Ring theory is formalized in PVS using the Isomorphism, Principal, Prime and Maximal Ideals Theorems

S V R SEKHAR REDDY
S V R Sekhar Reddy, Department of Mathematics, Government Degree College, Atmakur, Nandyal (Dist.) AP, India.

Abstract: **Key findings from ring theory are developed PVS in this paper. The PVS theory provides characterizations of the main, prime, and maximal ideals and full proofs of the three classical isomorphism theorems for rings. It is possible to apply algebraic concepts and qualities to other algebraic structures since they are expressed and defined in the widest possible sense. The components required to codify significant algebraic theorems are included in the development.**

Key words: - **Isomorphism theorems, Maximal ideals, Algebra and Prime ideals.**

1. INTRODUCTION

This work presents formalizations of the three isomorphism theorems for rings, characterizations of principal, prime and maximal ideals and a formal proof of the algebraic version of the Chinese remainder theorem developed in the Prototype Verification System (PVS). These developments belong to the PVS theory rings that specify and formalize notions and properties of rings as given in classical references on abstract algebra such as Hungerford's [1] textbooks. Indeed, Hungerford's textbook is the main reference for this formalization and the results about homomorphisms, prime, maximal and principal ideals follows the same presentation of this book [2].

Formalizing the theory of rings in PVS is mainly motivated by two reasons:

Firstly, ring theory has a wide range of applications in several fields of knowledge. For example, important areas such as combinatorics, algebraic cryptography and coding theory apply finite commutative rings. Regarding coding theory, commutative rings with identity and polynomials over such structures have an important role to describe redundant codes [3]. Also, ring theory forms the basis for algebraic geometry, which has applications in engineering systems, statistics, modeling of biological processes and computer algebra [4]. Other relevant application of ring theory is in the analysis of images. If the images are considered as a matrix whose elements belong to the ring Z*n*, properties about restoration and segmentation of images and detection of contours can be competently described [5] showed that the segmentation of digital images becomes more efficiently automated by applying the Z*n* to obtain index of similarity between images. Thus, a formalization of the main results of ring theory would make possible the formal verification of more complex theories involving rings in their scope.

Secondly, fully formalizing the theory of rings contributes to the enrichment of libraries of mathematics in PVS. An important and well-known library for PVS is the NASA PVS Library1 (*nasalib*) that contains many theories in several subjects, such as analysis [6], topology [7] and term rewriting systems [8]. In particular, *nasalib* contains the theory algebra [9], where basic concepts and properties about groups, rings and fields were formalized. However, the contents of the theory algebra about rings were restricted to definitions and just basic results obtained from such definitions. The first steps to enrich the theory algebra gave rise to the theory rings and initially included elaborated formalizations such as the binomial theorem for rings, a result establishing that every finite integral domain with cardinality greater than one is a field (i.e., commutative division ring or skew field) and the first isomorphism theorem, as shortly reported by three of the authors [10]. In such work, homomorphisms and cosets were separately defined in the particular context of rings and ideals in order to extend the previous specification of such concepts

given in the theory algebra [9] for groups and normal subgroups. To the best of our knowledge, the only formalizations on rings in PVS are in the theories algebra of *nasalib* and in the theory rings.

PVS is a proof assistant with a core logic that is based on classical higher-order logic, and that embeds the power of sub typing and dependent typing. Specifications in PVS are functional, and the PVS proof engine follows a Gentzen's sequent calculus style. The higher order features of PVS are adequate for specifying theorems about properties and relations, such as morphisms, quotients and ideals that appear naturally in the study of algebraic structures such as groups, rings and fields. As a proof assistant based on classical logic, PVS includes the law of excluded middle, and the PVS core logic includes, in its prelude, the axiom of choice. The development of the theory rings as well as the whole theory algebra does not include any axioms other than those provided as part of the core logic of PVS. The semantics of PVS and the relations between PVS proof commands and deductive rules can be consulted, respectively [11]. This paper discusses all necessary details about PVS required for understanding the description of the theory rings.

The main contributions of this work are listed below.

(i) Formalization of preliminary concepts on algebraic structures in a manner that allows their use in general contexts involving structures different from rings. The entire sub theories of the theory rings [12] related to homomorphisms cosets and quotient rings as well as the formalization of the first isomorphism theorem were restructured. In this work, homomorphisms are specified for groupoids [13], which are denoted with the name groupoids in the theory algebra, and cosets for arbitrary sets. Besides making the specification of the three isomorphism theorems clearer and proof obligations easier, the new specifications of homomorphisms and cosets could be applied to other structures than rings and groups.
(ii) Formalization of the three isomorphism theorems for rings that are classical landmarks in abstract algebra.
(iii) Formalization of definitions and properties about principal, maximal and prime ideals. Correctness of an algebraic description of the elements of a principal ideal is proved. Furthermore, alternative characterizations of prime and maximal ideals are provided: Prime ideals in a commutative ring are characterized by an algebraic condition on their elements, and prime and maximal ideals in commutative rings with identity are characterized by quotient rings.

