XII Summer Workshop in Mathematics

Interactively Proving Mathematical Theorems

Section 4: Ring Theory in PVS

Thaynara Arielly de Lima(IME) UFG
Mauricio Ayala-Rincón (CIC-MAT) UnB

In collaboration with:

Andréia Borges Avelar da Silva (FUP - UnB)

André Luiz Galdino (IMTec - UFG - Catalão)

Funded by FAPDF DE grant 00193.0000.2144/2018-81, CNPq Research Grant 307672/2017-4

February 10 - 14, 2020

Talk's Plan

1. The PVS Proof Assistant
    - The PVS Libraries
2. Motivation
3. Some algebraic structures
4. The First Isomorphism Theorem
    - Chinese Remainder Theorem - General Version for Rings
5. Conclusions and Future Work

The `prelude` library

The PVS has a native library, the `prelude`.

- It is a collection of basic *theories* containing specifications about:
  - functions;
  - sets;
  - predicates;
  - logic; among others.
- The theories in the prelude library are visible in all PVS contexts.
- It provides the infrastructure for the PVS typechecker and prover, as well as much of the basic mathematics needed to support specification and verification of systems.

The NASA PVS libraries

- The NASA PVS library *nasalib* has specifications and formalizations in several subjects, such as:
  - Set theory (`sets_aux`);
  - Metric and topological spaces theory (`topology`);
  - First order unification and term rewriting systems (`TRS`);
  - Termination of functional specifications (`CCG`);
  - Linear algebra (`linear_algebra`);
  - Graphs and directed graphs (`graphs` and `digraphs`);
  - Basic abstract algebra (`algebra` and `groups`);
- The *nasalib* is maintaned by the NASA LaRC formal methods group;
- The *nasalib* is the result of research developed by the NASA LaRC formal methods group and the cientific comunity in general;

The PVS NASA library `algebra`

The *theory* `algebra` brings definitions and basic results on abstract algebra, for instance about:

- groupoid, monoid, groups, abelian groups;
- homomorfisms of groups, factor groups;
- rings, commutative rings, rings with one, division rings;
- integral domain;
- fields;

The *subtheory* algebra@ring

```
ring[T:Type+,+:[T,T->T],*:[T,T->T],zero:T]: THEORY

BEGIN

   ASSUMING IMPORTING ring_def[T,+,*,zero]

       fullset_is_ring: ASSUMPTION ring?(fullset[T])

   ENDASSUMING

   IMPORTING abelian_group[T,+,zero],
             operator_defs_more[T]

   ring: NONEMPTY_TYPE = (ring?) CONTAINING fullset[T]

% To bring elegance into this theory we define unary and binary minus.
;
   -: MACRO [T->T]   = inv;
   -: MACRO [T,T->T] = (LAMBDA (x,y:T): x + inv[T,+,zero](y))

   w,x,y,z: VAR T
   R:       VAR ring
   S:       VAR set[T]
```

The *subtheory* algebra@ring

```
plus_associative       : LEMMA (x + y) + z = x + (y + z)
plus_commutative       : LEMMA x + y       = y + x
times_associative      : LEMMA (x * y) * z = x * (y * z)
right_distributive     : LEMMA x * (y + z) = (x * y) + (x * z)
left_distributive      : LEMMA (x + y) * z = (x * z) + (y * z)

zero_plus              : LEMMA zero + x  = x
plus_zero              : LEMMA x + zero  = x
negate_is_left_inv     : LEMMA -x + x = zero
negate_is_right_inv    : LEMMA x + -x = zero
cancel_right_plus      : LEMMA x + z = y + z IFF x = y
cancel_left_plus       : LEMMA z + x = z + y IFF x = y
negate_negate          : LEMMA -(-x) = x
cancel_right_minus     : LEMMA x - z = y - z IFF x = y
cancel_left_minus      : LEMMA z - x = z - y IFF x = y
negate_zero            : LEMMA -zero = zero
negate_plus            : LEMMA -(x + y) = -y - x
times_plus             : LEMMA (x + y)*(z + w) = x*z + x*w + y*z + y*w
idempotent_add_is_zero : LEMMA x + x = x IMPLIES x = zero
zero_times             : LEMMA zero * x = zero
times_zero             : LEMMA x * zero = zero
negative_times         : LEMMA (-x) * y = - (x * y)
times_negative         : LEMMA x * (-y) = - (x * y)
negative_times_negative: LEMMA (-x) * (-y) = x * y
```

