LPAR-24, 2023

Universidad Nacional de Colombia - Manizales

Formalization of Algebraic Theorems in PVS

Mauricio Ayala-Rincón (Universidade de Brasília - UnB)

Joint work with

Andréia Borges Avelar(UnB), André Luiz Galdino (UF Catalão), and

Thaynara Arielly de Lima (UF Goiás)

Funded by FAPDF DE grant No. 00193-00000229/2021-21,
CNPq Universal grant No. 313290/2021-0,
FAPEG Research grant No. 202310267000223

Campus La Nubia, Universidad Nacional de Colombia

June 6 2023

Motivation

- Ring theory has a wide range of applications in several fields of knowledge:
  - combinatorics, algebraic cryptography and coding theory apply finite (commutative) rings [1];
  - ring theory forms the basis for algebraic geometry, which has applications in engineering, statistics, biological modeling, and computer algebra [7].

  A complete formalization of ring theory would make possible the formal verification of elaborated theories involving rings in their scope.
- Formalizing rings will enrich the mathematical libraries of PVS:

  https://github.com/nasa/pvslib/tree/master/algebra

algebraic theories $\rightsquigarrow$ algebraic structures

1^{st} $\qquad$ 2^{nd}

Formalization approach

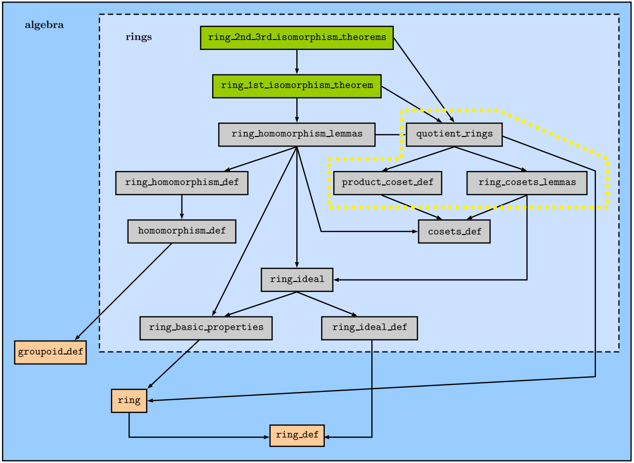


Figure: Hierarchy of the sub-theories for the three isomorphism theorems for rings (Taken from [2])

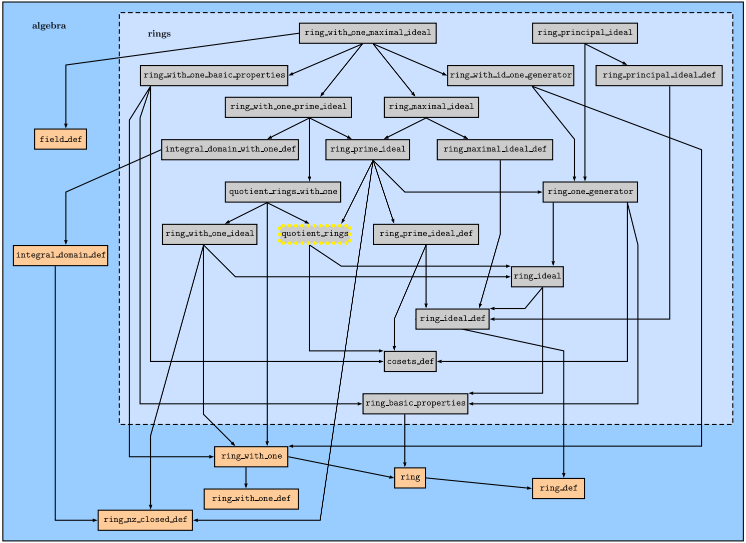


Figure: Hierarchy of the sub-theories related with principal, prime and maximal ideals (Taken from [2])