2. FORMALIZATION OF MORPHISMS AND BASIC ALGEBRAIC STRUCTURES

In this section, the PVS sub theories of rings and related to specification and formalization of morphisms and basic algebraic notions such as cosets, ideals, kernel and quotient are presented.

2.1 Formalization of Homomorphisms

The concept of ring homomorphism is the core of the theory for isomorphism theorems. The required definitions and properties about homomorphisms were formalized in the sub theories homomorphisms_def, ring_homomorphisms_def and ring_homomorphism_lemmas. Particularly, the sub theory homomorphisms_def presents an interesting contribution, once the definition of homomorphism was formalized for closed sets under a specific operation. This is a more general PVS formalization about homomorphisms of algebraic structures than the one given in the theory algebra of *nasalib*. In the sub theory ring_homomorphisms_def, the concept of homomorphism was extended in order to make feasible its use in a context of rings and the sub theory ring_homomorphism_lemmas brings the formalization of classical results involving ring homomorphisms.

2.2 Sub theory homomorphisms_def

Before the development of the theory rings [13], the only specification in PVS of homomorphism for algebraic structures was available in sub theory homomorphisms of the theory algebra [9] (see Specification 1).

Specification 1 Homomorphism for groups – sub theory nasalib/algebra@homomorphisms

```
homomorphism?(G1: group[T1,*,one1], G2: group[T2,o,one2],
phi: [(G1) -> (G2)]): bool =
(FORALL (a,b: (G1)): phi(a*b) = phi(a) o phi(b))
```

The parameters of a group are a non-empty type T, a binary operator *: [T, T-> T], and a constant of type

T. Thus, in the specification above G1 and G2 are groups of respective types group [T1,*, one1] and group[T2,o,one2] over the respective types T1 and T2, and with their associated binary operators and constants. In this specification, a function phi of type [(G1) -> (G2)], that is a function from G1 to G2, is an homomorphism, i.e., satisfying the predicate homomorphism?, whenever FORALL (a,b: (G1)): phi(a*b) = phi(a) o phi(b) holds. From this, the property phi(one1) = one2 can be inferred. Observe that this specification is specialized for groups. Two situations arise from this particular choice to formalize the notion of homomorphism:

(i) Obviously, such definition makes sense only in a context dealing with groups;
(ii) If such specification is used to describe a homomorphism $\phi : G \rightarrow H$, as proof obligations generated from the type checking, it is necessary to verify that *G* and *H* are groups. In other words, one must check that *G* and *H* are closed under specific operations and the associative law holds, a neutral element for such operations belongs to *G* and *H* and every element of *G* and *H* has an inverse. PVS generates proof obligations, called type correctness conditions (TCCs), related to the well-definedness property of functions and predicates and the termination of functional specifications. The TCCs are specified by static analysis as proof obligations that, when cannot be proved automatically, have to be verified manually. In the new approach, as shown in the code in Specification 2, a more general definition of homomorphism was specified in the sub theory homomorphisms_def for groupoids.

Specification 2 Specification of homomorphism in the sub theory homomorphisms_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))
```

Specification 2 requires that *R* and *S* be groupoids, declared as variables, specified as VAR in PVS, of respective types (groupoid?[T,s]) and (groupoid?[U, p]). A groupoid $(G, *)$ is just a non-empty set *G* closed under the binary operation $*$. Consequently, the specification of homomorphism developed in homomorphisms_def can be used in contexts involving monoids, semigroups, groups, rings, fields or any other one that deal with a structure containing a non-empty set satisfying the closure property for some operation. In this way, this choice results more adaptable and malleable than the one specialized for groups and available in nasalib/algebra@homomorphisms. Furthermore, the proof obligations generated by the new specification of homomorphism are easier to check, since verifying whether a structure is a groupoid has a much lower cost than checking whether the structure is a group. For structures as rings with two operators over the same type (typically, for multiplication and addition), this specification of homomorphism is used twice to guarantee that the (homomorphism) property holds for both operators.

Furthermore, classical results were formally proved in this sub theory, among them:
– if $\phi : R \rightarrow S$ is a ring homomorphism and *x* is an element of *R*, then ϕ(zero *R)* = zeros and $\phi(inv(x)) = inv(\phi(x))$,
Where *inv(x)* denotes the inverse of the element *x* according to the operation +*R*;
– the image of a ring homomorphism is a ring;
– the kernel of a homomorphism is an ideal;
– the characterization of an injective homomorphism ϕ is based on $ker(\phi)$.

3.2 Formalization of Basic Algebraic Structures
Quotient rings are the main structures involved in the isomorphism theorems, besides that they are involved in results that provide alternative characterizations of prime and maximal ideals. However, the construction of quotient rings depends on other objects such as ideals and cosets. The next subsections present these algebraic structures and formalizations of their properties.

3.2.1 Sub theory cosets_def

Let T be a non-interpreted type that is any abstract type, and let *G*, *H* and *I* be sets provided of a binary operation +, whose elements have the same non-interpreted type T. Furthermore, let *g* be an arbitrary element of type T. In the sub theory cosets_def, the sets *g*+*H*, *H* +*g* and *H* + *I* were specified as +*(*g, H*)*, +*(*H, g*)* and sum*(*H, I*)*, respectively, as illustrated in Specification 3.

Specification 3 The sets *g* + *H*, *g* + *H* and *H* + *I*

