

Introduzione

Oggetto della mia tesi sono le algebre di divisione reali di dimensione finita ed alcuni esempi di queste. In breve, un'algebra di divisione è un anello unitario nel quale ogni elemento non nullo ha un inverso moltiplicativo.

Tra gli esempi più noti che rientrano in tale definizione troviamo l'insieme dei numeri reali \mathbb{R} , l'insieme dei numeri complessi \mathbb{C} e l'insieme dei quaternioni \mathbb{H} .

È proprio grazie alla nascita di questi ultimi che lo studio delle algebre di divisione prese vita; infatti, prima che il geniale Hamilton, rinunciando alla commutatività del prodotto, creasse i suoi quaternioni, il mondo dei matematici era convinto che non potessero esistere sistemi di numeri ipercomplessi più grandi del campo complesso cioè sistemi che potessero costituire ancora delle algebre di divisione.

In questa dissertazione costruiremo dapprima l'insieme dei quaternioni hamiltoniani, poi introdurremo le algebre di divisione e ne daremo alcune proprietà: in particolare, dimostreremo che l'insieme dei quaternioni costituisce un'algebra di divisione e vedremo come tali oggetti possono essere utilizzati in varie discipline. Faremo vedere che così come i numeri complessi unitari possono essere utilizzati per rappresentare le rotazioni nel piano, i quaternioni unitari possono essere utilizzati per rappresentare le rotazioni nello spazio.

La parte centrale del lavoro è dedicata a dimostrare il seguente Teorema di Fröbenius

Teorema di Fröbenius 0.0.1. *Sia \mathcal{A} , un'algebra reale, quadratica, associativa, priva di divisori dello zero.*

Allora ci sono solo tre possibilità:

1. \mathcal{A} è isomorfa al campo dei numeri reali.

2. \mathcal{A} è isomorfa al campo dei numeri complessi.

3. \mathcal{A} è isomorfa all'algebra dei quaternioni reali.

Nell'ultima parte mostreremo che esistono algebre di divisione reali non associative, costruendo l'algebra degli Ottetti di Cayley. Quest'algebra è, a meno di isomorfismi l'unica algebra di divisione non associativa, come dimostrò Max Zorn nel 1933.

Più dettagliatamente, nel primo capitolo daremo una breve introduzione storica dell'argomento trattato.

Nel secondo capitolo costruiremo, così come fece lo stesso Hamilton, l'insieme dei quaternioni reali.

Nel terzo capitolo daremo alcune definizioni tra cui quella di algebra di divisione, dimostrandone poi qualche proprietà.

Nel quarto capitolo dimostreremo alcune importanti proprietà dei quaternioni; faremo vedere, per esempio, che tale insieme è un'algebra di divisione di dimensione quattro su \mathbb{R} , introdurremo lo spazio immaginario dell'algebra, mostreremo che \mathbb{H} è uno spazio vettoriale euclideo ed infine, vedremo come questi oggetti possano essere utilizzati in varie discipline.

Nel quinto capitolo, dopo aver verificato i risultati preliminari necessari, dimostreremo il teorema di Fröbenius.

Infine, nell'ultimo capitolo introdurremo l'insieme degli ottetti \mathbb{O} e ne illustreremo alcune proprietà.

L'introduzione dei numeri complessi fu un evento molto significativo nella storia della matematica. Dopo la loro interpretazione sul piano di Gauss e l'utilizzazione della loro moltiplicazione nel calcolo delle rotazioni nel piano, ci fu un certo fermento nelle esigenze di produrre altri sistemi algebrici che potessero rappresentare le rotazioni nello spazio tridimensionale.

Colui che per primo ottenne dei risultati in tal senso, fu l'Irlandese W. R. Hamilton quando, rinunciando alla commutatività del prodotto, inventò l'insieme dei suoi quaternioni, insieme quadrimensionale in grado di rappresentare il "mondo tridimensionale". I quaternioni costituiscono il primo esempio di algebra di divisione non commutativa.

La costruzione di tale struttura diede vita a quella che oggi è detta "l'epoca d'oro" dell'algebra.