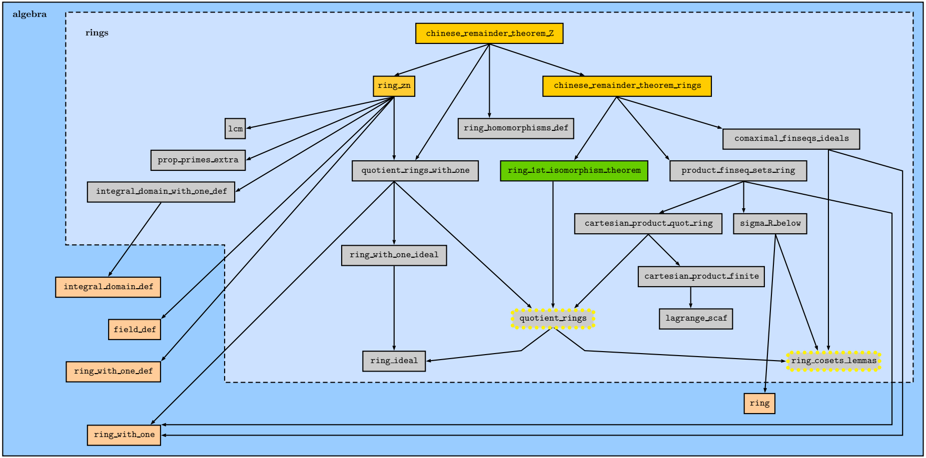
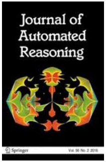


Figure: Hierarchy of the sub-theories related to the Chinese Remainder Theorem (Taken from [2])



[2] de Lima, Galdino, Avelar, Ayala-Rincón
Formalization of Ring Theory in PVS: Isomorphism Theorems, Principal, Prime and Maximal Ideals, Chinese Remainder Theorem
Journal of Automated Reasoning, 2021

https://doi.org/10.1007/s10817-021-09593-0

- Formalization of the general algebraic-theoretical version of the Chinese remainder theorem (CRT) for the theory of rings, proved as a consequence of the first isomorphism theorem.
- The number-theoretical version of CRT for the structure of integers is obtained as a consequence.

CRT for rings $\rightsquigarrow$ CRT for $\mathbb{Z}$

1^{st} 2^{nd}

$\underbrace{\qquad\qquad\qquad\qquad}$

Formalization approach

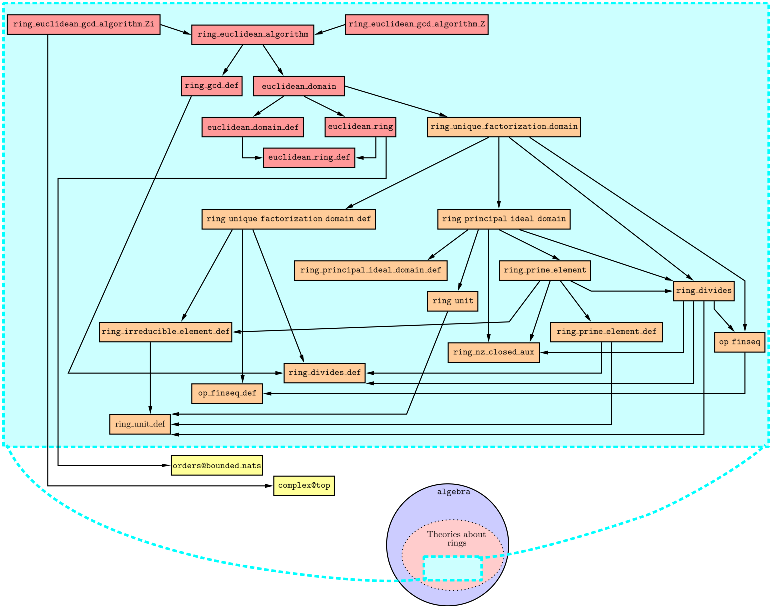


Figure: Euclidean Domains and Algorithms (Taken from [3])

A Euclidean ring is a commutative ring R equipped with a norm φ over $R \setminus \{zero\}$, 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.

```
euclidean_ring?(R): bool = commutative_ring?(R) AND
EXISTS (phi: [(R - {zero}) -> nat]):
  FORALL(a,b: (R)):
  ((a*b /= zero IMPLIES phi(a) <= phi(a*b)) AND
   (b /= zero IMPLIES
      EXISTS(q,r:(R)):
        (a = q*b+r AND (r = zero OR (r /= zero AND phi(r) < phi(b))))))



euclidean_domain?(R): bool = euclidean_ring?(R) AND
                             integral_domain_w_one?(R)
```

