Advanced Ring Theory

Labix

March 11, 2024

Abstract

- Abstract Alebra by Thomas W. Judson

Contents

1 Division Rings

1.1 The Structure of Quaternions

Definition 1.1.1: Quaternions

Define the quaternions as the quotient algebra

$$\mathbb{H} = \frac{\mathbb{R}\langle x_1, x_2, x_3\rangle}{I}$$

where $I = (x_1^2 + 1, x_2^2 + 1, x_3^2 + 1, x_1x_2x_3 + 1)$.

Elements of $\mathbb{H}$ are of the form $a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ for $a, b, c, d \in \mathbb{R}$ and by writing $\mathbf{i} = x_1 + I$, $\mathbf{j} = x_2 + I$ and $\mathbf{k} = x_3 + I$.

A quaternion is said to be real if $b = c = d = 0$. It is said to be imaginary if $a = 0$. Denote the set of all imaginary quaternions by $\mathbb{H}_0$.

Proposition 1.1.2

The quaternions satisfy the following multiplication table:

$\cdot$	1	$\mathbf{i}$	$\mathbf{j}$	$\mathbf{k}$
1	1	$\mathbf{i}$	$\mathbf{j}$	$\mathbf{k}$
$\mathbf{i}$	$\mathbf{i}$	-1	$\mathbf{k}$	$-\mathbf{j}$
$\mathbf{j}$	$\mathbf{j}$	$-\mathbf{k}$	-1	$\mathbf{i}$
$\mathbf{k}$	$\mathbf{k}$	$\mathbf{j}$	$-\mathbf{i}$	-1

Proof. We only need to consider products that does not involve 1. It clear for $t = 1, 2, 3$, $x_t^2 + 1 \in I$. This means that $x_t^2 + I = -1 + I$ and thus $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^1 = -1$. Similarly, we have that $x_1x_2x_3 + I = -1 + I$ and thus $\mathbf{ijk} = -1$. Multiplying this expression by $-\mathbf{i}$ on the left gives $\mathbf{jk} = \mathbf{i}$. We can also multiply the expression by $-\mathbf{k}$ on the right to get $\mathbf{ij} = \mathbf{k}$. Now multiply $\mathbf{i}$ to the left of the equation $\mathbf{ij} = \mathbf{k}$ to get $-\mathbf{j} = \mathbf{ik}$. We can also multiply $\mathbf{ij} = \mathbf{k}$ by $\mathbf{j}$ on the right gives $-\mathbf{i} = \mathbf{kj}$. Finally we have $\mathbf{j}(\mathbf{i} = \mathbf{jk}) \implies \mathbf{ji} = -\mathbf{k}$ and $(\mathbf{ji} = -\mathbf{k})(-\mathbf{i}) \implies \mathbf{j} = \mathbf{ki}$. □

Proposition 1.1.3

The elements $1, \mathbf{i}, \mathbf{j}, \mathbf{k}$ form a basis for the $\mathbb{R}$-algebra $\mathbb{H}$.

Proof. It is clear that $1, x_1, x_2, x_3, x_1x_2, x_1x_3, x_2, x_3, \ldots$ span $\mathbb{H}$. By writing x_1, x_2, x_3 each in terms of $1, \mathbf{i}, \mathbf{j}, \mathbf{k}$ respectively, we have can see that $1, \mathbf{i}, \mathbf{j}, \mathbf{k}$ span $\mathbb{H}$. It remains to show that they are linearly independent.

Consider the $\mathbb{R}$-algebra homomorphism $f : \mathbb{R}\langle x_1, x_2, x_3\rangle \to M_{2\times 2}(\mathbb{C})$ defined by $f(x_1) = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, $f(x_2) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $f(x_3) = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$. It is clear that $I \subseteq \ker(f)$ since $f(x_1^2 + 1) = f(x_2^2 + 1) = f(x_3^2 + 1) = f(x_1x_2x_3 + 1) = 0$. By the first and third isomorphism theorem for modules, we have that

$$\frac{\mathbb{H}}{\ker(f)/I} \cong \frac{\mathbb{R}\langle x_1, x_2, x_3\rangle}{\ker(f)} \cong \mathrm{im}(f)$$

This means that $\dim_{\mathbb{R}}(\mathbb{H}) \geq \dim_{\mathbb{R}}(\mathrm{im}(f))$. Since the matrices $f(x_1), f(x_2), f(x_3)$ and 1 are all linearly independent over $\mathbb{R}$, we have that $\mathrm{im}(f)$ is at least 4-dimensional. Hence the four spanning elements of $\mathbb{H}$ must be linearly independent. □

Proposition 1.1.4

The imaginary quaternions $\mathbb{H}_0$ form a three dimensional vector subspace of $\mathbb{H}$. The real quaternions form a subalgebra $\mathbb{R}$ of $\mathbb{H}$.

