PVS Day 2025

Workshop on the Prototype Verification System

Collocated with NFM 2025

The Algebra Library and Applications of Quaternions

Thaynara Arielly de Lima (UF Goiás)

Bruno Berto de Oliveira Ribeiro (Universidade de Brasília - UnB)

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

Mauricio Ayala-Rincón (UnB)

College of William & Mary, Computer Science Department - Williamsburg VA,

June 10th, 2025

Joint Work With

Bruno Berto de Oliveira Ribeiro (UnB)

Thaynara Arielly de Lima (UFG)

André Luiz Galdino (UFCat)

Andréia Borges Avelar (UnB)

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 [8].

  A complete formalization of ring theory would make possible the formal verification of elaborate theories involving rings in their scope.

- Formalizing rings will enrich the mathematical libraries of PVS:

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

$$\underbrace{\boxed{\text{algebraic theories}} \quad \leadsto \quad \boxed{\text{algebraic structures}}}_{\text{Formalization approach}}$$

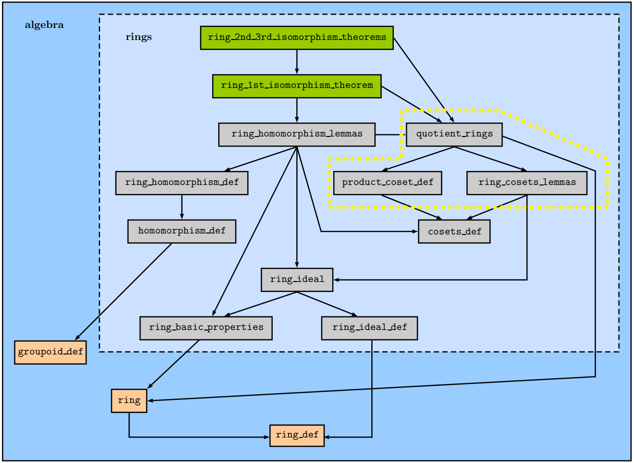


Figure: Hierarchy of the sub-theories for the three isomorphism theorems for rings (Taken from [2])

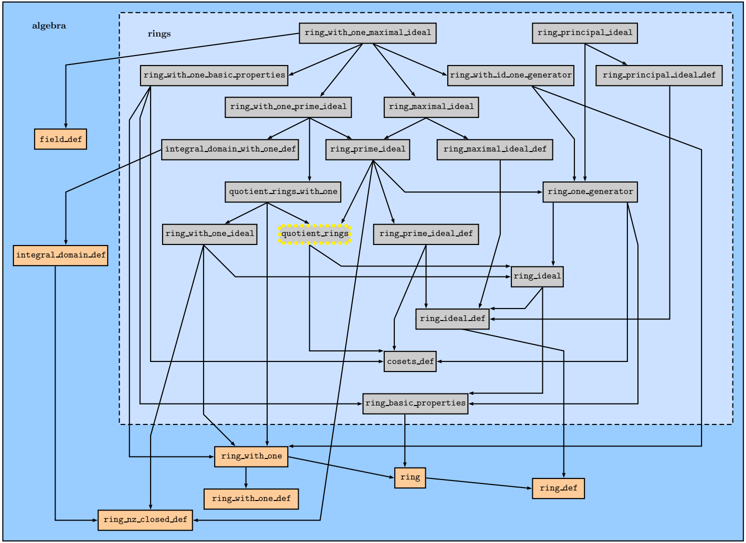


Figure: Hierarchy of the sub-theories related with principal, prime and maximal ideals (Taken from [2])

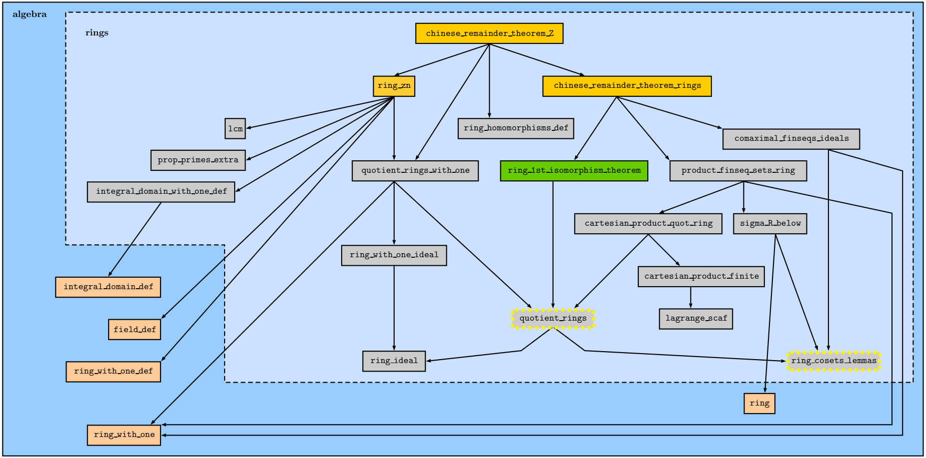
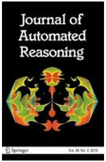


Figure: Hierarchy of the sub-theories related to the Chinese Remainder Theorem (Taken from [2])



[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.

$$\underbrace{\boxed{\text{Chinese Rem. Th. for rings}} \quad \rightsquigarrow \quad \boxed{\text{Chinese Rem. Th. for } \mathbb{Z}}}_{\text{Formalization approach}}$$