Nel 1840, il matematico Hopf mostrò che ogni algebra di divisione reale commutativa ha al più, dimensione due, vale a dire, che ogni tale algebra è isomorfa a quella dei numeri complessi. Nel 1845, Arthur Cayley produsse la sua algebra degli ottetti; algebra di divisione reale di dimensione otto, in cui non vale la legge associativa del prodotto. Nel 1853, Hamilton mostrò, creando quella che oggi è detta "algebra dei biquaternioni", (un sistema i cui elementi sono i quaternioni a coefficienti complessi), che non tutte le algebre sono di divisione, nel senso che, non tutti gli elementi non nulli di un'algebra sono invertibili e quindi non sempre si può operare una divisione. Nel 1860, inoltre, Kervaire e Milnor mostrarono separatamente che non esistono algebre di divisione reali di dimensione finita, associative o meno, all'infuori di quelle sopra citate. Nel 1887, il matematico tedesco Ferdinand Georg Fröbenius, dimostrò che esistono solo tre algebre di divisione reali associative, di dimensione finita, isomorficamente distinte che sono esattamente: l'algebra dei numeri reali \mathbb{R} , l'algebra dei numeri complessi \mathbb{C} e l'algebra dei quaternioni \mathbb{H} . Ed infine, Max Zorn dimostrò, nel 1933, che ogni algebra di divisione reale non associativa deve essere isomorficamente equivalente all'algebra degli ottetti di Cayley.

Poichè lo scopo del nostro lavoro è quello di dimostrare il Teorema di Fröbenius, teorema che ci fornisce una prima catalogazione delle algebre associative, cominciamo con l'introdurre le algebre di divisione ed alcune loro proprietà.

Definizione 0.0.1. *Sia V uno spazio vettoriale su un campo K dotato dell'operazione prodotto*

$$\begin{aligned} \cdot : V \times V &\rightarrow V \\ (\mathbf{p}, \mathbf{q}) &\rightarrow \mathbf{pq} \end{aligned}$$

Diciamo che V è un'algebra su K o una K -algebra se valgono le due leggi distributive del prodotto

$$(\mathbf{ap} + \mathbf{bq})\mathbf{r} = \mathbf{a}(\mathbf{pr}) + \mathbf{b}(\mathbf{qr}) \quad (1)$$

$$\mathbf{p}(\mathbf{aq} + \mathbf{br}) = \mathbf{a}(\mathbf{pq}) + \mathbf{b}(\mathbf{pr}) \quad (2)$$

per ogni $a, b \in K$, per ogni $\mathbf{p}, \mathbf{q}, \mathbf{r} \in V$.

Se vale la legge associativa del prodotto

$$\mathbf{p}(\mathbf{qr}) = (\mathbf{pq})\mathbf{r} \quad \text{per ogni } \mathbf{p}, \mathbf{q}, \mathbf{r} \in V \quad (3)$$

l'algebra è detta associativa.

Se vale la legge commutativa

$$\mathbf{pq} = \mathbf{qp} \quad \text{per ogni } \mathbf{p}, \mathbf{q} \in V \quad (4)$$

l'algebra è detta commutativa.

Un'algebra \mathcal{A} è detta priva di divisori dello zero se preso comunque $\mathbf{a} \in \mathcal{A} \setminus \{0\}$ allora non esiste $\mathbf{b} \in \mathcal{A} \setminus \{0\}$ tale che $\mathbf{ab} = 0$ cioè, se $\mathbf{ab} = 0$ allora si deve avere $\mathbf{a} = 0$ oppure $\mathbf{b} = 0$.

Diciamo inoltre che \mathcal{A} è un'algebra di divisione se le due equazioni

$$\mathbf{ax} = \mathbf{b} \quad \mathbf{ya} = \mathbf{b}$$

dove \mathbf{a} e \mathbf{b} sono due qualunque elementi dell'algebra ed $\mathbf{a} \neq 0$, ammettono un'unica soluzione.

