

# Teaching Interactive Proofs to Mathematicians

Mauricio Ayala-Rincón

Universidade de Brasília  
Brasília D.F., Brazil  
ayala@unb.br

Thaynara Arielly de Lima

Universidade Federal de Goiás  
Goiânia, Brazil  
thaynaradelima@ufg.br

This work discusses an approach to teach to mathematicians the importance and effectiveness of the application of Interactive Theorem Proving tools in their specific fields of interest. The approach aims to motivate the use of such tools through short courses. In particular, it is discussed how, using as case-of-study algebraic notions and properties, the use of the proof assistant Prototype Verification System PVS is promoted to interest mathematicians in the development of their mechanized proofs.

## 1 Introduction

Previous academic experiences at our institutions pointed out the relevance of teaching foundations of formal methods to Computer Science (CS) professionals [2]. In principle, what is expected is that when CS students learn the foundations of logical deduction in an introductory course in Computational Logic, they also develop technical capabilities to apply logical deduction and inductive methods to verify correctness properties of their programs through the use of proofs assistants. In the case of the institution of the first author, this is formulated in the teaching methodology for the course on Computational Logic offered to third-semester students in CS, who have a minimal background in programming, discrete mathematics, algebra and calculus [4]. The aim of the course is that CS students develop skills and expertise in this relevant application of mathematical deduction through the performance of verification exercises of correction of simple sorting algorithms (see the NASA PVS library theory `sorting`, developed by members of our group, at <https://github.com/nasa/pvslib>).

In this work, we show how we coined out a completely different teaching approach to motivate mathematicians to involve in their efforts in theorem proofs the routine of application of Interactive Theorem Proving tools (ITPs). The discussion is supported by a PVS theory used to give short tutorials to mathematicians with this aim and available at <http://ayala.mat.unb.br/publications.html>. The tutorial deals mainly with notions and theorems of algebra in which the authors have some expertise (see NASA PVS libraries of Formal Developments on algebra and groups available at <https://github.com/nasa/pvslib> and [25, 29]).

### 1.1 Motivation

We aim to establish an adequate teaching approach to present to mathematicians the power of ITPs by showing how these tools can contribute to understanding mathematical theories deeply by analyzing all the particularities and formal requirements to specify and prove mathematical notions and properties. The target audience is, researchers and graduate students in all areas of mathematics well-trained in pen-and-paper proofs, who are not expected to be truly interested in time-consuming investments in a long training in areas such as Mathematical Logic, Proof Theory, and Logical Deduction, but who may be truly interested in profiting from the benefits of such powerful computational tools.

Usually, researchers and students from the target audience are capable to use computational tools for numerical and symbolic computations (e.g., Mathematica, Octave, Matlab, Maple) as well as mathematical editors (e.g.,  $\text{\TeX}$ ,  $\text{\LaTeX}$ ), Internet search engines, and professional communication tools (Zoom, Skype, Teams, etc.), among others, but they are neither confident nor necessarily happy-users of such systems. Therefore, to involve them in dealing with another kind of computational tool as a proof assistant, the benefits for improving the precision and quality of their professional work (i.e., mathematical proofs) should be made explicit quickly.

The main benefits of proof assistants should be diligently illustrated to convince such an audience of the importance of following a formal discipline for proving and checking theorems:

1. The importance of specifying consistently mathematical notions respecting the dependency of each notion on previously specified notions, and without allowing any omission;
2. The necessity of fulfilling formally all required cases, avoiding any informal or intuitive argumentation, in the formalization of pen-and-paper proofs;
3. The importance of using such technologies to certify the correctness and quality of mathematical proofs.

With this in mind, an eight-hour tutorial using the proof assistant PVS has been developed. The given material briefly introduces the proof engine of the proof assistant presenting the mathematical background, indeed, Gentzen Sequent Calculus and Induction, just mentioning the existence of associated research fields such as Proof Theory in which proof assistants are based. But the emphasis of the tutorial is on illustrating, considering classical fields of mathematics such as analysis, algebra, and geometry, how an ITP as PVS may be applied to fully specify basic concepts and formalize non necessarily elementary theorems of these fields.

In this paper we illustrate the proposed tutoring methodology that essentially follows two steps of increasing precision: initially, motivating the application of the ITP to follow the logical reasoning involved in well-known proofs of popular mathematical theorems and then, focusing on algebra, illustrating how proofs might be fully formalized. All that is done without emphasizing the deductive underground formalisms such as Gentzen Calculus, Higher-Order deduction, and construction of inductive schemata, but just focusing on the technical aspect of the application of the ITP to prove their theorems of interest.

## 1.2 A Few Related Works

Initially, the tutorial provides an overview of PVS by highlighting aspects of its specification language and explaining the Sequent Calculus in which the proof engine of PVS is based, namely, Calculus à la Gentzen, besides to present examples where PVS has been successfully used both in academic and industrial environments. There is no innovation in such an approach, the emphasis on the target audience has been applied in several courses on formal methods. In addition to our course on Computational Logic for CS students previously mentioned, other approaches to teach formal methods to different audiences have been proposed. Restricting the discussion to a few and recently reported approaches that are focused on fulfilling quickly the specific interests of the attendants, we can mention the course on Deductive Verification in Why3 by Sandrine Blazy at the *Université Rennes 1*, to train undergraduate students to develop their own correctness proofs of non-trivial sorting and searching algorithms [7]; the course taught at the *École Nationale Supérieure d'Informatique pour L'Industrie et L'Entreprise*, as part of the Software Engineering curriculum, by Catherine Dubois et al, in which students develop skills on formal methods [11]; and, the course by Kristin Yvonne Rozier prepared for the Aerospace Engineering

departments at Iowa State University and the University of Cincinnati, to train attendants to look at a verification question and identify what formal methods and tools are applicable to check safety-critical systems [27]. It is interesting to stress Catherine Dubois et al's position (in [11]) ratifying the importance of the effectiveness of the teaching approach to meet the specific demands of the target audience (in our case Mathematicians, and their case, CS/Engineers):

*“Students are strongly focused on the direct applicability of the knowledge they are taught, and they are not all going to pursue a professional career in the development of critical systems. Our experience shows that students can gain confidence in formal methods when they understand that, through a rigorous mathematical approach to system specification, they acquire knowledge, skills and abilities that will be useful in their professional future.”*

Some other considerations that we share, and that although evident are very relevant when learning formal methods, were also pointed out by Bayer et al in [6], to whom we give special attention. According to this interesting report by undergraduate students from Jacobs University Bremen about their beginner's experience trying to formalize mathematical theorems: it is relevant to start from knowing the main features of the ITP to be used; having programming experience is not necessarily a plus; it is relevant to start from knowing the chosen ITP and what it indeed is; including ITP in the curricula in fields such as Engineering and Mathematics is not feasible and tutorials may be a better approach to reach the interest of these professionals and researchers; starting from formalizing simple theorems is better than proposing very ambitious tasks; being aware of all details of the pen-and-paper proofs is important to transfer them to the ITP; diminishing the grade of automation at the beginning, is more fruitful than using the full automation power of a proof assistant.

