

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 important results in ring theory, including as main formalizations 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 rings, as presented in abstract algebra textbooks, that is proved as a consequence of the First Isomorphism Theorem. From this general version of the CRT for rings, a formalization of the well-known specific number-theoretical version of the CRT for the ring of integers, which is the version usually found in such kind of formalizations, is obtained as a corollary.

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 textbooks on abstract algebra such as [18] and [10]. Indeed, [18] is the main reference and the results about homomorphisms, prime, maximal and principal ideals follow the same presentation of this book, whereas the Chinese Remainder Theorem follows the approach in [10]. Other textbooks (c.f. [17,2,20]) were employed mainly to consult different pen-and-paper proofs and to compare with related work.

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

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 [4]. Regarding coding theory, commutative rings with identity and polynomials over such structures have an important role to describe redundant codes according to [24]. Also, ring theory forms the basis for algebraic geometry, which has applications in engineering systems, statistics, modeling of biological processes and computer algebra [26]. Other relevant application of ring theory is in the analysis of images. According to [31], 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. [31] 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 Library⁴ (*nasalib*) that contains many theories in several subjects, such as analysis [6], topology [22], term rewriting systems [11], among others. In particular, *nasalib* contains the theory **algebra** [5], 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) and the First Isomorphism Theorem, as shortly reported in [30]. Homomorphisms and cosets were separately defined in the particular context of rings and ideals in [30] and just for groups and normal subgroups in [5]. 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**.

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 subtheories of the theory **rings** in [30] related to homomorphisms, cosets and quotient rings as well as the formalization of the First Isomorphism Theorem, were restructured. In this work, homomorphisms are specified for groupoids 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.

⁴ Available at <https://shemesh.larc.nasa.gov/fm/ftp/larc/PVS-library/>

- (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) To illustrate the usability of the development, 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, 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 as part of the *nasalib* both for PVS 6 and for the snapshot 1218 (Allegro) of PVS 7.0. The development is also available at <http://ayala.mat.unb.br/publications.html>.

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 [18, 17, 10, 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 $\varphi : R \rightarrow S$ 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 subtheories `ring_1st_isomorphism_theorem` and `ring_2nd_3rd_isomorphism_theorems` (see Figure 1). The subtheories of the theory `algebra` that were relevant for the formalization of the isomorphism theorems are just `groupoid` and `ring`, the other three theories were imported by subtheories related with formalization of properties of ideals in the next subsection.

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

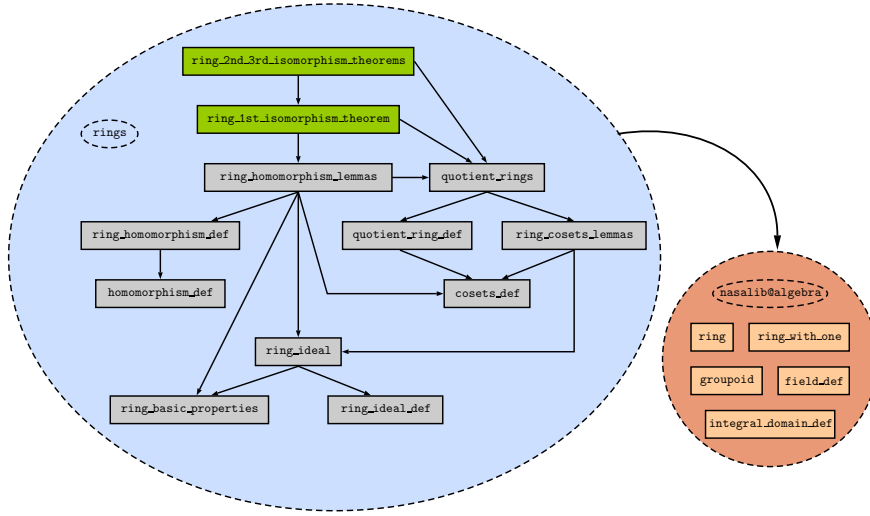


Fig. 1 Hierarchy of the subtheories for isomorphism theorems for rings: `ring_1st_isomorphism_theorem` and `ring_2nd_3rd_isomorphism_theorems`