Osserviamo che vale allora la seguente proposizione:

Proposizione 0.0.1. *Sia \mathcal{A} un'algebra di dimensione finita su K . Le seguenti affermazioni sono equivalenti:*

1. \mathcal{A} è un'algebra di divisione.
2. \mathcal{A} è priva di divisori dello zero.

Diamo inoltre la seguente definizione:

Definizione 0.0.2. *Sia \mathcal{A} un'algebra reale con elemento neutro \mathbf{e} ; definiamo lo spazio immaginario di \mathcal{A} , indicato con $\text{Im}\mathcal{A}$, l'insieme*

$$\text{Im}\mathcal{A} = \{\mathbf{a} \in \mathcal{A} \mid \mathbf{a}^2 \in \mathbb{R}\mathbf{e}, \mathbf{a} \notin \mathbb{R}\mathbf{e} \setminus \{0\}\}.$$

Siamo ora in grado di dimostrare che i quaternioni di Hamilton costituiscono un'algebra di divisione.

Definizione 0.0.3. *Definiamo l'insieme dei quaternioni e lo indichiamo \mathbb{H} l'insieme di oggetti della forma*

$$\mathbf{q} = q_0 + \mathbf{q} = q_0 + \mathbf{i}q_1 + \mathbf{j}q_2 + \mathbf{k}q_3 \quad q_0, q_1, q_2, q_3 \in \mathbb{R}; \quad (5)$$

cioè un quaternione è la somma di una parte scalare q_0 ed una parte vettoriale $\mathbf{q} = \mathbf{i}q_1 + \mathbf{j}q_2 + \mathbf{k}q_3$.

In questo insieme è definito il seguente prodotto; dati

$$\mathbf{p} = p_0 + \mathbf{i}p_1 + \mathbf{j}p_2 + \mathbf{k}p_3 \quad \text{e} \quad \mathbf{q} = q_0 + \mathbf{i}q_1 + \mathbf{j}q_2 + \mathbf{k}q_3$$

si ha

$$\mathbf{p}\mathbf{q} := p_0q_0 - \mathbf{p} \cdot \mathbf{q} + p_0\mathbf{q} + q_0\mathbf{p} + \mathbf{p} \times \mathbf{q}.$$

Se per ogni quaternione non nullo \mathbf{q} , poniamo $\mathbf{q}^{-1} := \frac{q_0 - (\mathbf{i}q_1 + \mathbf{j}q_2 + \mathbf{k}q_3)}{q_0^2 + q_1^2 + q_2^2 + q_3^2}$, possiamo verificare, grazie alla proposizione precedente, che \mathbb{H} è un'algebra di divisione associativa.

In particolare abbiamo allora che, dalla Definizione (??), si ha

$$\text{Im}\mathbb{H} = \{\mathbf{p} \in \mathbb{H} \mid \mathbf{p}^2 \in \mathbb{R}\}.$$

Notiamo che lo spazio immaginario di \mathbb{H} può anche essere visto come la parte vettoriale dell'algebra, infatti si ha

Teorema 0.0.1.

$$\text{Im}\mathbb{H} := \mathbb{R}\mathbf{i} + \mathbb{R}\mathbf{j} + \mathbb{R}\mathbf{k} \quad (6)$$

ed inoltre

$$\mathbb{H} = \mathbb{R} \oplus \text{Im}\mathbb{H} \quad (7)$$

Questo teorema ci permette di affermare che $\mathbb{H} \simeq \mathbb{R}^4$.

Ritornando alle algebre in generale, per dimostrare il Teorema di Fröbenius abbiamo bisogno di ulteriori definizioni e proposizioni.

Definizione 0.0.4. *Un'algebra \mathcal{A} è detta alternativa se per ogni coppia di elementi $\mathbf{a}, \mathbf{b} \in \mathcal{A}$ valgono le seguenti proprietà:*

- 1) $(\mathbf{a}\mathbf{b})\mathbf{b} = \mathbf{a}\mathbf{b}^2$
- 2) $\mathbf{b}(\mathbf{b}\mathbf{a}) = \mathbf{b}^2\mathbf{a}$ Diciamo invece che l'algebra è un'algebra quadratica se per ogni elemento $\mathbf{a} \in \mathcal{A}$ si può scrivere la seguente uguaglianza:

$$\mathbf{a}^2 = \alpha\mathbf{e} + \beta\mathbf{a} \text{ con } \alpha, \beta \in \mathbb{R}$$

Osserviamo che ogni algebra alternativa ammette un elemento neutro ed ancora che ogni algebra associativa è ovviamente alternativa.