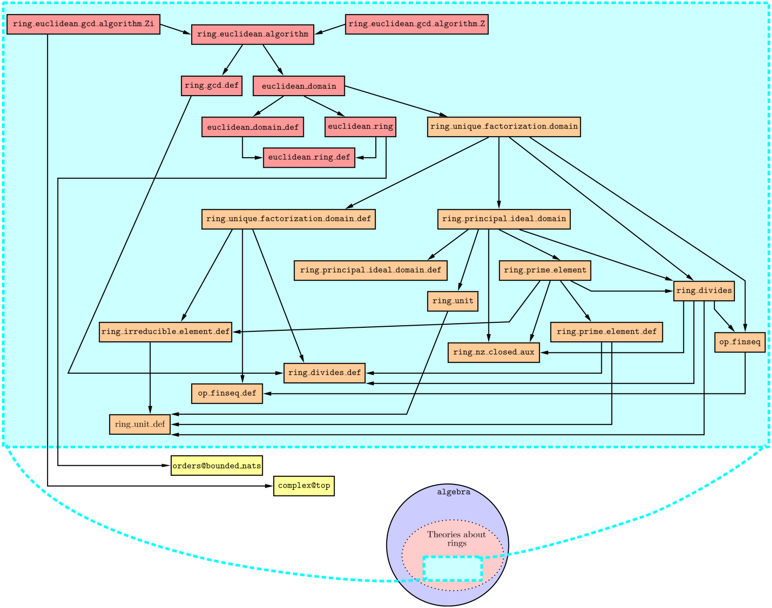


Figure: Euclidean Domains and Algorithms

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

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

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., [7], [6]), `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 $\texttt{Re}(y) = q_1 x + r_1$ and $\texttt{Im}(y) = q_2 x + r_2$, where (q_1, r_1) and (q_2, r_2) are computed by $\texttt{div\_rem\_appx}(\texttt{Re}(y), x)$ and $\texttt{div\_rem\_appx}(\texttt{Im}(y), x))$, 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, $\texttt{div\_rem\_appx}(y\,\bar{x}, x\,\bar{x})$ 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 $\mathbb{Z}[i]$: Euclidean_f_phi?[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))
```

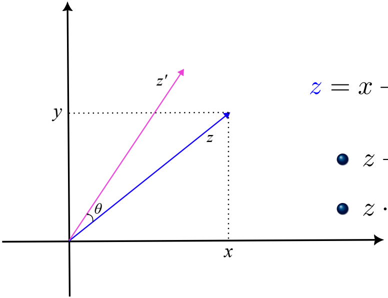
EPiC Computing

[4] Ayala-Rincón, de Lima, Avelar, Galdino
Formalization of Algebraic Theorems in PVS
Proceedings of 24th Int. Conf. on Logic for Programming, Artificial Intelligence and Reasoning, LPAR 2023

https://doi.org/10.29007/7jbv

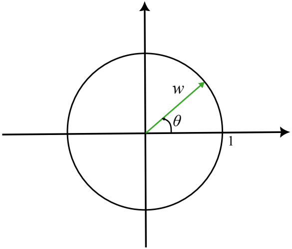
$$\underbrace{\boxed{\text{Euclidean algorithm for rings}} \quad \rightsquigarrow \quad \left\{ \begin{array}{l} \boxed{\text{Euclidean algorithm for } \mathbb{Z}} \\ \boxed{\text{Euclidean algorithm for } \mathbb{Z}[i]} \end{array} \right.}_{\text{Formalization approach}}$$

Complex numbers and bi-dimensional real space



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

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



$$w = \cos(\theta) + \sin(\theta)i$$

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

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

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.

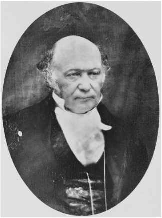


Figure: Sir William Rowan Hamilton, picture taken from [9]

On October 16, 1843, Hamilton realized he needed a four-dimensional structure 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 [9]

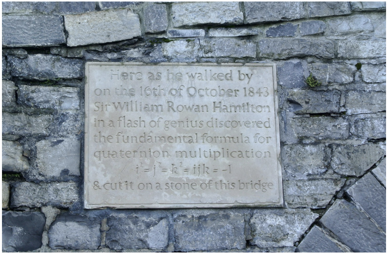


Figure: Broom bridge plaque in Dublin, picture taken from [12]

Hamilton's Quaternions

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

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

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

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

Hamilton's Quaternions

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

Identifying

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

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

Considering...

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

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

Conjugate and norm

Define:

- The *conjugate* of a quaternion $\mathbf{q}$ as

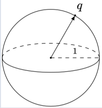
$$\begin{aligned}\bar{\mathbf{q}} &= q_0 - \underbrace{q_1\mathbf{i} - q_2\mathbf{j} - q_3\mathbf{k}}_{} \\ &= q_0 - \boldsymbol{q}\end{aligned}$$

  where $\boldsymbol{q}$ is the *pure part* of $\mathbf{q}$

- The *norm* of $\mathbf{q}$ is given as $|\mathbf{q}| = \sqrt{q_0^2 + q_1^2 + q_2^2 + q_3^2}$

Denote

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



A special function

Let $\mathbf{q}$ be a quaternion. Consider the function

$$\begin{array}{rccc} T_q: & \mathbb{H}^0 & \to & \mathbb{H} \\ & \mathbf{v} & \mapsto & \mathbf{q}\cdot\mathbf{v}\cdot\bar{\mathbf{q}} \end{array}$$

One can prove that:

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

Some properties of T_q

- T_q **is linear:**

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