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 then M is a maximal ideal.*

Results of this subsection were formalized in subtheories of `rings` depicted in Figure 2. Theorem 4 was formalized in the subtheories `ring_principal_ideal` and `ring_with_id.one_generator`, Theorems 5, 6, 7 and 8 were formalized in the subtheories `ring_prime_ideal`, `ring_with.one_prime_ideal`, `ring_maximal_ideal` and `ring_with.one_maximal_ideal`, respectively. The subtheories of the theory `algebra` imported for the formalization of the properties on ideals discussed here are `ring_with.one`, `integral_domain_def` and `field_def` that were omitted from Figure 2 for simplicity (see Figure 1).

3 Formalization of morphisms and basic algebraic structures

In this section, the PVS subtheories 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 subtheories `homomorphisms_def`, `ring_homomorphisms_def` and `ring_homomorphism_lemmas`. 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.

This specification requires that R and S be groupoids. A groupoid $(G, *)$ 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 ones 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 presented in `nasalib/algebra@homomorphisms`. Furthermore, the proof obligations generated by the new specification of homomorphism are easier to check, since verifying whether a structure is a groupoid has a much lower cost than checking whether the structure is a group.

3.1.2 Subtheory `ring_homomorphisms_def`

The definition of a ring homomorphism must consider homomorphisms related with each one of the two operations over a ring R . In order to facilitate the formalization of the properties about ring homomorphisms, the specification of the predicate `R_homomorphism?(R1, R2)(phi)` was provided in a context containing sets R_1 and R_2 whose elements have arbitrary types T_1 and T_2 respectively, where operations s_1 and p_1 are well defined over R_1 whereas s_2 and p_2 are also over R_2 (see Specification 3). This is done in subtheory `ring_homomorphisms_def`. Because the specification of `R_homomorphism?(R1, R2)(phi)` makes use of the definition `homomorphism?(R1, R2)(phi)` specified in `homomorphisms_def`, one must ensure that R_1 and R_2 are groupoids under the operations mentioned above.

Specification 3 Specification of `R_homomorphism?(R1, R2)(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 groupoids, a simpler characterization of ring homomorphisms obtained from the specification of

ring homomorphism, $\mathbf{R_homomorphism?}(R_1, R_2)(\phi)$, 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 $\varphi : R \rightarrow S$ is a ring homomorphism and x is an element of R then $\varphi(\text{zero}_R) = \text{zero}_S$ and $\varphi(\text{inv}(x)) = \text{inv}(\varphi(x))$, where $\text{inv}(x)$ denotes the inverse of the element x according to the operation $+_R$;
- the image of a ring homomorphism is a ring;
- the kernel of a homomorphism is an ideal;
- the characterization of an injective homomorphism φ based on $\text{ker}\varphi$.

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 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 $+(g, H)$, $+(H, g)$ and $\text{sum}(H, I)$, 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 $\text{sum}(H, I)$ can be used in the formalization of the Second Isomorphism Theorem, where H is a subring and I is an ideal of a ring R , as well as in other contexts involving the sum or any other binary operation of two arbitrary structures containing elements of the same type. For example, the hypothesis $R * R = R$ in Theorem 7 was specified as $\text{sum}[T, *](R, R) = R$. The sets $+(g, H)$ and $+(H, g)$ were used to specify the notion of cosets in a general way (see Specification 7). Also, generators of left and right cosets were defined as $\text{lc_gen}(G, H)$ and $\text{rc_gen}(G, H)$.

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 .

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 11.

Specification 11 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 groupoids 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 12.

Specification 12 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 12. But, in the subtheory `ring_homomorphism_lemmas`, R_1 and R_2 were considered as rings, structures of the form $(R_1, +_{R_1}, *__{R_1}, \text{zero}_{R_1})$ and $(R_2, +_{R_2}, *__{R_2}, \text{zero}_{R_2})$ and, as consequence of this, lemmas involving kernel were formally proved, among them:

- the kernel of a ring homomorphism $\varphi : R_1 \rightarrow R_2$ 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 subtheory `quotient_ring_def`, as show in Specification 13, where in particular $/(\mathbf{R}, \mathbf{I})$ is a prefix notation for R/I .