The theory `Euclidean_ring_def` includes two additional definitions to allow abstraction of acceptable Euclidean norms, ϕ, and associated functions, f_ϕ, fulfilling the properties of Euclidean rings.

```
Euclidean_pair?(R : (Euclidean_ring?), phi: [(R - {zero}) -> nat]) : bool =
    FORALL(a,b: (R)): ((a*b /= zero IMPLIES phi(a) <= phi(a*b)) AND
                       (b /= zero IMPLIES
                         EXISTS(q,r:(R)): (a = q*b+r AND
                             (r = zero OR (r /= zero AND phi(r) < phi(b))))))

Euclidean_f_phi?(R : (Euclidean_ring?),
                 phi : [(R - {zero}) -> nat] | Euclidean_pair?(R,phi))
                (f_phi : [(R) , (R - {zero}) -> [(R),(R)]]) : bool =
                 FORALL (a : (R), b :(R - {zero})):
                  IF a = zero THEN f_phi(a,b) = (zero, zero)
                  ELSE LET div = f_phi(a,b)`1, rem = f_phi(a,b)`2 IN
                     a = div * b + rem AND
                    (rem = zero OR (rem /= zero AND phi(rem) < phi(b)))
                  ENDIF
```

The relation `Euclidean_pair?`(R, ϕ) holds whenever ϕ is a Euclidean norm over R.

The curried relation `Euclidean_f_phi?`$(R, \phi)(f_\phi)$ holds, whenever `Euclidean_pair?`(R, ϕ) holds, and

$$f_\phi \ : \ R \times R \setminus \{zero\} \rightarrow R \times R$$

is such that for all pair in its domain, $f_\phi(a, b)$ gives a pair of elements, say (div, rem) satisfying the constraints of Euclidean rings regarding the norm ϕ:

$$\text{if } a \neq zero, a = div * b + rem \text{ and, if } rem \neq zero, \phi(rem) < \phi(b)$$

These definitions are correct since the existence of such a ϕ and f_ϕ is guaranteed by the fact that R is a Euclidean ring.

Also, notice that the decrement of the norm $(\phi(rem) < \phi(b))$ is the key to building an abstract Euclidean terminating procedure.

Using the previous two relations, a general abstract recursive Euclidean gcd algorithm is specified in the sub-theory `ring_euclidean_algorithm` as the curried definition `Euclidean_gcd_algorithm` .

```
Euclidean_gcd_algorithm(
        R : (Euclidean_domain?[T,+,*,zero,one]),
        (phi: [(R - {zero}) -> nat] | Euclidean_pair?(R,phi)),
        (f_phi: [(R),(R - {zero}) -> [(R),(R)]] |
                                  Euclidean_f_phi?(R,phi)(f_phi)))
        (a: (R), b: (R - {zero})) : RECURSIVE (R - {zero}) =
  IF  a = zero THEN b
  ELSIF  phi(a) >= phi(b) THEN
      LET rem = (f_phi(a,b))`2 IN
        IF rem = zero THEN b
        ELSE Euclidean_gcd_algorithm(R,phi,f_phi)(b,rem)
        ENDIF
  ELSE  Euclidean_gcd_algorithm(R,phi,f_phi)(b,a)
  ENDIF
MEASURE lex2(phi(b), IF a = zero THEN 0 ELSE phi(a) ENDIF)
```

The termination of the algorithm is guaranteed manually proving that two proof obligations (termination Type Correctness Conditions - TCC) generated by PVS hold. For instance:

```
euclidean_gcd_algorithm_TCC9: OBLIGATION
FORALL (R: (euclidean_domain?[T, +, *, zero, one]),
          (phi: [(difference(R, singleton(zero))) -> nat]
               | euclidean_pair?[T, +, *, zero](R, phi)),
          (f_phi: [[(R), (remove(zero, R))] -> [(R), (R)]]
               | euclidean_f_phi?[T, +, *, zero](R, phi)(f_phi)),
          a: (R), b: (remove[T](zero, R))):
    NOT a = zero AND phi(a) >= phi(b) IMPLIES
     FORALL (rem: (R)):
       rem = (f_phi(a, b))`2 AND NOT rem = zero IMPLIES
        lex2(phi(rem), IF b = zero THEN 0 ELSE phi(b) ENDIF) <
         lex2(phi(b), IF a = zero THEN 0 ELSE phi(a) ENDIF)
```

It uses the lexicographical `MEASURE` provided in the specification. The measure decreases after each possible recursive call.