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

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

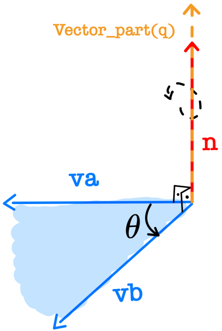
- **If $\mathbf{q} \in \mathbb{H}^1$ then $T_q(k\mathbf{q}) = k\mathbf{q}$, where $k \in \mathbb{R}$**;

Completeness of rotation using Hamilton's quaternions

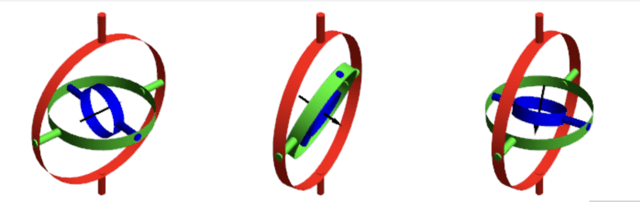
Consider $\boldsymbol{va}$ and $\boldsymbol{vb}$ linearly independent vectors from $\mathbb{R}^3$ such that $|\boldsymbol{va}| = |\boldsymbol{vb}|$. There exists a Hamilton's quaternion $\mathbf{q}$, such that

$$T_q(\boldsymbol{va}) = \boldsymbol{vb}$$

and $\boldsymbol{q}$ is the axis of rotation that leads $\boldsymbol{va}$ into $\boldsymbol{vb}$.



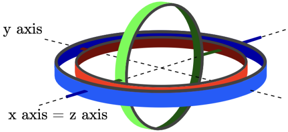
Benefits of rotating using Quaternions



Taken from [11]

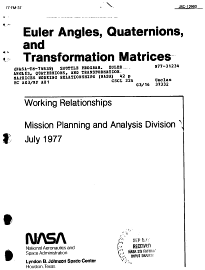
$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos(\alpha) & -\sin(\alpha) \\ 0 & \sin(\alpha) & \cos(\alpha) \end{bmatrix} \begin{bmatrix} \cos(\beta) & 0 & \sin(\beta) \\ 0 & 1 & 0 \\ -\sin(\beta) & 0 & \cos(\beta) \end{bmatrix} \begin{bmatrix} \cos(\gamma) & -\sin(\gamma) & 0 \\ \sin(\gamma) & \cos(\gamma) &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

Benefits of rotating using Quaternions - Avoiding Gimbal Lock



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

Figure: **Gimbal Lock**: taken from [10]


77-FM-37 JSC-12960

Euler Angles, Quaternions, and Transformation Matrices

(NASA-TM-74839) SHUTTLE PROGRAM. EULER ANGLES, QUATERNIONS, AND TRANSFORMATION MATRICES WORKING RELATIONSHIPS (NASA) 42 p HC A03/MF A01 CSCL 22A N77-31234 Unclas G3/16 37332

Working Relationships

Mission Planning and Analysis Division

July 1977

NASA
National Aeronautics and Space Administration
Lyndon B. Johnson Space Center
Houston, Texas

Implementations of quaternions have been considered in the NASA Space Shuttle Program. E.g., D. M. Henderson's Design Note NO. 1.4-8-020 relates quaternion transformation to the twelve three-axis Euler transformation(s):

$$T_q \leftrightsquigarrow \boxed{\begin{array}{ccc} XYZ & YXZ & ZXZ \\ XZY & YZX & ZYX \\ XYX & YXY & ZXZ \\ XZX & YZY & ZYZ \end{array}}$$

Applications

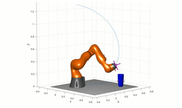
- Quaternions have been used in computer graphics, robotics, signal processing, bioinformatics, and orbital mechanics.

Tomb Raider (1996) is often cited as the first mass-market computer game to have used quaternions to achieve smooth 3D rotation.

MathWorks©

Aerospace ToolBox

Robotics ToolBox



Use Quaternions Math as Octave, Maple, Mathematica, Numpy, GeoGebra, etc

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:

```
i = (zero, one, zero, zero)
j = (zero, zero, one, zero)
k = (zero, zero, zero, one)
a_q = (a, zero, zero, zero)
b_q = (b, zero, zero, zero)
```

```
conjugate(v) = (v`x, inv(v`y),inv(v`z),inv(v`t))
red_norm(v) = v*conjugate(v)
+(u,v):quat=(u`x+v`x, u`y+v`y, u`z+v`z, u`t+v`t);
*(c,v):quat=(c * v`x, c * v`y, c * v`z, c * v`t);
*:[quat,quat -> quat]; %quat multiplication

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 several basic properties.

```
basis_quat: LEMMA
 FORALL (q: quat): q = q'x * one_q + q'y * i + q'z * j + q't * k
```

```
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 )
```

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

```
red_norm_charac: LEMMA FORALL (q: quat):
    red_norm(q) = (q`x * q`x +
                   inv(a) * (q`y * q`y) +
                   inv(b) * (q`z * q`z) +
                   (a * b) * (q`t * q`t),
                   zero, zero, zero)
```