Specification 13 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

/(\mathbf{R}, \mathbf{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 13), where A is a coset of an ideal I in R . Other properties about quotient rings were formalized in the subtheories `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 $\text{add}(A, B) = (a + b) + I$ and $\text{product}(A, B) = (a * b) + I$.
- (ii) A proof that $(R/I, \text{add}, \text{product}, I)$ 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 $\text{one}_R + I$ 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 $I \neq \text{one}_R + I$. This result is widely used in the formalization of Theorem 6 in order to guarantee that the quotient R/P has the identity $\text{one}_R + P \neq P$ 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 subtheories 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 $\phi : R \rightarrow S$ is a homomorphism of rings and I is an ideal of R , which is contained in the kernel of ϕ , then there is a homomorphism of rings $f : R/I \rightarrow S$ such that $f(a+I) = \phi(a)$ 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 is constructive. First, it was verified 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 monomorphisms 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 14 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 14 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 14 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 $\varphi : H \rightarrow (H + I)/I$ 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 $\varphi : R/J \rightarrow R/I$ such that $\ker(\varphi) = I/J$.*

The Second and Third Isomorphism Theorems, given in Specification 15, were formalized applying the First Isomorphism Theorem with Lemmas 2 and 3, respectively.

Specification 15 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 subtheories 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 16 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 $\{r*a + a*s + n*a + \sum_{i=1}^m r_i*a*s_i \mid r, s, r_i, s_i \in R; m \in \mathbb{N} \setminus \{0\}; n \in \mathbb{Z}\}$ 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 $F: \text{nat} \rightarrow T$; 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 16 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 17 and 18.

Specification 17 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 18 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 subtheories 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 19);

- `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 20).

Specification 19 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 20 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 17 and 18).

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 21).

Specification 21 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)}
```

In the subtheory `ring_prime_ideal` one can find the formalization of Theorem 5, whose specification is given by lemmas `prime_ideal_prop1` and `prime_ideal_prop2` (see Specification 22). 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 17) that states that `commutative_one_gen(R)(a)`, for any a in R , is an ideal in R .

Specification 22 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 23. 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 23), 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 `quotient_ring_def` (see Specification 13). 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 [18]. 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 23 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 24.

Specification 24 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 25) 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 26.

Specification 25 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 26 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 27 and 28. 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 [18] 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 27 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 28 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.

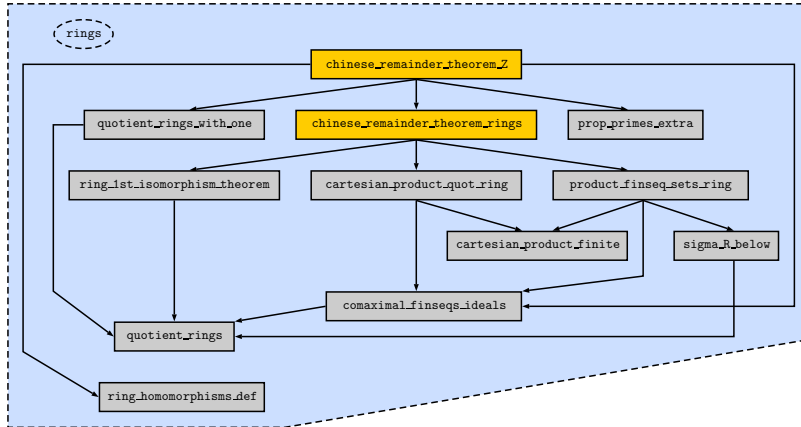


Fig. 3 Hierarchy of the subtheories for the Chinese Remainder Theorems for rings and integers

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 [10]).

Theorem 9 (Chinese Remainder Theorem: general algebraic version)

Let R be a ring with identity and A_1, A_2, \dots, A_k ideals in R . The map

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

is a ring homomorphism with kernel $A_1 \cap \dots \cap A_k$. If the condition $A_i + A_j = R$ holds for each $i, j \in \{1, \dots, k\}$ with $i \neq j$, which is called comaximality, then φ is surjective and the rings $R/(A_1 \cap \dots \cap A_k)$ and $R/A_1 \times \dots \times R/A_k$ 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 $A_1 \cap \dots \cap A_k$. See Specification 29.

Specification 29 φ is a homomorphism with kernel $A_1 \cap \dots \cap A_k$

