



# Formalization of Algebraic Theorems in PVS\*

## (Invited Talk)

Mauricio Ayala-Rincón<sup>1</sup>, Thaynara Arielly de Lima<sup>2</sup>, Andréia Borges Avelar<sup>3</sup>, and André Luiz Galdino<sup>4</sup>

<sup>1</sup> Universidade de Brasília - Brasília D.F., Brasil  
ayala@unb.br

<sup>2</sup> Universidade Federal de Goiás - Goiás, Brasil  
thaynaradelima@ufg.br

<sup>3</sup> Universidade de Brasília - Planaltina, Brasil  
andreiaavelar@unb.br

<sup>4</sup> Universidade Federal de Catalão - Catalão, Brasil  
andregaldino@ufcat.edu.br

### Abstract

This talk discusses current extensions on the theory `algebra` from the NASA/PVSlibrary on formal developments for the Prototype Verification System (PVS). It discusses the approach to formalizing theorems of the ring theory and how they are applied to infer properties of specific algebraic structures. As cases of study, we will present recent formalizations on the theories of Euclidean Domains and Quaternions. Moreover, we will show how a general verification of Euclid's division algorithm can be specialized to verify this algorithm for specific Euclidean Domains, and how the abstract theory of Quaternions can be parameterized to deal with the structure of Hamilton's Quaternions.

## 1 Introduction

The PVS `algebra` [↗](#) library, part of the NASA/PVSlib, was recently enriched with a series of theorems on rings. The extension includes complete formalizations of the isomorphism theorems for rings, principal, prime, and maximal ideals, and an abstract version of the Chinese Remainder Theorem (CRT), which holds for abstract rings, even non-commutative rings. The benefit of formalizing algebraic results from this abstract theoretical perspective was made evident by showing how, from the abstract version of CRT, the formally verified well-known numerical version of CRT for the ring of integers  $\mathbb{Z}$  is obtained [6]. In this talk, we discuss another substantial step towards enriching the PVS abstract algebra library by formalizing properties about factorization in commutative rings regarding both unique factorization domains, and Euclidean rings [7]. Roughly, unique factorization domains are abstract structures for which a general

---

\*Project supported by FAPDF DE 00193.00001175/21-11, CNPq Universal 409003/21-2, and FAPEG 202310267000223 grants. Speaker partially funded by CNPq grant 313290/21-0.

version of the Fundamental Theorem of Arithmetic holds. On the other hand, Euclidean rings are equipped with a norm that allows defining a suitable generalization of Euclid's division lemma and, therefore, of notions such as the greatest common divisor (`gcd`). The practicality of `gcd` is well-known in the ring  $\mathbb{Z}$ . Nevertheless, mathematicians know this notion is of general fundamental importance in abstract Euclidean domains for which, in general, `gcd` should and may be defined differently.

The primary motivation to formalize the theory of such structures is their theoretical and practical application potential. For instance, a general abstract version of the Euclidean algorithm can be specified to determine a `gcd` between sets of elements (Euclidean `gcd` algorithm) in a Euclidean domain. Thus, since structures as the ring of integers  $\mathbb{Z}$ , the Gaussian integers  $\mathbb{Z}[i]$ , and rings of polynomials over integral domains are Euclidean domains, the Euclidean `gcd` algorithm can be applied over them.

This document includes links to parts of the extended [algebra](#) [↗](#) theory in progress.

## 2 Formalization of Euclidean Domains and Algorithms

Notions such as prime element, division, and `gcd` between two elements and some landmark results, including the Fundamental Theorem of Arithmetic, Euclid's division lemma, and Euclidean Algorithm, are well established and widespread for the ring of integers. These concepts and general versions of exciting results are extended for abstract algebraic structures ([14], [8], [9]) and are the scope of our formalization [6, 7].

The notions of prime and irreducible elements rely on the concept of divisibility on a ring. The notions of divisibility and associated elements are specified as curried predicates abstracted for any ring given as their first argument, `R` ([ring\\_divides\\_def](#) [↗](#)).

In Hungerford's textbook, the definition of divisibility relies on a commutative ring. It avoids the discrimination between an element's left or right divisor, and since the primary results demand commutativity, it is a reasonable requirement. However, commutativity is not a crucial property in such a notion since it only depends on the multiplication operation in a ring. Because of that, we opted to generalize the definition and specify divisibility on non-necessarily commutative rings as ([divides?\(R\)\(a,b\)](#) [↗](#)). Another interesting remark is related to the specification of [associates?\(R\)\(a,b\)](#) [↗](#). Hungerford's textbook omits that the type of the parameters `a` and `b` are non-zero elements. Of course, this is obvious since it is required in the definition of [divides?\(R\)\(a,b\)](#). However, the lack of such a hypothesis is recurrent in several statements in the textbook (for instance, in Theorem 2.1).