The general function $T_q(v)$

```
T_q(q: quat)(v:(pure_quat)): (pure_quat) = q * v * conjugate(q)

T_q_is_linear: LEMMA FORALL (c,d: T, q: quat, v,w: (pure_quat)):
    T_q(q)(c * v + d * w) = c * T_q(q)(v) + d *  T_q(q)(w)

T_q_red_norm_invariant: LEMMA FORALL (q: quat, v:(pure_quat)):
    red_norm(q) = one_q IMPLIES red_norm(T_q(q)(v)) = red_norm(v)

T_q_invariant_red_norm: LEMMA FORALL (c: T, q: quat):
    red_norm(q) = one_q IMPLIES T_q(q)(c * pure_part(q)) = c * pure_part(q)
```

Characterization of Quaternions as Division Rings

```
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](fullset[quat]))
```

Formalization of Hamilton's Quaternion

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

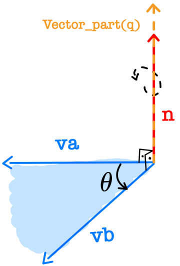
Rotation by Hamilton's Quaternions

```
Real_part(q: quat): real = q`x
Vect_part(q: quat): Vect3 = (q`y, q`z, q`t)

r_angle(a,b:(nzpure_quat)):nnreal_le_pi =
  angle_between(Vect_part(a),Vect_part(b))

n_rot_axis(a:(pure_quat),b:(pure_quat)|
 lin_independent?(Vect_part(a),Vect_part(b))):Vect3 =
 normalize(cross(Vect_part(a), Vect_part(b)))

rot_quat(a:(pure_quat),b:(pure_quat) |
 lin_independent?(Vect_part(a),Vect_part(b))):quat =
  LET  rot_angl_halve : nnreal_le_pi = r_angle(a,b)/ 2,
       sin_ha = sin(rot_angl_halve),
       cos_ha = cos(rot_angl_halve),
       n = n_rot_axis(a,b)
  IN (cos_ha,  sin_ha * n`x, sin_ha * n`y, sin_ha * n`z)
```



```
T_q_Real_charac: LEMMA FORALL (q: quat, a: (pure_quat)):
 Vect_part(T_q(q)(a)) = (2 * (Vect_part(q) * Vect_part(a))) * Vect_part(q) +
                        (sq(q`x) - sq(norm(Vect_part(q)))) * Vect_part(a) +
                        (2 * q`x) * cross(Vect_part(q), Vect_part(a))
```

```
Quat_Rot_Aux1 : LEMMA FORALL (a:(pure_quat), b:(pure_quat) |
lin_independent?(Vect_part(a), Vect_part(b))):
(Vect_part(rot_quat(a, b)) * Vect_part(a)) = 0

Quat_Rot_Aux2 : LEMMA FORALL (a:(pure_quat), b:(pure_quat) |
lin_independent?(Vect_part(a), Vect_part(b))):
LET q = rot_quat(a, b), theta = r_angle(a,b), norm_q = norm(Vect_part(q)) IN
 (sq(q`x) - sq(norm_q)) * Vect_part(a) = cos(theta) * Vect_part(a)

Quat_Rot_Aux3 : LEMMA FORALL (a:(pure_quat), b:(pure_quat) |
norm(Vect_part(a)) = norm(Vect_part(b)) AND
lin_independent?(Vect_part(a), Vect_part(b))):
LET q = rot_quat(a, b), theta = r_angle(a,b)  IN
 (2*q`x) * cross(Vect_part(q), Vect_part(a)) = Vect_part(b) - cos(theta) * Vect_part(a)
```

Rotation by Hamilton's Quaternions

```
Quaternions_Rotation: THEOREM
  FORALL (a:(pure_quat), b:(pure_quat) |
          norm(Vect_part(a)) = norm(Vect_part(b)) AND
          linearly_independent?(Vect_part(a), Vect_part(b))):
          LET q = rot_quat(a,b) IN
          b = T_q(q)(a)

Quaternions_Rotation_Deform: THEOREM
 FORALL (a:(pure_quat), b:(pure_quat) |
         linearly_independent?(Vect_part(a), Vect_part(b))):
 LET q =
 (sqrt(norm(Vect_part(b))/norm(Vect_part(a))))*
  rot_quat(a, norm(Vect_part(a))/norm(Vect_part(b))*b)
 IN  b = T_q(q)(a)
```

Lagrange's four-square theorem

Given a positive integer x there are four non-negative integers a, b, c, d such that

$$x = a^2 + b^2 + c^2 + d^2$$

Strategy:

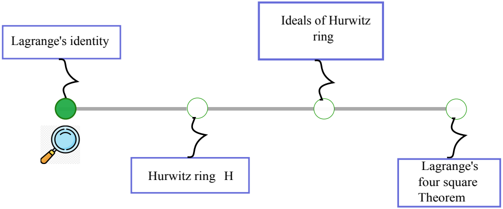
1. Prove that the product of the sum of four squares is also a sum of four squares (Lagrange's identity).

$$(a_0^2 + a_1^2 + a_2^2 + a_3^2) \cdot (b_0^2 + b_1^2 + b_2^2 + b_3^2) = (c_0^2 + c_1^2 + c_2^2 + c_3^2)$$

