XX Seminário Informal (,mas Formal!) 2023

Grupo de Teoria da Computação da UnB

Mechanizing Rings in PVS

The case of Quaternions

Thaynara Arielly de Lima (IME/UFG)

André Luiz Galdino(IMTec/UFCat)

Joint work with

Andréia Borges Avelar (FUP/UnB)

Mauricio Ayala-Rincón(CIC-MAT/UnB)

Funded by FAPDF 00193-00000229/2021-21, and
CNPq Research Grant 313290/2021-0

February 14 , 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 systems, statistics, modeling of biological processes, and computer algebra [3].

  A formalization of the main results of ring theory would make possible the formal verification of more complex theories involving rings in their scope.
- Fully formalizing the theory of rings contributes to the enrichment of libraries of mathematics in PVS;

  `https://github.com/nasa/pvslib/tree/master/algebra`
- Formalizing properties of abstract algebraic structures allows us to reuse such results in multiple contexts.

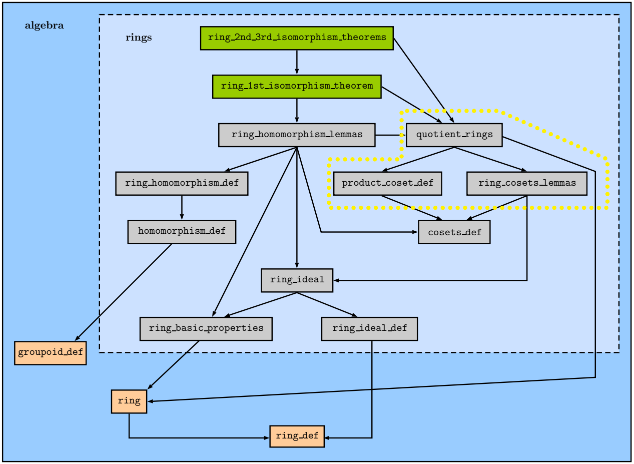


Figure: Hierarchy of the sub-theories for the three isomorphism theorems for rings: `ring_1st_isomorphism_theorem` and `ring_2nd_3rd_isomorphism_theorems` (Taken from [4])

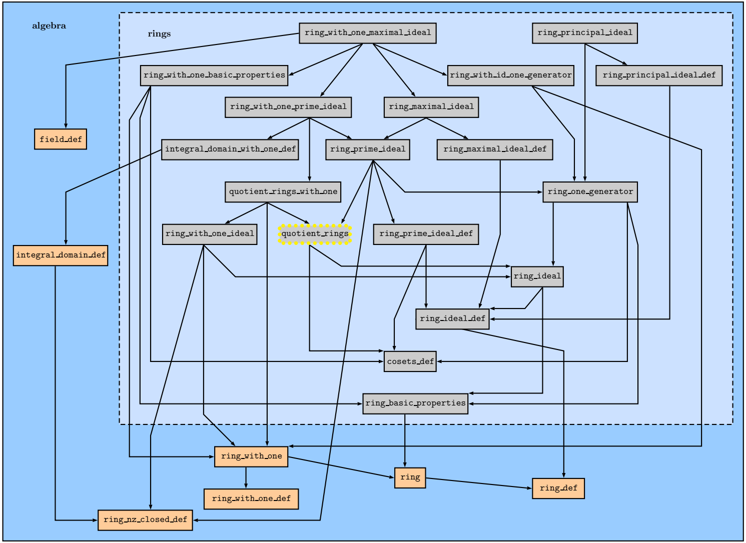


Figure: Hierarchy of the sub-theories related with principal, prime and maximal ideals (Taken from [4])

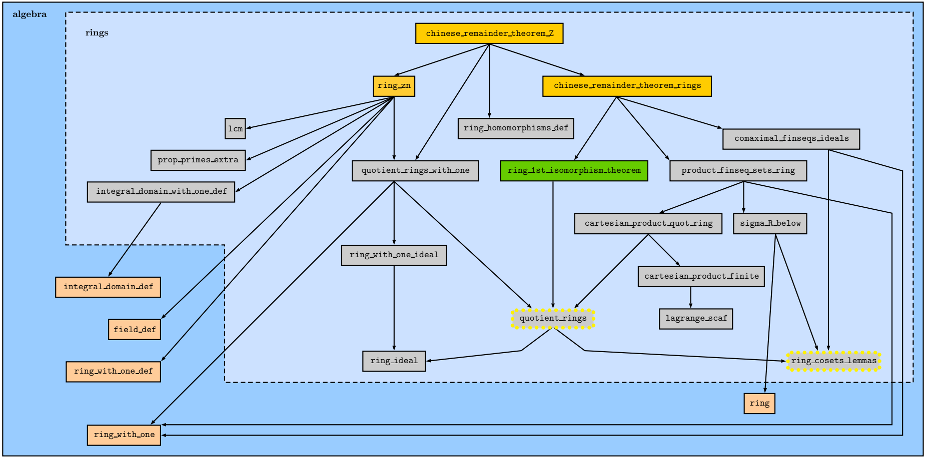


Figure: Hierarchy of the sub-theories related with Chinese Remainder Theorem (Taken from [4])

