Formalizing Ring Theory in PVS

Andréia B. Avelar da Silva[1](✉), Thaynara Arielly de Lima[2],
and André Luiz Galdino[3]

[1] Faculdade de Planaltina, Universidade de Brasília, Brasília D.F., Brazil
andreiaavelar@unb.br

[2] Instituto de Matemática e Estatística, Universidade Federal de Goiás,
Goiânia, Brazil
thaynaradelima@ufg.br

[3] Unidade Acadêmica Especial de Matemática e Tecnologia,
Universidade Federal de Goiás, Catalão, Brazil
andre_galdino@ufg.br

Abstract. This work describes the ongoing specification and formalization in the PVS proof assistant of some definitions and theorems of ring theory in abstract algebra, and briefly presents some of the results intended to be formalized. So far, some important theorems from ring theory were specified and formally proved, like the First Isomorphism Theorem, the Binomial Theorem and the lemma establishing that every finite integral domain with cardinality greater than one is a field. The goal of the project in progress is to specify and formalize in PVS the main theorems from ring theory presented in undergraduate textbooks of abstract algebra, but in the short term the authors intended to formalize: (i) the Second and the Third Isomorphism Theorems for rings; (ii) the primality of the characteristic of a ring without zero divisors; (iii) definitions of prime and maximal ideals and theorems related with those concepts. The developed formalization applies mainly a part of the NASA PVS library for abstract algebra specified in the *theory* `algebra`.

1 Introduction

Ring theory has a wide range of applications in the most varied fields of knowledge. According to [18], the segmentation of digital images becomes more efficiently automated by applying the $\mathbb{Z}_n$ ring to obtain index of similarity between images. Furthermore, according to [3] finite commutative rings has an important role in areas like combinatorics, analysis of algorithms, algebraic cryptography and coding theory. In particular in coding theory, finite fields (which are commutative rings with unity) and polynomials over finite fields has been widely applied in description of redundant codes [16].

Andréia B. Avelar da Silva was partially supported by District Federal Research Foundation - FAPDF.

J. Avigad and A. Mahboubi (Eds.): ITP 2018, LNCS 10895, pp. 40–47, 2018.
https://doi.org/10.1007/978-3-319-94821-8_3

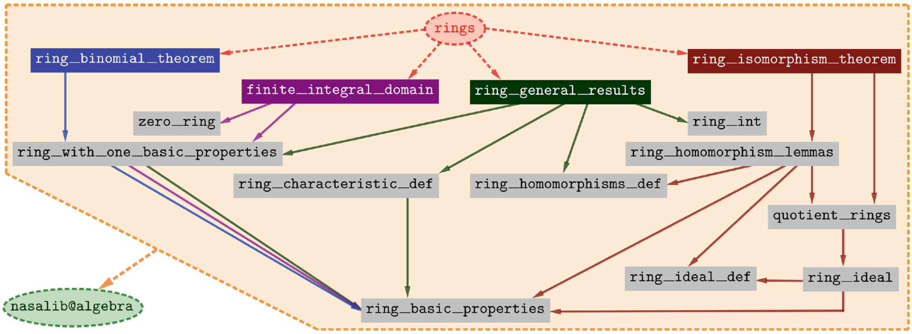

Fig. 1. Hierarchy of the PVS *theory* `rings`, which imports the *theory* `algebra` from *nasalib*. The four main branches developed so far are highlighted.

The authors has the project that consists in to formalize in the PVS proof assistant the basic theory for rings presented in undergraduate textbooks of abstract algebra. This 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 in Sect. 2. The PVS is a specification and verification system which provides an integrated environment for development and analysis of formal specifications. An important and well-known library for PVS is the NASA PVS Library[1] (*nasalib*) that contains many *theories* in several subjects, like analysis [5], topology [15], term rewriting systems [8], among others. In particular, a formal verification for basic abstract algebra is part of *nasalib*, in the *theory* `algebra` [4], where basic concepts about groups, rings and fields were specified. However the content of the *theory* `algebra`, for instance about rings, is essentially definitions and basic results obtained from such definitions. To the best knowledge of the authors, the only formalization involving rings in PVS is the *theory* `algebra`. The project proposed by the authors was motivated by the wish to contribute with the enrichment of mathematics formalizations in the available PVS libraries, by formalizing non basic results about rings that are not in *nasalib*.