```
+(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}

Since the elements of *H* and *I* have arbitrary types, the specification established as sum*(*H, I*)* can be used in the formalization of the second isomorphism theorem, where *H* is a subring and *I* is an ideal of a ring *R*, as well as in other contexts involving the sum or any other binary operation of two arbitrary structures containing elements of the same type. For example, the hypothesis *R∗ R = R* in Theorem 7 was specified as sum[T,*](R,R) = R. The sets *+(*g, H*)* and *+(*H, g*)* were used to specify the notion of cosets in a general way (see Specification 4). Also, generators of left and right cosets were defined as lc_gen(G,H)
and rc_gen(G,H). The use of the operator choose for specifying left and right coset generators requires proving proof obligations generated by type checking: None of the sets {a: T | G(a) AND A = a + H} and {a: T | G(a) AND
A = H + a} are empty sets. PVS proves automatically both these proof obligations by expanding the definitions of left_coset? and right_coset? and by skolemization.

Specification 4 Definition of cosets for arbitrary sets *G* and *H*

```
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)
lc_gen(G,H)(A:left_coset(G,H)) : T =
choose ({a: T | G(a) AND A = a + H})
rc_gen(G,H)(A:right_coset(G,H)) : T =
choose ({a: T | G(a) AND A = H + a})
```

In nasalib/algebra@cosets, one can find another specification of left and right cosets and cosets (see Specification 5). However, the formalization of cosets in the sub theory cosets_def has advantages in relation to that one since it is restricted to groups. Besides that, since cosets are defined over arbitrary types in cosets_def, in general, there are no proof obligations generated by type checking, whereas one must verify whether determined structure is a group, when the code in Specification 5 is considered.

Specification 5 Cosets in the context of groups in nasalib/algebra@cosets

```
left_coset(G:group ,H:subgroup(G))(a:(G)):
{s: set[T] | subset ?(s,G)} = a*H
```

3.2.2 Ideals

Ideals have a similar role for ring theory as normal subgroups have for group theory and a quotient ring *R/I* is well defined when one considers the left cosets of a ring *R* modulo an ideal *I* in *R* under specific operations, which shows that ideals are important structures to establish quotient rings. The sub theory ring_ideal_def brings the specification of the definition of ideals as shown in Specification 6.

Specification 6 Definition of ideals

```
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)
```

Several properties of ideals were formalized in the sub theory ring_ideal, among them those given in Specification 7.

Specification 10 Properties of ideals

```
R: VAR ring
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)
```

The lemma ideal_equiv provides a simpler characterization of ideals that is applied in the proofs of lemmas such as intersection_subring_ideal and ideal_transitive as well as in other proofs where it is required to show that
some structure is an ideal. Both the lemmas intersection_subring_ideal and ideal_transitive are crucial for checking proof obligations generated from the second isomorphism theorem, where it is required a quotient ring involving the intersection between a sub ring *H* and an ideal *I* in a ring *R*. The variable R is declared as a ring in both Specifications 6 and 7 . In the former, it is declared as a variable of type (ring?) that is defined in the PVS sub theory algebra@ring_def as the Boolean below, whereas in the latter, it was defined as a variable of type ring that despite being equivalent to the type (ring?)is specified using this Boolean as ring: NONEMPTY_TYPE = (ring?) CONTAINING fullset[T] in the PVS sub theory algebra@ring.

3.2.4 Kernel of a Homomorphism

In the sub theory ring_homomorphisms_def, the kernel of a homomorphism ϕ between groupoids $R1$ and $R2$ was defined as the set of elements of $R1$ mapped into some element zero$R2$ of $R2$ by ϕ, as shown in Specification 8.

Specification 8 Kernel of a homomorphism

```
R_kernel(R1,R2)(phi: R_homomorphism(R1,R2)):
set[T1] =
{a:T1 | R1(a) AND R2(zero 2) AND phi(a) = zero
2}
```

In the sub theory ring_homomorphisms_def, since $R1$ and $R2$ are not necessarily rings, one must require that the neutral element exists for $+R2$, which is denoted as zero2 in Specification 8. But, in the sub theory ring_homomorphism_lemmas,
$R1$ and $R2$ were considered as rings, structures of the form $(R1{+}R1, *R1, zeroR1)$ and $(R2{,}{+}R2 , *R2 , zeroR2)$ and, as consequence of this, lemmas involving kernel were formally proved, among them:
– the kernel of a ring homomorphism $\phi : R1 \rightarrow R2$ is an ideal (and particularly a ring) in $R1$, and
– ϕ is a monomorphism if and only if the kernel of ϕ is the set {zero $R1$ }.

The assertion that the kernel is an ideal is used to prove that the isomorphism presented in the first isomorphism theorem is, in fact, a ring homomorphism, since the quotient R/I is a ring if R is a ring and I is an ideal in R.