### 1.3 Organization

Section 2 illustrates how the use of ITPs is motivated through reasoning about classical proofs of popular theorems in different fields of mathematics; Section 3 presents how the relevance of ITPs is illustrated by tutoring full formalizations of notions of group theory and theorems about cyclic, torsion and symmetric groups in the HO predicate calculus; Finally, Section 4 discusses the extent to which the authors believe this approach reach the proposed objectives.

## 2 Motivating the Use of ITPs

The first step to interest mathematicians in the application of ITPs needs to be very simple but motivating. Then, our approach proposes the development of deduction exercises that are based almost on axiomatizations allowing mathematicians to follow the reasoning involved in well-known proofs of relevant mathematical results. For an interesting diversity of mathematicians, it is also important the development of examples from several fields. In this section, some of such examples are discussed in which almost only predicate deduction and elementar type theory is applied using the proof assistant PVS.

### 2.1 Algebra - Propositional Deductions on Groups

This example uses just propositional deduction and deals with proofs based on axioms and properties about symmetric, cyclic, and torsion groups. These properties are very familiar for advanced undergraduate, graduate in Mathematics and mathematicians (e.g. see textbooks in abstract algebra such

as [13], [22] or [21]). The objective of such an example is just introducing mathematicians to the elements of the ITP tool. Using such an example, we explain the environments of the proof assistant, in which specifications are given and proofs are executed. This includes a quick start on the syntax of the specification language, basic types, and the mechanics of the deductive engine, which for the case of PVS are a functional language and sequent calculus, respectively.

Propositional variables for `Cyclic`, `Abelian`, `Symmetric`, and finite degree (`FiniteDegree`) groups are specified. Also, a propositional variable for symmetric groups of degree greater than two is given, `nGT2`. Cyclic groups contain a generator  $y$  such that for each element  $x$  in the group, there exists an integer  $i$  such that  $x = y^i$ ; in Abelian groups the binary group operation,  $*$ , is commutative. The symmetric group of degree  $n$  is given by the set of  $n$ -permutations (bijective functions on the set  $\{1, \dots, n\}$ ) with neutral element given by the identity function and binary operator given by functional composition. A group is said to be of finite degree if for all  $x$  in the group there exists a natural  $n$  such that  $x^n$  is the neutral element. Indeed, the granularity of a group as a structure  $G = \langle S, *, e \rangle$ , where  $S$  is a non-empty set with a binary associative function  $*$  with neutral element  $e$ , and such that  $*$  allows inverses (i.e., for all  $x \in S$  there exists  $y$  such that  $x * y = y * x = e$ ), is not specified in this example but will be given in the next step of the tutoring approach, where full formalizations are provided.

Initially, some axioms specifying well-known properties are given.

```
Ax01 : AXIOM Cyclic => Abelian
Ax02 : AXIOM Symmetric_n AND nGT2 => NOT Abelian
Ax03 : AXIOM FiniteDegree <=> Torsion
Ax04 : AXIOM Finite => FiniteDegree
Ax05 : AXIOM NOT Finite <=> Infinite
Ax06 : AXIOM Abelian AND Torsion <=> AbelTorsion
```

And after that, simple propositional (well-know) consequences of these axioms are proposed to present the specification and proof environments of the ITP. For instance, the first conjecture below is a consequence of the first and second axiom; the second, of the third and fourth axioms, and so on.

```
Pr01 : CONJECTURE Symmetric_n AND Cyclic => NOT nGT2
Pr02 : CONJECTURE Finite => Torsion
Pr03 : CONJECTURE Cyclic AND Finite => AbelTorsion
Pr04 : CONJECTURE NOT Torsion => Infinite
```

In particular, in PVS, AXIOMS may be also called CONJECTURES that may be both promoted to LEMMAS once proofs are completed.

The discussion at this point includes providing information about the existence and importance of the field of proof theory and about the relation between PVS propositional proof commands and Gentzen's sequent rules; namely, PVS proof commands as (`flatten`) and (`split`) versus Gentzen rules as ( $L_{\wedge}$ ), ( $R_{\vee}$ ) and ( $R_{\rightarrow}$ ) and, ( $R_{\wedge}$ ), ( $L_{\vee}$ ) and ( $L_{\rightarrow}$ ), respectively (see e.g., Chapter 4 in [4] or slides that accompany the tutorial "Interactive Proving Mathematical Theorems" available at [http://ayala.mat.unb.br/Summer\\_UnB\\_2020](http://ayala.mat.unb.br/Summer_UnB_2020)). Also, at this point, it is relevant to explain how axioms, lemmas, and conjectures can be invoked or charged as antecedent formulas of the goal sequent using PVS commands as (`lemma`) and (`rewrite`).

Besides, it is important to clarify to the attendants the limitations of the propositional language used in such an example explaining that the expressiveness of the language and logical system of the ITP would be enough to provide precise specifications of all required notions and properties and to complete all holes in the proofs. For doing that, additional elements in the language such as quantifiers may be

discussed letting clear how one could, for example, specify (and formalize) with precision the axiom Ax01 above:

$$\underbrace{\exists y \in G : \forall x \in G : \exists i \in \mathbb{Z} : x = y^i}_{\text{Cyclic}} \Rightarrow \underbrace{\forall u, v \in G : u * v = v * u}_{\text{Abelian}}$$

Also, it would be of interest to discuss elements such as induction that will be required to formalize the intuitive and simple pencil-and-paper proof of this property; essentially, the observation below.

$$\exists i, j : u = y^j, v = y^i \Rightarrow y^i * y^j = y^{i+j} = y^{j+i} = y^j * y^i$$

## 2.2 Analysis - a Topological Proof of Infinitude of Primes

Probably, the most well-known proof of the infinitude of primes is the one presented in *Elements IX* and attributed to Euclid, but here we chose an elegant proof about this fact by using a topological argumentation due to Fürstenberg [14]. In the following, we will explain Fürstenberg's proof and how his lines of reasoning may be specified and formalized to lead the attendants to easily conclude. A detailed and readable explanation of such proof is available in Chapter 1 of [1].

Firstly, we consider sets of the form  $\{a + n \cdot b \mid n \in \mathbb{Z}\}$ , where  $a$  and  $b$  are integer numbers with  $b > 0$ . The elements of each such set provide an infinite arithmetic progression from  $a$  with period  $b$ . Sets that may be given in such a form satisfy the predicate `add_cyclic?`. In PVS, `add_cyclic?(N)` if and only if  $N$  is of type set [int] and  $N = \{a + n \cdot b \mid n : \text{int}\}$ , for  $a$  and  $b$  of respective types int and posnat.