The main contributions presented in this paper consist in the formalization of important theorems such that the First Isomorphism Theorem, the Binomial Theorem for rings and the result establishing that every finite integral domain with cardinality greater than one is a field. Furthermore, important concepts and lemmas from *nasalib theories* and `prelude` (the native library of PVS which contains a collection of theories about functions, sets, predicates, logic, numbers, among others) were generalized in order to build the ongoing *theory* `rings`. The present formalization follows the approach of the textbooks [2,7,11,12], but mainly the Hungerford textbook [12].

[1] Available at https://shemesh.larc.nasa.gov/fm/ftp/larc/PVS-library/.

2 The *theory* rings: Formalized so Far

In this section it will be described the collection of definitions, lemmas and theorems specified and formalized in the main *theory* rings. These results range from basic properties for rings, like an alternative characterization for subrings, to nontrivial formalizations, like the formalization of the classical First Isomorphism Theorem for rings.

```
subring_equiv: LEMMA
 subring?(S,R) IFF nonempty?(S) AND subset?(S,R)
 AND (FORALL (x,y:(S)):
      member(x-y,S) AND member(x*y,S))

R_sigma(low,high,F): Recursive T =
 IF low > high THEN zero ELSIF high = low
  THEN F(low) ELSE R_sigma(low,high-1,F)+F(high)
 ENDIF MEASURE abs(high+1-low)

left_zd?(x: nz_T): bool =
 EXISTS (y:nz_T): x*y = zero

nlzd: TYPE = {x:T | x = zero OR NOT left_zd?(x)}

nzd_cancel_left: LEMMA FORALL (a:nlzd, b,c:T):
 a*b = a*c IMPLIES (a = zero OR b = c)
----------------------------------------------
R_homomorphism?(R1,R2)(phi:[(R1)->(R2)]): bool =
 FORALL(a,b:(R1)):phi(s1(a,b))=s2(phi(a),phi(b))
             AND phi(p1(a,b))=p2(phi(a),phi(b))

R_monomorphism?(R1,R2)(phi:[(R1)->(R2)]): bool =
 injective?(phi) AND R_homomorphism?(R1,R2)(phi)

R_epimorphism?(R1,R2)(phi:[(R1)->(R2)]): bool =
surjective?(phi) AND R_homomorphism?(R1,R2)(phi)

R_isomorphism?(R1,R2)(phi:[(R1)->(R2)]): bool =
 R_monomorphism?(R1,R2)(phi)
 AND R_epimorphism?(R1,R2)(phi)

R_kernel(R1,R2)(phi: R_homomorphism(R1,R2)):
 subgroup[T1,s1,zero1](R1) = kernel(R1,R2)(phi)
----------------------------------------------
multiple_char: LEMMA
 (EXISTS (m:int): k = m * charac(R))
 IFF (FORALL (x:(R)): times(x, k) = zero)

char_1_zero_ring: LEMMA
 charac(R) = 1 IFF R = singleton(zero)
----------------------------------------------
power_commute: LEMMA x*y = y*x IMPLIES
 power(x,m)*power(y,i) = power(y,i)*power(x,m)

gen_times_int_one: LEMMA times(one,k) = zero
 IMPLIES times(x, k) = zero
```

Fig. 2. Highlighted specifications in the *subtheories* ring_basic_properties, ring_homomorphisms_def, ring_characteristic_def and ring_with_one_basic_properties.

The current state of formalization of the PVS *theory* rings, proposed by the authors, consists of some *subtheories* divided in four main branches (Fig. 1), each one dedicated to formalize lemmas involving: (i) characteristic of rings and rings with one; (ii) finite integral domain; (iii) Binomial Theorem for rings; (iv) homomorphism of rings. Those branches will be described in the following subsections. The basis of the development is constituted by some *subtheories* for fundamental definitions and results regarding ring theory, namely:

ring_basic_properties: This *subtheory* contains basic results about rings not specified in the *theory* algebra. The main contributions of this *subtheory* are: (i) An alternative characterization for subrings, Lemma subring_equiv (Fig. 2); (ii) The formalization of the recursive Function R_sigma that performs a summation of elements of arbitrary types and its properties (Fig. 2). In order to ensure its totality it was necessary to provide a decreasing measure applied to prove the TCC's (type correctness conditions - lemmas automatically generated by the prover during the process of type checking) for termination. Such function generalizes the summation of reals defined in the *nasalib theory* reals; and

(iii) The definition of a non zero divisor element type, necessary in the formalization of a more general cancellation law that holds in an arbitrary ring since the cancelled element has the non zero divisor type (Fig. 2).