3.2.5 Quotient Rings

Observing the isomorphism theorems for rings and the characterization of prime and maximal ideals as described in Theorems 1, 2, 3, 6 and 8, one can notice that quotient rings are relevant algebraic structures involved in such results. The algebra of quotient rings was specified in the sub theories cosets_def and product_coset_def, as shown in Specification 9, where in particular /(RI) is a prefix notation for R/I .

Specification 9 The algebraic structure quotient ring

```
R, I: VAR set[T]
lproduct(R,I)(A,B:left_coset(R,I)) : set[T]
= (lc_gen(R,I)(A) * lc_gen(R,I)(B)) + I
rproduct(R,I)(A,B:right_coset(R,I)) : set[T]
= I + (rc_gen(R,I)(A) * rc_gen(R,I)(B))
product(R,I)(A,B:coset(R,I)) : set[T] =
lproduct(R,I)(A,B)
add(R,I)(A,B:coset(R,I)) : set[T]
= (lc_gen(R,I)(A) + lc_gen(R,I)(B)) + I
/(R,I) : setof[set[T]] = {s:set[T] | coset ?(R,I)(s)}
```

In a context where A is a coset of an ideal I in a ring R, such as occurs in the sub theory quotient_rings, l product(R, I)(A) = r
Product (R,I)(A) holds since left and right cosets are the same (see Specification 9). where A is a coset of an ideal I in R. Other properties about quotient rings were formalized in the sub theories quotient_rings and quotient_rings_with_one, among them the ones presented below.
(i) A characterization of sum and product of cosets, denoted as add and product, respectively: if I is an ideal in a ring R and $A = a + I$ and $B = b + I$ are left cosets of I , then add$(A, B) = (a + b) + I$ and product$(A, B) = (a * b) + I$.
(ii) A proof that $(R/I$, add, product, $I)$ is a structure that is a ring, if I is an ideal in a ring R, and, in particular, that if R is commutative, then R/I is a commutative ring, and if R has an identity one R, then one $R + I$ is an identity of R/I . These assertions are crucial since the isomorphism theorems for rings ensure that there is a ring homomorphism between structures involving quotients.
(iii) A useful lemma to verify proof obligations generated by the third isomorphism theorem;

namely, if I and J are ideals of a ring R, then I/J is an ideal of R/J.
(iv) A lemma establishing that if R is a ring with identity one R and I is an ideal in R such that $I \_= R$, then $I \_=$ one $R + I$. This result is widely used in the formalization of Theorem 6 in order to guarantee that the quotient R/P has the identity one $R + P \_= P$ satisfying a required condition to ensure that R/P is an integral domain.

3. ISOMORPHISM THEOREMS FOR RINGS AND PROPERTIES OF IDEALS

The first subsection discusses the necessary background about the three isomorphism theorems for rings and the second subsection all the required background related to the properties formalized for principal, maximal and prime ideals.

3.1 Isomorphism Theorems for Rings

A ring is an algebraic structure described by a quadruple $(R,+R, *R,$ zero $R)$, where R is a non-empty set that is closed under the binary operations addition and multiplication, denoted, respectively, as $+R$ and $*R$, over R and contains a neutral additive element, namely the constant zero R. Furthermore, a ring is an Abelian group restricted to $(R,+ R,$ zero $R)$ and the associative law holds for the operation $*R$ as well as the right and left distributive laws of $*R$ over $+R$. If $x *R y = y *R x$ for all $x, y \in R$, then $(R+ R, *R,$ zero $R)$ is said to be a commutative ring. Furthermore, if R contains an element one R such that one $R *R x = x *R$ one $R = x$, then $(R+R, *R,$ zero $R,$ one $R)$ is called a ring with identity. More information about rings and other structures in abstract algebra, including those crucial for this formalization such as ideals, morphisms, kernel, cosets and quotients, can be found in the previous cited books [14, 2, 15, 1].

Basically, the isomorphism theorems for rings are results about homomorphisms between structures that are, in almost all cases, quotient rings. In the next paragraphs, the isomorphism theorems for rings will be enunciated in order to highlight the concepts and the algebraic structures involved in the formalization of such propositions. In the following, for simplicity, a ring $(R+ R, *R,$ zero $R)$ will be denoted by R and the subscripts of the operations will be omitted.

The first isomorphism theorem states that an arbitrary homomorphism from a ring R to a ring S induces an isomorphism between two specific rings, as presented below.