In the sub-theory [ring\\_divides](#) [↗](#), we formalized the properties related to the divisibility stated in Theorem 2.1. Some of them involve the object "unit". In a ring  $(R, +, *, zero, one)$  with multiplication identity `one`, an element `u` is called a *unit* if `u` is left- and right-invertible; that is, if there exist elements  $u_1^{-1}, u_2^{-1} \in R$  such that  $u * u_1^{-1} = u_2^{-1} * u = one$ .

**Theorem 2.1** (Th.3.2, Hungerford [14]). *Let  $a, b$  and  $u$  be elements of a commutative ring  $R$  with identity.*

- (i)  *$a$  divides  $b$  (denoted as  $a \mid b$ ) if and only if  $(b) \subset (a)$ , where  $(x)$  denotes the principal ideal generated by  $x$ .*
- (ii)  *$a$  and  $b$  are associates if and only if  $(a) = (b)$ .*
- (iii)  *$u$  is a unit if and only if  $u \mid r$  for all  $r \in R$ .*
- (iv)  *$u$  is a unit if and only if  $(u) = R$ .*

- (v) The relation “ $a$  and  $b$  are associates” is an equivalence relation on  $R$ .
- (vi) If  $a = br$ , where  $r \in R$  is a unit, then  $a$  and  $b$  are associates. If  $R$  is an integral domain, then the converse is true.

Theorem 2.1 has a straightforward formalization due to the robustness of the formal framework previously developed for rings and principal ideals [6]. The formalization of the properties (i), (ii), and (iv) illustrates it clearly. In fact, by definition,  $(a)$  denotes the intersection of all ideals in a ring  $R$  containing the element  $a$ . The lemma `principal_ideal_charac` in theory `ring_principal_ideal` characterizes  $(a)$  as the set `one_gen(R)(a)` in the theory `ring_one_generator`. The last characterization depends on a sum, specified as `R_sigma`, over elements of a function in the ring  $R$ , defined over abstract types, as given in the theory `ring_basic_properties`. The constructor `R_sigma` generalizes constructors in the PVSlib built for specific theories as the theory of reals. Also, since  $R$  is a commutative ring with identity, the lemma `commutative_id_one_gen_charac` provides a much simpler characterization of the set `one_gen(R)(a)`; indeed, such characterization simplifies the analysis of properties (i), (ii), and (iv) since  $(a)$  can be built as the set  $aR = \{ar : r \in R\}$ .

From the concepts of divisibility and unit, we specified prime and irreducible elements on a ring with identity as the predicates `ring_irreducible_element_def` and `ring_prime_element_def`, respectively.

In the ring of integers, prime and irreducible elements are indistinguishable. However, this is not true for all rings. For instance, 2 is prime but not irreducible in  $\mathbb{Z}_6$ . Theorem 2.2 gives some properties regarding prime and irreducible elements formalized in the subtheories `ring_prime_element` and `ring_principal_ideal_domain`. Among others, it shows that prime and irreducible elements are equal over principal ideal domains.

**Theorem 2.2** (Th.3.4, Hungerford [14]). *Let  $p$  and  $c$  be nonzero elements in an integral domain  $R$ .*

- (i)  $p$  is prime if and only if  $(p)$  is a nonzero prime ideal;
- (ii)  $c$  is irreducible if and only if  $(c)$  is maximal in the set  $S$  of all proper principal ideals of  $R$ .
- (iii) Every prime element of  $R$  is irreducible.
- (iv) If  $R$  is a principal ideal domain, then  $p$  is prime if and only if  $p$  is irreducible.
- (v) Every associate of an irreducible [resp. prime] element of  $R$  is irreducible [resp. prime].
- (vi) The only divisors of an irreducible element of  $R$  are its associates and the units of  $R$ .

Hungerford stated the result for integral domains but advised that a weakened hypothesis can be considered in some parts of the theorem. We formalize the results using the minimum number of required conditions and detect that items (i) and (vi) hold for commutative rings with identity.

Properties (i), (ii), and (iii) form the basis for the formalization of the characterization of primes as irreducible elements over principal ideal domains, given in property (iv) and specified as the lemma `PID_prime_el_iff_irreducible`.

It is important to stress here that in the pen-and-paper proof of property (iv) given in [14], Hungerford assumes the vital result that maximal elements in the previously mentioned set  $S$

are maximal ideals in  $R$ . We formalized this property without this assumption as the lemma [el\\_max\\_iff\\_one\\_gen\\_maximal](#) in the sub-theory `ring_principal_ideal_domain`.