The `Euclid_theorem` establishes the correctness of each recursive step regarding the abstract definition of gcd . It states that given adequate ϕ and f_ϕ, the gcd of a pair (a, b) is equal to the gcd of the pair (rem, b), where rem is computed by f_ϕ. Notice that since Euclidean rings allow a variety of Euclidean norms and associated functions (e.g., [6], [4]), gcd is specified as a relation.

```
Euclid_theorem : LEMMA
  FORALL(R:(Euclidean_domain?[T,+,*,zero,one]),
        (phi: [(R - {zero}) -> nat] | Euclidean_pair?(R, phi)),
        (f_phi: [(R),(R - {zero}) -> [(R),(R)]] |
                       Euclidean_f_phi?(R,phi)(f_phi)),
        a: (R), b: (R - {zero}), g : (R - {zero})) :
           gcd?(R)({x : (R) | x = a OR x = b}, g) IFF
           gcd?(R)({x : (R) | x = (f_phi(a,b))`2 OR x = b}, g)
```

```
 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))
```

Finally, the theorem `Euclidean_gcd_alg_correctness` formalizes the correctness of the abstract Euclidean algorithm. The proof is by induction. 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 the lexicographic measure decreases. Otherwise, when the recursive call is `Euclidean_gcd_algorithm`$(R, \phi, f_\phi)(b, rem)$ the measure decreases and by application of `Euclid_theorem`, one concludes.

```
Euclidean_gcd_alg_correctness : THEOREM
  FORALL(R:(Euclidean_domain?[T,+,*,zero,one]),
         (phi: [(R - {zero}) -> nat] | Euclidean_pair?(R, phi)),
         (f_phi: [(R),(R - {zero}) -> [(R),(R)]] |
                       Euclidean_f_phi?(R,phi)(f_phi)),
         a: (R), b: (R - {zero}) ) :
      gcd?(R)({x : (R) | x = a OR x = b},
              Euclidean_gcd_algorithm(R,phi,f_phi)(a,b))
```

Corollary Euclidean_gcd_alg_correctness_in_Z gives the Euclidean algorithm correctness for the Euclidean ring of integers, $\mathbb{Z}$. It states that the parameterized abstract algorithm, Euclidean_gcd_algorithm[int,+,*,0,1] satisfies the relation gcd?[int,+,*,0], for any $i, j \in \mathbb{Z}, j \neq 0$.

It follows from the correctness of the abstract Euclidean algorithm and requires proving that $\phi_{\mathbb{Z}}$ and $f_{\phi_{\mathbb{Z}}}$ fulfill the definition of Euclidean rings. The latter is formalized as lemma phi_Z_and_f_phi_Z_ok .

```
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))
```

Correctness of the Euclidean algorithm for the Euclidean ring $\mathbb{Z}[i]$ of Gaussian integers.

The Euclidean norm of a Gaussian integer $x = (\mathtt{Re}(x) + i\,\mathtt{Im}(x)) \in \mathbb{Z}[i]$, $\phi_{\mathbb{Z}[i]}(x)$, is selected as the natural given by the multiplication of x by its conjugate ($\bar{x} = \mathtt{conjugate}(x) = \mathtt{Re}(x) - i\,\mathtt{Im}(x)$): $\mathtt{Re}(x)^2 + \mathtt{Im}(x)^2$.

```
Zi: set[complex] = {z : complex | EXISTS (a,b:int): a = Re(z) AND b = Im(z)}

Zi_is_ring: LEMMA ring?[complex,+,*,0](Zi)

Zi_is_integral_domain_w_one: LEMMA integral_domain_w_one?[complex,+,*,0,1](Zi)

phi_Zi(x:(Zi) | x /= 0): nat = x * conjugate(x)

phi_Zi_is_multiplicative: LEMMA
   FORALL((x: (Zi) | x /= 0), (y: (Zi) | y /= 0)):
                  phi_Zi(x * y) = phi_Zi(x) * phi_Zi(y)
```

The auxiliary function `div_rem_appx` is used to specify the associated function $f_{\phi_{\mathbb{Z}[i]}}$ for the Euclidean ring $\mathbb{Z}[i]$.

For a pair of integers (a, b), $b \neq 0$, `div_rem_appx` computes the pair of integers (q, r) such that $a = q\,b + r$, and $|r| \leq |b|/2$; thus, $q\,b$ is the integer closest to a.

