Journal of Automated Reasoning manuscript No.
(will be inserted by the editor)

Formalization of Ring Theory in PVS

Isomorphism Theorems, Principal, Prime and Maximal Ideals, Chinese Remainder Theorem

Thaynara Arielly de Lima · André Luiz Galdino · Andréia Borges Avelar · Mauricio Ayala-Rincón(*)

Received: date / Accepted: date

Abstract This paper presents a PVS development of relevant results of the theory of rings. The PVS theory includes complete proofs of the three classical isomorphism theorems for rings, and characterizations of principal, prime and maximal ideals. Algebraic concepts and properties are specified and formalized as generally as possible allowing in this manner their application to other algebraic structures. The development provides the required elements to formalize important algebraic theorems. In particular, the paper presents the formalization of the general algebraic-theoretical version of the Chinese Remainder Theorem (CRT) for the theory of rings, as given in abstract algebra textbooks, proved as a consequence of the First Isomorphism Theorem. Also, the PVS theory includes a formalization of the number-theoretical version of CRT for the structure of integers, which is the version of CRT found in formalizations. CRT for integers is obtained as a consequence of the general version of CRT for the theory of rings.

Keywords PVS · Ring theory · Isomorphism theorems · Principal ideals · Prime ideals · Maximal ideals · Chinese Remainder Theorem for Rings

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 [20] and, Dummit and Foote's [12] textbooks. Indeed, Hungerford's textbook is the main reference for this formalization and the results about homomorphisms, prime, maximal and principal ideals

(*) Corresponding author

Universidade Federal de Goiás E-mail: thaynaradelima@ufg.br · Universidade Federal de Catalão E-mail: andre_galdino@ufg.br · Universidade de Brasília E-mail: andreiaavelar@unb.br · Universidade de Brasília E-mail: ayala@unb.br

follow the same presentation of this book, whereas the Chinese Remainder Theorem follows the approach in Dummit and Foote's textbook. Other references (such as Herstein's, Artin's and Jacobson's textbooks [19, 2, 22]) were employed mainly to consult different pen-and-paper proofs and to compare with related work.

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 [5]. Regarding coding theory, commutative rings with identity and polynomials over such structures have an important role to describe redundant codes according to Lidl and Niederreiter [26]. Also, ring theory forms the basis for algebraic geometry, which has applications in engineering systems, statistics, modeling of biological processes and computer algebra [30]. Other relevant application of ring theory is in the analysis of images. According to Suárez et. al. [35], if the images are considered as a matrix whose elements belong to the ring $\mathbb{Z}_n$, properties about restoration and segmentation of images and detection of contours can be competently described. In particular, Suárez et. al. [35] showed that the segmentation of digital images becomes more efficiently automated by applying the $\mathbb{Z}_n$ 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 Library[4] (*nasalib*) that contains many theories in several subjects, such as analysis [7], topology [24], term rewriting systems [13], among others. In particular, *nasalib* contains the theory `algebra` [6], where basic concepts and properties about groups, rings and fields were formalized. However, the contents of the theory `algebra` about rings was 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 in [34]. Homomorphisms and cosets were separately defined in the particular context of rings and ideals in [34] and just for groups and normal subgroups in [6]. 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 logic core that is based on classical higher-order logic, and that embeds the power of subtyping and dependent typing in its logic. 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, ideals, among others, that appear naturally in the study of algebraic structures such as groups, rings, fields, etc. As a proof assistant based on classical logic, PVS includes the middle excluded rule, and the PVS core logic includes, in its prelude,

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

the axiom of choice. The development of the theory `rings` as well as the whole theory `algebra` don't 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 in [28] and [3]. 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. All the sub-theories of the theory `rings` in [34] 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 magmas (as used in Bourbaki's Éléments de Mathématique), which are denoted with the name `groupoid`s 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.

(iv) A formal proof of the general algebraic version of the Chinese Remainder Theorem (CRT) for rings obtained as a consequence of the First Isomorphism Theorem for rings is presented. Also, to illustrate the usability of the development, the number-theoretical version of the CRT for integers was formalized as an application of the general case. The CRT for integers depends on a specification that required formalizations of specific properties about the ring $\mathbb{Z}_n$. As pointed out before, since (finite) commutative rings in general, and specially the ring $\mathbb{Z}_n$, have relevant applications, the development of formalizations for (finite) rings plays an important role as the basis of formalizations for other theories.

The paper is organized as follows: Section 2 presents a theoretical overview about the isomorphism theorems and theorems on ideals that were formalized, pointing out the required concepts and results. Section 3 details the interesting elements of the specification and formalization of the required basic definitions, algebraic structures and their properties. Section 4 discusses the interesting aspects about the formalization of the three isomorphism theorems for rings, while Section 5 the formalization of principal, maximal and prime ideals. Section 6 introduces the formalization of the general algebraic version of CRT for rings proved as a consequence of the First Isomorphism Theorem and, Section 7 discusses the formalization of the standard number-theoretical version of that theorem for integers. After that, Section 8 discusses related work and, finally, Section 9 concludes and brings suggestions for future works. The theory `rings` is available at `https://github.com/nasa/pvslib` (following the master branch for PVS 7.1) as

part of the *nasalib*, inside the theory `algebra`. The development is also locally available at `http://ayala.mat.unb.br/publications.html`, where instructions for checking the theory are provided in the README_top_rings file.

2 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 with the properties formalized for principal, maximal and prime ideals.

2.1 Isomorphism theorems for rings

A ring is an algebraic structure described by a quadruple $(R, +_R, *_R, \text{zero}_R)$, where R is a nonempty 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 $(R, +_R, \text{zero}_R)$ 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 $(R, +_R, *_R, \text{zero}_R)$ is said to be a commutative ring. Furthermore, if R contains an element one_R such that $\text{one}_R *_R x = x *_R \text{one}_R = x$ then $(R, +_R, *_R, \text{zero}_R, \text{one}_R)$ 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, quotients, etc. can be found in the previous cited books ([20,19,12,2]).

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 $(R, +_R, *_R, \text{zero}_R)$ 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 $\varphi : R \to S$ is a homomorphism then there is an isomorphism of rings from $R/ker(\varphi)$ to the image of φ, where $ker(\varphi)$ 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 subring and an ideal in a ring R, respectively. There is an isomorphism between the rings $H/(H \cap I)$ and $(H + I)/I$, where $H + I = \{x \in R \mid x = h + i,\ h \in H \text{ and } i \in I\}$.*

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 Figure 1). The sub-theories of the theory `algebra` that were relevant for the formalization of the isomorphism theorems are just `groupoid_def` and `ring`.

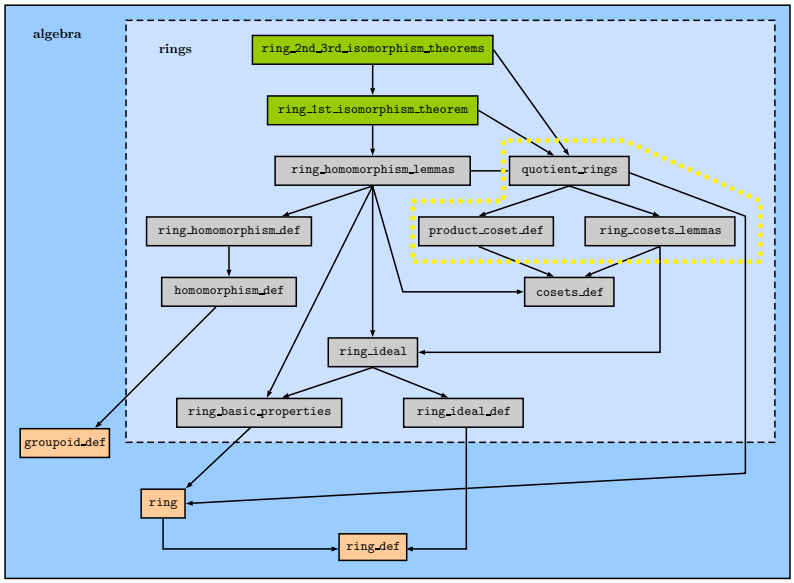

Fig. 1 Hierarchy of the sub-theories for the three isomorphism theorems for rings: `ring_1st_isomorphism_theorem` and `ring_2nd_3rd_isomorphism_theorems`

2.2 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 $\{r*a+a*s+n\cdot a+\sum_{i=1}^{m} r_i*a*s_i \mid r,s,r_i,s_i \in R; m \in \mathbb{N}\setminus\{0\}; n \in \mathbb{Z}\}$, where $n\cdot a$ denotes n summands of a if $n \geq 0$, and n summands of $-a$ if $n<0$;
(ii) if R is a commutative ring then $(a)=\{r*a+n\cdot a \mid r \in R; n \in \mathbb{Z}\}$;
(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 $P \neq R$ and for any ideals A, B in R, one has that $A*B \subset P$ implies $A \subset P$ or $B \subset P$, where $A*B=\{x \in R \mid x=a*b,\ a \in A \text{ and } b \in B\}$. 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 $P \neq R$ 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 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 $\neq$ 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 with the notion of prime numbers in the set of integers $\mathbb{Z}$. In fact, it is well-known that $n\mathbb{Z}=\{n*z \mid n \in \mathbb{N}; z \in \mathbb{Z}\}$ is an ideal in $\mathbb{Z}$. Notice that if $n\mathbb{Z}$ is a prime ideal then $n \neq 1$ (since $n\mathbb{Z} \neq \mathbb{Z}$) and, according to Theorem 5, whenever $a*b$ is an element of $n\mathbb{Z}$, one has that a or b is a member of $n\mathbb{Z}$. In other words, this means that if n divides $a*b$ then n divides a or b, whence $n\mathbb{Z}$ is a prime ideal if n is prime.