A topology consisting of *open* sets that are (possibly infinite) unions of such integer sets is given: `open?(X)` if and only if  $X$  is the union of sets that satisfy the predicate `add_cyclic?`, given by the predicate `Union_add_cyclics?`. In this topology, any non-empty open set is infinite, and complements of open sets are *closed*, and vice versa, as expected.

Also, finite intersections of open sets are open (i.e., `fin_int_open?(X) ⇒ open?(X)`) as finite unions of closed sets are closed (i.e., `fin_union_closed?(X) ⇒ closed?(X)`). Notice that a set of the form  $\{a + n \cdot b \mid n \in \mathbb{Z}\}$  is also closed since its complement is the (finite) union of `add_cyclic?` sets as below.

$$\bigcup_{j=1}^{b-1} \{(a + j) + n \cdot b \mid n \in \mathbb{Z}\}$$

Now, consider the set `per PRIMES` given by the union of all `add_cyclic?` sets of the form  $\{0 + n \cdot p \mid n \in \mathbb{Z}\}$ , where  $p$  in PRIMES. Notice that the complement of `per PRIMES` is the set  $\{-1, 1\}$ .

If PRIMES were finite, as a finite union of closed sets, `per PRIMES` would be closed too, and consequently, its complement  $\{-1, 1\}$  would be open, which contradicts the fact that any non-empty open set is infinite. Thus, PRIMES is infinite.

Below, we include a PVS specification of this proof that is mainly based on axioms (Ax00 - Ax09), letting to the mathematicians the task to prove five easy conjectures to complete Fürstenberg's proof.

```
add_cyclic?, open?, Union_add_cyclics?, fin_int_open?, fin_union_closed?
: pred[set[int]]
```

```
PRIMES : set[int]
X,Y : VAR set[int]
```

```

finite?: pred[set[int]] = is_finite[int]

Ax00: AXIOM add_cyclic?(emptyset)
Ax01: AXIOM open?(X) <=> Union_add_cyclics?(X)
Ax02: AXIOM Union_add_cyclics?(X) AND Union_add_cyclics?(Y) =>
      Union_add_cyclics?(union(X,Y))
Prop01: CONJECTURE open?(X) AND open?(Y) => open?(union(X,Y))
Ax03: AXIOM add_cyclic?(X) => Union_add_cyclics?(X)
Ax04: AXIOM fin_int_open?(X) => Union_add_cyclics?(X)
Prop02: CONJECTURE fin_int_open?(X) => open?(X)

closed?(X): bool = open?(complement(X))

Ax05: AXIOM X /= emptyset AND Union_add_cyclics?(X) => NOT finite?(X)
Ax06: AXIOM add_cyclic?(X) =>
      EXISTS (Y:set[int]): Union_add_cyclics?(Y) AND X = complement(Y)
Prop03: CONJECTURE add_cyclic?(X) => closed?(X)
Ax07: AXIOM fin_union_closed?(X) => closed?(X)
per_PRIMES: set[int] = complement({x: int | x = 1 OR x = -1})
Ax08: AXIOM Union_add_cyclics?(per_PRIMES)
Ax09: AXIOM finite?(PRIMES) => fin_union_closed?(per_PRIMES)
Prop04: CONJECTURE finite?({x: int | x = 1 OR x = -1})
Prop05: CONJECTURE NOT finite?(PRIMES)

```

In this theory we define open sets restricted to the topology to be considered in the proof, as one can see in specification Ax01. However, we point out that Prop01, Prop02 and Ax07 hold for any topology.

The specification uses PVS prelude set objects: `emptyset`, `is_finite`, and `complement` and a minimum of PVS prelude formulas on sets.

As an illustration the formalization of conjecture Prop05 consists just of application of axioms Ax07 and Ax09 to conclude `closed?(per_PRIMES)`. From that, one has that `open?({-1,1})` using a PVS prelude formula that states the nilpotency of the complement operator on sets. By Ax01 and Ax05 one obtains that this set is infinite, which using Prop04 gives the desired contradiction. Below, a few additional details on how this is done in PVS are provided. The full proof is part of the model tutorial<sup>1</sup> that accompanies this paper.

PVS separates the specification from the formalization in files with extensions “pvs” and “prf”, respectively. Goals in PVS are sequents. For proving Prop05, once the proof environment is open, the goal `finite?(PRIMES) ⊢` appears.

The PVS proof command (`lemma Ax09`) is then used to charge this axiom, and by propositional simplification the formula `fin_union_closed?(per_PRIMES)` becomes an antecedent of the goal sequent. Then, axiom Ax07 is invoked and instantiated with `per_PRIMES` (using the PVS proof command (`inst ‘pre_PRIMES’`)), obtaining, by propositional simplification, the sequent:

```
closed?(per_PRIMES), fin_union_closed?(per_PRIMES), finite?(PRIMES) ⊢
```

Expanding the definition of `closed?`, the formula `closed?(per_PRIMES)` becomes the antecedent formula `open?(complement(per_PRIMES))`. And then, expanding `per_PRIMES` one obtains the sequent:

<sup>1</sup><http://ayala.mat.unb.br/publications.html>

```
open?(complement(complement({1,-1}))),
fin_union_closed?(complement({1,-1}), finite?(PRIMES) ⊢
```

By applying a PVS prelude lemma on nilpotency of the operator complement on sets, the first formula becomes `open?({1,-1})`, and applying `Ax01` one obtains the sequent:

```
Union_add_cyclics?({1,-1}),
open?({1,-1}), fin_union_closed?(complement({1,-1})), finite?(PRIMES) ⊢
```

Invoking and instantiating adequately `Ax05` and then, by propositional simplification, one obtains the sequent:

```
{1,-1} ≠ ∅ ⇒ NOT finite?({1,-1}), Union_add_cyclics?({1,-1}),
open?({1,-1}), fin_union_closed?(complement({1,-1})), finite?(PRIMES) ⊢
```

The proof is then concluded, by application of `Prop04` that gives the formula `finite?({1,-1})` and expanding the definition of the empty set,  $\emptyset: \{x:\text{int} : \text{FALSE}\}$ . Thus,  $\{1,-1\} \neq \{x:\text{int} \mid \text{FALSE}\}$  is proved by decomposing the equality, using the PVS command (`decompose-equality`) that gives the inconsistent antecedent formula `FORALL(x : int): NOT (x = 1 OR x = -1)`. One concludes, instantiating this formula either with 1 or with -1.

For teaching issues, this theory does not consider algebraic aspects of sets of integers, but all the required aspects may be considered to obtain a complete formalization (as those in [5] and [12], obtained using CERES and Isabelle, respectively) as a nice further exercise.