Lemma `div_rev_appx_correctness` proves the equality $a = q\,b + r$.

```
div_rem_appx(a: int, (b: int | b /= 0)) : [int, int] =
  LET r = rem(abs(b))(a),
      q = IF b > 0 THEN ndiv(a,b) ELSE -ndiv(a,-b) ENDIF  IN
   IF r <= abs(b)/2 THEN (q,r)
   ELSE IF b > 0 THEN (q+1, r - abs(b))
        ELSE (q-1, r - abs(b))
        ENDIF
   ENDIF

div_rev_appx_correctness : LEMMA
   FORALL (a: int, (b: int | b /= 0)) :
      abs(div_rem_appx(a,b)`2) <= abs(b)/2 AND
      a = b * div_rem_appx(a,b)`1 +  div_rem_appx(a,b)`2
```

Construction of $f_{\phi_{\mathbb{Z}[i]}}$: For y, a Gaussian integer and x, a positive integer, let $\mathtt{Re}(y) = q_1 x + r_1$ and $\mathtt{Im}(y) = q_2 x + r_2$, where (q_1, r_1) and (q_2, r_2) are computed by $\mathtt{div\_rem\_appx}(\mathtt{Re}(y), x)$ and $\mathtt{div\_rem\_appx}(\mathtt{Im}(y), x))$, respectively.

Let $q = q_1 + iq_2$ and $r = r_1 + ir_2$, then $y = qx + r$. Also, notice that if $r \neq 0$ then $\phi_{\mathbb{Z}[i]}(r) \leq \phi_{\mathbb{Z}[i]}(x)$ since $r_1^2 + r_2^2 \leq x^2$.

For the case in which x is a non zero Gaussian integer, $\phi_{\mathbb{Z}[i]}(x) > 0$ holds.

Then, $\mathtt{div\_rem\_appx}(y\,\bar{x}, x\,\bar{x})$ computes $q, r' \in \mathbb{Z}[i]$ such that $y\,\bar{x} = q\,(x\,\bar{x}) + r'$, and $r' = 0$ or $\phi_{\mathbb{Z}[i]}(r') < \phi_{\mathbb{Z}[i]}(x\,\bar{x})$.

Finally, selecting $r = y - q\,x$ $(y = q\,x + r)$ and $r' = r\,\bar{x}$:

If $r \neq 0$, since $\phi_{\mathbb{Z}[i]}(r\,\bar{x}) < \phi_{\mathbb{Z}[i]}(x\,\bar{x})$, by lemma `phi_Zi_is_multiplicative` , we conclude that $\phi_{\mathbb{Z}[i]}(r) < \phi_{\mathbb{Z}[i]}(x)$.

```
f_phi_Zi(y: (Zi), (x: (Zi) | x /= 0)): [(Zi),(Zi)] =
  LET q = div_rem_appx(Re(y * conjugate(x)), x * conjugate(x))`1 +
          div_rem_appx(Im(y * conjugate(x)), x * conjugate(x))`1 * i,
      r = y - q * x IN (q,r)
```

Corollary `Euclidean_gcd_alg_ in_Zi` gives the correctness of the Euclidean algorithm for the Euclidean ring $\mathbb{Z}[i]$.
This is consequence of the correctness of the abstract Euclidean algorithm and lemma `phi_Zi_and_f_phi_Zi_ok` that states that $\phi_{\mathbb{Z}[i]}$ and $f_{\phi_{\mathbb{Z}[i]}}$ are adequate for $\mathbb{Z}[i]$: $\texttt{Euclidean\_f\_phi?}[\texttt{complex}, +, *, 0](\mathbb{Z}[i], \phi_{\mathbb{Z}[i]})(f_{\phi_{\mathbb{Z}[i]}})$.

```
phi_Zi_and_f_phi_Zi_ok: LEMMA
   Euclidean_f_phi?[complex,+,*,0](Zi,phi_Zi)(f_phi_Zi)

Euclidean_gcd_alg_in_Zi: COROLLARY
 FORALL(x: (Zi), (y: (Zi) | y /= 0)  ) :
     gcd?[complex,+,*,0](Zi)({z :(Zi) | z = x OR z = y},
      Euclidean_gcd_algorithm[complex,+,*,0,1](Zi, phi_Zi,f_phi_Zi)(x,y))
```

Euclidean algorithm for rings $\rightsquigarrow$ { Euclidean algorithm for $\mathbb{Z}$; Euclidean algorithm for $\mathbb{Z}[i]$ }

1^{st} $\quad$ 2^{nd}

Formalization approach

For about ten years, Sir William Rowan Hamilton tried to model three-dimensional space with a structure like "complex numbers", equipped with and closed under addition and multiplication.