The *subtheory* algebra @ring

```
   ring_is_abelian_group  : JUDGEMENT ring SUBTYPE_OF abelian_group

   subring_is_ring        : LEMMA subring?(S,R) IMPLIES ring?(S)

   sq(x):T = x*x

   sq_rew      : LEMMA x*x      = sq(x)
   sq_neg      : LEMMA sq(-x)   = sq(x)
   sq_plus     : LEMMA sq(x+y)  = sq(x) + x*y + y*x + sq(y)
   sq_minus    : LEMMA sq(x-y)  = sq(x) - x*y - y*x + sq(y)
   sq_neg_minus: LEMMA sq(x-y)  = sq(y-x)
   sq_zero     : LEMMA sq(zero) = zero

   AUTO_REWRITE+ zero_plus               % zero + x  = x
   AUTO_REWRITE+ plus_zero               % x + zero  = x
   AUTO_REWRITE+ negate_is_left_inv      % -x + x = zero
   AUTO_REWRITE+ negate_is_right_inv     % x + -x = zero
   AUTO_REWRITE+ negate_negate           % -(-x) = x
   AUTO_REWRITE+ negate_zero             % -zero = zero
   AUTO_REWRITE+ zero_times              % zero * x = zero
   AUTO_REWRITE+ times_zero              % x * zero = zero

END ring
```

The PVS NASA library `groups`

- The *theory* `groups` was developed by Galdino, A.L.;
- It provides a solid framework for specifications involving group theory;
- It complements the *theory* `algebra`;
- It has important results about group homomorphisms and the Sylow's Theorems.

Why Formalize Ring Theory in PVS?

- A complete formalization of ring theory would complement the framework provided by the *theories* `algebra` and `groups`;
- To the best of our knowledge, there is no other formalizations about ring theory in PVS.

Why Formalize Ring Theory in PVS?

Ring theory has a wide range of applications in the most varied fields of knowledge. For example:

- Segmentation of digital images becomes more efficiently automated by applying the $\mathbb{Z}_n$ ring to obtain index of similarity between images [Suárez 2014];

Why Formalize Ring Theory in PVS?

Ring theory has a wide range of applications in the most varied fields of knowledge. For example:

- Segmentation of digital images becomes more efficiently automated by applying the $\mathbb{Z}_n$ ring to obtain index of similarity between images [Suárez 2014];
- According to [Bini 2012], finite commutative rings has an important role in areas like
  - combinatorics;
  - analysis of algorithms;
  - algebraic cryptography;
  - coding theory.
    - In particular in coding theory, finite fields and polynomials over finite fields has been widely applied in description of redundant codes [Lidl & Niederreiter 1994].
- and so on...

Why Formalize Ring Theory in PVS?

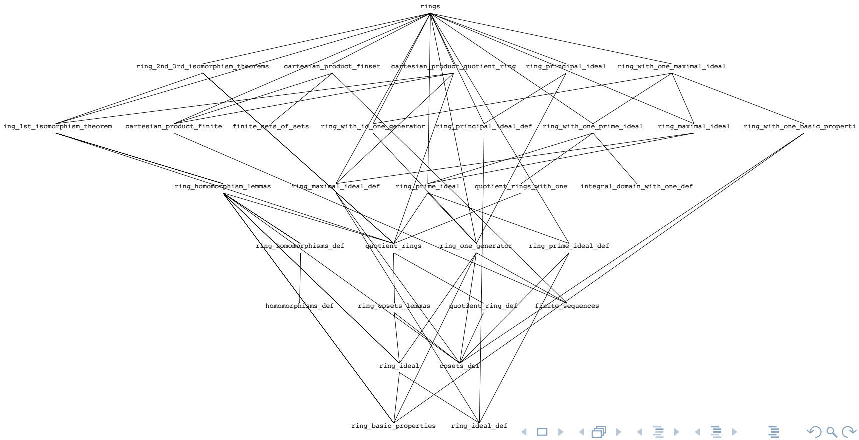
The project consists in formalizing in PVS the theory for rings as presented in textbooks of abstract algebra, for instance [Hungerford 1980, Artin 2010, Dummit 2003, Herstein 1975, Fraleigh 2003]. The formalization would make possible the formal verification of more complex theories involving rings in their scope.