The Fundamental Theorem of Arithmetic for integers states that any positive integer greater than 1 can be factorized as a unique product of primes. Unique Factorization Domains (UFDs) are integral domains satisfying an analogous to this theorem. The specification [ring\\_unique\\_factorization\\_domain\\_def](#) depends on a sequence of irreducible elements  $\text{fsIr?}(R)(\text{fsI})$  on a ring  $R$  with identity and a recursive operator  $\text{op_fseq}(\text{fsI})$ , as specified in the sub-theory [op\\_finseq\\_def](#), which multiplies the elements of such a sequence. The operator  $\text{op_fseq}(\text{fsI})$  is specified over an abstract structure  $(T, *, \text{one})$  equipped with a binary operation  $*$  and a constant  $\text{one}$ .

Such a general specification is very useful for formalization matters for two reasons. Firstly, it allows the use of the operator  $\text{op_fseq}(\text{fsI})$  in a variety of abstract and concrete structures (monoids, monads, groups, rings, integers, reals) by only adequately parameterizing the sub-theory [op\\_finseq\\_def](#). Secondly, it reduces proof obligations, called in PVS *Type Correctness Conditions (TCCs)*, automatically generated by the system, since the operator is defined for elements of an abstract type, increasing the grade of automation.

In sub-theory [ring\\_unique\\_factorization\\_domain](#), we formalized the landmark Theorem 2.3 about UFDs.

**Theorem 2.3** (Th.3.7, Hungerford [14]). *Every principal ideal domain is a unique factorization domain.*

The formalization of the Theorem 2.3 consists in proving the existence and uniqueness of a factorization as detailed in [7].

A Euclidean ring is a commutative ring  $R$  with a norm  $\varphi$  over  $R - \{\text{zero}\}$ , where an abstract version of the well-known Euclid's division lemma holds. Euclidean rings and domains are specified in the subtheories [euclidean\\_ring\\_def](#) and [euclidean\\_domain\\_def](#).

The fact that elements of Euclidean rings can be factorized as irreducible elements is formalized as Theorem 2.4, in sub-theory [euclidean\\_domain](#).

**Theorem 2.4** (Th.3.9, Hungerford [14]). *A Euclidean ring  $R$  is a principal ideal ring with identity. Consequently, every Euclidean domain is a unique factorization domain.*

The proof of this theorem applies the well-ordering principle over  $\varphi(I^*) = \{\varphi(x) \in \mathbb{N}; x \in I - \{\text{zero}\}\}$ , where  $I$  is a nonzero ideal in  $R$  and  $\varphi$  is a norm on  $R - \{\text{zero}\}$ . By choosing  $a \in I$  such that  $\varphi(a)$  is the minimum element of  $\varphi(I^*)$ ,  $b \in I$  satisfies  $b = qa + r$ , for some  $q \in R$  and  $r \in I$ . From this, one infers that  $r = 0$ , since  $r \neq 0$  contradicts the minimality of  $\varphi(a)$ . Therefore,  $b = qa$  and  $I \subset Ra \subset (a) \subset I$  imply that every ideal in  $R$  is a principal ideal. By Theorem 2.3, one has that a Euclidean principal ideal domain is a unique factorization domain.

In sub-theory [euclidean\\_domain](#), we also formalized the results stating that the ring of integers () and any arbitrary field () are Euclidean domains.

### 3 Formalization of gcd Algorithm for Euclidean Domains

The theory [Euclidean\\_ring\\_def](#) includes two definitions that abstract Euclidean norms and associated functions fulfilling the properties of Euclidean rings.

The first definition is the relation [Euclidean\\_pair?](#) Given a Euclidean ring  $R$  and a Euclidean norm of non-zero elements over the naturals  $\phi : R \setminus \{\text{zero}\} \rightarrow \mathbb{N}$ , [Euclidean\\_pair?](#)( $R, \phi$ ) holds if  $\phi$  satisfies the constraints of a Euclidean norm over  $R$ .

The second definition is the curried relation `Euclidean_f_phi?(R, phi)(f_phi)`. This relation holds if `Euclidean_pair?(R, phi)` does, and  $f_\phi$  is a function from  $R \times R \setminus \{zero\}$  to  $R \times R$ , such that for all pair of elements of  $R$  in its domain,  $f_\phi(a, b)$  gives a pair of elements, say  $(div, rem)$  satisfying the constraints of Euclidean rings for the norm  $\phi$ : if  $a \neq zero$ ,  $a = div * b + rem$ , and if  $rem \neq zero$ ,  $\phi(rem) < \phi(b)$ .