Theorem 1 (First Isomorphism Theorem) *If R and S are rings and ϕ: $R \rightarrow S$ is a homomorphism, then there is an isomorphism of rings from $R/ker(\phi)$ to the image of ϕ, where $ker(\phi)$ denotes the kernel of the ring homomorphism ϕ.*

The second isomorphism theorem deals with an isomorphism between two quotient rings involving intersection and sum of ideals, whereas the third isomorphism theorem is about an isomorphism between a quotient of quotient rings and another quotient ring.
Theorem 2 (Second Isomorphism Theorem) *Let H and I be a sub ring and an ideal in a ring R, respectively. There is an isomorphism between the rings $H/(H \cap I)$ and $(H + I)/I$, where $H + I = \{x \in R \mid x = h + i$, $h \in H$ and $i \in I\}$.*
Theorem 3 (Third Isomorphism Theorem) *Let J and I be ideals in a ring R. If $J \subset I$, then I/J is an ideal in R/J and there is an isomorphism of rings from $(R/J)/(I/J)$ to R/I .*

Theorems 1, 2 and 3 require some concepts and structures that deserve special mention, namely ring homomorphisms, kernel of a homomorphism, ideals in a ring and quotient rings R/I . A full formalization of the properties of these objects was necessary
in order to obtain the formalization of the isomorphism theorems for rings in PVS, as presented in the sub theories ring_1st_isomorphism_theorem and ring_2nd_3rd_isomorphism_theorems (see Fig. 1). The sub theories of the theory algebra that were relevant for the formalization of the isomorphism theorems are just groupoid_def and ring.

3.2 Principal, Prime and Maximal Ideals

Ideals are notable structures in ring theory since they play for rings a similar role as normal subgroups play for groups; for example, it is possible to characterize ideals as a kernel of a ring homomorphism. Formalizations of properties about principal, prime and maximal ideals are considered in this work.

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).

Essentially, *(a)* is the smallest ideal of *R* containing *a*. Theorem 4 provides an interesting characterization of principal ideals.

Theorem 4 (Principal Ideals) *Let R be a ring and a an element of R:*

(i) *the principal ideal (a) corresponds to the set* $\{r * a + a * s + n \cdot a + \_m\ i{=}1\ ri * a * si \mid r, s, ri, si \in R; m \in \mathrm{N} \setminus \{0\};\ n \in \mathrm{Z}\}$, *where* $n \cdot a$ *denotes n summands of a if* $n \geq 0$, *and n summands of* $-a$ *if* $n < 0$;
(ii) *if R is a commutative ring, then (a)* $= \{r * a + n \cdot a \mid r \in R;\ n \in \mathrm{Z}\}$;
(iii) *if R is a commutative ring and has an identity, then (a)* $= \{r * a\} = \{a * r\}$, *where* $r \in R$. An ideal *P* of a ring *R* is called a prime ideal if $P \_= R$, and for any ideals *A, B* in *R*, one has that $A * B \subset P$ implies $A \subset P$ or $B \subset P$, where $A * B = \{x \in R \mid x = a * b, a \in A$ and $b \in B\}$. Theorem 5 establishes a characterization of prime ideals for commutative rings.

Theorem 5 (Prime Ideals for Commutative Rings) *Let R be a ring, not necessarily commutative. If P is an ideal in R such that* $P \_= R$ *and for all* $a, b \in R$, *it holds that* $a * b \in P \Rightarrow a \in P$ *or* $b \in P$, (1) *then P is prime. Reciprocally, if P is a prime ideal in R and R is a commutative ring, then P satisfies condition* (1).
On the other hand, Theorem 6 provides a characterization of prime ideals with identity by a quotient ring.

Theorem 6 (Prime Ideals for Rings with Identity) *Let R be a commutative ring with identity one* $\_= zero$. *An ideal P in R is prime if and only if the quotient ring R/P is an integral domain.*

The concept of prime ideals is related to the notion of prime numbers in the set of integers Z. In fact, it is well known that $n\mathrm{Z} = \{n * z \mid n \in \mathrm{N};\ z \in \mathrm{Z}\}$ is an ideal in Z. Notice that if *n*Z is a prime ideal, then $n \_= 1$ (since $n\mathrm{Z} \_= \mathrm{Z}$) and, according to Theorem 5, whenever $a * b$ is an element of *n*Z, one has that *a* or *b* is a member of *n*Z. In other words, this means that if *n* divides $a * b$, then *n* divides *a* or *b*, whence *n*Z is a prime ideal if *n* is prime. Lastly, an ideal *M* in a ring *R* is said to be maximal if $M \_= R$ and for any ideal *N* in *R* such that $M \subset N \subset R$ either $N = M$, or $N = R$. Maximal ideals in commutative rings, under the condition stated in Theorem 7, are prime ideals.

Theorem 7 (Maximal Ideals in 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.*
Theorem 8 establishes a connection between maximal ideals and the nature of some quotient rings.

Theorem 8 (Maximal Ideals and Quotient Rings) *Consider an ideal M in a ring R with identity:*
(i) *If R is a commutative ring and M is a maximal ideal, then the quotient ring R/M is a field;*
(ii) *If the quotient ring R/M is a division ring (skew field), then M is a maximal ideal.*

Results of this sub section were formalized in sub theories of rings depicted in Fig. 2. Theorem 4 was formalized in the sub theories ring principal ideal (items (i) and (ii)) and ring_with_id_one_generator (item (iii)), and Theorems 5, 6, 7 and 8 were formalized in the sub theories ring_prime_ideal, ring_with_one_prime_ ideal, ring_maximal_ideal and ring_with_one_maximal_ideal, respectively. The sub theories of the theory algebra that are imported for the formalization of the properties on ideals discussed here are ring_with_one, integral_domain_def, field_def, ring, and ring_ nz_closed_def.