We treat the imaginary quaternions $\mathbb{H}_0$ as the standard 3-space with dot product

$$(b_1\mathbf{i} + c_1\mathbf{j} + d_1\mathbf{k}) \cdot (b_2\mathbf{i} + c_2\mathbf{j} + d_2\mathbf{k}) = b_1b_2 + c_1c_2 + d_1d_2$$

and cross product

$$\begin{aligned}(b_1\mathbf{i} + c_1\mathbf{j} + d_1\mathbf{k}) \times_c (b_2\mathbf{i} + c_2\mathbf{j} + d_2\mathbf{k}) &= (c_1d_2 - c_2d_1)\mathbf{i} + (d_1b_2 - d_2b_1)\mathbf{j} + (b_1c_2 - c_2b_1)\mathbf{k} \\ &= \begin{vmatrix} \mathbf{i} & \mathbf{j} & \mathbf{k} \\ b_1 & c_1 & d_1 \\ b_2 & c_2 & d_2 \end{vmatrix}\end{aligned}$$

Proposition 1.1.5

Let $a_1 + \mathbf{h}_1$ and $a_2, \mathbf{h}_2$ be quaternions such that $a_1, a_2 \in \mathbb{R}$ and $\mathbf{h}_1, \mathbf{h}_2 \in \mathbb{H}_0$. Then

$$(a_1 + \mathbf{h}_1)(a_2 + \mathbf{h}_2) = (a_1a_2 - \mathbf{h}_1 \cdot \mathbf{h}_2) + (a_1\mathbf{h}_2 + a_2\mathbf{h}_1 + \mathbf{h}_1 \times_c \mathbf{h}_2)$$

Definition 1.1.6: Conjugate and Norm

Let $x = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \in \mathbb{H}$ be a quaternion. Define the conjugate of x to be

$$x^* = a - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}$$

Also define the norm of x to be

$$\|x\| = \sqrt{a^2 + b^2 + c^2 + d^2}$$

Proposition 1.1.7

Let $x, y \in \mathbb{H}$ be quaternions. The following are true regarding the conjugate and norm of the quaternions:

- $xx^* = \|x\|$
- $(xy)^* = y^*x^*$
- $\|xy\| = \|x\|\|y\|$

Proof. □

Proposition 1.1.8

$\mathbb{H}$ is a division ring.

Proof. Let $x \in \mathbb{H}$. By the above proposition, we have that $x\frac{x^*}{\|x\|} = 1$ which means we have found an inverse $\frac{x^*}{\|x\|}$ of x. □

1.2 The Multiplicative Group of Quaternions

Definition 1.2.1: The Quaternionic Unitary Group

Define the quaternionic unitary group to be the subgroup

$$U(\mathbb{H}) = \{x \in \mathbb{H} \mid \|x\| = 1\}$$

of $\mathbb{H}^\times$.

Proposition 1.2.2

The multiplicative group $\mathbb{H}^\times$ is isomorphic to $\mathbb{R}_+^\times \times U(\mathbb{H})$, where $\mathbb{R}_+^\times$ is the multiplicative group of non-zero real numbers.

Proof. □

Proposition 1.2.3: Quaternionic Euler's Formula

Write a quaternion into the form $q = a + b\mathbf{x} \in \mathbb{H}$ where $a, b \in \mathbb{R}$ and $\mathbf{x} \in \mathbb{H}_0$ is purely imaginary such that $\|\mathbf{x}\| = 1$. Then

$$e^q = e^a(\cos(b) + \mathbf{x}\sin(b))$$

Proposition 1.2.4: Quaternionic De Moivre's Formula

Let $\mathbf{x} \in H_0$ be purely imaginary such that $\|\mathbf{x}\| = 1$. Let $n \in \mathbb{Z}$. Then

$$(\cos(b) + \mathbf{x}\sin(b))^n = \cos(nb) + \mathbf{x}\sin(nb)$$

1.3 3D Rotations using Quaternions

Recall the special orthogonal group in 3-dimensions is the group

$$\mathrm{SO}_3(\mathbb{R}) = \{M \in \mathrm{GL}_3(\mathbb{R}) | \det(M) = 1\}$$

Proposition 1.3.1

Let $M \in \mathrm{SO}_3(\mathbb{R})$ be a special orthogonal transformation. Then there exists an orthonormal basis of $\mathbb{R}^3$ such that the matrix decomposes into the direct sum $(1) \oplus R_\alpha$, where $R_\alpha = \begin{pmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{pmatrix}$ is a rotation in $\mathbb{R}^2$.