2. Prove the Lagrange's four-square theorem considering x as an odd prime number, since

$$2 = 1^2 + 1^2 + 0^2 + 0^2$$

Lagrange's identity and Norm of Quaternions

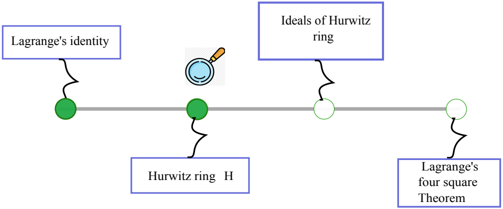



```
Lagrange_identity: LEMMA FORALL (a0, a1, a2, a3, b0, b1, b2, b3: real):
(a0^2 + a1^2 + a2^2 + a3^2) * (b0^2 + b1^2 + b2^2 + b3^2) =
  (a0*b0 - a1*b1 - a2*b2 - a3*b3)^2 + (a0*b1 + a1*b0 + a2*b3 - a3*b2)^2 +
  (a0*b2 - a1*b3 + a2*b0 + a3*b1)^2 + (a0*b3 + a1*b2 - a2*b1 + a3*b0)^2
```

Let $\mathbf{x} = (a_0, a_1, a_2, a_3)$ and $\mathbf{y} = (b_0, b_1, b_2, b_3)$ be Hamilton's quaternions. Then,

$$N(\mathbf{x}) \cdot N(\mathbf{y}) = N(\mathbf{x} \cdot \mathbf{y})$$

Special structure where a prime p is norm of some element




```
IMPORTING algebra@quaternions[rational,+,*,0,1,-1,-1]
Hurwitz_ring: set[quat] = {q: quat | EXISTS (x, y, z, t: int):
(q`x = x/2 AND q`y = x/2 + y AND q`z = x/2 + z AND q`t = x/2 + t)}

Hurwitz_ring_is_ring_w_one: THEOREM
    ring_with_one?[quat,+,*,zero_q, one_q](Hurwitz_ring)

Hurwitz_red_norm_charac: LEMMA FORALL (q: Hurwitz_ring):
    red_norm(q) = (q`x^2 + q`y^2 + q`z^2 + q`t^2,  0,  0,  0)

Hurwitz_red_norm_is_posint: LEMMA FORALL (q: Hurwitz_ring):
    integer?((red_norm(q))`x) AND (red_norm(q))`x >= 0
```

Other properties of the Hurwitz Ring

A left-division algorithm holds for the Hurwitz Ring

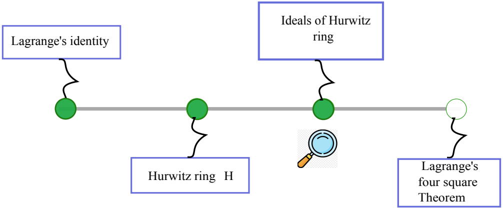
```
Hurwitz_left_division: THEOREM
  FORALL (a: Hurwitz_ring, b: Hurwitz_ring | red_norm(b)`x > 0):
   EXISTS (c, d: Hurwitz_ring): a = c*b+d AND red_norm(d)`x < red_norm(b)`x
```

$\Downarrow$

Every left-ideal L of the Hurwitz ring H has a generator

```
left_product_generator: LEMMA
    FORALL (L: Hurwitz_left_ideal):
        EXISTS (u: (L)):
               FORALL (x: (L)): EXISTS (r: Hurwitz_ring): x = r*u
```

When $L \neq (0)$, the generator $u \in L$ is an element whose norm is minimal over the nonzero elements of L.



We want to guarantee the existence of a left-ideal L of H such that:

- $\mathbf{p} = (p, 0, 0, 0) \in L$;
- $\mathbf{p} = \mathbf{r} \cdot \mathbf{u}$ for some $\mathbf{r} \in H$ and $\mathbf{u} \in L$

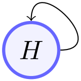
AND

- $p^2 = N(\mathbf{p}) = N(\mathbf{r}) \cdot N(\mathbf{u})$, where $N(\mathbf{r}) > 1$ and $N(\mathbf{u}) > 1$

$$\Downarrow$$

- $N(\mathbf{r}) = N(\mathbf{u}) = p$

May L be the Hurwitz ring?



$$H = \left\{ \left(\frac{x_0}{2}, \frac{x_0}{2} + x_1, \frac{x_0}{2} + x_2, \frac{x_0}{2} + x_3 \right) | x_i \in \mathbb{Z} \right\}$$

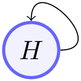
- The Hurwitz ring is an ideal of itself;
- $(p, 0, 0, 0) = \left(\frac{2p}{2}, \frac{2p}{2} - p, \frac{2p}{2} - p, \frac{2p}{2} - p \right) \in H$;

Since $H \neq (0)$, the generator $u \in H$ is an element whose norm is minimal over the nonzero elements of H.

$N(\mathbf{q}) = \left(\frac{x_0}{2}\right)^2 + \left(\frac{x_0}{2} + x_1\right)^2 + \left(\frac{x_0}{2} + x_2\right)^2 + \left(\frac{x_0}{2} + x_3\right)^2$ is minimal when $x_0 = 1$ and $x_1 = x_2 = x_3 = 0 \Rightarrow N(\mathbf{u}) = 1$.

$p^2 = N(\mathbf{p}) = N(\mathbf{r}) \cdot N(\mathbf{u})$, where $N(\mathbf{r}) > 1$ and $N(\mathbf{u}) > 1$ is not satisfied.