Lastly, 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 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 subsection were formalized in sub-theories of `rings` depicted in Figure 2. Theorem 4 was formalized in the sub-theories `ring_principal_ideal` (items *(i)* and *(ii)*) and `ring_with_id_one_generator` (item *(iii)*), 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`.

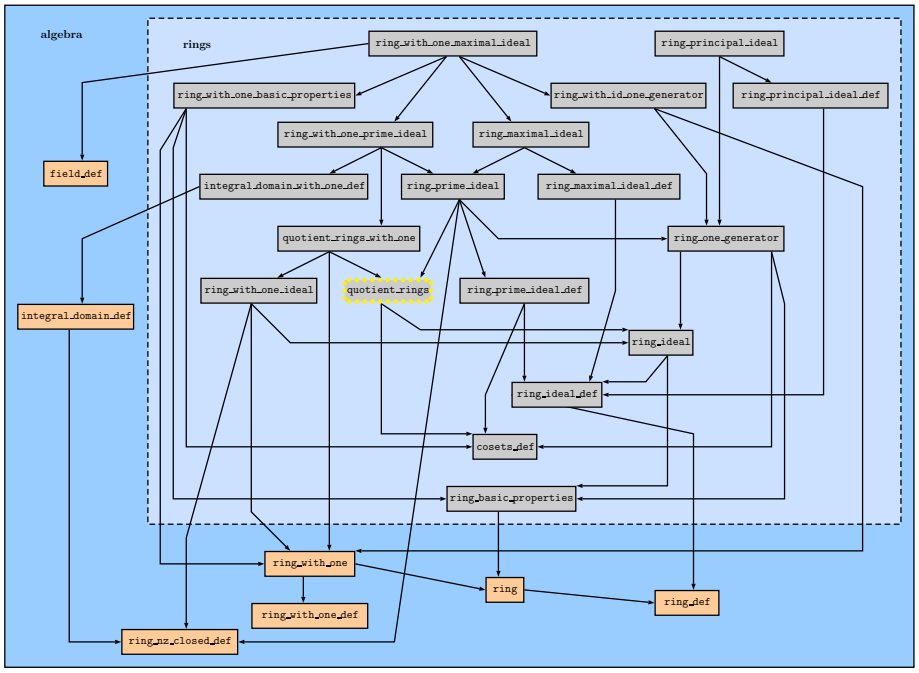

Fig. 2 Hierarchy of the sub-theories related with principal, prime and maximal ideals

3 Formalization of morphisms and basic agebraic structures

In this section, the PVS sub-theories of `rings` given in Figure 1 and related with specification and formalization of morphisms and basic algebraic notions such as cosets, ideals, kernel and quotient are presented.

3.1 Formalization of homomorphisms

The concept of ring homomorphism is the core of the theory for isomorphism theorems (see Figure 1). The required definitions and properties about homomorphisms were formalized in the sub-theories `homomorphisms_def`, `ring_homomorphisms_def`

and `ring_homomorphism_lemmas`(Figure 1 shows these sub-theories in the hierarchy). Particularly, the subtheory `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 subtheory `ring_homomorphisms_def`, the concept of homomorphism was extended in order to make feasible its use in a context of rings and the subtheory `ring_homomorphism_lemmas` brings the formalization of classical results involving ring homomorphisms.

3.1.1 Subtheory `homomorphisms_def`

Before the development of the theory `rings`, started in [34], the only specification in PVS of homomorphism for algebraic structures was available in subtheory `homomorphisms` of the theory `algebra` [6] (see Specification 1).

Specification 1 Homomorphism for groups - subtheory `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 nonempty 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., satisfies 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 $\varphi : G \to H$, 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.

In the new approach, as shown in the code in Specification 2, a more general definition of homomorphism was specified in the subtheory `homomorphisms_def` for magmas.

Specification 2 Specification of homomorphism in the subtheory `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))
```

This specification requires that R and S, declared as variables, which are specified as `VAR` in PVS of respective types `(groupoid?[T,s])` and `(groupoid?[U,p])`, be magmas. A magma $(G, *)$ is just a nonempty 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 nonempty 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 magma 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.

3.1.2 Subtheory `ring_homomorphisms_def`

Since the definition of a ring homormorphism must consider homomorphisms related with each one of the two operations over a ring R, to facilitate the formalization of the properties about ring homomorphisms, the specification of the predicate `R_homomorphism?(R_1,R_2)(phi)` was provided (see Specification 3). This curryfied predicate has as first parameters two sets `R_1` and `R_2`, whose elements have arbitrary types `T_1` and `T_2`, respectively. In addition, the binary operations `s_1` and `p_1` are closed over `R_1`, such that `groupoid?[T_1,s_1](R_1)` and `groupoid?[T_1,p_1](R_1)`, whereas `s_2` and `p_2` are also closed over `R_2`, such that `groupoid?[T_2,s_2](R_2)` and `groupoid?[T_2,p_2](R_2)` . This is done in subtheory `ring_homomorphisms_def`. Since `R_homomorphism`?$(\mathtt{R_1}, \mathtt{R_2})$`(phi)` makes use of the definition `homomorphism`?$(\mathtt{R_1}, \mathtt{R_2})$`(phi)` specified in `homomorphisms_def`, one must ensure that `R_1` and `R_2` are magmas under the operations mentioned above.

Specification 3 Specification of `R_homomorphism`?$(\mathtt{R_1}, \mathtt{R_2})$`(phi)`

```
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)
```

Injective, surjective and bijective homomorphisms are also formalized in the subtheory `ring_homomorphisms_def`, as presented in Specification 4.

Specification 4 Specification of injective, surjective and bijective homomorphisms

```
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)
```

3.1.3 Subtheory `ring_homomorphism_lemmas`

This subtheory mainly aims to formalize results about ring homomorphisms; within its scope, rings `R_1` and `R_2` are considered and, since rings are magmas, a simpler characterization of ring homomorphisms obtained from the specification of ring homomorphism, `R_homomorphism`?($\mathtt{R_1}, \mathtt{R_2}$)(`phi`), was formalized, as presented in Specification 5.

Specification 5 Characterization of a ring homomorphism

```
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))
```

Furthermore, classical results were formally proved in this subtheory, among them:

- if $\varphi : R \to S$ is a ring homomorphism and x is an element of R then $\varphi(\text{zero}_R) = \text{zero}_S$ and $\varphi(inv(x)) = inv(\varphi(x))$, 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 homormorphism is an ideal;
- the characterization of an injective homomorphism φ based on $ker\varphi$.

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 Subtheory `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 subtheory `cosets_def`, the sets $g + H$, $H + g$ and $H + I$ were specified as $+(\mathtt{g}, \mathtt{H})$, $+(\mathtt{H}, \mathtt{g})$ and $\mathtt{sum}(\mathtt{H}, \mathtt{I})$, respectively, as illustrated in Specification 6.

Specification 6 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 $\mathtt{sum}(\mathtt{H}, \mathtt{I})$ 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 $+(\mathtt{g}, \mathtt{H})$ and $+(\mathtt{H}, \mathtt{g})$ were used to specify the notion of cosets in a general way (see Specification 7). 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 typechecking: non of the sets {`a: T | G(a) AND A = a + H`} and {`a: T | G(a) AND A = H + a`}. PVS proves automatically both these proof obligations by expanding the definitions of `left_coset?` and `right_coset?` and by Skolemization.

Specification 7 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 8). However, the formalization of cosets in the subtheory `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 8 is considered.

Specification 8 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 subtheory `ring_ideal_def` brings the specification of the definition of ideals as shown in Specification 9.

Specification 9 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 subtheory `ring_ideal`, among them those given in Specification 10.

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 subring H and an ideal I in a ring R. The variable `R` is declared as a ring in both the Specifications 9 and 10. In the former, it is declared as a variable of type `(ring?)` that is defined in the PVS subtheory `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 subtheory `algebra@ring`.