ring_ideal_def: The concepts of left and right ideal, as well as the type ideal of a ring were established.

ring_homomorphisms_def: Such *subtheory* contains the definition of homomorphism of rings and its variants: injective, surjective and bijective homomorphism. In addition, the kernel of a homomorphism of rings (Fig. 2) is defined from the kernel of a homomorphism of groups specified in the *theory* algebra.

ring_characteristic_def: The specification of the notion of characteristic of a ring and basic results were established. Two lemmas deserve to be highlighted: multiple_char and char_1_zero_ring (Fig. 2). The former is a characterization of multiples of the characteristic of a ring, and the latter states the characteristic of the zero ring as being the integer 1.

ring_with_one_basic_properties: In this *subtheory* one has two important results, power_commute and gen_times_int_one (Fig. 2), to formalize a version of the Binomial Theorem for rings and properties involving characteristic of a ring.

Note that, in some specified lemmas in Fig. 2, the universal quantifier on free variables is implicit. This is possible because the PVS syntax allows one to declare free variables anywhere in the specification file before lemmas, functions and definitions that use those variables. Furthermore, it is possible to use a set inside parentheses to denote the type of its elements.

2.1 The *subtheory* ring_general_results

The main result in this branch consists in to determine the kernel of the homomorphism from the ring of integers to a ring R, illustrated in the Lemma homomorphism_Z_to_R (Fig. 3), as the set of multiples of the characteristic of the ring R. Its proof follows from the Lemmas gen_times_int_one and multiple_char, respectively.

It is intended to extend this *subtheory* establishing results about, for instance, the characteristic of non zero divisor rings and, in particular, of integral domains.

```
homomorphism_Z_to_R: LEMMA
 charac(R) > 0 IMPLIES
 (LET phi:[(fullset[int])->(R)] =
   (LAMBDA (m:int): times(one, m)) IN
  R_homomorphism?(fullset[int],R)(phi) AND
  R_kernel(fullset[int],R)(phi)
  ={x:int | EXISTS (k:int): x = k*charac(R)})
------------------------------------------------
R_bino_theo: LEMMA
 FORALL(x,y:(R)): x*y = y*x IMPLIES
  power(x+y,n) = R_sigma(0,n,F_bino(n,x,y))

F_bino(n,x,y): [nat -> T] = LAMBDA k:
 IF k > n THEN zero ELSE
 times(power(x,k)*power(y,n-k),C(n,k)) ENDIF
```

Fig. 3. Highlighted specifications in the *subtheories* ring_general_results and ring_binomial_theorem.

2.2 The *subtheory* finite_integral_domain

The *subtheory* finite_integral_domain extends the *subtheory* integral_domain from algebra. The most important theorem states that every finite integral domain with cardinality greater than 1 is a field. The formalization follows the approach in [11]. However, it is important to remark that in [11] a necessary hypothesis is omitted, since the author does not require that the cardinality of the finite integral domain is greater than 1, and the lack of this requirement makes the formal proof unachievable, once in this case the zero ring must be consider and obviously such integral domain is not a field.

Also, in this *subtheory* it was necessary to formalize a result generalizing the pigeonhole principle for an arbitrary set with elements of an arbitrary type, since the pigeonhole principle in the `prelude` is restricted to subsets of $\mathbb{N}$.

2.3 The *subtheory* `ring_binomial_theorem`

From the recursive Function `R_sigma` in `ring_basic_properties` and its properties and the Lemma `power_commute` in `ring_with_one_basic_properties` one can formally prove the Binomial Theorem for rings `R_bino_theo` (Fig. 3), where $\texttt{F\_bino}(n,x,y) = \binom{n}{k} \cdot x^k y^{n-k}$.

```
ideal_is_normal_subgroup: LEMMA
   ideal?(I,R) IMPLIES normal_subgroup?(I,R)
---------------------------------------------
cosets(R:ring,I:ideal(R)):TYPE
 = left_cosets(R,I)

add(R:ring,I:ideal(R)):
[cosets(R,I),cosets(R,I)->cosets(R,I)]
 = mult(R,I)

product(R:ring, I:ideal(R))
(A,B: cosets(R,I)):cosets(R,I) =
       lc_gen(R,I,A)*lc_gen(R,I,B) + I

ring_cosets: LEMMA FORALL(R:ring,I:ideal(R)):
 ring?[cosets(R,I),add(R,I),product(R,I),I]
 ({s:cosets(R,I) | EXISTS (a:(R)):s = a+I})
---------------------------------------------
image_homo_is_subring: LEMMA
 FORALL (phi: R_homomorphism(R1,R2)):
   subring?(image(phi)(R1),R2)

monomorphism_charac: LEMMA
 FORALL (phi: R_homomorphism(R1,R2)):
   R_monomorphism?(R1,R2)(phi) IFF
   R_kernel(R1,R2)(phi) = singleton(zero1))

kernel_homo_is_ideal: LEMMA
 FORALL (phi: R_homomorphism(R1,R2)):
   ideal?(R_kernel(R1,R2)(phi),R1)
---------------------------------------------
first_isomorphism_th: THEOREM
FORALL(phi: R_homomorphism(R,S)):
 R_isomorphic?[cosets(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]
   (/[T,+,*,zero]
    (R,R_kernel(R,S)(phi)),image(phi)(R))
```