### 2.3 Geometry - Pick's Theorem

Euler's formula states that if  $G$  is a connected plane graph with  $n$  vertices,  $e$  edges and  $f$  faces, then (see the example in Fig. 1):

$$n - e + f = 2$$

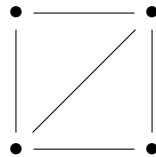


Figure 1: Euler's formula for three faces (the external face counts), four vertices and five edges

Pick's theorem from 1899 is a classical consequence from Euler's formula that establishes another formula for the area of *integral polygons* in  $\mathbb{R}^2$ , where the vertices of such integral polygons belong to the lattice  $\mathbb{Z}^2$ . See the example in Fig. 2.

An *elementary* polygon is a convex integral polygon that intersects only its vertices in the lattice  $\mathbb{Z}^2$ . See an example also in Fig. 2. Elementary polygons that are triangles have an area equal to  $1/2$ . Thus, the area of any integral polygon is the half of the number of elementary triangles inside the polygon, for any triangulation of the polygon in elementary triangles. See an example in Fig. 3.

Pick's theorem sees an elementary triangulation of an integral polygon as a plane graph and applies Euler's formula to express its area in terms of its vertices.

Let  $f$  be the number of faces in an elementary triangulation of an integral polygon  $P$ ,  $n = n_i + n_b$  be the number of vertices in the polygon that is equal to the sum of internal and boundary vertices,  $e = e_i + e_b$  be the number of edges in the polygon that is equal to the sum of internal and boundary

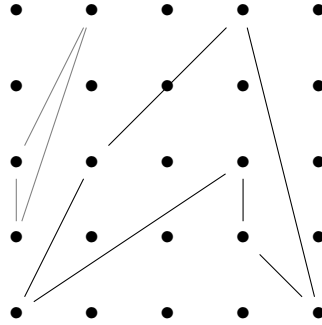


Figure 2: An elementary Polygon (gray) and an integral Polygon (black) - with vertices in  $\mathbb{Z}^2$

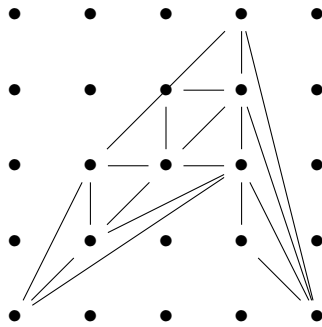


Figure 3: Triangulation of an Integral Polygon in Elementary Polygons

edges. First, notice that the number of boundary vertices and edges is the same. Also, notice that each elementary triangle in the boundary has a boundary and two internal edges, and any internal elementary triangle has three internal edges. These simple observations are given as axioms Ax01, Ax02, Ax03 and Ax04 in the PVS specification below, where  $n_i$ ,  $n_b$ ,  $n$ ,  $e_i$ ,  $e_b$  and  $e$  are of type natural (`nat`),  $f$  of type natural positive (`posnat`) and,  $\text{Area}_p$  of type real (`real`). In particular, the left-hand side of Ax04 counts the number of edges in each of the  $f - 1$  elementary triangles, but each internal edge is counted twice.

```
Ax01 : AXIOM ni + nb = n
Ax02 : AXIOM ei + eb = e
Ax03 : AXIOM eb = nb
Ax04 : AXIOM 3 * (f - 1) = 2 * ei + eb
EulerFormula : AXIOM n - e + f = 2
AreaIntPoly : AXIOM Areap = (f - 1) / 2
```

Pick's theorem establishes the area of any integral polygon  $P$  in terms of its internal and boundary vertices by the formula:

$$\text{Area}_P = n_i + n_b/2 - 1$$

Euler's formula and the area of an integral polygon,  $\text{Area}_P$ , are thus given as axioms. The second is given as the sum of the area of the  $f - 1$  elementary triangles in the triangulation of the polygon.



Below, Prop01 is a simple reformulation of Ax04, and Prop02 is a consequence of Prop 01 and Ax02. Prop03 is a reformulation of Prop02. Finally, Pick’s theorem is obtained from Prop02, (a simple variant of) the Euler’s formula, Ax01 and Ax03, and the previous axiom for the area of integral polygons.

Prop01 : CONJECTURE  $3 * f = 2 * e_i + 2 * e_b - e_b + 3$

Prop02 : CONJECTURE  $3 * f = 2 * e - e_b + 3$

Prop03 : CONJECTURE  $f = 2 * (e - f) - e_b + 3$

EulerFormula\_variant : CONJECTURE  $e - f = n - 2$

Pick\_Theorem : CONJECTURE  $\text{Area}_p = n_i + n_b / 2 - 1$

An example such this one allows introducing attendants the algebraic deductive engine of the proof assistant illustrating the grade of numerical automation of the system. Of course, a complete formalization of this proof (as the one reported in [19] using HOL Light) is an interesting challenge for the attendants.

### 3 Teaching *Mathematical Deduction*

After presenting examples such as the ones given in the previous section, the second step of the tutoring approach aims to teach the real usability of ITPs by illustrating how mathematical notions can be specified with precision and how elaborated proofs can be completely formalized. For this proposal, we illustrate here how we do this with algebraic notions and properties. Also, we remark the importance of providing information about important mathematical formal developments.

#### 3.1 Complete Formalizations About Cyclic and Torsion Groups

From Subsection 2.1, that brings classical theorems about groups from abstract algebra, it is expected that the attendants had realized that it is necessary a more powerful language (than the one of propositional logic) to reach a full formalization of such mathematical theorems. For example, the specification of the group,  $\langle S, *, e \rangle$ , itself requires the language of predicate logic to quantify elements of the group to specify, for instance, closure of the binary operator  $*$ : *for all  $x, y$  in  $S$ ,  $x * y$  belongs to  $S$ .*

In the PVS theories `pred_algebra` and `symmetric_n`, (part of the tutorial cited in the introduction) we present a full formalization of axioms and conjectures presented in Subsection 2.1. In the tutorial, the adequate specification of the required definitions and properties are discussed, and attendants are encouraged to prove the proposed theorems following a progressively increasing level of difficulty. By illustrating fully formalizations of mathematical objects that are part of their professional reality attendants are not only motivated to apply ITPs in their research but also to reasoning more thoroughly about issues and gaps that frequently happen in their pen-and-paper proofs.

Besides motivating and promoting the increase of skills in formalization of mathematics, this methodology also enables attendants to realize the effectiveness of ITPs as important tools to document mathematics, certify proofs, and check their correctness. All that naturally contributes to a better understanding of mathematical theories, since by using an ITP it is impossible to omit details of the proof or to reach the conclusion of a theorem omitting hypothesis. This contrasts with the pen-and-paper proving approach that usually accepts results omitting *simple* but *crucial* steps that are accepted as “trivial” or as “analogously” provable.