4. FORMALIZATION OF THE THREE ISOMORPHISM THEOREMS FOR RINGS

This section discusses the PVS sub theories of rings related to the three isomorphism theorems for rings. The sub theory ring_1st_isomorphism_theorem contains the formalization of the first isomorphism theorem as well as a series of auxiliary lemmas presented as items in Lemma 1.
Lemma 1 (Aux. lemma for the First Isomorphism Theorem) *If* $\varphi: R \rightarrow S$ *is a homomorphism of rings and I is an ideal of R, which is contained in the kernel of* φ, *then there is a homomorphism of rings f:* $R/I \rightarrow S$ *such that* $f(a + I) = \varphi(a)$ *for all* $a \in R$ *and:*
(i) *the image of f is equal to the image of* φ;
(ii) $ker(f) = ker(\varphi)/I$;
(iii) *f is an epimorphism iff* φ *is an epimorphism;*
(iv) f *is a monomorphism iff* $ker(\varphi) = I$;
(v) f *is an isomorphism iff* φ *is an epimorphism and* $ker(\varphi) = I$.
The formalization of Lemma 1 builds the homomorphism *f* as $f(a + I) = \varphi(a)$ explicitly and verifies that *f* is a well-defined function that satisfies

the definition of R_homomorphism. Items (i) and (ii) were obtained by proving equality of sets, whereas item (iii) was verified by the expansion of the definition of R_epimorphism. Item (ii) and the characterization of monomorphism from the kernel were used for proving item (iv). Lastly, one can obtain item (v) as a natural consequence of items (iii) and (iv). The first isomorphism theorem was given as shown in Specification 10, and roughly speaking, its formalization was obtained by considering the ideal $I = ker(\phi)$ in item (v) of Lemma 1.The first four parameters of R_isomorphic? in Specification 10 correspond to the type, the addition and multiplication and the neutral element for the addition of the quotient ring $R/ker(\phi)$, whereas the last four are the parameters for the image of ϕ that is a sub ring of S.

Specification 10 First Isomorphism Theorem for rings (Theorem 1)

```
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))
```

The sub theory ring_2nd_3rd_isomorphism_theorems brings the formalization of the second and third isomorphism theorems. An auxiliary lemma for each one of these theorems was required, as presented below.

Lemma 2 (Aux. lemma for the Second Isomorphism Theorem) *If H is a sub ring and I is an ideal of a ring R, then there is an epimorphism* $\phi: H \rightarrow (H+I)/I$ *such that ker* $(\phi) = H \cap I$.

Lemma 3 (Aux. lemma for the Third Isomorphism Theorem) *If I and J are ideals in a ring R and* $J \subset I$, *then there is an epimorphism* $\phi: R/J \rightarrow R/I$ *such that ker* $(\phi) = I/J$. The second and third isomorphism theorems, given in Specification 11, were formalized applying the first isomorphism theorem with Lemmas 2 and 3, respectively.

Specification 11 Second and Third Isomorphism Theorems for rings (Theorems 2 and 3)

```
second_isomorphism_th: THEOREM
subring ?(H,R) AND ideal ?(I,R) IMPLIES
R_isomorphic ?[ coset(H,intersection(H,I)),
add(H,intersection(H,I)),
product(H,intersection(H,I)),
intersection(H,I),coset(sum(H,I),I),
add(sum(H,I),I),product(sum(H,I),I),I]
(H/intersection(H,I), sum(H,I)/I)
third_isomorphism_th: THEOREM
(ideal ?(I,R) AND ideal ?(J,R) AND subset ?(J,I))
IMPLIES
R_isomorphic ?[ coset[coset(R,J),add(R,J)](R/J,I/J),
add[coset(R,J),add(R,J),
product(R,J)](R/J,I/J),
product[coset(R,J),add(R,J),
product(R,J)](R/J,I/J), I/J,
coset(R,I),add(R,I),product(R,I),I]
(/[ coset(R,J),add(R,J),product(R,J)](R/J,I/J),R/I)
```

5. FORMALIZATION OF PROPERTIES ABOUT IDEALS

In this section, the PVS sub theories of rings presented and related to formalizations about principal, prime and maximal ideals are discussed.

5.1 Ideals Generated by One Element

The sub theory ring_one_generator brings auxiliary lemmas to formalize, as described in the next three subsections, the alternative characterizations of principal and prime ideals as stated in Theorems 4 and 5 as well as the results about maximal ideals as described in Theorems 7 and 8 .

Specification 12 presents the main definitions of this sub theory, built from a specific element a of a ring R. The subset of R defined as the set of elements generated as $\{r * a + a * s + n \cdot a + \_m\ i{=}1\ ri * a * si \mid r, s, ri, si \in R; m \in \mathbb{N}\setminus\{0\}; n \in \mathbb{Z}\}$ is specified as one_gen(R)(a). It depends on two functions: (i) the recursive function R_sigma (low, high, F) that adds a number of high − low elements, which are determined by F : nat → T; and, (ii) F_one_gen(R,a,F,G), which performs the product on the left and right sides of a by members of R chosen by the functions F and G.