Definizione 0.0.5. *Sia \mathcal{A} un'algebra con elemento neutro \mathbf{e} , siano $\mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathcal{A}$, diciamo che questi elementi costituiscono una tripletta hamiltoniana se le nove condizioni di Hamilton sono verificate, cioè se:*

$$\mathbf{u}^2 = \mathbf{v}^2 = \mathbf{w}^2 = -\mathbf{e}$$

$$\mathbf{w} = \mathbf{u}\mathbf{v} = -\mathbf{v}\mathbf{u}$$

$$\mathbf{u} = \mathbf{v}\mathbf{w} = -\mathbf{w}\mathbf{v}$$

$$\mathbf{v} = \mathbf{w}\mathbf{u} = -\mathbf{u}\mathbf{w}.$$

Possiamo allora verificare che valgono i seguenti fatti:

Teorema di esistenza delle triplette hamiltoniane 0.0.1. *Sia \mathcal{A} un'algebra alternativa, priva di divisori dello zero e con elemento neutro \mathbf{e} , ed*

inoltre, sia U un sottospazio bidimensionale di $\text{Im}\mathcal{A}$.

Allora, per ogni $\mathbf{u} \in U$ tale che $\mathbf{u}^2 = -\mathbf{e}$, esiste un elemento $\mathbf{v} \in U$ tale che $\mathbf{u}, \mathbf{v}, \mathbf{w} = \mathbf{uv}$ formano una tripletta hamiltoniana.

Proposizione 0.0.2. *Sia \mathcal{A} un'algebra quadratica, con elemento neutro \mathbf{e} . allora, $\text{Im}\mathcal{A}$ è un sottospazio vettoriale di \mathcal{A} e si ha:*

$$\mathcal{A} = \mathbb{R}\mathbf{e} \oplus \text{Im}\mathcal{A}$$

Lemma 0.0.1. *Sia \mathcal{A} un'algebra priva di divisori dello zero, e sia \mathbf{e} l'elemento unità dell'algebra; allora esiste $\mathbf{u} \in \text{Im}\mathcal{A}$ tale che $\mathbf{u}^2 = -1$.*

Proposizione 0.0.3. *Data un'algebra \mathcal{A} con elemento neutro \mathbf{e} , siano $\mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathcal{A}$ tre elementi che costituiscono una tripletta hamiltoniana, allora abbiamo che:*

1. *L'applicazione $f : \mathbb{H} \rightarrow \mathcal{A}$ tale che $f(\mathbf{q}) = f(q_0 + q_1\mathbf{i} + q_2\mathbf{j} + q_3\mathbf{k}) = q_0\mathbf{e} + q_1\mathbf{u} + q_2\mathbf{v} + q_3\mathbf{w}$ è un omomorfismo iniettivo di algebre.*
2. *$\mathbb{R}\mathbf{u} + \mathbb{R}\mathbf{v} + \mathbb{R}\mathbf{w} \subseteq \text{Im}\mathcal{A}$ ed in particolare $\text{Im}\mathcal{A}$ contiene un sottospazio vettoriale di dimensione tre.*

Siamo ora in grado di dimostrare il seguente teorema.

Teorema di Fröbenius 0.0.2. *Sia \mathcal{A} , un'algebra reale, quadratica, associativa, priva di divisori dello zero.*

Allora ci sono solo tre possibilità:

1. *\mathcal{A} è isomorfa al campo dei numeri reali.*
2. *\mathcal{A} è isomorfa al campo dei numeri complessi.*
3. *\mathcal{A} è isomorfa all'algebra dei quaternioni reali.*

Dimostrazione:

Necessariamente si deve avere che $\dim\mathcal{A} \geq 1$, inoltre poiché \mathcal{A} è associativa allora è anche un'algebra alternativa e quindi per quanto osservato nel paragrafo precedente ammette un elemento neutro \mathbf{e} .