```
ring?(S): bool = abelian_group?[T,+,zero](S)  AND
                 semigroup?[T,*](S)            AND
                 left_distributive?[(S)](*,+) AND
                 right_distributive?[(S)](*,+)
```

In general, this discrimination is relevant when it is necessary to check that an arbitrary set satisfies the properties of a specific algebraic structure as in the case of ring above. The theory `ring` (as happens similarly in theories `field`, `group`, etc.) contains the assumption that `T` is a ring, specified as `fullset_is_ring: ASSUMPTION ring?(fullset[T])` as given in Specification 11, where also the Lemma

`plus_commutative` is specified. This assumption is not mandatory, however it simplifies the specification of some results. For instance, omitting such assumption, one should quantify variables `R` of type `(ring?)`, `x, y` of type `(R)`: `FORALL(R: (ring?), x,y:(R)): x + y = y + x`.

Specification 11 Lemma of subtheory `ring` about commutative property

```
fullset_is_ring: ASSUMPTION ring?(fullset[T])
x,y: VAR T
plus_commutative: LEMMA x + y = y + x
```

Consider a hypothetical PVS subtheory `hyp_theory` and suppose one wants to check in it that for an arbitrary set whose elements have type `T`, say `S : set[T]`, `ring?(S)` holds. For this, one must verify that addition is commutative on `S`, an obligation expressed in `abelian_group?[T,+,zero](S)`. If subtheory `ring` were imported with parameters `[T, +, *, zero]` by `hyp_theory`, one may be wrongly assuming that `T` is a ring, and can apply directly the Lemma `plus_commutative` (Specification 11). In order to contour this issue, the subtheory `ring_def` can be imported by `hyp_theory` with the same parameters allowing in this manner the correct inference of the commutativity of `+` in `S`. For this reason, the theory `algebra` includes definitional sub-theories (with names using the suffix `_def`) for several structures such as `ring_ideal_def`, `ring_with_one_def`, and `ring_nz_closed_def` (in Figure 2).

3.2.3 Subtheory `ring_cosets_lemmas`

In the subtheory `cosets_def`, a coset was specified for sets G and H whose elements have arbitrary types (see Specification 7). However, in a context where elements of type T under operations $+$ and $*$ constitute a ring, such as required in the subtheory `ring_cosets_lemmas`, one can formalize a lemma asserting that a set A is a left coset if and only if it is a right coset. From this, it is possible to establish a characterization of cosets from left cosets, as shown in Specification 12.

Specification 12 Characterization of cosets from left cosets

```
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))
```

The subtheory `ring_cosets_lemmas` brings the formalization of other interesting results, such as:

(i) when I is an ideal of a ring R, any member of a coset A of I in R is a generator of A, that is, $A = a + I$, for any $a \in A$;
(ii) if H is a subring and I is an ideal of R then $H + I$ is a subring of R and I is an ideal in $H + I$.

The result in Item (i) above is important to establish a characterization of sum and product of cosets formalized in the subtheory `quotient_rings`, as will

be discussed. The result in item (*ii*) is widely used in branches of the proof of the Second Isomorphism Theorem and its auxiliary lemmas.

3.2.4 Kernel of a homomorphism

In the subtheory `ring_homomorphisms_def`, the kernel of a homomorphism φ between magmas R_1 and R_2 was defined as the set of elements of R_1 mapped into some element zero_{R_2} of R_2 by φ, as shown in Specification 13.

Specification 13 Kernel of a homomorphism

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

In the subtheory `ring_homomorphisms_def`, since R_1 and R_2 are not necessarily rings, one must require that the neutral element exists for $+_{R_2}$, which is denoted as zero_2 in Specification 13. But, in the subtheory `ring_homomorphism_lemmas`, R_1 and R_2 were considered as rings, structures of the form $(R_1, +_{R_1}, *_{R_1}, zero_{R_1})$ and $(R_2, +_{R_2}, *_{R_2}, zero_{R_2})$ and, as consequence of this, lemmas involving kernel were formally proved, among them:

- the kernel of a ring homomorphism $\varphi : R_1 \to R_2$ is an ideal (and particularly a ring) in R_1 and,
- φ is a monomorphism if and only if the kernel of φ is the set $\{\text{zero}_{R_1}\}$.

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` (Figures 1 and 2), as show in Specification 14, where in particular `/(R,I)` is a prefix notation for R/I.

Specification 14 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 R is a ring, such as occurs in the subtheory `quotient_rings`, `lproduct(R,I)(A) = rproduct(R,I)(A)` holds since left and right cosets are the same (see Specification 14), 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 $\texttt{add}(A, B) = (a + b) + I$ and $\texttt{product}(A, B) = (a * b) + I$.
(ii) A proof that $(R/I, \texttt{add}, \texttt{product}, I)$ 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 $I \neq R$ then $I \neq one_R + I$. This result is widely used in the formalization of Theorem 6 in order to guarantee that the quotient R/P has the identity $one_R + P \neq P$ satisfying a required condition to ensure that R/P is an integral domain.

4 Formalization of the three isomorphism theorems for rings

This section discusses the PVS sub-theories of `rings` related with the three isomorphism theorems for rings (See Figure 1).

The subtheory `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 $\phi : R \to S$ is a homomorphism of rings and I is an ideal of R, which is contained in the kernel of ϕ, then there is a homomorphism of rings $f : R/I \to S$ such that $f(a+I) = \phi(a)$ for all $a \in R$ and:*

(i) the image of f is equal to the image of ϕ;
(ii) $ker(f) = ker(\phi)/I$;
(iii) f is an epimorphism iff ϕ is an epimorphism;
(iv) f is a monomorphism iff $ker(\phi) = I$;
(v) f is an isomorphism iff ϕ is an epimorphism and $ker(\phi) = I$.

The formalization of Lemma 1 builds the homomorphism f as $f(a+I) = \phi(a)$ 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 monomorphims 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 15 and, roughly speaking, its formalization was obtained by considering the ideal $I =$

$ker(\varphi)$ in item (v) of Lemma 1. The first four parameters of `R_isomorphic?` in Specification 15 correspond to the type, the addition and multiplication and the neutral element for the addition of the quotient ring $R/ker(\varphi)$, whereas the last four are the parameters for the image of φ that is a subring of S.

Specification 15 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 subtheory `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 subring and I is an ideal of a ring R then there is an epimorphism $\varphi : H \to (H + I)/I$ such that $ker(\varphi) = H \cap I$.*

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 $\varphi : R/J \to R/I$ such that $ker(\varphi) = I/J$.*

The Second and Third Isomorphism Theorems, given in Specification 16, were formalized applying the First Isomorphism Theorem with Lemmas 2 and 3, respectively.

Specification 16 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 in Figure 2 and related with formalizations about principal, prime and maximal ideals are discussed.

5.1 Ideals generated by one element

The subtheory `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 17 presents the main definitions of this subtheory, built from a specific element a of a ring R. The subset of R defined as the set of elements generated as $\{r*a+a*s+n\cdot a+\sum_{i=1}^{m} r_i*a*s_i \mid r,s,r_i,s_i \in R; m \in \mathbb{N}\setminus\{0\}; n \in \mathbb{Z}\}$ 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 those given in Specifications 18 and 19.

Specification 18 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)
```

Specification 19 A simpler characterization for `one_gen(R)(a)`, when R is commutative and has an identity, as part of the subtheory `ring_with_id_one_generator`

```
R : VAR (ring_with_one?)

commutative_id_one_gen_charac: LEMMA
 FORALL(a:(R)): commutative_ring?(R) IMPLIES
 one_gen(R)(a) = +[T,*](a,R)
```

5.2 Principal ideals

There are two sub-theories 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 20);
– `ring_principal_ideal` that brings several properties, having as main result the formalization of the characterization of prime ideals from the constructor `one_gen(R)(a)` that establishes a shape for the elements of principal ideals as enunciated in Theorem 4 (i) (see Specification 21).

Specification 20 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))
```

Specification 21 Characterization of principal ideals from `one_gen(R)(a)`

```
principal_ideal_charac: LEMMA
 FORALL(R: (ring?), a:(R)):
 principal_ideal(R)(a) = one_gen(R)(a)
```

The proofs of the items (ii) and (iii) of Theorem 4 are obtained combining the Lemma `principal_ideal_charac` with Lemmas `commutative_one_gen_charac` and `commutative_id_one_gen_charac`, respectively (Specifications 18 and 19).

5.3 Prime ideals

The subtheory `ring_prime_ideal_def` gives the specification of prime ideals in a ring R defining the type `prime_ideal` (see Specification 22).

Specification 22 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)}
```

The formalization of Theorem 5 is in the subtheory `ring_prime_ideal`. This theorem is specified as lemmas `prime_ideal_prop1` and `prime_ideal_prop2` (see Specification 23). 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 18) that states that `commutative_one_gen(R)(a)`, for any `a` in `R`, is an ideal in `R`.

Specification 23 Characterization of prime ideals in commutative rings

```
R: VAR ring
P: VAR set[T]
a,b: VAR T

prime_ideal_prop1: LEMMA
 (ideal?(P,R) AND P/=R AND
  FORALL (a,b: (R)): member(a*b,P)
  IMPLIES member(a,P) OR member(b,P))
 IMPLIES prime_ideal?(P,R)

prime_ideal_prop2: LEMMA
 commutative_ring?(R) AND prime_ideal?(P,R) IMPLIES
 FORALL (a,b: (R)): member(a*b,P)
 IMPLIES member(a,P) OR member(b,P)
```

The subtheory `ring_with_one_prime_ideal` contains the proof of Theorem 6 formalized as Lemma `prime_ideal_charac` presented in Specification 24. In this specification `monad?`, taken from the theory `algebra`, is a unary predicate for checking whether the set given as argument is closed under operation $*$, and includes the element `one`, which behaves as multiplicative identity over the whole input set. The formalization of this Lemma depends mainly on Lemma `prime_ideal_nz_closed` (also in Specification 24), which states that for a commutative ring R and a prime ideal P in R, the quotient ring R/P is closed under the product, when the neutral element for the addition is removed. This means that the set $R/P \setminus \{P\}$ is closed under the `product` operation defined in subtheory `product_coset_def` (see Specification 14). Furthermore, for specifying Theorem 6 it was necessary to define the unary predicate `integral_domain_w_one` that is nothing more than the usual notion of integral domain found in abstract algebra textbooks, and in particular the one found in [20]. This predicate holds for commutative rings with $one_R \neq zero_R$ and without zero divisors. In the theory `algebra` this notion does not impose the constraint $one_R \neq zero_R$.