Fig. 4. Highlighted specifications in the *subtheories* `ring_ideal`, `quotient_ring`, `ring_homomorphism_lemmas` and `ring_isomorphism_theorems`.

2.4 The *subtheory* `ring_isomorphism_theorems`

The *subtheory* `ring_isomorphism_theorems` is the more elaborated one among the four highlighted *subtheories* in Fig. 1. At this point, the most important lemma of such *subtheory* is the First Isomorphism Theorem for rings. In order to formalize the results in `ring_isomorphism_theorems` relevant notions related with ideals, quotient rings and homomorphisms of rings were specified in the *subtheories*:

`ring_ideal`: The main lemma formalized in this *subtheory* states that the ideal of ring is a normal subgroup (Fig. 4). This result was strongly applied to verify the TCC's in the *subtheory* `ring_isomorphism_theorems`, generated from the specification of quotient rings, in the *subtheory* `quotient_ring`, which in turn imports the *subtheory* `factor_groups` from the *theory* `algebra`, where it is required that the type of the parameters in the quotient of groups has to be a group G and a normal subgroup of G.

`quotient_rings`: The algebra of quotient rings is builded by specifying the type `cosets` and defining the operations of addition, `add`, and multiplication, `product`, between two cosets (Fig. 4). From that it was formalized that the structure `(cosets(R,I),add(R,I),product(R,I),I)` (Fig. 4) is a ring, where `R` is a ring and `I` is an ideal of `R`.

`ring_homomorphism_lemmas`: Classical results were formalized, such as, given a function $\phi : R \to S$ from a ring $(R, +_R, *_R, e_R)$ to a ring $(S, +_S, *_S, e_S)$, if ϕ is a homomorphism then: (i) the kernel of ϕ, denoted as $ker(\phi)$, is an ideal of R; (ii) the image of ϕ is a subring of S; and (iii) ϕ is a monomorphism iff the kernel of ϕ is the set $ker(\phi) = \{e_R\}$ (Fig. 4).

Additionally, in order to formalize the First Isomorphism Theorem (Theorem 1), whose specification is in Fig. 4 (Theorem `first_isomorphism_th`), it was necessary to specify and prove, in the *subtheory* `ring_isomorphism_theorems`, other six auxiliary lemmas corresponding to the Lemma 1.

Lemma 1. *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 there is a unique homomorphism of rings $f : R/I \to S$ such that $f(a + I) = \phi(a)$ for all $a \in R$. The image of f is equal to the image of ϕ and $ker(f) = ker(\phi)/I$. f is an isomorphism if and only if ϕ is an epimorphism and $ker(\phi) = I$.*

Theorem 1 (First Isomorphism Theorem). *If $\phi : R \to S$ is a homomorphism of rings then ϕ induces an isomorphism of rings from $R/ker(\phi)$ to the image of ϕ.*

3 Related Work

In the literature, abstract algebra formalizations are available. In Coq results about groups, rings and ordered fields were formalized as part of the FTA project [9]. Also in Coq, [6] presents a formalization of rings with explicit divisibility. In Nuprl and in Mizar it is provided a formal proof of the Binomial Theorem for rings, [13,17] respectively. In ACL2 it is builded a hierarchy of algebraic structures ranging from setoids to vector spaces focused on the verification of computer algebra systems [10]. The Algebra Library of Isabelle/HOL [1] presents an interesting collection of results in the algebraic hierarchy of rings, mainly about groups, factorization over ideals, ring of integers and polynomial ring. To the best of the authors knowledge, only in Mizar it was formalized the First Isomorphism Theorem for rings [14]. However, the Mizar formalization differs from the one presented in this paper in the sense that Mizar is a system of first order set theory whereas PVS is a higher order logic system.