Specification 17 The set one_gen(R)(a) generated by the element a of a ring R

```
F_one_gen(R : ring , a : (R), F,G: [nat -> (R)]):
[nat -> (R)] = LAMBDA (i : nat) : F(i)*a*G(i)
one_gen(R)(a:(R)): set[(R)] =
```

```
{t: (R) | EXISTS (r,s: (R), n:int , F,G: [nat ->(R)], m:nat):
t = r*a+a*s+times(a,n) + R_sigma(0,m, F_one_gen(R,a,F,G))}
```

Among other properties, one_gen(R)(a) was proved to be an ideal of the ring *R*. Furthermore, if *R* is commutative or has an identity, simpler characterizations of one_gen(R)(a) were developed as the given in Specifications 13.

Specification 13 Properties about one_gen and a simpler characterization for one_gen(R)(a), when *R* is commutative

```
one_gen_is_ideal:LEMMA
FORALL(R: ring ,a:(R)): ideal ?(one_gen(R)(a),R)
commutative_one_gen(R)(a:(R)): set[(R)] =
{t: (R) | EXISTS (r:(R), n:int): t = r*a+times(a,n)}
commutative_one_gen_charac: LEMMA
FORALL(R:( commutative_ring?),a:(R)):
one_gen(R)(a) = commutative_one_gen(R)(a)
```

5.2 Principal Ideals

The sub theory concerning principal ideals, ring_principal_ideal_def that contains the definition of principal ideals from the family of ideals in a ring *R* containing a specific element $a \in R$, specified as fam_ideal(R:(ring?))(a:(R)), and considering the intersection of all such ideals (see Specification 14);

Specification 14 Definition of principal ideals

```
R : VAR set[T]
fam_ideal(R:( ring ?))(a:(R)): setof[set[(T)]] =
{A: ideal(R) | member(a,A)}
principal_ideal(R:( ring ?))(a:(R)): set[T] =
Intersection(fam_ideal(R)(a))
```

5.3 Prime Ideals

The sub theory ring_prime_ideal_def gives the specification of prime ideals in a ring *R* defining the type prime_ideal (see Specification 15).

Specification 15 Definition of prime ideals

```
IMPORTING cosets_def[T,*]
R: VAR (ring ?)
A, B, P: VAR set[T]
prime_ideal ?(P,R): bool =
ideal ?(P,R) AND P/=R AND
FORALL (A,B:ideal(R)): subset ?(sum(A,B),P)
IMPLIES subset ?(A,P) OR subset ?(B,P)
prime_ideal(R): TYPE = {P: set[T] | prime_ideal ?(P,R)}
```

These lemmas establish a useful characterization of prime ideals in commutative rings. The formalization of both these lemmas is mainly based on case analysis on the definitions, as given in algebra textbook proofs. In addition for proving the second lemma, it is necessary to apply a corollary (inferred from lemmas in Specification 13) that states that commutative_one_gen(R)(a), for any a in R, is an ideal in R.

5.4 Maximal Ideals

In the sub theory ring_maximal_ideal_def, the definition of and the type of maximal ideals were specified, as shown in Specification 16.

Specification 16 Definition of maximal ideals

```
R: VAR (ring ?)
M,N: VAR set[T]
maximal_ideal ?(M,R): bool =
ideal ?(M,R) AND M/=R AND
FORALL(N:ideal(R)): subset ?(M,N) AND subset ?(N,R) IMPLIES
N = M OR N = R
maximal_ideal(R): TYPE = {M: set[T] | maximal_ideal ?(M,R)}
```

In the sub theory ring_maximal_ideal_def, Theorem 7 was specified (see Specification 17), and since for every ring *R* with identity it holds that $R * R = R$, it was proved that maximal ideals in commutative rings with identity are prime ideals as illustrated in Specification 18.

Specification 17 Maximal versus prime ideals on commutative rings

```
maximal_prime_ideal: LEMMA
FORALL (R:( commutative_ring?), M: maximal_ideal(R)):
sum[T ,*](R,R) = R IMPLIES prime_ideal ?(M,R)
```

Specification 18 Maximal versus prime ideals on commutative rings with identity

```
R: VAR ring_with_one
M: VAR set[T]
ring_one_maximal_prime_ideal: LEMMA
```

commutative_ring ?(R) AND maximal_ideal ?(M,R) IMPLIES
prime_ideal ?(M,R)

6. CONCLUSIONS AND FUTURE WORK

This paper presents complete formalizations in PVS of the three isomorphism theorems for rings, central results about principal, prime and maximal ideals, specifications of the main structures and concepts and formalizations of all properties required to obtain such formal proofs. The preliminary concepts were specified following a general approach that allows their use in contexts involving structures other than rings such as monoids, semigroups, groups and fields.