Specification 24 Characterization of prime ideals in commutative rings with identity

```
R: VAR ring_with_one[T,+,*,zero,one]
P: VAR set[T]

prime_ideal_nz_closed: LEMMA
 (commutative_ring?(R) AND prime_ideal?(P,R)) IMPLIES
  nz_closed?
   [coset[T,+](R,P),add[T,+,*](R,P),product[T,+,*](R,P),P]
   (R/P)

prime_ideal_charac: LEMMA
 (commutative_ring?(R) AND monad?[T,*,one](remove(zero,R))
  AND ideal?(P,R)) IMPLIES
 (prime_ideal?(P,R) IFF
 integral_domain_w_one?[coset[T,+](R,P),add[T,+,*](R,P),
                        product[T,+,*](R,P),
                        P,+[T,+](one,P)]
  (R/P))
```

5.4 Maximal ideals

In the subtheory `ring_maximal_ideal_def`, the definition of and the type of maximal ideal were specified, as shown in Specification 25.

Specification 25 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 subtheory `ring_maximal_ideal`, Theorem 7 was specified (See Specification 26) 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 the Specification 27.

Specification 26 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 27 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)
```

Theorem 8 was fully formalized as Lemmas `maximal_ideal_quot_field` and `quot_div_ring_maximal_ideal`; in this manner, the characterization of maximal ideals by quotient rings was established as shown in Specifications 28 and 29. The characterization of principal ideals given in Theorem 4 is essential to formalize Lemmas `maximal_prime_ideal` and `maximal_ideal_quot_field`. The latter is proved by firstly (i) ensuring that R/M is a commutative ring with identity without zero divisors by Lemmas `maximal_prime_ideal` and `prime_ideal_nz_closed` and secondly by (ii) establishing that every element $a + M \neq M$, $a \in R$, of R/M has a multiplicative inverse. Technical details can be seen in [20] and will be omitted, however one can point out that it is crucial to consider the ideal $M + (a)$ generated from the principal ideal (a) and the shape of its elements to show this property.

Specification 28 Characterization of maximal ideals by quotient rings

```
maximal_ideal_charac: LEMMA
 (commutative_ring?(R) AND ideal?(M,R)) IMPLIES
 (maximal_ideal?(M,R) IFF
```

```
 division_ring?[coset[T,+](R,M),add(R,M),product(R,M),
                M,+[T,+](one,M)](R/M))
```

Specification 29 Auxiliary lemmas to characterize maximal ideals by quotient rings

```
maximal_ideal_quot_field: LEMMA
 FORALL(M: maximal_ideal(R)):
 commutative_ring?(R) IMPLIES
 field?[coset[T,+](R,M),add(R,M),product(R,M),
        M,+[T,+](one,M)](R/M)

quot_div_ring_maximal_ideal: LEMMA
 FORALL(M:ideal(R)):
 division_ring?[coset[T,+](R,M),add(R,M),product(R,M),
                M,+[T,+](one,M)](R/M) IMPLIES
 maximal_ideal?(M,R)
```

6 Algebraic version of CRT

This section discusses the formalization of the Chinese Remainder Theorem for rings, formalized as consequence of the First Isomorphism Theorem. The subtheories related with this part of the formalization of the theory `rings` are given in Figure 3, where also the subtheory including the formalization of CRT for integers, to be discussed in the next section, appears.

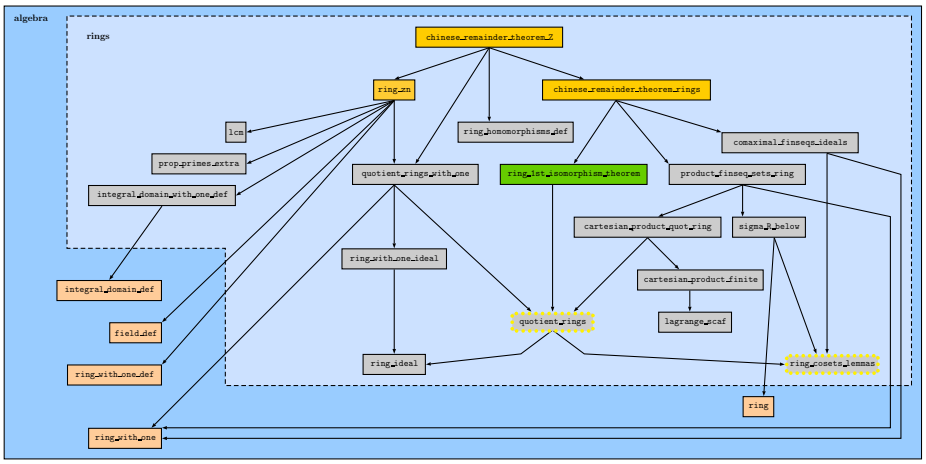

Fig. 3 Hierarchy of the sub-theories for the Chinese Remainder Theorems for the theory of rings and the ring of integers

In the literature, a general algebraic version of CRT for arbitrary rings and ideals is classically given as enunciated in Theorem 9 (e.g., see [12]).

Theorem 9 (Chinese Remainder Theorem: general algebraic version) *Let R be a ring with identity and $A_1, A_2, \ldots, A_k$ ideals in R. The map*

$$\begin{aligned} \varphi : R &\to R/A_1 \times \ldots \times R/A_k \\ r &\mapsto (r + A_1, \ldots, r + A_k) \end{aligned}$$

is a ring homomorphism with kernel $A_1 \cap \ldots \cap A_k$. *If the condition* $A_i + A_j = R$ *holds for each* $i, j \in \{1, \ldots, k\}$ *with* $i \neq j$, *which is called comaximality, then* φ *is surjective and the rings* $R/(A_1 \cap \ldots \cap A_k)$ *and* $R/A_1 \times \ldots \times R/A_k$ *are isomorphic.*

The general algebraic version of the CRT for rings as enunciated in Theorem 9 was fully formalized and the three crucial steps to obtain such proof are described in the remaining of this section.

Step 1. Prove that φ, as given in the statement of the theorem, is a ring homomorphism with kernel $A_1 \cap \ldots \cap A_k$, as given in Specifications 30, 31 and 32.

The notion of Cartesian product is given in Specification 30, part of the subtheory `Cartesian_product_finite`. The constructor `Cartesian_product_n` receives as input `fsA`, a finite sequence of sets of type `T`, and gives as output the set of finite sequences of length the same as the length of `fsA`, of elements of type `T`. An element `fsz` of such set of sequences of length `fsA` is such that its ith components belongs to the ith set in the sequence `fsA`. In PVS, finite sequences of type `T` are data structures that consist of their length, say `n`, and a function from `below[n]` to `T`; for instance, `(# length := n, seq := (LAMBDA (i:below[n]): i) #)` is the sequence of the first n naturals.

Specification 30 Constructor for formalization of finite Cartesian product

```
fsz: VAR finseq[T]
fsA: VAR finseq[set[T]]

Cartesian_product_n(fsA): set[finseq[T]] =
   IF length(fsA) = 0 THEN emptyset
   ELSE {fsz | length(fsz) = length(fsA) AND
               FORALL (i: below(length(fsz))): member(fsz(i), fsA(i))}
   ENDIF
```

The technical elements required to formalize that $R/A_1 \times \ldots \times R/A_k$ is indeed a ring are contained in the sub-theories `Cartesian_product_finite` and `Cartesian_product_quot_ring`, see Specification 31. In a context where elements of type `T` under operations `+` and `*` and constant `zero` constitute a ring, the predicate `fsRI(R)` checks if a finite sequence of sets of type `T` are ideals in `R`; and the constructor `fsQ(R)` builds the finite sequence of quotient rings `R/fsA(i)` for the input `fsA`, where `fsRI?(R)(fsA)` holds. Thus, `Cartesian_product_n(fsQ(R)(fsA))` is the Cartesian product of such quotients, and the constructors `Sfs` and `Pfs` specify the operations of addition and multiplication for this Cartesian product. Finally, that this Cartesian product is a ring is the main result formalized as Lemma `Cartesian_product_quot_ring_is_ring` in Specification 31. The formalization of this fact required proving that such addition and multiplication operators satisfy the properties of rings for `Cartesian_product_n(fsQ(R)(fsA))`, such as closure of the operators, existence of the identity for the addition (that is the sequence of ideals), property of additive inverses, distributivity, etc.

Specification 31 Addition and multiplication (`Sfs(fsA)` and `Pfs(fsA)`, resp.) for the ring of Cartesian product of quotient rings

```
R: VAR ring[T,+,*,zero]
fsA: VAR finseq[set[T]]
                                        % Predicate for sequence of ideals
```