4 Conclusions and Future Work

The formalization presented in this paper shows the beginning of a project where it is planned to develop in PVS the specification and formal verification of the main theorems from ring theory. Some important theorems were formalized, as well as several auxiliary results necessary to complete the current formalization (Sect. 2). In numbers the *theory* `rings` consists of 141 proved formulas, from which 68 are TCC's. The specification files have together 1134 lines and their size is 64 KB; the proof files have 17503 lines and 1.2 MB.

The next step would be the formalization of: (i) the Second and the Third Isomorphism Theorems; (ii) the Correspondence Theorem for rings; (iii) a theorem establishing the primality of the characteristic of a ring without zero divisors, in particular of a integral domain; (iv) definitions of prime and maximal ideals and theorems related with those concepts, as for example the equivalence between fields and the non existence of a proper ideal in commutative rings with one.

Ring theory has a number of applications, for example, coding theory, segmentation of digital images, cryptography, among others. In this sense, this formalization forms a basis for future formal verifications of more elaborated *theories* involving rings and their properties.

References

1. Aransay, J., Ballarin, C., Hohe, S., Kammüller, F., Paulson, L.C.: The Isabelle/HOL Algebra Library. Technical report, University of Cambridge - Computer Laboratory, October 2017. http://isabelle.in.tum.de/library/HOL/HOL-Algebra/document.pdf
2. Artin, M.: Algebra, 2nd edn. Pearson, Upper Saddle River (2010)
3. Bini, G., Flamini, F.: Finite commutative rings and their applications, vol. 680. Springer Science & Business Media (2012)
4. Butler, R., Lester, D.: A PVS Theory for Abstract Algebra (2007). http://shemesh.larc.nasa.gov/fm/ftp/larc/PVS-library/pvslib.html. Accessed 22 Jan 2018
5. Butler, R.W.: Formalization of the integral calculus in the PVS theorem prover. J. Formalized Reasoning **2**(1), 1–26 (2009)
6. Cano, G., Cohen, C., Dénès, M., Mörtberg, A., Siles, V.: Formalized linear algebra over elementary divisor rings in coq. Logical Meth. Comput. Sci. **12**(2), Jun 2016
7. Dummit, D.S., Foote, R.M.: Abstract Algebra, 3rd edn. Wiley, New York (2003)
8. Galdino, A.L., Ayala-Rincón, M.: A PVS theory for term rewriting systems. Electron. Notes Theoret. Comput. Sci. **247**, 67–83 (2009)
9. Geuvers, H., Pollack, R., Wiedijk, F., Zwanenburg, J.: A constructive algebraic hierarchy in coq. J. Symbolic Comput. **34**(4), 271–286 (2002)
10. Heras, J., Martín-Mateos, F.J., Pascual, V.: Modelling algebraic structures and morphisms in acl2. Appl. Algebra Eng. Commun. Comput. **26**(3), 277–303 (2015)
11. Herstein, I.N.: Topics in Algebra, 2nd edn. Xerox College Publishing, Lexington (1975)
12. Hungerford, T.W.: Algebra, Graduate Texts in Mathematics, vol. 73. Springer-Verlag, New York-Berlin (1980)
13. Jackson, P.B.: Enhancing the Nuprl Proof Development System and Applying it to Computational Abstract Algebra. Ph.D. thesis, Cornell University (1995)

14. Kornilowicz, A., Schwarzweller, C.: The first isomorphism theorem and other properties of rings. Formalized Math. **22**(4), 291–301 (2014)
15. Lester, D.: A PVS Theory for Continuity, Homeomorphisms, Connected and Compact Spaces, Borel sets/functions (2009). http://shemesh.larc.nasa.gov/fm/ftp/larc/PVS-library/pvslib.html. Accessed 22 Jan 2018
16. Lidl, R., Niederreiter, H.: Introduction to finite fields and their applications. Cambridge University Press, Cambridge (1994)
17. Schwarzweller, C.: The binomial theorem for algebraic structures. Formalized Math. **09**(3), 559–564 (2001)
18. Suárez, Y.G., Torres, E., Pereira, O., Pérez, C., Rodríguez, R.: Application of the ring theory in the segmentation of digital images. Int. J. Soft Comput. Math. Control **3**(4) (2014)