Both definitions are correct since the existence of such a  $\phi$  and  $f_\phi$  is guaranteed by the fact that  $R$  is a Euclidean ring. Also, notice that the decrement of the norm, i.e.,  $\phi(rem) < \phi(b)$ , is the key to implementing an abstract Euclidean terminating procedure.

The Euclidean gcd algorithm is specified in the sub-theory `ring_euclidean_algorithm` as the curried definition `Euclidean_gcd_algorithm`. The types of its arguments guarantee the correctness of this algorithm. Indeed, since the arguments  $R, \phi$ , and  $f_\phi$  should satisfy `Euclidean_f_phi?(R, phi)(f_phi)`,  $R$  is a Euclidean ring with associated Euclidean norm  $\phi$  and adequate division and remainder functions given by  $f_\phi$ . The termination of the algorithm is obtained by discharging a proof obligation (termination TCC) generated by PVS. Termination is proved using the lexicographical MEASURE in the algorithm specification that decreases after each possible recursive call. For `Euclidean_gcd_algorithm(R, phi, f_phi)(a, b)`, if  $a \neq zero$ ,  $\phi(a) \geq \phi(b)$  and  $rem \neq zero$ , the recursive call is `Euclidean_gcd_algorithm(R, phi, f_phi)(b, rem)`, and  $(\phi(b), \phi(a))$  is greater than  $(\phi(rem), \phi(b))$ , since  $\phi(b) > \phi(rem)$ . In the other case, if  $a \neq zero$ , and  $\phi(b) > \phi(a)$ , the recursive call is `Euclidean_gcd_algorithm(R, phi, f_phi)(b, a)`, and  $(\phi(b), \phi(a))$  is greater than  $(\phi(a), \phi(b))$ .

The correctness proof results as a corollary of the `Euclid_theorem`. It states the correctness of each recursive step regarding the definition of `gcd` given in Specification 1. Essentially, this theorem states that given a Euclidean norm  $\phi$  and associated function  $f_\phi$ , the gcd of a pair  $(a, b)$  is equal to the gcd of the pair  $(rem, b)$ , where  $rem$  is computed as the second projection of  $f_\phi(a, b)$ . Notice that since Euclidean rings allow a variety of Euclidean norms and associated functions (e.g., [14], [9]), the definition of gcd is not specified as a function but as the relation “gcd?”.

Finally, the theorem `Euclidean_gcd_alg_correctness` formalizes the correctness of the Euclidean algorithm by induction, using the lexicographic MEASURE. For an input pair  $(a, b)$ , in the inductive step of the proof, when  $\phi(b) > \phi(a)$  and the recursive call swaps the arguments, one assumes that

$$\text{gcd?}(R)(\{b, a\}, \text{Euclidean\_gcd\_algorithm}(R, \phi, f_\phi)(b, a))$$

From this, one concludes that

$$\text{gcd?}(R)(\{a, b\}, \text{Euclidean\_gcd\_algorithm}(R, \phi, f_\phi)(a, b)).$$

Otherwise, when the recursive call is `Euclidean_gcd_algorithm(R, phi, f_phi)(b, rem)`, which happens if  $\phi(a) \geq \phi(b)$ , and  $rem$  is the second component of  $f_\phi(a, b)$ ; by induction hypothesis one has that

$$\text{gcd?}(R)(\{b, rem\}, \text{Euclidean\_gcd\_algorithm}(R, \phi, f_\phi)(b, rem))$$

Finally, by application of `Euclid_theorem`, one concludes that the abstract general Euclidean algorithm computes a gcd for the pair  $(a, b)$  correctly.

Now, we show how the correctness of the abstract algorithm `Euclidean_gcd_algorithm` is easily inherited, under adequate parameterizations, for the structures of integers  $\mathbb{Z}$  and Gaussian integers  $\mathbb{Z}[i]$ . The lines of reasoning follow those given in discussions on factorization in commutative rings and multiplicative norms in textbooks (e.g., Section 47 in [9], or Chapter 3, Section 3 in [14]).