May L be the Hurwitz ring?



$$H = \left\{\left(\frac{x_0}{2}, \frac{x_0}{2} + x_1, \frac{x_0}{2} + x_2, \frac{x_0}{2} + x_3\right) | x_i \in \mathbb{Z}\right\}$$

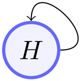
- The Hurwitz ring is an ideal of itself;
- $(p, 0, 0, 0) = \left(\frac{2p}{2}, \frac{2p}{2} - p, \frac{2p}{2} - p, \frac{2p}{2} - p\right) \in H$;

Since $H \neq (0)$, the generator $u \in H$ is an element whose norm is minimal over the nonzero elements of H.

$N(\mathbf{q}) = \left(\frac{x_0}{2}\right)^2 + \left(\frac{x_0}{2} + x_1\right)^2 + \left(\frac{x_0}{2} + x_2\right)^2 + \left(\frac{x_0}{2} + x_3\right)^2$ is minimal when $x_0 = 1$ and $x_1 = x_2 = x_3 = 0 \Rightarrow N(\mathbf{u}) = 1$.

$p^2 = N(\mathbf{p}) = N(\mathbf{r}) \cdot N(\mathbf{u})$, where $N(\mathbf{r}) > 1$ and $N(\mathbf{u}) > 1$ is not satisfied.

May L be the Hurwitz ring?



$$H = \left\{ \left(\frac{x_0}{2}, \frac{x_0}{2} + x_1, \frac{x_0}{2} + x_2, \frac{x_0}{2} + x_3 \right) | x_i \in \mathbb{Z} \right\}$$

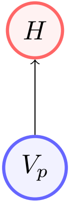
- The Hurwitz ring is an ideal of itself;
- $(p, 0, 0, 0) = \left(\frac{2p}{2}, \frac{2p}{2} - p, \frac{2p}{2} - p, \frac{2p}{2} - p \right) \in H$;

Since $H \neq (0)$, the generator $u \in H$ is an element whose norm is minimal over the nonzero elements of H.

$N(\mathbf{q}) = \left(\frac{x_0}{2}\right)^2 + \left(\frac{x_0}{2} + x_1\right)^2 + \left(\frac{x_0}{2} + x_2\right)^2 + \left(\frac{x_0}{2} + x_3\right)^2$ is minimal when $x_0 = 1$ and $x_1 = x_2 = x_3 = 0 \Rightarrow N(\mathbf{u}) = 1$.

$p^2 = N(\mathbf{p}) = N(\mathbf{r}) \cdot N(\mathbf{u})$, where $N(\mathbf{r}) > 1$ and $N(\mathbf{u}) > 1$ is not satisfied.

May L be the Prime Hurwitz ideal V_p?



$$V_p = \left\{ \left(\frac{p \cdot x_0}{2}, p \cdot \left(\frac{x_0}{2} + x_1 \right), p \cdot \left(\frac{x_0}{2} + x_2 \right), p \cdot \left(\frac{x_0}{2} + x_3 \right) \right) | x_i \in \mathbb{Z} \right\}$$

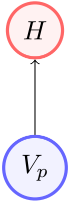
- V_p is an ideal of the Hurwitz ring H;
- $(p, 0, 0, 0) = \left(\frac{p \cdot 2}{2}, p \cdot \left(\frac{2}{2} - 1 \right), p \cdot \left(\frac{2}{2} - 1 \right), p \cdot \left(\frac{2}{2} - 1 \right) \right) \in V_p$;

Since $V_p \neq (0)$, the generator $u \in V_p$ is an element whose norm is minimal over the nonzero elements of V_p.

$N(\mathbf{q}) = p^2 \left[\left(\frac{x_0}{2} \right)^2 + \left(\frac{x_0}{2} + x_1 \right)^2 + \left(\frac{x_0}{2} + x_2 \right)^2 + \left(\frac{x_0}{2} + x_3 \right)^2 \right]$ is minimal when $x_0 = 1$ and $x_1 = x_2 = x_3 = 0 \Rightarrow N(\mathbf{u}) = p^2$.

$p^2 = N(\mathbf{p}) = N(\mathbf{r}) \cdot N(\mathbf{u})$, where $N(\mathbf{r}) > 1$ and $N(\mathbf{u}) > 1$ is not satisfied.

May L be the Prime Hurwitz ideal V_p?



$$V_p = \left\{ \left(\frac{p \cdot x_0}{2}, p \cdot \left(\frac{x_0}{2} + x_1 \right), p \cdot \left(\frac{x_0}{2} + x_2 \right), p \cdot \left(\frac{x_0}{2} + x_3 \right) \right) | x_i \in \mathbb{Z} \right\}$$

- V_p is an ideal of the Hurwitz ring H;
- $(p, 0, 0, 0) = \left(\frac{p \cdot 2}{2}, p \cdot \left(\frac{2}{2} - 1 \right), p \cdot \left(\frac{2}{2} - 1 \right), p \cdot \left(\frac{2}{2} - 1 \right) \right) \in V_p$;

Since $V_p \neq (0)$, the generator $u \in V_p$ is an element whose norm is minimal over the nonzero elements of V_p.

$$N(\mathbf{q}) = p^2 \left[\left(\frac{x_0}{2} \right)^2 + \left(\frac{x_0}{2} + x_1 \right)^2 + \left(\frac{x_0}{2} + x_2 \right)^2 + \left(\frac{x_0}{2} + x_3 \right)^2 \right]$$ is minimal when $x_0 = 1$ and $x_1 = x_2 = x_3 = 0 \Rightarrow N(\mathbf{u}) = p^2$.