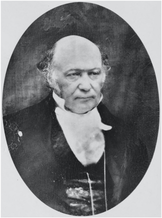
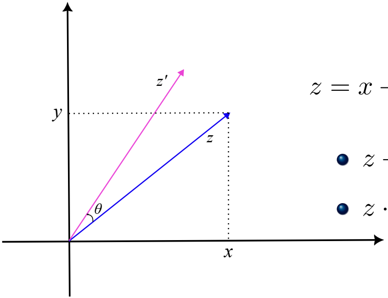


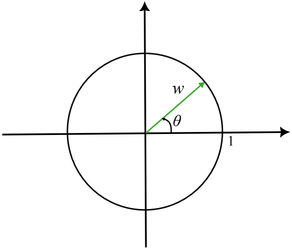
Figure: Sir William Rowan Hamilton, picture taken from [8]

Complex numbers and bi-dimensional real space



$$z = x + yi \qquad w = c + di$$

- $z + w = (x + c) + (y + d)i$
- $z \cdot w = (xc - yd) + (xd + yc)i$



$$z' = x\cos(\theta) - y\sin(\theta) + (x\sin(\theta) + y\cos(\theta))i$$

$$\boxed{z' = z \cdot w}$$

On October 16, 1843, Hamilton realized he needed a structure containing four dimensions to model the three-dimensional real space.

It provided some peculiar/special results...

- The advent of an algebraic structure at the intersection of many mathematical topics such as non-commutative ring theory, number theory, geometric topology, etc.

"The most famous act of mathematical vandalism"

Figure: Sand sculpture by Daniel Doyle, picture taken from [8]

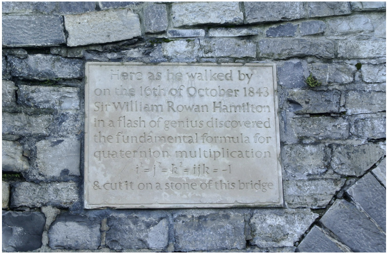


Figure: Broom bridge plaque in Dublin, picture taken from [11]

Hamilton's Quaternions

The structure $\langle \mathbb{H}, +, \cdot, one_q, i, j, k \rangle$, where:

- $\mathbb{H} = \{q_0 one_q + q_1 i + q_2 j + q_3 k \mid q_\ell \in \mathbb{R},\ \text{for } 0 \leq \ell \leq 3\}$;
- $i^2 = j^2 = i \cdot j \cdot k = -1 + 0i + 0j + 0k = -one_q$;

For p and $q \in \mathbb{H}$:

- $p + q = (p_0 + q_0) + (p_1 + q_1)i + (p_2 + q_2)j + (p_3 + q_3)k$
- $$p \cdot q = \begin{array}{l} (p_0q_0 - p_1q_1 - p_2q_2 - p_3q_3) \\ +(p_0q_1 + p_1q_0 + p_2q_3 - p_3q_2)i \\ +(p_0q_2 - p_1q_3 + p_2q_0 + p_3q_1)j \\ +(p_0q_3 + p_1q_2 - p_2q_1 + p_3q_0)k \end{array}$$

Hamilton's Quaternions

Hamilton's Quaternions can be seen as a four dimensional vector space over the field of real numbers.

Identifying

- $one_q \leftrightsquigarrow (\mathbf{1}, 0, 0, 0)$
- $i \leftrightsquigarrow (0, \mathbf{1}, 0, 0)$
- $j \leftrightsquigarrow (0, 0, \mathbf{1}, 0)$
- $k \leftrightsquigarrow (0, 0, 0, \mathbf{1})$

$$\mathbb{H} \cong \mathbb{R}^{\mathbf{4}}$$

Considering...

- $\mathbb{H}^0 = \{q \mid q_0 = 0\} \subset \mathbb{H}$;

$$\mathbb{H}^{\mathbf{0}} \cong \mathbb{R}^{\mathbf{3}}$$

Conjugate and norm

Define:

- The conjugate of a quaternion q as

$$\begin{aligned}\bar{q} &= q_0 - q_1 i - q_2 j - q_3 k \\ &= q_0 - \boldsymbol{q}\end{aligned}$$

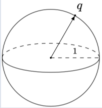
  where $\boldsymbol{q}$ denotes $q_1 i + q_2 j + q_3 k$

- The norm of q as

$$|q| = \sqrt{q_0^2 + q_1^2 + q_2^2 + q_3^2}$$

Denote

- $\mathbb{H}^1 = \{q \in \mathbb{H} \; ; \; |q| = 1\}$



A special function

Let q be a quaternion. Consider the function

$$\begin{aligned} T_q : \quad \mathbb{H}^0 &\to \mathbb{H} \\ v &\mapsto q \cdot v \cdot \bar{q} \end{aligned}$$