Se $\dim \mathcal{A} = 1$ allora $\mathcal{A} \simeq \mathbb{R}$ è banalmente vero.

Se $\dim \mathcal{A} = 2$, sia $\mathbf{u} \in \mathcal{A}$ un elemento linearmente indipendente con \mathbf{e} , tale che $\mathbf{u}^2 = -\mathbf{e}$, un tale elemento esiste per il Lemma (??), e sia

$$F : \mathbb{C} \rightarrow \mathcal{A}$$

l'omomorfismo di algebre definito da

$$x + yi \rightarrow x\mathbf{e} + y\mathbf{u}.$$

Osserviamo che essendo \mathbf{e}, \mathbf{u} linearmente indipendenti tale omomorfismo è iniettivo. Ma allora, poiché $\dim \mathbb{C} = 2 = \dim \mathcal{A}$, F risulta essere biettiva e quindi è un isomorfismo.

Dunque se $\dim \mathcal{A} = 2$ allora $\mathcal{A} \simeq \mathbb{C}$.

Supponiamo ora che $\dim \mathcal{A} \geq 3$.

Dal teorema di esistenza delle triplette hamiltoniane abbiamo che, presi $\mathbf{u}, \mathbf{v} \in \text{Im} \mathcal{A}$ linearmente indipendenti, con $\mathbf{u}^2 = -\mathbf{e}$, esiste un elemento $\mathbf{w} = \mathbf{uv} \in \text{Im} \mathcal{A}$ tale che $\mathbf{u}, \mathbf{v}, \mathbf{w}$ formano una tripletta di Hamilton.

Sia allora $\mathbf{x} \in \text{Im} \mathcal{A}$. Abbiamo visto dalla Proposizione (??) che $\text{Im} \mathcal{A}$ è un sottospazio vettoriale di \mathcal{A} . Allora $\mathbf{u} + \mathbf{x}, \mathbf{v} + \mathbf{x} \in \mathcal{A}$; quindi $\mathbf{u}\mathbf{x} + \mathbf{x}\mathbf{u} = \alpha\mathbf{e}, \mathbf{v}\mathbf{x} + \mathbf{x}\mathbf{v} = \beta\mathbf{e}, \mathbf{w}\mathbf{x} + \mathbf{x}\mathbf{w} = \gamma\mathbf{e}$ con $\alpha, \beta, \gamma \in \mathbb{R}$.

Adesso se moltiplichiamo a destra la prima equazione per \mathbf{v} , e la seconda, a sinistra, per \mathbf{u} , e le sottraiamo, ricordando che l'algebra è associativa e che $\mathbf{uv} = \mathbf{w} = -\mathbf{vu}$ otteniamo:

$$(\mathbf{u}\mathbf{x} + \mathbf{x}\mathbf{u})\mathbf{v} - \mathbf{u}(\mathbf{v}\mathbf{x} + \mathbf{x}\mathbf{v}) = \alpha\mathbf{v} - \beta\mathbf{u}$$

cioè

$$(\mathbf{u}\mathbf{x}\mathbf{v} + \mathbf{x}\mathbf{w})\mathbf{v} - \mathbf{w}\mathbf{x} - \mathbf{u}\mathbf{x}\mathbf{v} = \alpha\mathbf{v} - \beta\mathbf{u}$$

e dunque

$$\mathbf{x}\mathbf{w} - \mathbf{w}\mathbf{x} = \alpha\mathbf{v} - \beta\mathbf{u}.$$

Sommando la terza equazione otteniamo

$$\mathbf{x}\mathbf{w} - \mathbf{w}\mathbf{x} + \mathbf{x}\mathbf{w} + \mathbf{w}\mathbf{x} = \alpha\mathbf{v} - \beta\mathbf{u} + \gamma\mathbf{e}$$

e cioè

$$2\mathbf{x}\mathbf{w} = \alpha\mathbf{v} - \beta\mathbf{u} + \gamma\mathbf{e}.$$