The rings development was integrated as part of algebra. The amount of formalized results indicates this formalization contributed significantly to the enrichment of algebra theory. In contrast with other interactive proof assistants, the PVS interactive theorem proving environment stores the proof commands in ".prf" files associated but separated from the specification ".pvs" files. The proofs of the generated TCCs are also stored in the ".prf files." The PVS proof interactive engine allows the execution of the stored proofs directly from the specification files. Ring theory has many relevant applications in fields such as coding theory, segmentation of digital images and cryptography. In this sense, the rings PVS theory development conforms a robust basis toward constructing more elaborated theories involving rings, their properties and applications.

The formalization of factorization in commutative rings with identity is an interesting future work. Since the notion of divisibility and prime elements can be defined in commutative rings with identity, a formalization of an analog of the fundamental theorem of arithmetic for principal ideal domains would be of great relevance. Furthermore, developments of sub theories about rings of polynomials, including notions of factorization and a division algorithm in such rings and the formalization of Eisenstein's irreducibility criterion, are important landmarks that might enrich the theory rings. Another interesting formalization would be the concept of the ring of fractions defined from an equivalence relation over a commutative ring *R* and a multiplicative subset *S* of *R*. This notion allows defining localization of a ring and developing formalizations of concrete structures like the ring Z*pn* ,
for *p* a prime number, as an example of local rings. The rings PVS theory is of great interest as a consistent basis to formalize theorems related to arbitrary ring structures as non-commutative rings, covering results on algebraic structures as matrix rings, quaternions and Weyl and Clifford algebras. Target formalizations may include Wedderburn's little theorem, Artin–Zorn theorem, Artin–Wedderburn theorem, Jacobson density theorem and Nakayama's lemma. Besides, the rings PVS theory is also of interest for formalizations related to applications in fields such as matrix computations, bilinear complexity, and quantum mechanics, and calculations involving three-dimensional rotations, symmetries, deformations, and representations (e.g., [13,14]).

REFERENCES

[1] Hungerford, T.W.: Algebra. Graduate Texts in Mathematics, vol. 73. Springer, New York (1980). (Reprint of the 1974 original)
[2] Dummit, D.S., Foote, R.M.: Abstract Algebra, 3rd edn. Wiley, Hoboken (2003)
[3] Lidl, R., Niederreiter, H.: Introduction to Finite Fields and Their Applications. Cambridge University Press, Cambridge (1994)
[4] Ayala-Rincón, M., de Moura, F.L.C.: Applied Logic for Computer Scientists: Computational Deduction and Formal Proofs. UTiCS. Springer (2017). https://doi.org/10.1007/978-3-319-51653-0
[5] Ballarin, C.: Exploring the structure of an algebra text with locales. J. Autom. Reason. (2019). https:// doi.org/10.1007/s10817-019-09537-9
[6] Butler, R.W.: Formalization of the integral calculus in the PVS theorem prover. J. Formaliz. Reason. 2(1), 1–26 (2009). https://doi.org/10.6092/issn.1972-5787/1349
[7] 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 31 March 2019
[8] Galdino, A.L., Ayala-Rincón, M.: A PVS theory for term rewriting systems. Electron. Notes Theor. Comput. Sci. 247, 67–83 (2009). https://doi.org/10.1016/j.entcs.2009.07.049

[9] Butler, R., Lester, D.: A PVS *theory* for abstract algebra (2007). http://shemesh.larc.nasa.gov/fm/ftp/larc/ PVS-library/pvslib.html. Accessed 31 March 2019.

[10] da Silva, A.B.A., de Lima, T.A., Galdino, A.L.: Formalizing ring theory in PVS. In: 9th International Conference on Interactive Theorem Proving ITP. Lecture Notes in Computer Science, vol. 10895, pp. 40–47. Springer (2018). https://doi.org/10.1007/978-3-319-94821-8_3

[11] Owre, S., Shankar, N.: The Formal Semantics of PVS. Technical Report 97-2R, SRI International Computer Science Laboratory, Menlo Park (1997) (revised 1999).

[12] Cano, G., Cohen, C., Dénès, M., Mörtberg, A., Siles, V.: Formalized linear algebra over elementary divisor rings in Coq. Log. Methods Comput. Sci. 12(2:7), 1–23 (2016). https://doi.org/10.2168/LMCS- 12(2:7)2016.

[13] Bourbaki, N.:Élèments de mathématique. Algèbre: chapitres 1 à 3. Springer, Berlin (2006). Réimpression inchangée de la 2e éd. 1970 Edition

[14] Artin, M.: Algebra, 2nd edn. Pearson, London (2010)

[15] Herstein, I.N.: Topics in Algebra, 2nd edn. Xerox College Publishing, Lexington (1975).

[16] Dougherty, S., Leroy, A.F.A., Puczyłowski, E., Solé, P.: Noncommutative Rings and Their Applications. Contemporary Mathematics (2015). https://doi.org/10.1090/conm/634

[17] Dougherty, S., Leroy, A.: Euclidean self-dual codes over non-commutative Frobenius rings.Appl.Algebra Eng. Commun. Comput. 27(3), 185–203 . (2016). https://doi.org/10.1007/s00200-015-0277-0