One can prove that:

$$\begin{aligned} T_q : \quad \mathbb{H}^0 &\to \mathbb{H}^0, \text{ or equivalently} \\ T_q : \quad \mathbb{R}^3 &\to \mathbb{R}^3 \end{aligned}$$

Some properties of T_q

- T_q **is linear:**

$$T_q(av + bu) = aT_q(v) + bT_q(u), \text{ for all } a, b \in \mathbb{R} \text{ and } v, u \in \mathbb{R}^3.$$

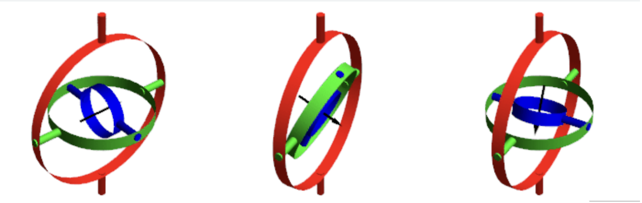
- **If** $q \in \mathbb{H}^1$ **then** T_q **preserves the norm of** v:

$$|T_q(v)| = |q \cdot v \cdot \bar{q}| = |q| \cdot |v| \cdot |\bar{q}| = |v|$$

- **If** $q \in \mathbb{H}^1$ **then** $T_q(k\boldsymbol{q}) = k\boldsymbol{q}$**, where** $k \in \mathbb{R}$;

In fact, one can prove that T_q is a rotation of an angle $\theta = 2\arccos(q_0)$, whose axis has the same direction as $\boldsymbol{q}$.

Benefits of rotating using Quaternions



Taken from [10]

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos(\alpha) & -\sin(\alpha) \\ 0 & \sin(\alpha) & \cos(\alpha) \end{bmatrix} \begin{bmatrix} \cos(\beta) & 0 & \sin(\beta) \\ 0 & 1 & 0 \\ -\sin(\beta) & 0 & \cos(\beta) \end{bmatrix} \begin{bmatrix} \cos(\gamma) & -\sin(\gamma) & 0 \\ \sin(\gamma) & \cos(\gamma) & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Benefits of rotating using Quaternions - Avoiding Gimbal Lock

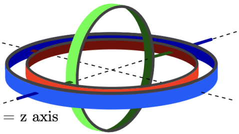
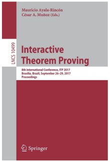


Figure: **Gimbal Lock**: taken from [9]

For $\beta = \frac{\pi}{2}, R = \begin{bmatrix} 0 & 0 & 1 \\ \sin(\alpha+\gamma) & \cos(\alpha+\gamma) & 0 \\ -\cos(\alpha+\gamma) & \sin(\alpha+\gamma) & 0 \end{bmatrix}$

Formalization of Quaternions



Gabrielli, A., Maggesi, M. (2017)
Formalizing Basic Quaternionic Analysis.
ITP 2017. Lecture Notes in Computer Science, vol 10499.

https://doi.org/10.1007/978-3-319-66107-0_15

Lawrence C. Paulson (2018)
Quaternions.
Archive of Formal Proofs.

https://isa-afp.org/entries/Quaternions.html

Both of them are **restricted to** Hamilton's 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 theory `quaternions_def[T:Type+,+,*:[T,T->T],zero,one,a,b:T]` uses an abstract type `T`, and assumes `group[T,+,zero]`, and axioms:

```
sqr_i           :AXIOM i * i = a_q
sqr_j           :AXIOM j * j = b_q
ij_is_k         :AXIOM i * j = k
ji_prod         :AXIOM j * i = inv(k)
sc_quat_assoc   :AXIOM c*(u*v) = (c*u)*v
sc_comm         :AXIOM (c*u)*v = u*(c*v)
sc_assoc        :AXIOM c*(d*u) = (c*d)*u
q_distr         :AXIOM distributive?[quat](*, +)
q_distrl        :AXIOM (u + v) * w = u * w + v * w
q_assoc         :AXIOM associative?[quat](*)
one_q_times     :AXIOM one_q * u = u
times_one_q     :AXIOM u * one_q = u
```

The PVS theory `quaternions` assumes `field[T,+,*,zero,one]` and formalizes the characterization of quaternion multiplication (`q_prod_charac`);

```
q_prod_charac: LEMMA FORALL (u,v:quat):
 u * v = (u`x * v`x + u`y * v`y * a + u`z * v`z * b + u`t * v`t * inv(a) * b,
          u`x * v`y + u`y * v`x + (inv(b)) *  u`z * v`t + b* u`t * v`z,
          u`x * v`z + u`z * v`x +a * u`y * v`t + inv(a) * u`t * v`y,
          u`x * v`t + u`y * v`z + inv(u`z * v`y) + u`t * v`x )
```