Even though the authors participated in the development of several elaborated results in algebra, the theorems included in the tutorial were calibrated in such a manner that they bring simple but challenging

formalizations exercises to the attendants. The tutorial includes specification of groups, subgroups, and cyclic, torsion and symmetric groups, and basic properties such as unicity of the identity of groups, left- and right-cancellative laws, the inverse of the inverse equals identity, and the inverse of multiplications equals swapped multiplication of the inverses, among others. Also, more elaborated results such as cyclic groups are Abelian, finite groups are torsion groups, finiteness of symmetric groups, the set of natural exponents of an element of a finite group is a subgroup, etc.

In the following, we depict the formalization of the property *Every cyclic group is Abelian* to exemplify how more complex mathematical formalizations are introduced along with the tutorial.

Firstly, in the theory `pred_algebra` which contains as parameters a non-interpreted non-empty type `T`, a binary operator `*`: `[T,T -> T]` and a constant `e` of type `T`, we specify the structure of groups and Abelian groups as a predicate.

```
G : VAR set[T]      % G is a variable of type set of elements of T
                  % (G) would be the type of elements of G, subtype of T

closed?(G): bool = FORALL (x,y:(G)): member(x*y,G)

inv_exists?(G): bool = FORALL (x:(G)): EXISTS (y:(G)): x * y = e AND y * x = e

group?(G): bool = closed?(G) AND associative?[(G)](*) AND member(e,G) AND
                identity?[(G)]*(e) AND inv_exists?(G)

abelian_group?(G): bool = group?(G) AND commutative?[(G)](*)
```

Such specification is naturally explained to the attendants without much justification about the logical system required (HO predicate logic). Some of the used predicates are included in the prelude of PVS, for instance, `associative?`, `commutative?` and `identity?`. For the first two, it is necessary to provide arguments about the type `(G)` over which the operator `*` is associative or commutative, and for the third one, additionally, the argument `e` that acts as a neutral element for the operator `*` over `(G)`.

Also, we introduce the specification of the inverse of an element in a group, `inv` by using the PVS indefinite operator `choose` that is well-defined over non-empty sets.

```
inv(G:(group?))(x:(G)): (G) = choose({y:(G) | x * y = e AND y * x = e})
```

At this point, we have the opportunity to enrich the discussion on types explaining the *type correctness conditions* (TCCs) that are generated by PVS along the process of type checking. The PVS type checker generates for the function `inv` the TCC `nonempty?({y:(G) | x * y = e AND y * x = e})`. This TCC should be proved manually using the type of `G` and expanding the definition of `group?`. In PVS TCCs are proof obligations that when cannot be automatically proved, the user should discharge to obtain *complete* formalizations.

In order to define cyclic groups, we specify the exponent of an element `y` of `T` to a natural `n` regarding the operator `*`, as a recursive function over the type of natural numbers (`nat`) and, then, we extend such function over integer numbers for elements of type `(G)` using the inverse of `y`.

```
^(y : T, n : nat ) : RECURSIVE T =
    IF n = 0 THEN e ELSE y * ^(y, n-1) ENDIF
    MEASURE n
```

$$\hat{\ } (G: (\text{group?})) (y: (G), i: \text{int}) : T = \text{IF } i \geq 0 \text{ THEN } \hat{\ } (y, i) \\ \text{ELSE } \hat{\ } (\text{inv}(G)(y), -i) \text{ ENDIF}$$

In PVS the specifier must provide a decreasing MEASURE to define each recursive function, and this measure, stated in functions of the parameters of the function, should decrease along chains of successive recursive calls. For the case of  $\hat{\ } (y, n)$  above, the measure  $n$  is the simplest adequate choice. When the type checker is executed, it provides the *termination* TCC `caret_TCC2` below, whose proof ensures the termination of such function.

$$\text{caret\_TCC2: OBLIGATION FORALL } (n: \text{nat}): \text{NOT } n = 0 \text{ IMPLIES } n - 1 < n$$

Finally, to extend the notion of exponent from naturals to integers (that is only possible over groups), the operator  $\hat{\ } (G)(y: (G), i: \text{int})$  is specified as  $\hat{\ } (y, i)$  if  $i$  is a natural number, and otherwise as  $\hat{\ } (\text{inv}(G)(y), -i)$ .

The next step is to specify the notion of a cyclic group and then the property that states that every cyclic group is Abelian.

$$\text{cyclic?}(G): \text{bool} = \text{group?}(G) \text{ AND} \\ \text{EXISTS } (y: (G)): \\ \text{FORALL } (x: (G)): \text{EXISTS } (n: \text{int}): \hat{\ } (G)(y, n) = x$$

In order to prove that cyclic groups are Abelian, accordingly to the usual mathematical intuition about why this property holds, as mentioned in the end of Subsection 2.1 (i.e., any pair of elements  $u, v$  of a cyclic group are such that if  $y$  is the generator of the group then for some integers  $i$  and  $j$ ,  $u * v = y^i * y^j = y^{i+j} = y^{j+i} = y^j * y^i$ ), we ask the attendants to assume the *conjectures* `power_add_aux` and `power_add_aux2` presented below, and apply them to establish by case analysis on the sign of  $i$  and  $j$  the required law for integer exponents, as given by the conjecture `power_add`. PVS allows us to specify and prove a lemma using previously specified but unproved “conjectures”. However, to provide a full formalization of a lemma all proofs of the previously used conjectures as well as all TCCs must be completed. The recommended discipline is to specify any unproved lemma as a “CONJECTURE” and only after it is proved, as a “LEMMA”. At this point of the discussion it is relevant to stress to attendants the big gap between intuition and formalization, letting clear why the proofs of *lemmas* `power_add_aux` and `power_add_aux2` require much too additional effort; indeed, they require careful applications of mathematical induction on the exponents. These proofs are proposed to the attendants as further exercise or homework on induction.

$$\text{power\_add\_aux: CONJECTURE} \\ \text{FORALL } (G: (\text{group?}), y: (G), n, m: \text{nat}): \hat{\ } (y, n) * \hat{\ } (y, m) = \hat{\ } (y, n+m)$$

$$\text{power\_add\_aux2: CONJECTURE} \\ \text{FORALL } (G: (\text{group?}), y: (G), n, m: \text{nat}): \hat{\ } (G)(y, m) * \hat{\ } (G)(\text{inv}(G)(y), n) = \\ \hat{\ } (G)(y, m - n)$$

$$\text{power\_add: CONJECTURE} \\ \text{FORALL } (G: (\text{group?}), y: (G), i, j: \text{int}): \hat{\ } (G)(y, i) * \hat{\ } (G)(y, j) = \hat{\ } (G)(y, i+j)$$

In PVS, inductive proofs may be performed by application of the proof commands `(induct)` and `(measure-induct)` that build simple and strong induction schemes, respectively. For instance, for the

case of the conjecture `power_add_aux` above, the application of simple induction on  $n$  with the proof command (`induct "n"`) generates the expected goals, given below.