Specification 1: gcd definition for commutative rings - sub-theory `ring_gcd_def` [↗](#)

```

gcd?(R)(X: {X | NOT empty?(X) AND subset?(X,R)}, d:(R - {zero})): bool =
  (FORALL a: member(a, X) IMPLIES divides?(R)(d,a)) AND
  (FORALL (c:(R - {zero})):
    (FORALL a: member(a, X) IMPLIES divides?(R)(c,a)) IMPLIES
    divides?(R)(c,d))

```

Specification 2: Correctness of the parameterization of the abstract Euclidean algorithm for the Euclidean ring  $\mathbb{Z}$  - sub-theory `ring_euclidean_gcd_algorithm_Z` [↗](#)

```

phi_Z(i : int | i /= 0) : posnat = abs(i)

f_phi_Z(i : int, (j : int | j /= 0)) : [int, below[abs(j)]] =
  ((IF j > 0 THEN ndiv(i,j) ELSE -ndiv(i,-j) ENDIF), rem(abs(j))(i))

phi_Z_and_f_phi_Z_ok : LEMMA Euclidean_f_phi?[int,+,*,0](Z,phi_Z)(f_phi_Z)

Euclidean_gcd_alg_correctness_in_Z : COROLLARY
  (FORALL(i: int, (j: int | j /= 0) ) :
    gcd?[int,+,*,0](Z)({x : (Z) | x = i OR x = j},
      Euclidean_gcd_algorithm[int,+,*,0,1](Z, phi_Z,f_phi_Z)(i,j))

```

For the Euclidean ring  $\mathbb{Z}$ , the Euclidean norm  $\phi_{\mathbb{Z}}$  is selected as the absolute value while the associated function  $f_{\phi_{\mathbb{Z}}}$  is built using the integer division and remainder, specified in the PVS prelude libraries as `div` and `rem`: for  $a \in \mathbb{Z}, b \in \mathbb{Z} \setminus \{0\}$ , `div(a,b)` computes the integer division of  $a$  by  $b$ , and, for  $b \in \mathbb{Z}^+ \setminus \{0\}$ , `rem(b)(a)` computes the remainder of  $a$  by  $b$ .

The correctness of the Euclidean algorithm for the ring of integers is specified as the corollary `Euclidean_gcd_alg_correctness_in_Z` [↗](#). It states that for the Euclidean ring of integers  $\mathbb{Z}$ , and any  $i, j \in \mathbb{Z}, j \neq 0$ , the parameterized abstract algorithm, `Euclidean_gcd_algorithm[int,+,*,0,1]` satisfies the relation `gcd?[int,+,*,0]`:

$$\text{gcd?}[int, +, *, 0](\mathbb{Z})(\{i, j\}, \text{Euclidean\_gcd\_algorithm}[int, +, *, 0, 1](\mathbb{Z}, \phi_{\mathbb{Z}}, f_{\phi_{\mathbb{Z}}})(i, j))$$

The proof of this corollary follows from the theorem of correctness for the abstract Euclidean algorithm, `Euclidean_gcd_alg_correctness`. It requires proving that the chosen Euclidean measure  $\phi_{\mathbb{Z}}$ , and the associated function  $f_{\phi_{\mathbb{Z}}}$  fulfill the conditions in the definition of Euclidean rings. The latter is formalized as lemma `phi_Z_and_f_phi_Z_ok` [↗](#): `Euclidean_f_phi?[int,+,*,0](Z,phi_Z)(f_phi_Z)`.

For Gaussian integers,  $x = (\text{Re}(x) + i \text{Im}(x)) \in \mathbb{Z}[i]$ , the Euclidean norm,  $\phi_{\mathbb{Z}[i]}(x)$ , is selected as  $\text{Re}(x)^2 + \text{Im}(x)^2$ . An adequate associated function  $f_{\phi_{\mathbb{Z}[i]}}$  (`f_phi_Zi` [↗](#)) is specified through the auxiliary function `div_rem_appx` [↗](#). For a pair of integers  $(a, b)$ ,  $b \neq 0$ , this function computes the pair of integers  $(q, r)$  such that  $a = qb + r$ , and  $|r| \leq |b|/2$ ; thus,  $qb$  is the integer closest to  $a$ . The equality  $a = qb + r$  is formalized as lemma `div_rev_appx_correctness` [↗](#).


Now, we explain the construction of the function  $f_{\phi_{\mathbb{Z}[i]}}$  [↗](#). For  $y$ , a Gaussian integer and  $x$ , a positive integer, let  $\text{Re}(y) = q_1x + r_1$  and  $\text{Im}(y) = q_2x + r_2$ , where  $(q_1, r_1)$  and  $(q_2, r_2)$  are computed with the auxiliary function `div_rem_appx` (with respective inputs  $(\text{Re}(y), x)$  and  $(\text{Im}(y), x)$ ). Let  $q = q_1 + iq_2$  and  $r = r_1 + ir_2$ , then  $y = qx + r$ . Notice that if  $r \neq 0$  then  $\phi_{\mathbb{Z}[i]}(r) \leq \phi_{\mathbb{Z}[i]}(x)$ , since  $r_1^2 + r_2^2 \leq x^2/2 \leq x^2$ . For the case in which  $x$  is a non zero Gaussian integer,  $\phi_{\mathbb{Z}[i]}(x) > 0$  holds.