$p^2 = N(\mathbf{p}) = N(\mathbf{r}) \cdot N(\mathbf{u})$, where $N(\mathbf{r}) > 1$ and $N(\mathbf{u}) > 1$ is not satisfied.

May L be the Prime Hurwitz ideal V_p?

$$\begin{tikzcd} H \\ V_p \arrow[u] \end{tikzcd}$$

$$V_p = \left\{ \left(\frac{p \cdot x_0}{2}, p \cdot \left(\frac{x_0}{2} + x_1 \right), p \cdot \left(\frac{x_0}{2} + x_2 \right), p \cdot \left(\frac{x_0}{2} + x_3 \right) \right) | x_i \in \mathbb{Z} \right\}$$

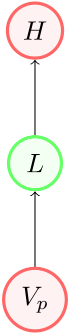
- V_p is an ideal of the Hurwitz ring H;
- $(p, 0, 0, 0) = \left(\frac{p \cdot 2}{2}, p \cdot \left(\frac{2}{2} - 1 \right), p \cdot \left(\frac{2}{2} - 1 \right), p \cdot \left(\frac{2}{2} - 1 \right) \right) \in V_p$;

Since $V_p \neq (0)$, the generator $u \in V_p$ is an element whose norm is minimal over the nonzero elements of V_p.

$$N(\mathbf{q}) = p^2 \left[\left(\frac{x_0}{2} \right)^2 + \left(\frac{x_0}{2} + x_1 \right)^2 + \left(\frac{x_0}{2} + x_2 \right)^2 + \left(\frac{x_0}{2} + x_3 \right)^2 \right]$$ is minimal when $x_0 = 1$ and $x_1 = x_2 = x_3 = 0 \Rightarrow N(\mathbf{u}) = p^2$.

$p^2 = N(\mathbf{p}) = N(\mathbf{r}) \cdot N(\mathbf{u})$, where $N(\mathbf{r}) > 1$ and $N(\mathbf{u}) > 1$ is not satisfied.

The existence of an intermediate ideal L



- $\mathbf{p} = (p, 0, 0, 0) \in L$;
- $\mathbf{p} = \mathbf{r} \cdot \mathbf{u}$ for some $\mathbf{r} \in H$ and $\mathbf{u} \in L$

AND

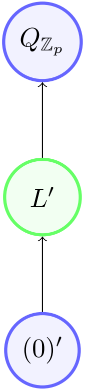
- $p^2 = N(\mathbf{p}) = N(\mathbf{r}) \cdot N(\mathbf{u})$, where $N(\mathbf{r}) > 1$ and $N(\mathbf{u}) > 1$

$$\Downarrow$$

- $N(\mathbf{r}) = N(\mathbf{u}) = p$

We need to prove that V_p is not a maximal left ideal

The existence of an intermediate ideal L



V_p is not a maximal ideal:

- Specification of quaternions over $\mathbb{Z}_p$:

  $Q_{\mathbb{Z}_p} = \{(a_0, a_1, a_2, a_3) | a_i \in \mathbb{Z}_p\}$

- Prove that $Q_{\mathbb{Z}_p}$ is not a division ring;

```
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](fullset[quat]))
```

- Apply the result that a ring, which is not a division ring, has a left-ideal different from the trivial ones.

The existence of an intermediate ideal L

V_p is not a maximal ideal:

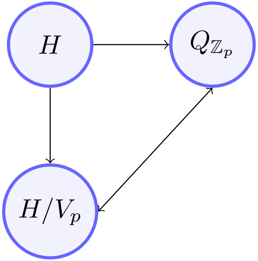
$$H \longrightarrow Q_{\mathbb{Z}_p}$$

- Building an epimorphism $\varphi : H \to Q_{\mathbb{Z}_p}$ such that $ker(\varphi) = V_p$;

$$\begin{aligned}
\varphi\left(\left(\frac{x}{2}, \frac{x}{2}+y, \frac{x}{2}+z, \frac{x}{2}+t\right)\right) \quad = \quad & (2^{p-2}\cdot x + p\mathbb{Z}, \\
& (2^{p-2}\cdot x + y) + p\mathbb{Z}, \\
& (2^{p-2}\cdot x + z) + p\mathbb{Z}, \\
& (2^{p-2}\cdot x + t) + p\mathbb{Z})
\end{aligned}$$

The existence of an intermediate ideal L

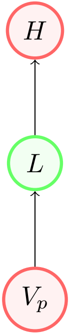
V_p is not a maximal ideal:



- Building an epimorphism $\varphi : H \to Q_{\mathbb{Z}_p}$ such that $ker(\varphi) = V_p$;
- Using the First Isomorphism Theorem to prove that $H/V_p \cong Q_{\mathbb{Z}_p}$.
- Conclude using

```
maximal_ideal_charac2: THEOREM
ideal?(M,R) AND maximal_left_ideal?(M,R) =>
division_ring?(/[T,+](R,M))
```

The existence of an intermediate ideal L



- $\mathbf{p} = (p, 0, 0, 0) \in V_p$ implies $\mathbf{p} \in L$;
- $\mathbf{p} = \mathbf{r} \cdot \mathbf{u}$ for some $\mathbf{r} \in H$ and $\mathbf{u} \in L$

