process would take most of the first half of the internship.

We decided to operate using an online format. When we could, we would meet in person every few days to talk about the project and where it was heading. These meetings were the main anchor of our activities, with our work being done around them. When we weren't in meetings, we would work alone or in a pair on our tasks. Indeed, we had a general idea from the beginning of what we would build towards and our frequent meetings served to set intermediate tasks that we could accomplish to get closer to our goal.

These intermediate tasks would consist in either defining some mathematical structure or proving some lemmas about the previously defined structures. We would first do this in a LaTeX file maintained by Mr. Strub (this served the purpose of allowing us to write proofs and definitions "on paper") before formalizing in Coq what we had previously written.

This internship started on the 16th of July and ended on the 26th of August. During this time participants of this internship would work from Ecole Polytechnique's campus, Iran and the south of France before coming back to have a final meeting in person where we concluded the internship. We would once again like to extend our thanks to those that made this internship possible and specifically to Mr. Strub for accompanying us throughout the project.

Contents

1 Description of the Institution

1.1 Name and history

This internship was held at LIX ("Laboratoire d'Informatique de l'X"), known in English as "The Computer Science Laboratory of École Polytechnique". LIX is a mixed research unit, gathering teams from the École polytechnique, member of Institut Polytechnique de Paris and the National Center for Scientific Research (CNRS). It is also partnered with the Inria Saclay Ile de France center.

LIX was created in 1988 and soon after became a mixed research unit in 1989. The institution moved to a new location next to the Ecole Polytechnique campus in 2012. It was around this time that the Inria Saclay center moved into the building as well.

Figure 1: Inside of the Turing building, where we would meet in person.

With the evolution of the Plateau de Saclay, LIX has been increasingly involved in the development of initiatives based on the plateau. It is thus very active within the emerging scientific and technological initiatives near Ecole Polytechnique's campus.

1.2 LIX's Activity

LIX has been at the forefront of mathematics and computer science since it's foundation. Still a leader in its fields in the academic world, LIX has developed strong industry ties with French

companies such as Thalès and Dassault Aviation and continues to expand its list of collaborators with international companies such as Cisco or Microsoft Research.

LIX counts about 120 researchers, 50% of who are permanent staff. This research effort is divided into 13 teams, each focusing on its own area of expertise. LIX as a whole can be said to specialize in three main areas of research:

- algorithms, combinatorics and models;
- distributed systems and security;
- symbolic calculation and proofs.

Tying in with École Polytechnique's long history of mathematics, LIX tends to emphasize it's interactions with mathematics. Indeed, three of the 13 teams work directly on computer mathematics (combinatoric models, algebraic models, complex system optimization) and most research teams are heavily involved with mathematics in various ways: cryptography, data science, number theory, geometric computing, proof automation...

LIX's members are strongly involved in teaching at all programs at École Polytechnique. LIX also collaborates with master's programs across the Paris region and has contracts with public bodies (Ministry of Higher Education, Research and Innovation, INRIA etc.) and international organizations.

1.3 Why LIX?

LIX was a very attractive opportunity for us as students of École Polytechnique. With a strong link to the school, it was particularly suited to allowing us to explore a potential future research environment (whether for computer science projects, our bachelor thesis or even our master's). It would also allow us to interact with some of our professors outside of the context of a classroom

and within the context of a research team. This immersion within a polytechnique lab would help us tailor our path through education to better fit our careers and desires.

2 Internship activities and position

2.1 Work conditions and functions

The internship had a hybrid setting, where we had a few in-person meetings and did the majority of the work in an online format. The reason for the hybrid setting was mostly geographical issues since we weren't always in Paris at the same time over the duration of the summer. We met every two or three days during the week to do some trouble shooting and to discuss the next tasks to be done.

We used the version control software "Git" to share the project files between us and we would update it regularly so that everyone would have access to the latest version as early as possible. We also had direct access to our supervisor for quick contact and trouble-shooting through the messaging app Signal.

We spend the first three weeks of the internship learning more about the Mathematical Component library in Coq and doing exercises to be more fluent in order to use it for the project. Afterwards we followed a list of mathematical statements, proofs and definitions that we needed to formalize. This list would keep growing during the length of the internship, with a final objective being the coercion of ideals in a commutative ring to a semi-ring.

The main objective of the internship project was thus to formalize the algebraic concept of Ideals. Using our file with mathematical definitions and lemmas as a guide, we were able to formalize Ideals within a commutative ring in Coq. The path we followed was quite straightforward: prove some lemmas mathematically ("on paper", if you will) then transcribe them into Coq.

We thus started by defining ideals and expanded our project by adding more and more structures: ideals generated by sets, sum of ideals, product of ideals, ... Every time we defined

a new structure we had access to new propositions and lemmas that we could prove: "the intersection of a family of ideals is an ideal", "the sum of two ideals is the ideal generated by their union", etc.