Therefore, `div_rem_appx(y conjugate(x), x conjugate(x))`, where `conjugate(x) = (Re(x) -`



$i \operatorname{Im}(x)$ ), can be computed obtaining  $q, r' \in \mathbb{Z}[i]$  such that  $y \operatorname{conjugate}(x) = q(x \operatorname{conjugate}(x)) + r'$ , and  $r' = 0$  or  $\phi_{\mathbb{Z}[i]}(r') < \phi_{\mathbb{Z}[i]}(x \operatorname{conjugate}(x))$ .


By selecting  $r = y - qx$ , we obtain  $y = qx + r$  and  $r \operatorname{conjugate}(x) = r'$ .





Finally, when  $r \neq 0$ , since  $\phi_{\mathbb{Z}[i]}(r \operatorname{conjugate}(x)) < \phi_{\mathbb{Z}[i]}(x \operatorname{conjugate}(x))$ , by application of the lemma [phi\\_Zi\\_is\\_multiplicative](#) , we conclude that  $\phi_{\mathbb{Z}[i]}(r) < \phi_{\mathbb{Z}[i]}(x)$ .

The formalization of the correctness of the Euclidean algorithm for Gaussian integers obtained by parameterizations with  $\mathbb{Z}[i]$ , its Euclidean norm  $\phi_{\mathbb{Z}[i]}$  and associated function  $f_{\phi_{\mathbb{Z}[i]}}$  follows as the simple corollary [Euclidean\\_gcd\\_alg\\_in\\_Zi](#) . This is proved using the correctness of the abstract Euclidean algorithm and lemma [phi\\_Zi\\_and\\_f\\_phi\\_Zi\\_ok](#) . The latter states that the Euclidean norm  $\phi_{\mathbb{Z}[i]}$  and its associated function  $f_{\phi_{\mathbb{Z}[i]}}$  are adequate for the Euclidean ring  $\mathbb{Z}[i]$ : [Euclidean\\_f\\_phi](#)[complex, +, \*, 0]( $\mathbb{Z}[i]$ ,  $\phi_{\mathbb{Z}[i]}$ )( $f_{\phi_{\mathbb{Z}[i]}}$ ).

## 4 The theory of Quaternions

The theory of quaternions is built from any field (specified in PVS as a commutative division ring) over four-dimensional vector spaces ( $[x, y, z, t]$ ).

The specification of quaternions uses an abstract type  $T$  with binary operators for an addition  $+$  and a multiplication  $*$  over  $T$ , with identity elements **zero** and **one**, respectively. The elements of type  $T$  with  $+$  and **zero** is a group. The specification includes axioms for quaternion addition and multiplication, including the quaternions axioms  $i^2 = a$ ,  $j^2 = b$ , for given parameters,  $a$  and  $b$  of  $T$ , the associativity for quaternion multiplication, the distributivity of addition on multiplication; and, properties for the scalar product between elements of type  $T$  and quaternions. All that is provided in the theory [quaternion\\_def](#) . At this point, no additional properties on  $T$  are assumed.

Furthermore, in the PVS theory [quaternions](#) , using these axioms, and assuming  $T$  with  $+$ ,  $*$ , **zero**, and **one** is a field, a series of properties of the theory of quaternions are formalized. These properties include the characterization of quaternion multiplication ([q\\_prod\\_charac](#) ); the fact that quaternions are a ring with unity ([quat\\_is\\_ring\\_w\\_one](#) ); and the characterization of quaternions as division rings ([quat\\_div\\_ring\\_char](#) ).

Typical results on the theory of quaternions also include equalities as the ones below, where  $p, q$  are quaternions, and  $\bar{p}$  denotes the conjugate of  $p$  given as  $[p'x, -p'y, -p'z, -p't]$ .

$$\overline{pq} = \bar{q}\bar{p} \quad \img alt="external link icon" data-bbox="258 622 273 637"/>$$

$$q\bar{q} = \bar{q}q \quad \img alt="external link icon" data-bbox="258 637 273 652"/>$$

$$|\bar{q}| = |q| \quad \img alt="external link icon" data-bbox="258 652 273 667"/>$$

$$|pq| = |p||q| \quad \img alt="external link icon" data-bbox="285 667 300 682"/>$$

$$q^{-1} = \bar{q}/|q|^2 \quad \img alt="external link icon" data-bbox="285 682 300 697"/> , \text{ whenever the quaternion algebra is a division ring.}$$

A quaternion algebra is a division ring whenever all non-zero element  $q$  satisfies  $\bar{q}q \neq \text{zero}_q$ .