```

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))

```

To do this, firstly, it was necessary to ensure that the domain and codomain of φ are rings, that is, one must prove that the Cartesian product of quotient rings with adequate operations and constant is a ring.

The development includes the first formalization of Cartesian product of sets of arbitrary types in the subtheory `Cartesian_product_finite`. The last subtheory together with the subtheory `Cartesian_product_quot_ring` contain the technical elements required to formalize that $R/A_1 \times \dots \times R/A_k$ is indeed a ring.

The constructor `Cartesian_product_n` that is based on finite sequences, was developed in order to specify a finite Cartesian product for arbitrary sets. See code in Specification 30, part of the subtheory `Cartesian_product_finite`.

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

```

In a context where elements of type T under operations $+$ and $*$ constitute a ring, the operations of addition (`Sfs`) and multiplication (`Pfs`) were specified for a finite Cartesian product of quotient rings, see Specification 31. Furthermore, it was formalized as Lemma `Cartesian_product_quot_ring_is_ring` that this Cartesian product is a ring. For this the constructs `fsRI(R)` and `fsQ(R)` were specified based on the data structure of finite sequences. These constructors represent a finite sequence of ideals and a finite sequence of quotient rings, respectively.

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

```

R: VAR ring[T,+,*,zero]
fsA: VAR finseq[set[T]]
fsQ: VAR finseq[setof[set[T]]]
                                     % Predicate for sequence of ideals
fsRI?(R)(fsA): bool = FORALL (i: below[length(fsA)]): ideal?(fsA(i), R)

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 was proved to be a homomorphism by checking the definition conditions, whereas the characterization of the kernel of φ as the intersection $A_1 \cap \dots \cap A_k$ was established by extensionality (i.e., extensional equality), observing that the neutral element for addition over the Cartesian product of quotient $R/A_1 \times \dots \times R/A_k$ is the sequence of ideals (A_1, \dots, A_k) .

Step 2. Prove that φ is surjective. This step uses the hypothesis that the ideals A_1, \dots, 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 32.

Specification 32 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 33, is to build a sequence $s = (s(1), \dots, s(k))$ over R such that $s(i) \in A_j$ for all

$j \neq i$ and $s(i) + A_i = \text{one} + A_i$. The elements of this sequence are characterized as $s(i) = \prod_{j=1}^{i-1} (\text{one} - x_j) * \prod_{j=i+1}^k (\text{one} - x_j)$, where $x_j \in A_i$ and $y_j = (\text{one} - x_j) \in A_j$ for each $j = 1, \dots, i-1, i+1, k$. 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 $\text{one} = x_i + y_j$ whenever $i \neq j$. By performing calculations over $s(i)$, since A_i is closed under addition and multiplication, one can infer that $s(i) = \text{one} + a$, where $a \in A_i$. Consequently, $s(i) + A_i = \text{one} + (a + A_i) = \text{one} + A_i$. Now, it is not difficult to establish that the map φ is surjective. Consider $y = (r_1 + A_1, \dots, r_k + A_k) \in R/A_1 \times \dots \times R/A_k$, 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 $(\sum_{i=1}^k s(i) * r_i) + A_i = (s(i) * r_i) + A_i$, since $s(j) \in A_i$ for $i \neq j$. Consequently, $(\sum_{i=1}^k s(i) * r_i) + A_i = (\text{one} + A_i) * (r_i + A_i) = r_i + A_i$ and $\varphi(x) = y$.

Specification 33 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 $0 \leq i, j \leq \text{length}(\text{fsA}) - 1$, `oneSet(R, fsA)(i, j) = \{x \in \text{fsA}(i) | (\text{one} - x) \in \text{fsA}(j), \text{ 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 34. Specifically, to construct s , the sequence `fs` in `product_fs_rec(fs)` has length $k - 1$ and was built from a choice function for nonempty sets established in the native library of PVS, where for each $1 \leq j \leq k, j \neq i, \text{fs}(i) = \text{one} - \text{choose}(\text{oneSet}(R, \text{fsA})(i, j))$. 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 35).

Specification 34 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 35 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 $R/(A_1 \cap \dots \cap A_k)$ and $R/A_1 \times \dots \times R/A_k$ are isomorphic.

Specification 36 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 36) is a direct consequence of the First Isomorphism Theorem. In fact, in Theorem 1 one must consider the ring homomorphism

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

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

7 Formalization of the number-theoretical CRT

This section shows how the general version of CRT for rings, explained in previous section, is used to formalize the CRT for integers (see Figure 3, subtheory `chinese_remainder_theorem_Z`). This is an interesting application showing how formalized results about general abstract algebraic structures may be applied to obtain important results about properties of numerical structures.

The Chinese Remainder Theorem for integers is well-known as a classical result in number theory with applications in computing and coding [9], security [15] [9], signal processing [23] 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 (Chinese Remainder Theorem: number-theoretical version for \mathbb{Z}) *Let m_1, m_2, \dots, m_k be positive integers such that m_i and m_j are coprime for $i \neq j$ and let $m = m_1 \cdot m_2 \cdot \dots \cdot m_k$. Then there is an isomorphism between the rings Z_m and the Cartesian product $Z_{m_1} \times \dots \times Z_{m_k}$.*

Specification 37 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 conclude that there is an isomorphism between the rings Z_m and the Cartesian product $Z_{m_1} \times \dots \times Z_{m_k}$, where $m = m_1 \cdot m_2 \dots m_k$.

Instantiating Theorem 9 as before, one can initially infer that there is a homomorphism from \mathbb{Z} to $Z_{m_1} \times \dots \times Z_{m_k}$. 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, \dots, 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 $i, j \in \{1, \dots, k\}$ with $i \neq j$. This shows that there is an isomorphism between the rings Z_m and $Z_{m_1} \times \dots \times Z_{m_k}$, where m is as above, since $m_1\mathbb{Z} \cap \dots \cap m_k\mathbb{Z} = m\mathbb{Z}$. Thus, the number-theoretical version of the CRT is concluded.

Specification 37 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)

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 LET lcm = n*m/gcd(n,m) IN
  intersection(nZ(n),nZ(m)) = nZ(lcm)

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))))