2.2 Task examples

In order to start the formalization of Ideals within a commutative ring, we began by defining it by its properties. Every ideal contains zero, the sum of two members of the ideal is also in the ideal, and the multiplication of a member of an ideal with another non-member is in the ideal (left multiplication).

```
Section Ideal.
Context (R : comRingType).

Definition is_ideal (p : pred R) :=
  [/\ p 0
    , forall x y, p x -> p y -> p (x + y)
    & forall x y, p y -> p (x * y)].

Record ideals := Ideal {
  ideal :> pred R; _ : is_ideal ideal
}.

Lemma is_idealS (p : ideals) : is_ideal p.
Proof. by case: p. Qed.
```

Figure 2: Definition of an ideal and lemma stating that an ideal is an ideal in Coq

From the definition of an ideal we deduce that the intersection of families of ideals is also an ideal. Using this we defined the ideal generated by a set and we proved that it is in fact an ideal. Mathematically speaking, we would write this as follows:

Let X be a subset of R. The *ideal generated by* X, written $\langle X \rangle$, is defined as:

$$\langle X \rangle = \bigcap \{\mathfrak{a} \in \mathfrak{I} \mid X \subseteq \mathfrak{a}\}.$$

We proved the lemma that a member of a set is inside the ideal generated by the set. We

formalized the concept of a principal ideal. We defined the sum of two ideals. We proved that the sum of two ideals generated by two sets, is equivalent to the ideal generated by the union of the sets.

For any subsets X and Y of R, we have:

$$\langle X \rangle + \langle Y \rangle = \langle X \cup Y \rangle.$$

Let $\mathfrak{a}$ and $\mathfrak{b}$ be two ideals of R. Then, the product of $\mathfrak{a}$ and $\mathfrak{b}$, written $\mathfrak{a} \cdot \mathfrak{b}$ or $\mathfrak{ab}$, is defined as:

$$\mathfrak{ab} = \left\{ \sum_{i<n} a_i b_i \;\middle|\; n \in \mathbb{N}, a_0, \ldots, a_{n-1} \in \mathfrak{a}, b_0, \ldots, b_{n-1} \in \mathfrak{b} \right\}.$$

Also for any subsets X and Y of R, we have:

$$\langle X \rangle \langle Y \rangle = \langle X \otimes Y \rangle$$

where $X \otimes Y = \{xy \mid x \in X, y \in Y\}$.

```
Definition is_idealM_r (p q : pred R) : pred R :=
  fun x =>
    decide (
      exists2 s : seq (R * R), forall y, y \in s -> y.1 \in p /\ y.2 \in q &
      x = \sum_(y <- s) y.1 * y.2).
```

Figure 3: Definition of multiplication of two ideals in Coq

We would then expand with further definitions and lemmas with the final objective showing that ideals with our definition of addition and multiplication follows the properties of a commutative semi-ring.

3 Assessment of the Internship

3.1 Educational value of the internship

Due to the short length of the internship, we spent a relatively long amount of time getting our knowledge of the topic to a sufficient level. Indeed, we needed to familiarize ourselves with the techniques that would allow us to use the Coq proof assistant to suit our needs. The first half of our internship was largely devoted to learning.

One of the main sources of knowledge was the previously mentioned Coq Winter School[5]. This week-long course focused on the SSReflect proof language and a mathematics library called MathComp (Mathematical Components). Following the directions of our internship supervisor, we were specifically looking at the lesson on algebra as we intended on formalizing algebraic objects. The course was divided in 7 lessons, with each lesson constituting of a lecture and an exercise session. As we were not following this course live, we relied on the material as a support to learn. Once done, we had covered the basic arithmetic, big operators (such as $\sum$) and the definition of algebraic objects.

In regards to the implementation of algebraic objects, we felt it was necessary to go further than what was instructed by the online course. Therefore we read a paper on the implementation of mathematical structures in Coq[2]. This exercise was particularly enriching as it constituted in reading and understanding a full academic paper. Finally, to further bolster our understanding of the MathComp library, we would complement our other learnings with a book[3] containing the MathComp documentation.

During the preliminary phase of the internship we also focused on the mathematical aspect of our project. Indeed, although we had briefly studied group theory during our fist year we lacked a sufficiently strong basis to properly work on commutative algebra. Since our project

dealt with ideals in the context of a commutative algebra, we read the beginning of a textbook[4] about commutative algebra in order to ensure our comprehension of the project and its goals.

3.2 Career influence of the internship

Due to this internship being quite short (relative to graduate level internships for example), we were not able to cover much ground in terms of advancing the project. This means that although we were able to get some experience in formal proofs and the use of Coq for formalizing mathematical objects, we did not acquire enough experience to build an expertise that would be beneficial for our careers.