Characterizing quaternions as division rings requires that the parameter ring have characteristics different from two. Under this constraint, it is possible to prove that:

$$\forall x, y \in T : ax^2 + by^2 \neq \text{one} \implies \forall t \in T : t^2 + a^{-1} \neq \text{zero} \quad \img alt="external link icon" data-bbox="695 758 710 773"/>$$

From this, under the same constraint, it is possible to prove that:

$$\forall x, y \in T : ax^2 + by^2 \neq \text{one} \implies \forall t \in T : at^2 + b \neq \text{zero} \quad \img alt="external link icon" data-bbox="688 813 703 828"/>$$

Finally, under this constraint, we obtain the characterization of quaternions as division rings:

$\forall x, y \in T : ax^2 + by^2 \neq one \iff \text{division\_ring?}[\text{quat}, +, *, \text{zero}_q, \text{one}_q](\text{fullset}[\text{quat}])$  

Once again, following the general approach to specifying quaternions from abstract fields, we can obtain specific quaternions as the well-known Hamilton’s quaternions. For this, the theory of quaternions is imported, using the field of reals as a parameter, and the real  $-1$  for the parameters  $a$  and  $b$ : `IMPORTING quaternions[real,+,*,0,1,-1,-1]`.

## 5 Related Work and conclusions

### 5.1 Related work

Several formalizations focus on specific ring structures as the ring of integers. Such developments range from simple formalization exercises, such as correctness proofs of `gcd` algorithms for  $\mathbb{Z}$ , to elaborated mechanical proofs of the Chinese Remainder theorem for  $\mathbb{Z}$ . The latter started from Zhang and Hua’s RRL (Rewrite Rule Laboratory) mechanization [24], followed by different approaches in Mizar, HOL Light, hol98, Coq [22], ACL2 [20], and VeriFun [23]. Nevertheless, the general algebraic abstract approach is followed by a few developments. Such an approach is followed in the Isabelle/HOL Algebra Library (see [2], [1], and [3]). Also, the Lean mathlib library [17] formalizes that a Euclidean domain is a principal ideal domain and a principal ideal domain is a unique factorization domain. The former is given as formally verified construction from a definition. From this instance, it is possible to infer that the Gaussian integers are a Euclidean domain and thus a principal ideal. Also, the Euclidean algorithm can be adapted to structures as the Gaussian integers.

In Coq, results about groups, rings, and ordered fields were formalized as part of the FTA project [11]; this work gave rise to the formalization of the Feit and Thompson’s proof of the Odd Order Theorem [12]. Also, there are formalizations of real ordered fields [5], finite fields [19], and rings with explicit divisibility [4]. In Nuprl and Mizar, there are proofs of the Binomial Theorem for rings in [15] and [21], respectively, and a Mizar formalization of the First Isomorphism Theorem for rings [16]. ACL2 provides a hierarchy of algebraic structures ranging from setoids to vector spaces that aims the formalization of computer algebra systems [13].

There are formalizations of Hamilton’s quaternions in HOL Light and Isabelle/HOL (e.g., [10], [18]). In contrast, some elements of the general theory of quaternions built over any abstract field, as in our case, were developed as part of the Lean mathlib library [17].

### 5.2 Conclusions

In contrast to other works, restricted to specific ring structures, our formalization approach focuses on the theory of abstract rings, as done in the Lean- and Isabelle-related libraries (cf [17], and [3], respectively) discussed in the related work. Advantages of such an approach include increasing the interest of mathematicians in formalizations and having practical general presentations of computational algebraic properties portable to specific ring structures.

## References

- [1] Jesús Aransay, Clemens Ballarin, Martin Baillon, Paulo Emílio de Vilhena, Stephan Hohe, Florian Kammüller, and Lawrence C. Paulson. The Isabelle/HOL Algebra Library. Technical re-