Why Formalize Ring Theory in PVS?

The project consists in formalizing in PVS the theory for rings as presented in textbooks of abstract algebra, for instance [Hungerford 1980, Artin 2010, Dummit 2003, Herstein 1975, Fraleigh 2003]. The formalization would make possible the formal verification of more complex theories involving rings in their scope.

This is an ongoing formalization and the lemmas already verified constitute the *theory* `rings`, which is a collection of subtheories that will be described next.

Theory rings



Subtheory cosets_def

```
 +(g,H): set[T] = {t:T | EXISTS (h:(H)): t = g+h} ;

+(H,g): set[T] = {t:T | EXISTS (h:(H)): t = h+g} ;

sum(H,I): set[T] = {t:T | EXISTS (h:(H), k:(I)): t = h + k}
```

Subtheory cosets_def

```
left_coset?(G,H)(A:set[T]):bool = (EXISTS(a:(G)): A = a+H)

right_coset?(G,H)(A:set[T]):bool = (EXISTS(a:(G)): A = H+a)

coset?(G,H)(A:set[T]):bool =
        left_coset?(G,H)(A) AND right_coset?(G,H)(A)
```

In ring_cosets_lemmas

```
fullset_is_ring: ASSUMPTION ring?(fullset[T])

A,S,I : VAR set[T]

lcoset_iff_rcoset: LEMMA
     (left_coset?(S,I)(A) IFF right_coset?(S,I)(A))

lcoset_iff_coset: LEMMA
      (left_coset?(S,I)(A) IFF coset?(S,I)(A))
```

In quotient_ ring_def[T,+,*]

```
R, I: VAR set[T]

/(R,I) : setof[set[T]] = {s:set[T] | coset?(R,I)(s)}

add(R,I)(A,B:coset(R,I)) : set[T]= (lc_gen(R,I)(A) + lc_gen(R,I)(B)) + I

product(R,I)(A,B:coset(R,I)) : set[T]= (lc_gen(R,I)(A) * lc_gen(R,I)(B)) + I
```

In quotient_rings

```
add_is_coset: LEMMA
    FORALL (R: ring, I: ideal(R), A, B: coset(R, I)):
       EXISTS (a: (R)) : add(R,I)(A,B) = a + I

product_is_coset: LEMMA
    FORALL (R: ring, I: ideal(R), A, B: coset(R, I)):
       EXISTS (a: (R)) : product(R,I)(A,B) = a + I

product_charac: LEMMA
    FORALL (R: ring, I: ideal(R), a,b: (R)):
       product(R,I)(a+I,b+I) = (a*b) + I

quotient_group_is_ring: LEMMA
    FORALL(R: ring, I: ideal(R)):
       ring?[coset(R,I), add(R,I), product(R,I), I](R/I)
```

Subtheory ring_ideal_def

$$(m\mathbb{Z} = \{m \cdot z; z \in \mathbb{Z} \text{ e } m \in \mathbb{N}\}, +_{\mathbb{Z}}, \cdot_{\mathbb{Z}}, 0);$$

- $m\mathbb{Z}$ is a ring and $m\mathbb{Z} \subset \mathbb{Z}$;
- Consider $r \in \mathbb{Z}$ and $l \in m\mathbb{Z}$

$$l \cdot r = r \cdot l = r \cdot (m \cdot k) = m \cdot (r \cdot k) \in m\mathbb{Z}.$$

($m\mathbb{Z}$ “swallows” $\mathbb{Z}$)

```
R: VAR (ring?)
I: VAR set[T]

left_swallow?(I,R): bool = FORALL (r:(R), x:(I)): member(r * x,I)
right_swallow?(I,R): bool = FORALL (r:(R), x:(I)): member(x * r,I)

left_ideal?(I,R): bool = subring?(I,R) AND left_swallow?(I,R)
right_ideal?(I,R): bool = subring?(I,R) AND right_swallow?(I,R)

ideal?(I,R): bool = left_ideal?(I,R) AND right_ideal?(I,R)
```