```
fsRI?(R)(fsA): bool =  FORALL (i: below[length(fsA)]): ideal?(fsA(i), R)
                                    % Type predicate for sequences of ideals
fsI(R): TYPE = {fsA: finseq[set[T]] | fsRI?(R)(fsA)}
                                                  % Sequence of quotient rings
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
         % Addition of elements of the Cartesian product of quotient 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
          % Product of elements of the Cartesian product of quotient rings
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)))
```

The map φ, given in Specification 32, was proved to be a homomorphism by checking that `R_homomorphism?(R,cartesian_product_n(fsQ(R)(fsA)))(phi)` holds, which is done by verification of the conditions of ring homomorphism. The characterization of the kernel of φ as the intersection $A_1 \cap \ldots \cap A_k$ (last line in Specification 32) was established by extensional equality on the sets (i.e., for all x, $x \in \ kernel(\varphi)$ if and only if $x \in A_1 \cap \ldots \cap A_k$), observing that the neutral element for addition over the Cartesian product of the quotient $R/A_1 \times \ldots \times R/A_k$ is the sequence of ideals $(A_1, \ldots, A_k)$. This result requires application of a key lemma for subrings (lemma `self_coset` in theory `ring_cosets_lemmas`, see Fig. 1) that states that if A is a subring of R then for all $x \in R$, $x + A = A$ iff $x \in A$. Thus, the formalization of the equality proceeds in both directions according to the following argumentation: by definition of φ, $\varphi(x) = (x + A_1, \ldots, x + A_k)$, and by definition of *kernel*, $x \in kernel(\varphi)$ iff $\varphi(x) = (A_1, \ldots, A_k)$. Consequently, $x \in A_i$ for all $i \in \{1, \ldots, k\}$ and so $x \in A_1 \cap \ldots \cap A_k$.

Specification 32 φ is a homomorphism with kernel $A_1 \cap \ldots \cap A_k$

```
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))
```

Step 2. Prove that φ is surjective. This step uses the hypothesis that the ideals $A_1, \ldots, A_k$ are pairwise comaximal (i.e., $A_i + A_j = R$ when $i \neq j$). This proof is constructive and the interesting substeps and technical details are explained below.

The concepts of comaximal and sequence of pairwise comaximal ideals were defined as in Specification 33.

Specification 33 Definition of comaximal ideals

```
comaximal_ideals?(R)(M,N): bool =
  ideal?(M,R) AND ideal?(N,R) AND sum(M,N) = R

fsICM?(R)(fsA): bool = fsRI?(R)(fsA) AND
                       (FORALL (i,j: below[length(fsA)]):
                         i /= j IMPLIES comaximal_ideals?(R)(fsA(i),fsA(j)))

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

The key to prove the surjectivity of φ, Lemma `surjective_aux_1` in Specification 34, is to build a sequence $s = (s(1), \ldots, s(k))$ over R such that $s(i) \in A_j$ for all $j \neq i$ and $s(i) + A_i = one + A_i$. The elements of this sequence are characterized as $s(i) = \prod_{j=1}^{i-1}(one - x_j) * \prod_{j=i+1}^{k}(one - x_j)$, where $x_j \in A_i$ and $y_j = (one - x_j) \in A_j$ for each $j = 1, \ldots, i-1, i+1, k$. Notice that, the sequence s is well-defined since the ideals A_i and A_j are comaximal for $i \neq j$ and the ring R has identity; consequently, there exist elements $x_i \in A_i$ and $y_j \in A_j$ such that $one = x_i + y_j$ whenever $i \neq j$. By performing calculations over $s(i)$, since A_i is closed under addition and multiplication, one can infer that $s(i) = one + a$, where $a \in A_i$. Consequently, $s(i) + A_i = one + (a + A_i) = one + A_i$. Now, it is not difficult to establish that the map φ is surjective. Consider $y = (r_1 + A_1, \ldots, r_k + A_k) \in R/A_1 \times \ldots \times R/A_k$, where $r_i \in R, 1 \leq i \leq k$, the sequence s as defined before and $x = \sum_{i=1}^{k} s(i) * r_i \in R$. Fixing an index, one can infer that $\left(\sum_{i=1}^{k} s(i) * r_i\right) + A_i = (s(i) * r_i) + A_i$, since $s(j) \in A_i$ for $i \neq j$. Consequently, $\left(\sum_{i=1}^{k} s(i) * r_i\right) + A_i = (one + A_i) * (r_i + A_i) = r_i + A_i$ and $\varphi(x) = y$.

Specification 34 Auxiliary lemma to prove the surjectivity of φ

```
surjective_aux_1: LEMMA
    FORALL (R: ring_with_one, fsA: fsICM(R)):
      EXISTS (s: finseq[(R)] | length(s) = length(fsA)):
         FORALL (i: below[length(fsA)]):
            s(i) + fsA(i) = one + fsA(i)  AND
            (FORALL (j: below[length(fsA)] | j /= i):  member(s(i),fsA(j)))
```

The sequence s needed to formalize the Lemma `surjective_aux_1` was specified from the set `oneSet(R,fsA)` defined from a ring R and a sequence of sets `fsA` such that for all $0 \leq i, j \leq$ length(`fsA`) $- 1$, `oneSet(R,fsA)(i,j)` $= \{x \in$ `fsA`$(i) | (one - x) \in$ `fsA`(j), whenever $j \neq i\}$ and a recursive function that multiplies elements of a given sequence of elements of arbitrary type; namely, the function `product_fs_rec(fs)` in Specification 35. Specifically, to construct s, the sequence `fs` in `product_fs_rec(fs)` has length $k-1$ and was built from the `choose` operator in the native library of PVS, which specifies the axiom of choice. Thus, for each $1 \leq j \leq k$, $j \neq i$, `fs`$(i) = one -$ `choose`(`oneSet`(`R`, `fsA`)(`i`, `j`)). Obviously, a

proof obligation regarding the non emptiness of `oneSet(R,fsA)(i,j)` arises which was formalized in the Lemma `oneSet_nonempty` by considering the sequence of sets `fsA` as comaximal ideals (See Specification 36).

Specification 35 Function that multiplies the elements of a sequence

```
fs: VAR finseq[T]

product_fs_rec(fs)(i: below[length(fs)]): RECURSIVE T =
        IF i = 0 THEN seq(fs)(0)
        ELSE seq(fs)(i) * product_fs_rec(fs)(i-1)
        ENDIF MEASURE i
```

Specification 36 Non emptiness of the set `oneSet(R,fsA)(i,j)` for a sequence of comaximal ideals

```
fsA: VAR finseq[set[T]]

oneSet_nonempty: LEMMA
  FORALL (R: ring_with_one, fsA: fsICM(R) | length(fsA) > 1,
          i: below[length(fsA)], (j: below[length(fsA)] | j /= i)):
      NOT empty?(oneSet(R, fsA)(i,j))
```

Step 3. Prove that $R/(A_1 \cap \ldots \cap A_k)$ and $R/A_1 \times \ldots \times R/A_k$ are isomorphic.

Specification 37 Chinese Remainder Theorem for rings

```
Chinese_Remainder_Theorem: LEMMA
 FORALL (R: ring_with_one, fsA: fsICM(R) | length(fsA) /= 0):
           R_isomorphic?(R/Intersection(seq2set(fsA)),
                         Cartesian_product_n(fsQ(R)(fsA)))
```

Now, one can notice that `Chinese_Remainder_Theorem` (see Specification 37) is a direct consequence of the First Isomorphism Theorem. In fact, in Theorem 1 one must consider the ring homomorphism

$$\begin{aligned} \varphi : R &\to R/A_1 \times \ldots \times R/A_k \\ r &\mapsto (r + A_1, \ldots, r + A_k) \end{aligned}$$

Thus, by the Step 1 one can ensure that $ker(\varphi) = A_1 \cap \ldots \cap A_k$ and by the Step 2 that the image of φ is $R/A_1 \times \ldots \times R/A_k$.

7 Formalization of the number-theoretical CRT

This section shows how the general version of CRT for the theory of rings is applied to formalize the CRT for the structure of integers (see Figure 3, subtheory `chinese_remainder_theorem_Z`). This is a well-known crucial application that shows how formalized abstract results in the theory of rings are applied to obtain important properties about numerical structures. Besides, it is illustrated how CRT for integers can be applied to obtain numerical properties by explaining how the well-known result that "the product of two positive integers equals the product of their greatest common divisor and least common multiple" is formalized.

CRT for integers is well-known as a classical result in number theory with applications in computing and coding [11], security [17] [11], signal processing [25] and other fields. The number-theoretical version of CRT states that an integer number can be characterized by a sequence of its remainders modulo some integers and, basically, this consists in solving a system of congruences. From the point of view of algebraic structures, the standard version of CRT can be formulated in a more general setting as a ring isomorphism, as shown in Theorem 10.

Theorem 10 (CRT: number-theoretical version for $\mathbb{Z}$) *Let $m_1, m_2, \ldots, m_k$ be positive integers such that m_i and m_j are coprime for $i \neq j$ and let $m = m_1 * m_2 * \ldots * m_k$. Then there is an isomorphism between the rings Z_m and the Cartesian product $Z_{m_1} \times \ldots \times Z_{m_k}$.*

Specification 38 contains the Corollary `chinese_remainder_th_for_int` that is the CRT for $\mathbb{Z}$. The Corollary is preceded by the main results used in its proof; indeed, lemmas `nz_fs_intersection`, `nZ_ideal` and, `nZ_mZ_comaximal`.