Se ora moltiplichiamo a destra per \mathbf{w} otteniamo

$$-2\mathbf{x} = \alpha\mathbf{u} + \beta\mathbf{v} + \gamma\mathbf{w}.$$

Questo risultato ci dice che ogni elemento $\mathbf{x} \in \text{Im}\mathcal{A}$ si scrive come combinazione lineare di $\mathbf{u}, \mathbf{v}, \mathbf{w}$ cioè che $\text{Im}\mathcal{A} \subseteq \mathbb{R}\mathbf{u} + \mathbb{R}\mathbf{v} + \mathbb{R}\mathbf{w}$.

Poiché dalla Proposizione (??) abbiamo che $\mathbb{R}\mathbf{u} + \mathbb{R}\mathbf{v} + \mathbb{R}\mathbf{w} \subseteq \text{Im}\mathcal{A}$, questo mi permette di concludere che $\text{Im}\mathcal{A} = \mathbb{R}\mathbf{u} + \mathbb{R}\mathbf{v} + \mathbb{R}\mathbf{w}$. Dalla Proposizione (??) abbiamo che $\mathcal{A} = \mathbb{R}\mathbf{e} \oplus \text{Im}\mathcal{A}$, dunque la dimensione di \mathcal{A} è quattro. Inoltre \mathcal{A} , per il primo punto della Proposizione (??), contiene una sottoalgebra isomorfa ad \mathbb{H} quindi $\mathcal{A} \simeq \mathbb{H}$.

Q.E.D.



Un interessante corollario a questo teorema ci dice che tutte e sole le algebre di divisione reali associative, di dimensione finita, sono a meno di isomorfismi, $\mathbb{R}, \mathbb{C}, \mathbb{H}$.

A questo punto possiamo dare l'unico esempio di algebra di divisione reale non associativa che conosciamo.

Definizione 0.0.6. Sia $\mathbb{O} := \{\mathbf{a} = (\mathbf{p}, \mathbf{q}), \mathbf{p}, \mathbf{q} \in \mathbb{H}\}$ in cui è definita la seguente moltiplicazione

$$\mathbf{ab} = (\mathbf{p}, \mathbf{q})(\mathbf{r}, \mathbf{s}) := (\mathbf{pr} - \bar{\mathbf{s}}\mathbf{q}, \mathbf{q}\bar{\mathbf{r}} + \mathbf{sp}) \quad (8)$$

Possiamo osservare che tale insieme è uno spazio vettoriale di dimensione otto, inoltre possiamo vedere che esso è un'algebra quadratica, alternativa, priva di divisori dello zero, quindi un'algebra di divisione. Allora dal Teorema di Fröbenius segue che non può essere associativa.

Bibliografia

- [1] H. D. Ebbinghaus, H. Hermes, F. Hirzebruch, M. Koecher, K. Mainzer, J. Neukirch, A. Prestel, R. Remmert: Numbers, Springer-Verlag, 1991.
- [2] I. L. Kantor, A. S. Solodovnikov: Hypercomplex numbers: an elementary introduction to algebras, Springer-Verlag, 1989.
- [3] U. Bottazzini: Storia della matematica moderna e contemporanea, Utet, 1997.
- [4] F. R. Pfaff: A commutative multiplication of number triplets, American Math. Monthly, 107 (2000), 156-162.
- [5] V. S. Varadarajan: Algebra in ancient and modern times, Math. World, 2, AMS, 1998.
- [6] J. C. McConnell: Division algebras- beyond the quaternions, American Math. Monthly, 85 (1998), 154-162.
- [7] J.H.M. Wedderburn: On hypercomplex numbers, Proc. London Math. Soc., 6 (1907), 77-118.
- [8] E. Sernesi, Geometria 1, Bollati Boringhieri, 1989.
- [9] E. Giusti, Analisi matematica 2, Bollati Boringhieri, 1991.