Subtheory ring_ideal

```
R: VAR (ring?)
I: VAR set[T]

ideal_equiv: LEMMA
  ideal?(I,R) IFF
  (nonempty?(I) AND subset?(I,R) AND
   FORALL (x,y:(I), r:(R)): member(x - y,I) AND member(x*r,I)
                            AND member(r*x,I))

ideal_transitive: LEMMA
 subring?(H,R) AND ideal?(I,R) AND subset?(I, H)
   IMPLIES ideal?(I,H)

intersection_subring_ideal: LEMMA
 subring?(H,R) AND ideal?(I,R)
   IMPLIES ideal?(intersection(H,I),H)

self_ideal: LEMMA
  ideal?(R,R)
```

Homomorphism

$$\varphi : (R, +) \to (S, *)$$
$$\varphi(a + b) = \varphi(a) * \varphi(b)$$

homomorphism_def

```
R:  VAR (groupoid?[T,s])
S:  VAR (groupoid?[U,p])

homomorphism?(R, S)(phi: [(R) -> (S)]): bool =
  FORALL(a,b: (R)): phi(s(a,b)) = p(phi(a),phi(b))

monomorphism?(R, S)(phi: [(R) -> (S)]): bool =
  injective?(phi) AND homomorphism?(R,S)(phi)

epimorphism?(R, S)(phi: [(R) -> (S)]): bool =
  surjective?(phi) AND homomorphism?(R,S)(phi)

isomorphism?(R, S)(phi: [(R) -> (S)]): bool =
  monomorphism?(R, S)(phi) AND epimorphism?(R, S)(phi)
```

Ring homomorphism

ring_homomorphisms_def

```
R_homomorphism?(R1, R2)(phi: [(R1) -> (R2)]): bool =
   groupoid?[T1,s1](R1) AND groupoid?[T1,p1](R1) AND
   groupoid?[T2,s2](R2) AND groupoid?[T2,p2](R2) AND
   homomorphism?[T1,s1,T2,s2](R1, R2)(phi) AND
   homomorphism?[T1,p1,T2,p2](R1, R2)(phi)

R_kernel(R1,R2)(phi: R_homomorphism(R1,R2)): set[T1] =
   {a:T1 | R1(a) AND R2(zero2) AND phi(a) = zero2}

%----------------------------------------
R1, R2 : VAR ring
R_homo_equiv: LEMMA
 FORALL(phi:[(R1)->(R2)]): R_homomorphism?(R1,R2)(phi) IFF
  FORALL(x,y:(R1)): phi(s1(x,y)) = s2(phi(x),phi(y)) AND
                    phi(p1(x,y)) = p2(phi(x),phi(y))
```

The First Isomorphism Theorem

ring_homomorphisms_def

```
first_isomorphism_th: THEOREM
 FORALL(phi: R_homomorphism(R,S)):
 R_isomorphic?[coset(R, R_kernel(R,S)(phi)),
               add(R, R_kernel(R,S)(phi)),
               product(R, R_kernel(R,S)(phi)),
               R_kernel(R,S)(phi),
               D, s, p, zerod]
       (R/R_kernel(R,S)(phi), image(phi)(R))
```

Auxiliary lemmas

If $\phi : R \to S$ is a homomorphism of rings and I is an ideal of R which is contained in the kernel of ϕ, then:

1. there is a unique homomorphism of rings $f : R/I \to S$ such that $f(a+I) = \phi(a)$ for all $a \in R$;
2. the image of f is equal to the image of ϕ;
3. $ker(f) = ker(\phi)/I$;
4. f is an epimorphism iff ϕ is an epimorphism;
5. f is a monomorphims iff $ker(\phi) = I$;
6. f is an isomorphism iff ϕ is an epimorphism and $ker(\phi) = I$.

Chinese Remainder Theorem - General Version for Rings

Standard version for integers

Let $m_1, m_2, \ldots, m_r$ be positive integers such that m_i and m_j are coprime whenever $i \neq j$ and $m = m_1 \cdot m_2 \cdots m_r$. Then

$$\mathbb{Z}/(m_1 \cdots m_r)\mathbb{Z} = \mathbb{Z}/m_1\mathbb{Z} \cap \cdots \cap m_r\mathbb{Z} \cong \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_r\mathbb{Z}$$

General Version

Let $A_1, A_2, \ldots, A_r$ be ideals in a ring R with identity $1 \neq 0$. If for each $i, j \in \{1, \ldots, r\}$ the ideals A_i e A_j are comaximal $(A_i + A_j = R)$ whenever $i \neq j$ then

$$R/(A_1 \cap \cdots \cap A_r) \cong R/A_1 \times \cdots \times R/A_r$$

Chinese Remainder Theorem - General Version for Rings

- Prove that

$$\begin{array}{rccc} \varphi: & R & \to & R/A_1 \times \cdots \times R/A_r \\ & r & \mapsto & (r + A_1, \ldots, r + A_r) \end{array}$$

  is a surjective ring homomorphism whose kernel is $A_1 \cap \ldots \cap A_r$;
- Prove the theorem as a direct consequence of the First Isomorphism Theorem.