Induction base:  $\text{FORALL}(G, y, m) : \hat{(y,0)} * \hat{(y,m)} = \hat{(y,m)}$

Induction step:  $\text{FORALL } j : \text{FORALL}(G, y, m) : \hat{(y,j)} * \hat{(y,m)} = \hat{(y,j+m)} \text{ IMPLIES}$   
 $\text{FORALL}(G, y, m) : \hat{(y,j+1)} * \hat{(y,m)} = \hat{(y,j+1+m)}$

Proving these goals require expanding both the definition of the operator  $\hat{\phantom{x}}$ , and of the notion of a group and, the second goal requires additionally Skolemization (using PVS commands as `(skolem)` or `(skeep)`), propositional decomposition and adequate instantiation of the induction hypothesis.

Finally, the conjecture `cyc_abel` specifies the property that cyclic groups are Abelian.

`cyc_abel: CONJECTURE cyclic?(G) IMPLIES abelian_group?(G)`

Notice that the properties `cyclic?` and then `abelian_group?` hold just for groups, then one have to prove only that from `cyclic?(G)` one can infer `commutative?[(G)](*)`. This is obtained by using `power_add` and the commutativity of integers (indeed, of real numbers regarding addition to prove that  $y^{i+j} = y^{j+i}$ ) that are provided in the prelude of PVS.

The theory `pred_algebra` includes also torsion groups specified as below.

`torsion?(G): bool = group?(G) AND FORALL (y:(G)): EXISTS (n: posnat) : y^n = e`

A thought-provoking example is a conjecture that finite groups are torsion groups.

`finite_torsion: CONJECTURE`

`FORALL (G: (group?)): is_finite(G) IMPLIES torsion?(G)`

This is proved showing that for any  $y$  element of  $G$ , the function  $f : \text{below}[N+1] \rightarrow \{y^0, \dots, y^{N-1}\}$ , where  $N$  is the cardinality of  $G$ , cannot be injective. Here, `below[N+1]` is the subtype of naturals  $\{0, \dots, N\}$ . Indeed, if  $f$  were not injective, there would exist  $i < j \leq N$  such that  $y^i = y^j$ , from which using properties of the operator  $\hat{\phantom{x}}$  one concludes that  $y^{j-i} = e$ . Non injectivity of  $f$  is proved assuming that it is injective. In PVS, the predicate `is_finite(G)` is characterized by the existence of an injective function  $g : (G) \rightarrow \text{below}[N]$ . The contradiction is obtained since composition of injective functions is injective (formalized in the lemma `composition_injective` of the PVS prelude library) that would imply that  $g \circ f : \text{below}[N+1] \rightarrow \text{below}[N]$  is injective.

The last example is the conjecture that for any finite group  $G$  and element  $y$  in it, the set of natural powers of  $y$  (`power_gen(y)`) is indeed a subgroup of  $G$ , specified below.

`power_gen(x:T): set [T] = { y: T | EXISTS (n:nat) : y = x^n }`

`subgroup?(H:set [T], G:(group?): bool = subset?(H,G) AND group?(H)`

`power_gen_fin_group_is_subgroup: CONJECTURE`

`FORALL (G: (group?), y:(G)): is_finite(G) IMPLIES subgroup?(power_gen(y), G)`

The proof consists in showing that the set `power_gen(y)`, for  $y$  in  $G$  is a subset of  $G$  and satisfies all properties of groups. The interesting part of the proof is showing the existence of inverses: for any natural  $n$  there exists a natural  $m$  such that  $y^n * y^m = y^m * y^n = e$ . From the previous conjecture (`finite_torsion`)  $G$  is a torsion group, which implies that there exists a non-zero natural  $k$  such that  $(y^n)^k = e$ . This allows the choice of  $m$  as  $n(k-1)$  and with this choice and properties of power one concludes that  $y^n * y^{n(k-1)} = y^{n(k-1)} * y^n = y^{nk}$ . An additional property of power, `power_mult_aux`, given below, would be required to prove that  $y^{nk} = (y^n)^k$  and conclude.

```
power_mult_aux: CONJECTURE
  FORALL (G:(group?), y:(G), m,n: nat): (y^n)^m = y^(n*m)
```

### 3.2 Formalizations About Symmetric Groups

More elaborated examples should be discussed to make evident to the attendants that ITPs can be indeed applied to perform serious mathematical proofs, which is not at all a consensus for the mathematicians. Thus, in addition to the previous basic examples, the tutorial contains additional and more elaborated results. We illustrate this with the properties of a concrete structure that satisfies the definition of groups: symmetric groups. It is formalized in the theory `symmetric[n]` included below, where the parameter `n` is the degree of the symmetric group that is a positive natural number.

```
symmetric[n:posnat]: THEORY
  BEGIN

  IMPORTING pred_algebra[ [below[n] -> below[n]], o, LAMBDA(i: below[n]): i],
            sets_aux@set_of_functions[below[n],below[n]]

  symmetric: set[[below[n] -> below[n]]] =
    {f : [below[n] -> below[n]] | bijective?(f)}

  group_symmetric: CONJECTURE group?(symmetric)

  sym_gt2_notabelian: CONJECTURE
    n >=3 IMPLIES NOT abelian_group?(symmetric)

  sym_cyc_lt2: CONJECTURE cyclic?(symmetric) IMPLIES n < 3

  symmetric_is_finite: CONJECTURE is_finite(symmetric)

  symmetric_is_torsion: CONJECTURE torsion?(symmetric)

  power_gen_subgroup_sym: CONJECTURE
    FORALL (y:(symmetric)): subgroup?(power_gen(y),symmetric)

  END symmetric
```

The first interesting aspect of this formalization is importing the theory `pred_algebra` whose parameters were given by the triple `[T, *: [T,T -> T], e:T]`, a non-interpreted non-empty type `T`, a binary operator `*` and a constant `e` of type `T`, and where groups were specified (see Subsection 3.1). This theory is imported by `symmetric[n]` with arguments

```
[ [below[n] -> below[n]], o, LAMBDA(i: below[n]): i ]
```

Through this importation, the type `T` is interpreted as the set of functions from  $\{0, \dots, n-1\}$  into  $\{0, \dots, n-1\}$ , the binary operator `*`, as the composition of functions `o`, and the constant `e`, as the identity function, `LAMBDA(i: below[n]): i`.