```

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 37). Indeed, in order to prove the inclusion $\frac{n * m}{gcd(n, m)}\mathbb{Z} \subset n\mathbb{Z} \cap m\mathbb{Z}$, required to prove `nZ_mZ_intersection`, it is necessary to prove $n * \frac{m}{gcd(n, m)}\mathbb{Z} \subset n\mathbb{Z}$ and $\frac{n * m}{gcd(m, n)}\mathbb{Z} = m * \frac{n}{gcd(n, m)}\mathbb{Z} \subset m\mathbb{Z}$. For doing this, commutativity of \mathbb{Z} is re-

quired 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`: $m_1\mathbb{Z} \cap \dots \cap m_k\mathbb{Z} = (m_1 \cdot \dots \cdot m_k)\mathbb{Z}$.

8 Related work

Regarding previous PVS work in theories `algebra` ([5]) and `rings` ([30]), 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 groupoids 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.

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 [12]; further related formalizations in Coq deal with finite group theory [14] 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 [13]. Also in Coq, formalizations of real ordered fields [8] and finite fields (to check elliptic curve cryptography) [25], and a formalization of rings with explicit divisibility [7] are available. In Nuprl and Mizar it is provided a formal proof of the Binomial Theorem for rings, [19,28], respectively. In ACL2 a hierarchy of algebraic structures ranging from setoids to vector spaces is built focusing on the formalization of computer algebra systems [16]. 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 [21] (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 the number-theoretical version) was performed using the inductive engine of the Rewrite Rule Laboratory RRL [33]. After that, other formalizations of this theorem, also from the number-theoretical perspective, that is for the structure of integers, have been reported. The author in [29] discusses different aspects of formalizations of the CRT in Mizar, HOL Light, hol98 and Coq. Also, number-theoretical formalizations of CRT in ACL2 and VeriFun have been briefly discussed, respectively, in [27] and [32].