The number-theoretical version of the CRT, Theorem 10, is obtained as a corollary of the general algebraic version of CRT, Theorem 9. Before instantiating the algebraic version of CRT, lemma `nZ_fs_intersection` is applied. In sequence, Theorem 9 is instantiated with the ring of integers, $\mathbb{Z}$, and the ideals $m_i\mathbb{Z}$ in $\mathbb{Z}$, where $1 \leq i \leq k$ and $m_i \in \mathbb{Z}$ and, for guaranteeing typing properties of this instantiation of the algebraic version of CRT, the other two lemmas, `nZ_ideal` and `nZ_mZ_comaximal`, are applied. Since the quotient $\mathbb{Z}/m_i\mathbb{Z}$ is Z_{m_i} (the ring of integers modulo m_i), one can concluded that there is an isomorphism between the rings Z_m and the Cartesian product $Z_{m_1} \times \ldots \times Z_{m_k}$, where $m = m_1 * m_2 \ldots m_k$.

Instantiating Theorem 9 as before, one can initially infer that there is a homomorphism from $\mathbb{Z}$ to $\mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_k}$. Furthermore, for arbitrary integers m and n, $m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$, where d is the greatest common divisor of m and n. Consequently, if $m_1, m_2, \ldots, m_k$ are positive integers such that m_i and m_j are coprime for $i \neq j$, $m_i\mathbb{Z} + m_j\mathbb{Z} = \mathbb{Z}$ for each $i, j \in \{1, \ldots, k\}$ with $i \neq j$. This shows that there is an isomorphism between the rings Z_m and $Z_{m_1} \times \ldots \times Z_{m_k}$, where m is as above, since $m_1\mathbb{Z} \cap \ldots \cap m_k\mathbb{Z} = m\mathbb{Z}$. Thus, the number-theoretical version of the CRT is concluded.

Specification 38 Chinese Remainder Theorem for integers

```
nZ(n): set[int] = {x | EXISTS k: x=n*k}

fs_rel_primes(fsn): bool =
    FORALL (i,j: below[length(fsn)]): i /= j IMPLIES rel_prime(fsn(i),fsn(j))

Z_commutative_ring_w_one: LEMMA commutative_ring_with_one?[int,+,*,0,1](Z)

nZ_ideal: LEMMA FORALL n: ideal?(nZ(n),Z)

Z(n): setofsets[int] = Z/nZ(n)

Zn_card_n: LEMMA card(Z(n)) = n

nZ_mZ_sum: LEMMA sum(nZ(n),nZ(m)) = nZ(gcd(n,m))

nZ_mZ_comaximal: LEMMA comaximal_ideals?(Z)(nZ(n),nZ(m)) IFF rel_prime(n,m)

nZ_mZ_intersection: LEMMA intersection(nZ(n),nZ(m)) = nZ(lcm(n,m))
```

```
nZ_mZ_rel_prime_intersection: COROLLARY
    rel_prime(n,m) IMPLIES intersection(nZ(n),nZ(m)) = nZ(n*m)

nZ_fs_intersection: LEMMA
  (length(fsn) /= 0 AND fs_rel_primes(fsn))
     IMPLIES
       LET fsnZ: finseq[set[int]] =
           (# length := length(fsn),
              seq:= (LAMBDA (i:below[length(fsn)]): nZ(fsn(i))) #) IN
        Intersection(seq2set(fsnZ)) = nZ(product(fsn))

chinese_remainder_th_for_int : COROLLARY
  FORALL (fspn: finseq[posnat] | length(fspn) /= 0 AND fs_rel_primes(fspn)) :
     R_isomorphic?(Z/nZ(product(fspn)),
                   cartesian_product_n[set[int]](fsQ(Z)(fsnZ(fspn))))

gcd_lcm_property: COROLLARY lcm(n,m) = n*m/gcd(n,m)
```

Despite the fact that commutativity of $\mathbb{Z}$ is used in this formalization for algebraic simplifications, which are not always essential, it is important to stress here that the crucial use of commutativity of $\mathbb{Z}$ appears in the formalization of Lemma `nZ_mZ_intersection`. Lemma `nZ_mZ_intersection` is used for proving Corollary `nZ_mZ_rel_prime_intersection` and Lemma `nZ_fs_intersection` (see Specification 38). Indeed, in order to prove the inclusion $lcm(m,n)\mathbb{Z} \subset n\mathbb{Z} \cap m\mathbb{Z}$, required to prove `nZ_mZ_intersection`, one can proceed as following. Consider $x \in lcm(n,m)\mathbb{Z}$, which means that $x = lcm(n,m) * z$ for some $z \in \mathbb{Z}$. Since there are integers k and l such that $l * m = lcm(n,m) = k * n$, one has that $x = l * m * z = k * n * z$. And since the ring of integers is commutative, one has $x = m * (l * z)$ and $x = n * (k * z)$. Consequently, $x \in n\mathbb{Z} \cap m\mathbb{Z}$. Thus, commutativity of $\mathbb{Z}$ is required to guarantee that when m and n are coprime, $m\mathbb{Z} \cap n\mathbb{Z} = (m * n)\mathbb{Z}$, and this is used for proving the required generalization in Lemma `nZ_fs_intersection`: $m_1\mathbb{Z} \cap \ldots \cap m_k\mathbb{Z} = (m_1 * \ldots * m_k)\mathbb{Z}$.

This section is closed illustrating the use of CRT for $\mathbb{Z}$ (Theorem 10) to formalize $lcm(n,m) * gcd(n,m) = n * m$, for n and m positive integers (See Corollary `gcd_lcm_property` in Specification 38). This result is obtained instantiating Theorem 10 with the sequence of relative primes $(\frac{n}{gcd(n,m)}, \frac{m}{gcd(n,m)})$ obtaining the isomorphism between the structures below.

$$\mathbb{Z}/(\frac{n}{gcd(n,m)} * \frac{m}{gcd(n,m)})\mathbb{Z} \simeq \mathbb{Z}_{\frac{n}{gcd(n,m)}} \times \mathbb{Z}_{\frac{m}{gcd(n,m)}}$$

Notice that, since the integers $\frac{n}{gcd(n,m)}$ and $\frac{m}{gcd(n,m)}$ are relative primes, applying lemmas `nZ_fs_instersection`, `nZ_mZ_rel_prime_intersection` (in Specification 38) one obtains:

$$\left(\frac{n}{gcd(n,m)} * \frac{m}{gcd(n,m)}\right)\mathbb{Z} = \frac{n}{gcd(n,m)}\mathbb{Z} \bigcap \frac{m}{gcd(n,m)}\mathbb{Z}$$

Then, applying lemma `nZ_mZ_intersection` (also, in Specification 38), one obtains:

$$\frac{n}{gcd(n,m)}\mathbb{Z} \bigcap \frac{m}{gcd(n,m)}\mathbb{Z} = lcm\left(\frac{n}{gcd(n,m)}, \frac{m}{gcd(n,m)}\right)\mathbb{Z}$$

Consequently, the finite structures below are isomorphic and have the same cardinality.

$$\mathbb{Z}/\left(lcm(\frac{n}{gcd(n,m)},\frac{m}{gcd(n,m)})\right)\mathbb{Z} \;\simeq\; \mathbb{Z}_{\frac{n}{gcd(n,m)}} \times \mathbb{Z}_{\frac{m}{gcd(n,m)}}$$

Since $\mathbb{Z}_n$ is defined as $\mathbb{Z}/n\mathbb{Z}$, for all positive integer n and the cardinality of $\mathbb{Z}_n$ is n (see `Z(n)` and lemma `Zn_card_n` in Specification 38), using properties of finite Cartesian product, one obtains that

$$lcm(\frac{n}{gcd(n,m)},\frac{m}{gcd(n,m)}) \;=\; \frac{n}{gcd(n,m)} * \frac{m}{gcd(n,m)}$$

Finally, since $lcm(d*i, d*j) = d*lcm(i,j)$, for positive integers d, i and j, one concludes the desired result.

$$\frac{1}{gcd(n,m)} * lcm(n,m) \;=\; \frac{n}{gcd(n,m)} * \frac{m}{gcd(n,m)}$$

8 Related work

Emmy Noether introduced the isomorphism theorems for modules in her seminal work [27] giving rise to an interpretation of such theorems as general laws of isomorphisms for several algebraic structures such as groups, rings and fields [36].

Regarding previous PVS work in theories `algebra` ([6]) and `rings` ([34]), discussed in the introduction, the present formalization adapts and substantially extends part of `rings` using `algebra` as a basis. All previous results about groups were maintained, while those in theory `rings` were adapted trying to obtain definitions as general as possible. An interesting feature of the generality is expressed in the specification of the notion of homomorphism, now given for the simple structure of magmas in such a manner that it can be applied to several other more elaborated algebraic structures, including monoids, semigroups, groups, rings as well as fields.