Thus, the set `symmetric` is specified as the subset of all bijective functions on `below[n]`. And then the first interesting task is to prove the conjecture `group_symmetric` that states that `symmetric`

is indeed a group: `group?(symmetric)`. The proof of `group_symmetric` is, mainly, based on the PVS prelude theory for functions since it provides results such as “*Compositions of bijective functions are also bijective functions*”, “*Bijective functions have bijective inverses*”, “*Function composition is associative*” and “*The identity function is bijective*”.

A well-known property about symmetric groups with a degree greater than 2 is that they are not Abelian (Conjecture `sym_gt2_notabelian`). The proof of this result consists in providing explicitly two elements of `symmetric` that do not commute regarding the binary operator `o`. For instance, one can construct as witnesses the functions  $f$  that maps 0 into 1, 1 into 0 and fixes all other elements of the domain, and  $g$  that maps 0 into 2, 2 into 0 and fixes all other elements of the domain. Constructive proofs of existential formulas are provided in such a manner. The above-mentioned functions  $f$  and  $g$  can be specified in PVS, respectively, as

```
LAMBDA (i:below[n]) : IF i>=2 THEN i ELSIF i = 0 THEN 1 ELSE 0 ENDIF
LAMBDA (i:below[n]) : IF i>=3 THEN i ELSIF i = 0 THEN 2
                      ELSIF i = 1 THEN 1 ELSE 0 ENDIF
```

Using these functions the proof resumes to show that  $f \circ g \neq g \circ f$ , which can be done using the fact that  $(f \circ g)(0) = 2$  and  $(g \circ f)(0) = 1$ .

The Conjecture `sym_cyc_lt2` is proved as corollary of `sym_gt2_notabelian` because cyclic groups are Abelian.

An interesting formalization, that may illustrate to the attendants how much mathematicians (they!) appeal to their intuition when they develop pen-and-paper proofs is the one of the next conjecture in the theory `symmetric[n]: symmetric_is_finite`. In general, they justify the finiteness of the symmetric group of degree  $n$  just through the observation that the set of bijective functions correspond to the set of  $n!$  permutations on a set of  $n$  elements, without worrying about building a proof of this fact. Without concrete proof of this fact, further complete formalizations would be impossible (such as the fact that symmetric groups are torsion groups). Since in PVS the predicate `is_finite(S)` is characterized by the existence of a natural number  $N$  and an injective function  $f: (S) \rightarrow \text{below}[N]$ , to prove that the group `symmetric` is finite, it is necessary to make explicit such an injective function for some adequate  $N$ . This formalization is obtained by application of a lemma in the imported theory `sets_aux@set_of_functions` of the NASA PVS library which states that the cardinality of the set of functions from a finite domain to a finite co-domain of respective cardinalities  $m$  and  $n$  is  $n^m$ . This is specified as the existence of a bijective function, say  $h$ , from this set of functions to the type `below[n^m]`. The formalization is concluded proving that the restriction of  $h$  to the domain `symmetric` is an injective function, which implies the finiteness of `symmetric`.

As a corollary of the previous result and the fact that finite groups are torsion groups (see conjecture `finite_torsion` in the end of Subsection 3.1) one obtains the formalization of the conjecture `symmetric_is_torsion`. All other properties of finite groups are then inherited by symmetric groups, such as the fact that `power_gen(f)`, for any bijective function  $f$  on `below[n]` (see Subsection 3.1) is a subgroup of `symmetric`.

### 3.3 Information About Formal Developments

Some information should be provided to attendants about serious mathematical important formal developments. Restricting our attention just to algebraic theorems, we can mention, for instance, the NASA PVS Formal Developments library contains general results on algebra [8] as well advanced results on group theory such as the Sylow's Theorems [15], and Isomorphism Theorems for groups and rings, and

the Chinese Remainder Theorem for Non-commutative rings [25], among others. Also, results about groups, rings, and ordered fields are formalized in Coq as part of the FTA project [16]. Other important formalizations in Coq deal with finite group theory [18] culminating in the formalization of the Feit and Thompson’s proof of the Odd Order Theorem that states that every finite group of odd order is solvable [17]. Also in Coq, formalizations of real ordered fields [10] and finite fields [26], and formalization of rings with explicit divisibility [9] are available. Formalizations of the Binomial Theorem for rings are available in Nuprl [23] and Mizar [28]. In ACL2 a hierarchy of algebraic structures ranging from setoids to vector spaces is built focusing on the formalization of computer algebra systems [20]. The Algebra Library of Isabelle/HOL [3] provides a wide range of theorems on mathematical structures, including results on rings, groups, factorization over ideals, rings of integers and polynomial rings. A formalization of the First Isomorphism Theorem for rings is also available in Mizar [24].

## 4 Discussion

The main interest of this position paper is to show how ITPs can be promoted among users of related areas, who do not necessarily require or desire to develop a strong background in proof theory and mathematical deduction, but who just need or want to apply these tools in their areas of expertise. Usually, we can reach the attention of mathematicians in workshops in which their time availability is restricted and for which short-courses and tutorials should be limited to a few hours (usually, from two to at most eight hours). Because of this, our proposal requires a huge effort to adopt nice well-known mathematical examples that fulfil the real interests of the attendants, it focuses on the mathematical aspects of the proofs and omits long dissertations about logical systems, deduction and proof theory. Also, our position is that good graduation and diversity of the complexity of the selected examples contributes to illustrate clearly to the attendants the real power of ITPs to prove elaborated mathematical theorems. This contrast with the high flexibility we have when teaching logical deduction to CS students in our one-semester sixty-four-hour course on Computational Logic, mentioned in the introduction, for which we have enough time and can focus on natural and sequent calculus-based deduction and spend at least a third of the semester training students in the application of deductive tools ([2, 4]).

## References

- [1] Martin Aigner & Günter M. Ziegler (2018): *Proofs from THE BOOK*, 6th edition. Springer, doi:10.1007/978-3-662-57265-8.
- [2] Ariane Alves Almeida, Ana Cristina Rocha-Oliveira, Thiago Mendonça Ferreira Ramos, Flávio Leonardo C. de Moura & Mauricio Ayala-Rincón (2019): *The Computational Relevance of Formal Logic Through Formal Proofs*. In: *Proceedings 3rd Formal Methods Teaching FMTea, LNCS 11758*, Springer, pp. 81–96, doi:10.1007/978-3-030-32441-4\_6.
- [3] Jesús Aransay, Clemens Ballarin, Martin Baillon, Paulo Emílio de Vilhena, Stephan Hohe, Florian Kammüller & Lawrence C. Paulson (2019): *The Isabelle/HOL Algebra Library*. Technical Report, Isabelle Library, University of Cambridge Computer Laboratory and Technische Universität München. Available at <https://isabelle.in.tum.de/dist/library/HOL/HOL-Algebra/document.pdf>.
- [4] Mauricio Ayala-Rincón & Flávio Leonardo C. de Moura (2017): *Applied Logic for Computer Scientists: Computational Deduction and Formal Proofs*. UTiCS, Springer, doi:10.1007/978-3-319-51653-0.
- [5] Matthias Baaz, Stefan Hetzl, Alexander Leitsch, Clemens Richter & Hendrik Spohr (2008): *CERES: An analysis of Fürstenberg’s proof of the infinity of primes*. *Theor. Comput. Sci.* 403(2-3), pp. 160–175, doi:10.1016/j.tcs.2008.02.043.