There are however some less direct benefits to our future professional lives that we have been able to glean from this internship. For example, the Coq proof assistant is written in a language called Ocaml. This language is known as a functional programming language and it shares a large amount of syntax and predicates with Coq. This internship thus gave us some time to internalize some of the logic behind the use of functional programming languages. As Computer Science majors, this is a major advantage as it is inevitable that we encounter functional programming sooner or later.

Another benefit that was brought by this internship was the opportunity to try and delve into a specific field of computer science. Generally, we only get a few experiences with very specific fields before having to decide on what master's to pursue (computer science projects, bachelor thesis, ...). Having the opportunity to try formal proofs in a more involved way allows us to have a firmer grasp on what this specific field of computer science and mathematics contains. Hence, we will be able to better orient ourselves in the future.

3.3 Relation to classes

The programming language used to formalize the internship project is called Coq. Coq is a programming language used to formalize mathematical theorems and proofs. We had initially encountered Coq in our "Logics and Proofs" course in our second year.

Logic and Proofs (CSE 203) was an introduction to logic. Its goal was to familiarize students with formal methods for representing mathematical statements and reasoning about them. It encompassed propositional calculus, first-order logic, and deduction systems, as well as related technologies (e.g. Coq, the language we used as a proof assistant) for building mechanized proofs.

The final project of the course was about regular expressions. We started to define what languages and regular languages were and proceeded to construct theorems and prove them. The final project of the course gave us a glimpse into how to formalize concepts step by step. Thanks to that, we had an easier time adapting to formalize more complicated mathematical concepts for the internship.

This internship acted as a continuation of the CSE203 course. We learnt deeper and more fundamental concepts, getting a firmer grasp on the functioning of the Coq language and its use. The topics covered were also outside of the scope of our course, but were somewhat linked to some material that we had covered in one of our math courses (MAA104). Hence, we spent some time reviewing the mathematics necessary to our project.

4 Conclusion

4.1 Conclusions derived from the internship

Although our internship was quite short, the experience left quite an impression on the both of us. We were both interested by the subject covered and were delighted to work in an engaging union between mathematics and computer science. The transition between what we had seen in our classes and the practical applications we were working on made the internship fit extremely well within our academic track.

Spending the beginning of the internship completely focused on learning allowed us to get a good grasp of the subject at hand and made for a very smooth transition into work. Although we were constantly learning along the way, the studying we started with was crucial as without it we would have been quite lost.

The work itself was quite enjoyable. Using frequent coordination meetings, we always knew what we had to do and were only left with finding out how to do it. Our tasks often resembled exercises and were quite fun to work on.

Finally, working with algebraic and mathematical structures reinforced our general knowledge of the basic structures of mathematics. An example of this would quite literally be the definition of the real numbers[1]. The project also allowed us to further our knowledge about ideals and explore some commutative algebra.

4.2 General observations

The online format that we opted for during most of the internship (an online call every two or three days and communication by text for any intermediate questions) was quite well suited for this project. This may be hard to generalize to other projects but the mathematical aspect of

having lemmas to prove made splitting work into tasks quite easy. The work was also quite fun as it required some thinking in order to solve the (literal) problems we were faced with.

On a more personal level, this internship made us appreciate how much easier it is to work when we enjoy the tasks at hand. Even without in-person meetings (that we all agreed were more enjoyable than the online calls) and while working separately we were quite happy.

Finally, this internship taught us how a computer science research project is structured. Indeed, our project was part of a much larger work and would serve only as an elementary brick in a much larger foundation. Seeing how our supervisor constructed our internship in such a way that we were able to contribute to a greater project was quite humbling and for that we are very grateful.

References

[1] Norbert A'Campo. *A natural construction for the real numbers*. 2003. arXiv: math/0301015 [math.GN].

[2] François Garillot et al. "Packaging Mathematical Structures". In: *Theorem Proving in Higher Order Logics*. Ed. by Stefan Berghofer et al. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 327–342. ISBN: 978-3-642-03359-9.

[3] Assia Mahboubi and Enrico Tassi. *Mathematical Components*. Zenodo, Jan. 2021. DOI: 10.5281/zenodo.4457887. URL: https://doi.org/10.5281/zenodo.4457887.

[4] Pawel Sosna. *COMMUTATIVE ALGEBRA, LECTURE NOTES*. Hamburg University, 2014. URL: https://www.math.uni-hamburg.de/home/sosna/commalg/commalgebra.pdf.

[5] Enrico TASSI. *Coq winter SCHOOL 2017-2018 (SSReflect & mathcomp)*. Dec. 2017. URL: https://team.inria.fr/marelle/en/coq-winter-school-2017-2018-ssreflect-mathcomp/.