Chinese Remainder Theorem - General Version for Rings

$R/A_1 \times \cdots \times R/A_r$ is a ring:

```
R: VAR ring[T,+,*,zero]
fsA: VAR finseq[set[T]]
fsQ: VAR finseq[setof[set[T]]]

fsRI?(R)(fsA): bool =
         FORALL (i: below[length(fsA)]): ideal?(fsA(i), R)

fsI(R): TYPE = {fsA: finseq[set[T]] | fsRI?(R)(fsA)}

fsQ(R)(fsA: fsI(R)): finseq[setof[set[T]]] =
 IF length(fsA) = 0 THEN empty_seq
  ELSE (# length := length(fsA),
        seq := (LAMBDA (i:below[length(fsA)]): R/fsA(i)) #)
 ENDIF
```

Chinese Remainder Theorem - General Version for Rings

```
Sfs(R)(fsA:fsI(R))(fsx,
                   fsy:(cartesian_product_n(fsQ(R)(fsA)))):
                                           finseq[set[T]] =
 IF length(fsA) = 0 THEN empty_seq
  ELSE (# length := length(fsA),
             seq := (LAMBDA (i: below[length(fsA)]):
                         add(R,fsA(i))(fsx(i), fsy(i))) #)
 ENDIF

Pfs(R)(fsA:fsI(R))(fsx,
                   fsy:(cartesian_product_n(fsQ(R)(fsA)))):
                                           finseq[set[T]] =
 IF length(fsA) = 0 THEN empty_seq
  ELSE (# length := length(fsA),
             seq := (LAMBDA (i: below[length(fsA)]):
                     product(R,fsA(i))(fsx(i), fsy(i))) #)
 ENDIF

cartesian_product_quot_ring_is_ring: LEMMA
 FORALL (fsA: fsI(R)): length(fsA) /= 0 IMPLIES
                  ring?(cartesian_product_n(fsQ(R)(fsA)))
```

Chinese Remainder Theorem - General Version for Rings

```
CRT_aux_1: LEMMA
    FORALL (fsA: fsI(R) | length(fsA) /= 0):
     LET phi = LAMBDA (x: (R)): (# length := length(fsA),
               seq := (LAMBDA (i: below[length(fsA)]): x + fsA(i)) #) IN
     R_homomorphism?[T,+,*,zero,
                     (cartesian_product_n[set[T]](fsQ(R)(fsA))),
                     Sfs(R)(fsA), Pfs(R)(fsA),fsA]
       (R,cartesian_product_n[set[T]](fsQ(R)(fsA)))(phi)
      AND
      R_kernel[T,+,*,zero,
               (cartesian_product_n[set[T]](fsQ(R)(fsA))),
               Sfs(R)(fsA), Pfs(R)(fsA),fsA]
       (R,cartesian_product_n[set[T]](fsQ(R)(fsA)))(phi)=
       Intersection(seq2set(fsA))
```

```
CRT_aux_2: LEMMA
    FORALL (R: ring_with_one, fsA: fsICM(R)):
     LET phi = LAMBDA (x: (R)): (# length := length(fsA),
               seq := (LAMBDA (i: below[length(fsA)]): x + fsA(i)) #) IN
     surjective?[(R),(cartesian_product_n[set[T]](fsQ(R)(fsA)))](phi)
```

Teoria `rings`: Other relevant formalizations

Second and Third Isomorphism Theorems

Let I and J be ideals in a ring R.

(i) Second Isomorphism Theorem:
The rings $I/(I \cap J)$ and $(I + J)/J$ are isomorphic.

(ii) Third Isomorphism Theorem:
IF $I \subset J$, then J/I is an ideal in R/I and the rings $(R/I)/(J/I)$ and R/J are isomorphic.

Theory `rings`: other relevant formalizations

Principal ideals

Let R be a ring and a an element of R. Consider the family of all ideals of R which contain a. The intersection of the ideals in this family is called a principal ideal generated by a and denoted as (a).