AND

- $p^2 = N(\mathbf{p}) = N(\mathbf{r}) \cdot N(\mathbf{u})$, where $N(\mathbf{r}) > 1$ and $N(\mathbf{u}) > 1$

by using

```
Hurwitz_prod_inv_exists: LEMMA
   FORALL (h: (Hurwitz_ring)):
   red_norm(h)`x = 1 IFF
   EXISTS(r: (Hurwitz_ring)): h*r = one_q AND r*h = one_q
```

$$\Downarrow$$

$$p = N(\mathbf{u})$$

Euler's Trick

- $\mathbf{u} \in H \Longrightarrow \mathbf{u} = \left(\frac{m_0}{2}, \frac{m_0}{2} + m_1, \frac{m_0}{2} + m_2, \frac{m_0}{2} + m_3\right)$, $m_i \in \mathbb{Z}$.
- $2\mathbf{u} = (m_0, m_0 + 2m_1, m_0 + 2m_2, m_0 + 2m_3)$ and
  $N(2\mathbf{u}) = m_0^2 + (m_0 + 2m_1)^2 + (m_0 + 2m_2)^2 + (m_0 + 2m_3)^2$
- On the other hand, $N(2\mathbf{u}) = 4N(\mathbf{u}) = 4p$

Euler's Trick

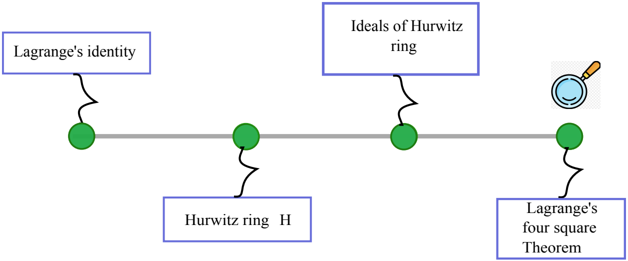
If $2a = x_0^2 + x_1^2 + x_2^2 + x_3^2$, where $a, x_0, x_1, x_2, x_3 \in \mathbb{Z}$ then

$$a = y_0^2 + y_1^2 + y_2^2 + y_3^2 \text{ for some } y_0, y_1, y_2, y_3 \in \mathbb{Z}$$

Proof: Depending on the parity of x_i, choose

$$y_0 = \frac{x_0 + x_1}{2}, y_1 = \frac{x_0 - x_1}{2}, y_2 = \frac{x_2 + x_3}{2}, y_3 = \frac{x_2 - x_3}{2}$$

Lagrange's four-square theorem

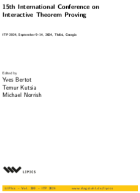


Given a positive integer x there are four non-negative integers a, b, c, d such that

$$x = a^2 + b^2 + c^2 + d^2$$

Proof: By induction on x.

Formalization of Quaternion Algebras


15th International Conference on
Interactive Theorem Proving

Edited by
Yves Bertot
Temur Kutsia
Michael Norrish

LIPIcs

[5] de Lima, Galdino, Oliveira Ribeiro, Ayala-Rincón

A Formalization of the General Theory of Quaternions

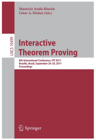
Proc. of 15th Interactive Theorem Proving, ITP 2024.

https://doi.org/10.4230/LIPIcs.ITP.2024.11

The formalization approach follows the same principle:

$$\underbrace{\boxed{\text{Quaternions theory over any field}} \rightsquigarrow \begin{cases} \boxed{\text{Hamilton's Quaternions } (Q[\mathbb{R}])} \\ \boxed{\text{Lagrange's 4 sq. Th. } (Q[\mathbb{Q}], Q[\mathbb{Z}_p])} \end{cases}}_{\text{Formalization approach}}$$

Related Work - Formalization of Quaternions



Andrea Gabrielli and Marco Maggesi (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

Reynald Affeldt and Cyril Cohen (2017)
Formal foundations of 3D geometry to model robot manipulators.
CPP 2017. ACM Proceedings.

https://doi.org/10.1145/3018610.30186

All of them are **restricted to** Hamilton's Quaternions.

Lean Mathlib includes general definitions and results about Quaternions.

Mathlib.Algebra.Quaternion

Conclusions

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.

$$\underbrace{\boxed{\text{algebraic theories}} \quad \rightsquigarrow \quad \boxed{\text{algebraic structures}}}_{\text{Formalization approach}}$$

- Completing the theory of rings (rings of polynomials/polynomial factorization)
- Formalizing properties of Hamilton's quaternions.
- Enriching automation of PVS strategies for abstract structures.

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. In Proceedings LSFA 2023. EPTCS 402, 2024, pp. 18-33
- Ayala-Rincón, M., de Lima, T.A., Galdino, A.L., Avelar, A.B., Formalization of Algebraic Theorems in PVS. In EPiCS Proc. LPAR-24, 2023.
- de Lima, T.A., Galdino, A.L., de Oliveira Ribeiro, B.B., Ayala-Rincón, M., A Formalization of the General Theory of Quaternions. In LiPIcs Proc. ITP 2024
- Fraleigh, John B., A First Course in Abstract Algebra, Pearson, 2003 (1967).
- Hungerford, Thomas W., Algebra, Graduate Texts in Mathematics, vol. 73, 1980 (1974).

References II

- Putinar, M. and Sullivant, S.,Emerging Applications of Algebraic Geometry. Springer New York (2008)
- Voight, John: Quaternion Algebras, ed.1. Springer Cham (2021)
- 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.