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`)

```
quat_is_ring_w_one: LEMMA ring_with_one?[quat,+,*,zero_q,one_q](quat)

quat_div_ring_char: LEMMA
charac(fullset[T]) /= 2 IMPLIES
((FORALL (x,y:T): a*(x*x) + b*(y*y) /= one) IFF
division_ring?[quat,+,*,zero_q,one_q](quat)
```

Typical results on the theory of quaternions also include equalities as the ones below, where p, q are quaternions.

$\overline{pq} = \bar{q}\bar{p}$

$q\bar{q} = \bar{q}q$

$|\bar{q}| = |q|$

$|pq| = |p||q|$

$q^{-1} = \bar{q}/|q|^2$, whenever the quaternion algebra is a division ring.

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

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

$$\forall x, y \in T : ax^2 + by^2 \neq one \Longrightarrow \forall t \in T : t^2 + a^{-1} \neq zero$$

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

$$\forall x, y \in T : ax^2 + by^2 \neq one \Longrightarrow \forall t \in T : at^2 + b \neq zero$$

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

$$\forall x, y \in T : ax^2 + by^2 \neq one \Longleftrightarrow \texttt{division\_ring?}[\texttt{quat}, +, *, \texttt{zero}_\texttt{q}, \texttt{one}_\texttt{q}](\texttt{quat})$$

Formalization of Quaternion Algebras

Hamilton's quaternions are obtained importing the theory of quaternions 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]
```

The formalization approach follows the same principle:

Quaternions theory over any field $\rightsquigarrow$ Hamilton's Quaternions (over $\mathbb{R}$

1^{st} 2^{nd}

Formalization approach

Conclusion and work in progress

Our formalizations follow academic mathematical principles: first, formalize abstract theories with their generic properties; second, obtain particular structures as instantiations of the general theory and proceed with the formalization of their specialized properties.

$$\underbrace{\underset{1^{st}}{\boxed{\text{algebraic theories}}} \quad \rightsquigarrow \quad \underset{2^{nd}}{\boxed{\text{algebraic structures}}}}_{\text{Formalization approach}}$$

- Completing the theory of rings.
- Formalizing properties of Hamilton's quaternions.

References I

- Bini, G., Flamini, F.: Finite commutative rings and their applications, vol. 680. Springer Science & Business Media (2012)
- de Lima, T.A., Avelar, A.B., Galdino, A.L., Ayala-Rincón, M., Formalization of Ring Theory in PVS: Isomorphism Theorems, Principal, Prime and Maximal Ideals, Chinese Remainder Theorem. Journal of Automated Reasoning, vol. 65. p. 1231–1263 (2021)
- de Lima, T.A., Avelar, A.B., Galdino, A.L., Ayala-Rincón, M., Formalizing Factorization on Euclidean Domains and Abstract Euclidean Algorithms. To appear in LSFA (2023)
- Fraleigh, John B., A First Course in Abstract Algebra, Pearson, 2003 (1967).
- Galdino, André Luiz: Quatérnions e Rotações. Lecture Notes (in Portuguese). (2022)
- Hungerford, Thomas W., Algebra, Graduate Texts in Mathematics, vol. 73, 1980 (1974).
- Putinar, M. and Sullivant, S.,Emerging Applications of Algebraic Geometry. Springer New York (2008)
- Voight, John: Quaternion Algebras, ed.1. Springer Cham (2021)

References II

Zeitlhöfler, Julian.:Nominal and observation-based attitude realization for precise orbit determination of the Jason satellites. PhD thesis. (2019)

Don't Get Lost in Deep Space: Understanding Quaternions. All about circuits, 2017. Available in https://www.allaboutcircuits.com/technical-articles/dont-get-lost-in-deep-space-understanding-quaternions/. Accessed on Feb.,13th, 2023.

File:Inscription on Broom Bridge (Dublin) regarding the discovery of Quaternions multiplication by Sir William Rowan Hamilton.jpg, 2017. Available in https://commons.wikimedia.org/wiki/File:Inscription_on_Broom_Bridge_%28Dublin%29_regarding_the_discovery_of_Quaternions_multiplication_by_Sir_William_Rowan_Hamilton.jpg. Accessed on Feb.,13th, 2023.