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

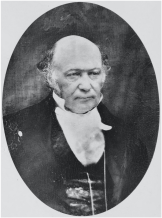
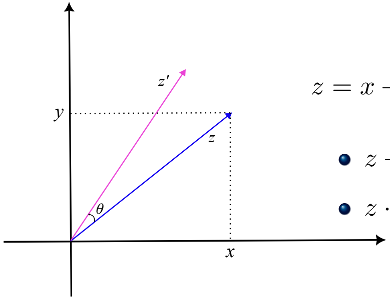


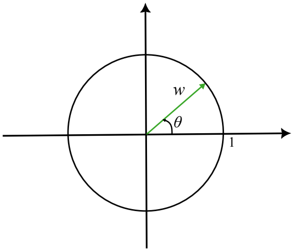
Figure: Sir William Rowan Hamilton, picture taken from [2]

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 [2]

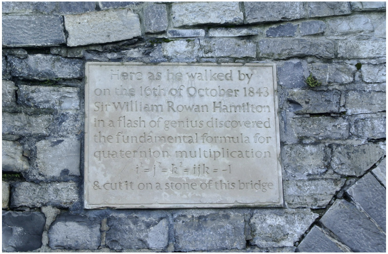


Figure: Broom bridge plaque in Dublin, picture taken from [8]

Hamilton's Quaternions

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

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

If $\boldsymbol{p = p_0 + p_1 i + p_2 j + p_3 k}$ and $\boldsymbol{q = q_0 + q_1 i + q_2 j + q_3 k}$ then:

- $p + q = (p_0 + q_0) + (p_1 + q_1)i + (p_2 + q_2)j + (p_3 + q_3)k$
- $$\begin{aligned} p \cdot q \quad = \quad & (p_0 q_0 - p_1 q_1 - p_2 q_2 - p_3 q_3) \\ & +(p_0 q_1 + p_1 q_0 + p_2 q_3 - p_3 q_2)i \\ & +(p_0 q_2 - p_1 q_3 + p_2 q_0 + p_3 q_1)j \\ & +(p_0 q_3 + p_1 q_2 - p_2 q_1 + p_3 q_0)k \end{aligned}$$

Hamilton's Quaternions

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

Identifying ...

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

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

Considering...

- $\mathbb{H}^0 = \{q = 0 + q_1 i + q_2 j + q_3 k\} \subset \mathbb{H}$;

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

Conjugate and norm

Define:

- The conjugate of a quaternion q as

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

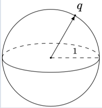
  where $\boldsymbol{q}$ denotes $q_1 i + q_2 j + q_3 k$

- 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:**

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

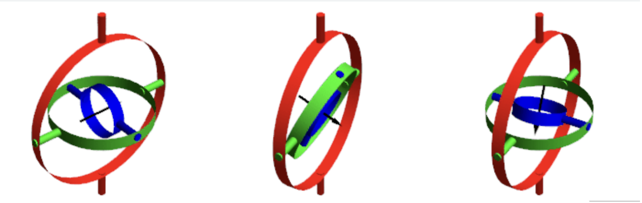
- **If $q \in \mathbb{H}^1$ then T_q preserves norm of v:**

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

- **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 [6]

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

Benefits of rotating using Quaternions - Avoiding Gimbal Lock

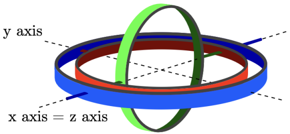
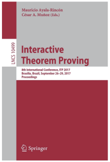


Figure: **Gimbal Lock**: taken from [7]

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 Quaternion Algebras - Related Work



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

`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`, Formal proof development

Both of them are restricted to Hamilton's Quaternions.

Formalization of Quaternion Algebras

Our formalization follows the principles established in previous works: formalize abstract structures and obtain particular cases as instantiation of the general case.

(Near) Future work

- Formalizing characterization of Quaternion Algebras as Division Rings;
- Formalizing Hamilton's Quaternions as an instance of a Quaternion Algebras;
- Formalizing the connection between Quaternions Algebra as a four-dimensional space vs an F-algebra.

References I

- Bini, G., Flamini, F.: Finite commutative rings and their applications, vol. 680. Springer Science & Business Media (2012)
- John Voight: Quaternion Algebras, ed.1. Springer Cham (2021)
- Putinar, M. and Sullivant, S.,Emerging Applications of Algebraic Geometry. Springer New York (2008)
- de Lima, T.A., Avelar da Silva, 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)
- Galdino, André Luiz.:Quatérnions e Rotações. Notes (in Portuguese). (2022)
- 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.

References II

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

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.