8.1 Relation with other formalizations

There are several formalizations containing a wide range of theorems for several abstract algebra structures. In Coq results about groups, rings and ordered fields were formalized as part of the FTA project [14]; further related formalizations in Coq deal with finite group theory [16] 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 [15]. Also in Coq, formalizations of real ordered fields [9] and finite fields (to check eliptic curve cryptography) [29], and a formalization of rings with explicit divisibility [8] are available. In Nuprl and Mizar it is provided a formal proof of the Binomial Theorem for rings, [21,32], respectively. In ACL2 a hierarchy of algebraic structures ranging from setoids to vector spaces is built focusing on the formalization of computer algebra systems [18]. Lean's library mathlib, also contains quite a bit of abstract algebra. It contains a definition of the First Isomorphism Theorem for groups, but no definition of isomorphism theorem for rings. It includes also a definition of an abstract version of the Chinese

Remainder Theorem for commutative rings, but without formalization of its proof [10].

The Algebra Library of Isabelle/HOL [1] provides a wide range of theorems on mathematical structures, including results on rings, groups, factorization over ideals, rings of integers and polynomial rings. This library contains formalizations of the First and Second Isomorphism theorems for groups and more recently incorporated also a Formalization of the First Isomorphism Theorem for rings as well as an algebraic version of the Chinese Remainder Theorem for commutative rings with identity [1]. A formalization of the First Isomorphism Theorem for rings is also available in Mizar [23] (which, as ACL2, is a first-order set theoretical based framework). This formalization differs from the one given here in which the flexibility of higher order logic, basis of the PVS deductive engine, gives rise in a natural manner to specifications and formalizations that are close to the ones in textbooks on algebra.

Regarding the Chinese Remainder theorem, the first known computerized formalization of its number-theoretical version was performed using the inductive engine of the Rewrite Rule Laboratory RRL by Zhang and Hua [38]. After that, other formalizations of this theorem, also from the number-theoretical perspective, i.e., for the specific commutative rings of integers, have been reported. Schwarzweller discusses different aspects of formalizations of the CRT in Mizar, HOL Light, hol98 and Coq [33]. Also, number-theoretical formalizations of CRT in ACL2 and VeriFun have been briefly discussed, respectively, by Russinoff in [31] and Walther in [37].

In contrast with all these number-theoretical formalizations, both the Isabelle proof given by Aransay et al. in [1] and the one reported in this paper are formalizations of algebraic versions of this theorem. Ballarin in [4] explains how the locales of Isabelle were explored in order to provide the concise formalizations of the algebraic notions and results in [1], which cover the first part of Jacobson's textbook on Basic Algebra [22]. Differently from the formalization presented in this paper, the one in [1] includes the additional hypothesis of commutativity, that is indeed unnecessary. This hypothesis would be required only if one wants to prove that the ring $R/(A_1 \cdot \ldots \cdot A_k)$ is isomorphic to the ring $R/(A_1 \cap \ldots \cap A_k)$ as well as to the ring $R/A_1 \times \ldots \times R/A_k$, as stated in versions of this theorem as those given in Dummit and Foote's [12] and Hungerford's books [20]. The operator $\cdot$ above refers to the set of linear combinations of products of elements of each ideal, i.e., $A_1 \cdot \ldots \cdot A_k = \{\sum_1^n x_{i_1} * \ldots * x_{i_k} \mid n \in \mathbb{N}, x_{i_j} \in A_j, \text{ for } 1 \leq j \leq k\}$. Indeed, this isomorphism is a consequence of the identity $A_1 \cdot \ldots \cdot A_k = A_1 \cap \ldots \cap A_k$, which depends on the commutativity. Also, notice that this holds of course for the number theoretical version of the CRT since $\mathbb{Z}$ is commutative.

8.2 Formalization versus pen-and-paper proofs

We discuss some interesting aspects of the formalization regarding the pen-and-paper proofs as they are presented in algebra textbooks such as Hungerford's, and Dummit and Foote's textbooks [20], [12].

First, several concepts were formalized in a more general manner than in textbooks. For instance, in Hungerford's textbook, the definitions of left and right cosets are stated for groups. Following this approach, in the subtheory `cosets`

of the theory `algebra` from *nasalib*, the definition was specified over a group `(G,*,one)` and a subgroup H of G as:

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

We generalize this specification of left and right cosets over sets of type `set[T]` with a binary operation `+` as:

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

In this manner it is possible to apply this definition over other structures different from groups, thus reducing the number of proofs obligations generated by PVS since it is not necessary to check that `G` and `H` are respectively a group and a subgroup.

Second, some proofs were modified. The specification of the CRT for ring theory follows the presentation by Dummit and Foote's in [12] but the formalization differs of the proof presented in such textbook in some aspects. For example, Dummit and Foote consider the theorem for a ring R with identity $one \neq zero$ excluding the zero ring as a possible case, which is not required in the formalization. Also, Dummit and Foote's proof considers only the case of two ideals, arguing that the general case can be verified easily by induction. Formalizing CRT for rings following this approach, if possible, would have a higher cost than our direct proof. For example, in order to formalize that the map

```
phi = LAMBDA (x: (R)): (# length := length(fsA),
            seq := (LAMBDA (i: below[length(fsA)]): x + fsA(i)) #)
```

defined from a ring `R` to the Cartesian product $\texttt{R}/A_1 \times \ldots \times \texttt{R}/A_k$ over a sequence $\texttt{fsA} = (A_1, \ldots, A_k)$ of ideals (see Specification 32) is a homomorphism, one must verify, for instance, that for all $j \leq k$, and a, b in `R`, $(a+b)+A_j = (a+A_j)+(b+A_j)$ holds. It can be easily verified, for all $j \leq k$, applying a lemma that establishes a characterization for addition of cosets of a quotient ring. Notice that, it has an equivalent cost of the analysis for two ideals in a proof by induction, where $k = 2$. Besides, in the induction step, the analysis given for two ideals cannot be replied in a straightforward manner since one has to build structures such as an ideal A such that $(R/A_1 \times \ldots \times R/A_n) \simeq R/A$, to be able to apply the reasoning for two ideals to conclude that the map `phi` is a homomorphism from `R` to $R/A \times R/A_{n+1}$.

Finally, it is worth highlighting the difference between the formalization in PVS and the version presented in Hungerford's textbook of the following result about homomorphism of rings:

Lemma 4 (Items 2 and 4, Corollary 2.21 in [20]) *If R is a ring with $one_R \neq zero_R$ then R has no proper ideals iff every nonzero homomorphism of rings from R to S is a monomorphism.*

R has no proper ideal means that the only ideals of R are R and $\{zero_R\}$. Hungerford argues that if $I \neq R$ then the canonical map $\pi : R \to R/I$ satisfying $\pi(r) = r + I$, $r \in R$, is a nonzero homomorphism, whose kernel is equal to I. Since π is a monomorphism iff $ker(\pi) = \{zero_R\}$, one can infer that π is a monomorphism iff $I = \{zero_R\}$, that is iff R has no proper ideals. Despite this, it was not possible to specify such a result using just an "if and only if" formula. We partitioned such lemma into two other, as shown in the Specification 39. In order to guarantee the generality of the rings R and S, we had to let clear that these structures have no necessarily the same types. Because of this, R and S were declared as ring variables over types `T1` and `T2`: `R: ring_with_one[T1,s1,p1,zero1,one1]`

and `S:ring[T2,s2,p2,zero2]` (see Lemma `mono_no_prop_id`). In order to prove necessity of the Lemma 4 (Lemma `no_prop_id_mono`), one has to provide an instantiation for the homomorphism π, whose co-domain is $S = R/I$, but if the type of the ring S were assigned as `T2` such instantiation would not be possible since the type of ring R/I is `coset(R,I)`. Since the sufficiency of Lemma 4 does not depend of the canonical homomorphism π, it is not necessary to restrict the type of the ring S as shown in the Lemma `mono_no_prop_id`.

Specification 39 Specification that differs of its enunciated in algebra textbooks

```
no_prop_id_mono: LEMMA
(FORALL(R:ring_with_one[T1,s1,p1,zero1,one1],I: ideal[T1,s1,p1,zero1](R)):
 (FORALL(S:ring[coset[T1,s1](R,I),add[T1,s1](R,I),product(R,I),I],
  phi:R_homomorphism[T1,s1,p1,zero1,coset[T1,s1](R,I),add[T1,s1](R,I),
                     product(R,I),I](R,S)):
 NOT zero_homomorphism?[T1,s1,p1,zero1,coset[T1,s1](R,I),add[T1,s1](R,I),
                        product(R,I),I](R,S)(phi) IMPLIES
 R_monomorphism?[T1,s1,p1,zero1,coset[T1,s1](R,I),add[T1,s1](R,I),
                 product(R,I),I](R,S)(phi)) IMPLIES
 I = R OR I = singleton(zero1))

mono_no_prop_id: LEMMA
(FORALL(R: ring_with_one[T1,s1,p1,zero1,one1],S:ring[T2,s2,p2,zero2],
 phi:R_homomorphism[T1,s1,p1,zero1,T2,s2,p2,zero2](R, S)):
  (FORALL(I: ideal[T1,s1,p1,zero1](R)):(I = R OR I = singleton(zero1)))
   IMPLIES (NOT zero_homomorphism?(R,S)(phi) IMPLIES
   R_monomorphism?(R,S)(phi)))
```

9 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. Furthermore, to illustrate the advantages and possible applications of such a general algebraic approach, an elaborated and complete formalization of the Chinese Remainder Theorem for rings was developed. Also, it was discussed how a full formalization of the Chinese Remainder Theorem for integers was obtained as a corollary of the general algebraic version of CRT for rings. For doing that, additional formalizations of properties of the rings $\mathbb{Z}$ and $\mathbb{Z}_n$ were necessary.