Let R be a ring and $a \in R$.

1. The principal ideal (a) corresponds to the set $\{r * a + a * s + n \cdot a + \sum_{i=1}^{m} r_i * a * s_i | r, s, r_i, s_i \in R; m \in \mathbb{N} \setminus \{0\}; n \in \mathbb{Z}\}$, where $n \cdot a$ denotes n summands of a if $n \geq 0$, and n summands of $-a$ if $n < 0$;
2. If R is a commutative ring then $(a) = \{r * a + n \cdot a | r \in R; n \in \mathbb{Z}\}$;
3. If R is a commutative ring and has an identity then $(a) = \{r * a\} = \{a * r\}$, where $r \in R$.

Theory `rings`: other relevant formalizations

Prime ideals

An ideal P of a ring R is called a prime ideal if $P \neq R$ and for any ideals A, B in R, one has that $A * B \subset P$ implies $A \subset P$ or $B \subset P$, where $A * B = \{x \in R \mid x = a * b,\ a \in A \text{ and } b \in B\}$.

Prime Ideals for Commutative Rings

Let R be a ring. If P is an ideal in R such that $P \neq R$ and for all $a, b \in R$ it holds that

$$a * b \in P \Rightarrow a \in P \text{ or } b \in P \tag{1}$$

then P is prime. Reciprocally, if P is a prime ideal in R and R is a commutative ring then P satisfies the Condition (1).

Theory `rings`: other relevant formalizations

Prime Ideals for Rings with Identity

Let R be a commutative ring with identity $one_R \neq zero_R$. An ideal P in R is prime iff the quotient ring R/P is an integral domain.

Theory `rings`: other relevant formalizations

Maximal ideals

An ideal M in a ring R is said to be maximal if $M \neq R$ and for any ideal N in R such that $M \subset N \subset R$ either $N = M$ or $N = R$.

Maximal Ideals in Idempotent Commutative Rings

If R is a commutative ring such that $R * R = R$ and M is a maximal ideal in R then M is a prime ideal.

Maximal Ideals and Quotient Rings

Consider M an ideal in a ring with identity R.

1. If R is a commutative ring and M is a maximal ideal then the quotient ring R/M is a field;
2. If the quotient ring R/M is a division ring then M is a maximal ideal.

Future developments

(i) Formalization of the correlation between: (a) fields; (b) no existence of maximal and proper ideals; (c) monomorphisms;

(ii) Development of *subtheories* about factorization in commutative rings;

(iii) Development of *subtheories* about ring of polynomials.

References I

- Suárez, Y.G., Torres, E., Pereira, O., Pérez, C., Rodríguez, R.: Application of the ring theory in the segmentation of digital images. International Journal of Soft Computing, Mathematics and Control **3**(4) (2014)
- Bini, G., Flamini, F.: Finite commutative rings and their applications, vol. 680. Springer Science & Business Media (2012)
- Lidl, R., Niederreiter, H.: Introduction to finite fields and their applications. Cambridge University Press, Cambridge (1994)
- Hungerford, T.W.: Algebra, Graduate Texts in Mathematics, vol. 73. Springer-Verlag, New York-Berlin (1980), reprint of the 1974 original
- Artin, M.: Algebra. Pearson, 2 edn. (Aug 2010)
- Dummit, D.S., Foote, R.M.: Abstract Algebra. Wiley, 3 edn. (Jul 2003)
- Herstein, I.N.: Topics in algebra. Xerox College Publishing, Lexington, Mass.-Toronto, Ont., 2 edn. (1975)

References II

Andréia Borges Avelar and André Luiz Galdino and Flávio Leonardo Cavalcanti de Moura and Mauricio Ayala-Rincón. First-order unification in the PVS proof assistant. Logic Journal of the IGPL, v.22, n.5, pag. 758–789, (2014)

Ricky Butler and David Lester. A PVS *Theory* for Abstract Algebra. Nasa Langley Research Center (2007) Available at: http://shemesh.larc.nasa.gov/fm/ftp/larc/PVS-library/pvslib.html (Accessed in September 27, 2019)

Andréia B. Avelar da Silva and Thaynara Arielly de Lima and André Luiz Galdino. Formalizing Ring Theory in PVS. Interactive Theorem Proving - 9th International Conference, ITP 2018, pag. 40–47 (2018)