- port, Isabelle Library, University of Cambridge Computer Laboratory and Technische Universität München, June 2019.
- [2] Jesús Aransay and Jose Divasón. Formalisation of the computation of the echelon form of a matrix in Isabelle/HOL. *Formal Aspects Comput.*, 28(6):1005–1026, 2016.
  - [3] Clemens Ballarin. Exploring the structure of an algebra text with locales. *Journal of Automated Reasoning*, 64:1093–1121, 2019.
  - [4] Guillaume Cano, Cyril Cohen, Maxime Dénès, Anders Mörtberg, and Vincent Siles. Formalized linear algebra over Elementary Divisor Rings in Coq. *Logical Methods in Computer Science*, 12(2:7):1–23, June 2016.
  - [5] Cyril Cohen and Assia Mahboubi. Formal proofs in real algebraic geometry: from ordered fields to quantifier elimination. *Logical Methods in Computer Science*, 8(1:2):1–40, 2012.
  - [6] Thaynara Arielly de Lima, André Luiz Galdino, Andréia Borges Avelar, and Mauricio Ayala-Rincón. Formalization of Ring Theory in PVS - Isomorphism Theorems, Principal, Prime and Maximal Ideals, Chinese Remainder Theorem. *J. Autom. Reason.*, 65(8):1231–1263, 2021.
  - [7] Thaynara Arielly de Lima, André Luiz Galdino, Andréia Borges Avelar, and Mauricio Ayala-Rincón. Formalizing Factorization on Euclidean Domains and Abstract Euclidean Algorithms. Technical report, Universidade de Brasília, Departments of Mathematics and CS, Brasília D.F., 2023. Accepted in LSFA 2023.
  - [8] David S. Dummit and Richard M. Foote. *Abstract Algebra*. Wiley, 3 edition, July 2003.
  - [9] John B. Fraleigh. *A First Course in Abstract Algebra*. Pearson, 7th edition, 2003.
  - [10] Andrea Gabrielli and Marco Maggesi. Formalizing Basic Quaternionic Analysis. In *Proc. 8th International Conference on Interactive Theorem Proving ITP*, volume 10499 of *Lecture Notes in Computer Science*, pages 225–240. Springer, 2017.
  - [11] Herman Geuvers, Randy Pollack, Freek Wiedijk, and Jan Zwanenburg. A constructive algebraic hierarchy in Coq. *Journal of Symbolic Computation*, 34(4):271–286, 2002.
  - [12] Georges Gonthier, Andrea Asperti, Jeremy Avigad, Yves Bertot, Cyril Cohen, François Garillot, Stéphane Le Roux, Assia Mahboubi, Russell O’Connor, Sidi Ould Biha, Ioana Pasca, Laurence Rideau, Alexey Solovyev, Enrico Tassi, and Laurent Théry. A Machine-Checked Proof of the Odd Order Theorem. In *4th International Conference on Interactive Theorem Proving ITP*, volume 7998 of *Lecture Notes in Computer Science*, pages 163–179. Springer, 2013.
  - [13] Jónathan Heras, Francisco Jesús Martín-Mateos, and Vico Pascual. Modelling algebraic structures and morphisms in ACL2. *Applicable Algebra in Engineering, Communication and Computing*, 26(3):277–303, Jun 2015.
  - [14] Thomas W. Hungerford. *Algebra*, volume 73 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1980. Reprint of the 1974 original.
  - [15] Paul Bernard Jackson. *Enhancing the Nuprl Proof Development System and Applying it to Computational Abstract Algebra*. PhD thesis, Cornell University, 1995.
  - [16] Artur Kornilowicz and Christoph Schwarzweller. The First Isomorphism Theorem and Other Properties of Rings. *Formalized Mathematics*, 22(4):291–301, 2014.
  - [17] The mathlib Community. The Lean Mathematical Library. In *Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs, CPP 2020*, pages 367–381. ACM, 2020.
  - [18] Lawrence C. Paulson. Quaternions. *Arch. Formal Proofs*, 2018, 2018.
  - [19] Jade Philipoom. Correct-by-Construction Finite Field Arithmetic in Coq. Master’s thesis, Master of Engineering in Computer Science, MIT, 2018.
  - [20] David M. Russinoff. 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.
  - [21] Christoph Schwarzweller. The Binomial Theorem for Algebraic Structures. *Journal of Formalized*

*Mathematics*, 12(3):559–564, 2003.

- [22] Christoph Schwarzweiler. The Chinese Remainder Theorem, its Proofs and its Generalizations in Mathematical Repositories. *Studies in Logic, Grammar and Rhetoric*, 18(31):103–119, 2009.
- [23] Christoph Walther. A Machine Assisted Proof of the Chinese Remainder Theorem. Technical Report VFR 18/03, FB Informatik, Technische Universität Darmstadt, 2018.
- [24] Hantao Zhang and Xin Hua. Proving the Chinese Remainder Theorem by the Cover Set Induction. In *11th International Conference on Automated Deduction CADE*, volume 607 of *Lecture Notes in Computer Science*, pages 431–445. Springer, 1992.