From a total of 1356 formulas formalized in theory `algebra`, the development reported in this paper (`rings` theory) consists of 583 formalized formulas (lemmas and theorems), from which CRT for rings includes 315 formulas, counting all its dependencies. The amount of formalized results indicates this formalization contributed significantly to the enrichment of theory `algebra`.

Ring theory has many relevant applications in fields such as coding theory, segmentation of digital images, cryptography, among others. In this sense, the `rings` PVS theory development conforms a robust basis towards 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 ring 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 $\mathbb{Z}_{p^n}$, for p a prime number, as an example of local rings.

References

1. Aransay, J., Ballarin, C., Baillon, M., de Vilhena, P.E., Hohe, S., Kammüller, F., Paulson, L.C.: The Isabelle/HOL Algebra Library. Tech. rep., Isabelle Library, University of Cambridge Computer Laboratory and Technische Universität München (2019). URL https://isabelle.in.tum.de/dist/library/HOL/HOL-Algebra/document.pdf
2. Artin, M.: Algebra, 2 edn. Pearson (2010)
3. Ayala-Rincón, M., de Moura, F.L.C.: Applied Logic for Computer Scientists: Computational Deduction and Formal Proofs. UTiCS. Springer (2017). URL https://doi.org/10.1007/978-3-319-51653-0
4. Ballarin, C.: Exploring the structure of an algebra text with locales. Journal of Automated Reasoning (2019). URL https://doi.org/10.1007/s10817-019-09537-9
5. Bini, G., Flamini, F.: Finite commutative rings and their applications, vol. 680. Springer Science & Business Media (2012)
6. Butler, R., Lester, D.: A PVS *Theory* for Abstract Algebra (2007). URL http://shemesh.larc.nasa.gov/fm/ftp/larc/PVS-library/pvslib.html. Accessed in March 31, 2019
7. Butler, R.W.: Formalization of the Integral Calculus in the PVS Theorem Prover. Journal of Formalized Reasoning **2**(1), 1–26 (2009). URL https://doi.org/10.6092/issn.1972-5787/1349
8. Cano, G., Cohen, C., Dénès, M., Mörtberg, A., Siles, V.: Formalized linear algebra over Elementary Divisor Rings in Coq. Logical Methods in Computer Science **12**(2:7), 1–23 (2016). URL https://doi.org/10.2168/LMCS-12(2:7)2016
9. Cohen, C., Mahboubi, A.: Formal proofs in real algebraic geometry: from ordered fields to quantifier elimination. Logical Methods in Computer Science **8**(1:2), 1–40 (2012). URL https://doi.org/10.2168/LMCS-8(1:2)2012
10. mathlib Community, T.: The Lean Mathematical Library. In: Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs, CPP 2020, pp. 367–381. ACM (2020). URL https://doi.org/10.1145/3372885.3373824
11. Ding, C., Pei, D., Salomaa, A.: Chinese Remainder Theorem: Applications in Computing, Coding, Cryptography. World Scientific Publishing Co., Inc., River Edge, NJ, USA (1996). URL https://doi.org/10.1142/3254
12. Dummit, D.S., Foote, R.M.: Abstract Algebra, 3 edn. Wiley (2003)
13. Galdino, A.L., Ayala-Rincón, M.: A PVS Theory for Term Rewriting Systems. Electronic Notes in Theoretical Computer Science **247**, 67–83 (2009). URL https://doi.org/10.1016/j.entcs.2009.07.049
14. Geuvers, H., Pollack, R., Wiedijk, F., Zwanenburg, J.: A constructive algebraic hierarchy in Coq. Journal of Symbolic Computation **34**(4), 271–286 (2002). URL https://doi.org/10.1006/jsco.2002.0552
15. Gonthier, G., Asperti, A., Avigad, J., Bertot, Y., Cohen, C., Garillot, F., Roux, S.L., Mahboubi, A., O'Connor, R., Biha, S.O., Pasca, I., Rideau, L., Solovyev, A., Tassi, E., Théry, L.: A Machine-Checked Proof of the Odd Order Theorem. In: 4th International Conference on Interactive Theorem Proving ITP, *Lecture Notes in Computer Science*, vol. 7998, pp. 163–179. Springer (2013). URL https://doi.org/10.1007/978-3-642-39634-2_14

16. Gonthier, G., Mahboubi, A., Rideau, L., Tassi, E., Théry, L.: A Modular Formalisation of Finite Group Theory. In: 20th International Conference Theorem Proving in Higher Order Logics TPHOLs, *Lecture Notes in Computer Science*, vol. 4732, pp. 86–101. Springer (2007). URL https://doi.org/10.1007/978-3-540-74591-4_8
17. Großschädl, J.: The Chinese Remainder Theorem and its Application in a High-Speed RSA Crypto Chip. In: 16th Annual Computer Security Applications Conference ACSAC, pp. 384–393. IEEE Computer Society (2000). URL https://doi.org/10.1109/ACSAC.2000.898893
18. Heras, J., Martín-Mateos, F.J., Pascual, V.: Modelling algebraic structures and morphisms in ACL2. Applicable Algebra in Engineering, Communication and Computing **26**(3), 277–303 (2015). URL https://doi.org/10.1007/s00200-015-0252-9
19. Herstein, I.N.: Topics in algebra, 2 edn. Xerox College Publishing, Lexington, Mass.-Toronto, Ont. (1975)
20. Hungerford, T.W.: Algebra, *Graduate Texts in Mathematics*, vol. 73. Springer-Verlag, New York-Berlin (1980). Reprint of the 1974 original
21. Jackson, P.B.: Enhancing the Nuprl Proof Development System and Applying it to Computational Abstract Algebra. Ph.D. thesis, Cornell University (1995)
22. Jacobson, N.: Basic Algebra I, second edn. Dover Books on Mathematics. Dover Publications (2009)
23. Kornilowicz, A., Schwarzweller, C.: The First Isomorphism Theorem and Other Properties of Rings. Formalized Mathematics **22**(4), 291– 301 (2014). URL https://doi.org/10.2478/forma-2014-0029
24. Lester, D.: A PVS *Theory* for Continuity, Homeomorphisms, Connected and Compact Spaces, Borel sets/functions (2009). URL http://shemesh.larc.nasa.gov/fm/ftp/larc/PVS-library/pvslib.html. Accessed in March 31, 2019
25. Liang, H., Li, X., Xia, X.: Adaptive Frequency Estimation with Low Sampling Rates Based on Robust Chinese Remainder Theorem and IIR notch Filter. Advances in Adaptive Data Analysis **1**(4), 587–600 (2009). URL https://doi.org/10.1142/S1793536909000230
26. Lidl, R., Niederreiter, H.: Introduction to finite fields and their applications. Cambridge University Press, Cambridge (1994)
27. Noether, E.: Abstrakter Aufbau der Idealtheorie in algebraischen Zahl- und Funktionenkörpern. Mathematische Annalen **96**(1), 26–61 (1927)
28. Owre, S., Shankar, N.: The Formal Semantics of PVS. Tech. Rep. 97-2R, SRI International Computer Science Laboratory, Menlo Park CA 94025 USA (1997, revised 1999)
29. Philipoom, J.: Correct-by-Construction Finite Field Arithmetic in Coq. Master's thesis, Master of Engineering in Computer Science, MIT (2018)
30. Putinar, M., Sullivant, S.: Emerging Applications of Algebraic Geometry. The IMA Volumes in Mathematics and its Applications. Springer New York (2008). URL https://doi.org/10.1007/978-0-387-09686-5
31. Russinoff, D.M.: A Mechanical Proof of the Chinese Remainder Theorem. UTCS Technical Report - no longer available - ACL2 Workshop 2000 TR-00-29, University of Texas at Austin (2000)
32. Schwarzweller, C.: The Binomial Theorem for Algebraic Structures. Journal of Formalized Mathematics **12**(3), 559–564 (2003). URL http://mizar.org/JFM/Vol12/binom.html
33. Schwarzweller, C.: The Chinese Remainder Theorem, its Proofs and its Generalizations in Mathematical Repositories. Studies in Logic, Grammar and Rhetoric **18**(31), 103–119 (2009). URL https://philpapers.org/rec/SCHTCR-12
34. 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). URL https://doi.org/10.1007/978-3-319-94821-8_3
35. 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). URL https://doi.org/10.14810/ijscmc.2014.3405
36. van der Waerden, B.L.: Algebra, vol. I. Springer-Verlag New York (1991)
37. Walther, C.: A Machine Assisted Proof of the Chinese Remainder Theorem. Technical Report VFR 18/03, FB Informatik, Technische Universität Darmstadt (2018)
38. Zhang, H., Hua, X.: Proving the Chinese Remainder Theorem by the Cover Set Induction. In: 11th International Conference on Automated Deduction CADE, *Lecture Notes in Computer Science*, vol. 607, pp. 431–445. Springer (1992). URL https://doi.org/10.1007/3-540-55602-8_182