In contrast with all these number-theoretical formalizations, both the Isabelle proof given in [1] and the one reported in this paper are formalizations of algebraic versions of this theorem. In [3] it is explained 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 [20]. 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 $R/(A_1 \cdot \dots \cdot A_k)$ is isomorphic to the ring $R/(A_1 \cap \dots \cap A_k)$ as well as to the ring $R/A_1 \times \dots \times R/A_k$, as stated in versions of this theorem as those given in [10] and [18]. The operator \cdot above refers to the set of linear combinations of products of elements of each ideal¹. Indeed, this isomorphism is a consequence of the identity $A_1 \cdot \dots \cdot A_k = A_1 \cap \dots \cap A_k$, which depends on the commutativity. Also, notice that this holds of course for the numer theoretical version of the CRT since \mathbb{Z} is commutative.

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, as well as 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 and it was discussed how, by providing a few additional formalizations of properties of the rings Z and Z_n , a full formalization of the Chinese Remainder Theorem for integers was obtained as a corollary of the general algebraic version of CRT for rings.

The whole development consists of 511 formalized formulas, from which CRT for rings includes 285 formulas counting all its dependencies. The specification consists of 2.400 lines of code and 74K, and the formalization of 5.2M and 83.293 lines.

Ring theory has a number of important applications in coding theory, segmentation of digital images, cryptography, among others. In this sense, the development of the PVS theory `rings` conforms a robust basis towards the construction of more elaborated theories involving rings, their properties and application.

As future work, one can highlight the development of results about factorization in commutative rings with identity: since the notion of divisibility and prime elements could be defined in such structures, a formalization of an analogue of the Fundamental Theorem of Arithmetic for principal ideal domains would be of great interest. Furthermore, developments of subtheories about rings of polynomials, including notions of factorization and a division algorithm in such rings as well as formalization of the Eisenstein’s irreducibility criterion are important landmarks that might enrich the theory `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

¹ $A_1 \cdot \dots \cdot A_k = \{\sum_1^n x_{i_1} * \dots * x_{i_k} \mid n \in \mathbb{N}, x_{i_j} \in A_j, \text{ for } 1 \leq j \leq k\}$

- 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. 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>
 4. Bini, G., Flamini, F.: Finite commutative rings and their applications, vol. 680. Springer Science & Business Media (2012)
 5. 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
 6. 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>
 7. 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](https://doi.org/10.2168/LMCS-12(2:7)2016)
 8. 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](https://doi.org/10.2168/LMCS-8(1:2)2012)
 9. 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>
 10. Dummit, D.S., Foote, R.M.: Abstract Algebra, 3 edn. Wiley (2003)
 11. 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>
 12. 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>
 13. 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
 14. 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
 15. 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>
 16. 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>
 17. Herstein, I.N.: Topics in algebra, 2 edn. Xerox College Publishing, Lexington, Mass.-Toronto, Ont. (1975)
 18. Hungerford, T.W.: Algebra, *Graduate Texts in Mathematics*, vol. 73. Springer-Verlag, New York-Berlin (1980). Reprint of the 1974 original
 19. Jackson, P.B.: Enhancing the Nuprl Proof Development System and Applying it to Computational Abstract Algebra. Ph.D. thesis, Cornell University (1995)
 20. Jacobson, N.: Basic Algebra I, second edn. Dover Books on Mathematics. Dover Publications (2009)
 21. 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>
 22. 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
 23. 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>

24. Lidl, R., Niederreiter, H.: Introduction to finite fields and their applications. Cambridge University Press, Cambridge (1994)
25. Philipoom, J.: Correct-by-Construction Finite Field Arithmetic in Coq. Master's thesis, Master of Engineering in Computer Science, MIT (2018)
26. 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>
27. 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)
28. 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>
29. 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>
30. 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
31. 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>
32. Walther, C.: A Machine Assisted Proof of the Chinese Remainder Theorem. Technical Report VFR 18/03, FB Informatik, Technische Universität Darmstadt (2018)
33. 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