- [6] Jonas Bayer, Marco David, Abhik Pal & Benedikt Stock (2019): *Beginners' Quest to Formalize Mathematics: A Feasibility Study in Isabelle*, pp. 16–27. doi:10.1007/978-3-030-23250-4\_2.
- [7] Sandrine Blazy (2019): *Teaching Deductive Verification in Why3 to Undergraduate Students*. In: *Proceedings 3rd Formal Methods Teaching FMTea, LNCS 11758*, Springer, pp. 52–66, doi:10.1007/978-3-030-32441-4\_4.
- [8] Ricky Butler & David Lester (2007): *A PVS Theory for Abstract Algebra*. Available at <https://github.com/nasa/pvslib/tree/pvs7.0/algebra>. Accessed in June 17, 2020.
- [9] Guillaume Cano, Cyril Cohen, Maxime Dénès, Anders Mörtberg & Vincent Siles (2016): *Formalized linear algebra over Elementary Divisor Rings in Coq*. *Logical Methods in Computer Science* 12(2:7), pp. 1–23, doi:10.2168/LMCS-12(2:7)2016.
- [10] Cyril Cohen & Assia Mahboubi (2012): *Formal proofs in real algebraic geometry: from ordered fields to quantifier elimination*. *Logical Methods in Computer Science* 8(1:2), pp. 1–40, doi:10.2168/LMCS-8(1:2)2012.
- [11] Catherine Dubois, Virgile Prevosto & Guillaume Burel (2019): *Teaching Formal Methods to Future Engineers*. In: *Proceedings 3rd Formal Methods Teaching FMTea, LNCS 11758*, Springer, pp. 69–80, doi:10.1007/978-3-030-32441-4\_5.
- [12] Manuel Eberl (2020): *Fürstenberg's topology and his proof of the infinitude of primes*. *Arch. Formal Proofs* 2020. Available at [https://www.isa-afp.org/entries/Furstenberg\\_Topology.html](https://www.isa-afp.org/entries/Furstenberg_Topology.html).
- [13] John B. Fraleigh (2002): *A First Course in Abstract Algebra*, 7th edition. Pearson.
- [14] Hillel Fürstenberg (1955): *On the Infinitude of Primes*. *Amer. Math. Monthly* 62(5), p. 353, doi:10.2307/2307043.
- [15] André Luiz Galdino (2011): *A PVS Theory for Groups*. Available at <https://github.com/nasa/pvslib/tree/pvs7.0/groups>. Accessed in June 17, 2020.
- [16] Herman Geuvers, Randy Pollack, Freek Wiedijk & Jan Zwanenburg (2002): *A Constructive Algebraic Hierarchy in Coq*. *Journal of Symbolic Computation* 34(4), pp. 271–286, doi:10.1006/jsc.2002.0552.
- [17] Georges Gonthier, Andrea Asperti, Jeremy Avigad, Yves Bertot, Cyril Cohen, François Garillot, Stéphane Le Roux, Assia Mahboubi, Russell O'Connor, Sidi Ould Biha, Ioana Pasca, Laurence Rideau, Alexey Solovyev, Enrico Tassi & Laurent Théry (2013): *A Machine-Checked Proof of the Odd Order Theorem*. In: *4th International Conference on Interactive Theorem Proving ITP, LNCS 7998*, Springer, pp. 163–179, doi:10.1007/978-3-642-39634-2\_14.
- [18] Georges Gonthier, Assia Mahboubi, Laurence Rideau, Enrico Tassi & Laurent Théry (2007): *A Modular Formalisation of Finite Group Theory*. In: *20th International Conference Theorem Proving in Higher Order Logics TPHOLs, LNCS 4732*, Springer, pp. 86–101, doi:10.1007/978-3-540-74591-4\_8.
- [19] John Harrison (2011): *A formal proof of Pick's Theorem*. *Math. Struct. Comput. Sci.* 21(4), pp. 715–729, doi:10.1017/S0960129511000089.
- [20] Jónathan Heras, Francisco Jesús Martín-Mateos & Vico Pascual (2015): *Modelling algebraic structures and morphisms in ACL2*. *Applicable Algebra in Engineering, Communication and Computing* 26(3), pp. 277–303, doi:10.1007/s00200-015-0252-9.
- [21] Israel (Yitzchak) Nathan Herstein (1975): *Topics in algebra*, 2nd edition. John Wiley & Sons.
- [22] Thomas W. Hungerford (1980): *Algebra*. *Graduate Texts in Mathematics* 73, Springer, doi:10.1007/978-1-4612-6101-8. Reprint of the 1974 original.
- [23] Paul Bernard Jackson (1995): *Enhancing the Nuprl Proof Development System and Applying it to Computational Abstract Algebra*. Ph.D. thesis, Cornell University.
- [24] Artur Kornilowicz & Christoph Schwarzweller (2014): *The First Isomorphism Theorem and Other Properties of Rings*. *Formalized Mathematics* 22(4), pp. 291–301, doi:10.2478/forma-2014-0029.



- [25] Thaynara Arielly de Lima, André Luiz Galdino, Andréia B. Avelar & Mauricio Ayala-Rincón (2020): *Formalization of Ring Theory in PVS - Isomorphism Theorems, Principal, Prime and Maximal Ideals, Chinese Remainder Theorem*. Available at <http://ayala.mat.unb.br/publications.html>.
- [26] Jade Philipoom (2018): *Correct-by-Construction Finite Field Arithmetic in Coq*. Master's thesis, Master of Engineering in Computer Science, MIT.
- [27] Kristin Yvonne Rozier (2019): *On Teaching Applied Formal Methods in Aerospace Engineering*. In: *Proceedings 3rd Formal Methods Teaching FMTea, LNCS 11758*, Springer, pp. 111–131, doi:10.1007/978-3-030-32441-4\_8.
- [28] Christoph Schwarzweller (2003): *The Binomial Theorem for Algebraic Structures*. *Journal of Formalized Mathematics* 12(3), pp. 559–564. Available at <http://mizar.org/JFM/Vol12/binom.html>.
- [29] Andréia B. Avelar da Silva, Thaynara Arielly de Lima & André Luiz Galdino (2018): *Formalizing Ring Theory in PVS*. In: *9th International Conference on Interactive Theorem Proving ITP, LNCS 10895*, Springer, pp. 40–47, doi:10.1007/978-3-319-94821-8\_3.