Now we know that every special orthogonal transformation is just a rotation in the plane orthogonal to e_1. In generality, we write $R_{\mathbf{x}}^\alpha$ for the anti-clockwise rotation in angle α in the plane orthogonal to $\mathbf{x} \in \mathbb{R}^3$. We can use the quaternions to write out a formula for applying the special orthogonal transformation to a vector.

Lemma 1.3.2

Let $\mathbf{x} \in \mathbb{H}_0 \cap U(\mathbb{H})$ be an imaginary unit. Let $\theta \in \mathbb{R}$. Then

$$R_{\mathbf{x}}^{2\theta}(\mathbf{w}) = e^{\theta\mathbf{x}}\mathbf{w}e^{-\theta\mathbf{x}}$$

for all $\mathbf{w} \in \mathbb{H}_0$.

This leads tot he fundamental fact behind the theory of spinors in Geometry and Physics.

Theorem 1.3.3

The conjugation action map

$$\phi : U(\mathbb{H}) \to \mathrm{SO}(\mathbb{H}_0) \cong \mathrm{SO}_3(\mathbb{R})$$

defined by $\phi(x)(\mathbf{z}) = x\mathbf{z}x^{-1}$ for $\mathbf{z} \in \mathbb{H}_0$ and $x \in U(\mathbb{H})$ is a surjective two to one group homomorphism.

1.4 Division Rings over Real and Complex Numbers

Proposition 1.4.1

The only finite dimensional $\mathbb{C}$-division algebra is $\mathbb{C}$.

Proof. Let D be a finite dimensional $\mathbb{C}$-division algebra. Then in particular, $\mathbb{C} \subseteq D$. Suppose that $a \in D$. Then the minimal polynomial $\mu_a(x)$ is an irreducible element of $\mathbb{C}[x]$. By the fundamental theorem of algebra, $\mu_a(x) = x - \alpha$ with $\alpha \in \mathbb{C}$. This means that $a = \alpha \in \mathbb{C}$ and thus $D = \mathbb{C}$. □

Proposition 1.4.2

The only odd dimensional $\mathbb{R}$-division algebra is $\mathbb{R}$.

Proof. Let D be an $\mathbb{R}$-division algebra of odd dimension n. Then in particular, $\mathbb{R} \subseteq D$. Let $a \in D$. In linear algebra we know that the $\mathbb{R}$-linear map $L : D \to D$ defined by $L(d) = ad$ admits a real eigenvalue $\alpha \in D$ and eigenvector v. Then $av = \alpha v$ implies that $(a - \alpha)v = 0$. Since D is a division algebra, we have that $a = \alpha \in \mathbb{R}$. Thus $\mathbb{R} = D$. □

Theorem 1.4.3: Frobenius Theorem

A finite dimensional division algebra over $\mathbb{R}$ is isomorphic to $\mathbb{R}$, $\mathbb{C}$ or $\mathbb{H}$.

Theorem 1.4.4

The only countably generated division algebra over $\mathbb{R}$ up to isomorphism is either $\mathbb{R}$, $\mathbb{C}$ or $\mathbb{H}$.

1.5 Finite Division Rings

Lemma 1.5.1

Let R be a division ring. Then $Z(R)$ is a field. Moreover, R is a $Z(R)$-algebra.

Corollary 1.5.2

Let D be a finite division ring. Then the following statements are true regrading D.

- $Z(D)$ is a finite field $\mathbb{F}_{p^n}$ for some $n \in \mathbb{N} \setminus \{0\}$
- The dimension of D, $m = \dim_{Z(D)} D$ over $Z(D)$ is finite
- $|D| = p^{nm}$

Lemma 1.5.3

Let R be a division ring and $x \in R$. Then $C_R(x)$ is a division ring and a $Z(R)$-subalgebra.

Proposition 1.5.4

Let D be a finite division ring of dimension m over its center $Z(D) = \mathbb{F}_q$, where $q = p^n$ for some prime p and $n \in \mathbb{N} \setminus \{0\}$. Then there exists positive integers $d_1, \ldots, d_k$ such that $d_i | m$, $d_i < m$ and

$$q^m = q + \sum_{i=1}^{k} \frac{q^m - 1}{q^{d_i} - 1}$$

Theorem 1.5.5: Little Wedderburn's Theorem

A finite division ring is a field.

1.6 Laurent Series

Definition 1.6.1: Laurent Series

Let R be a ring. A Laurent series in variable x with coefficients in a ring R is an expression of the form

$$\sum_{n=m}^{\infty} a_n x^n$$

for $m \in \mathbb{Z}$ and $a_n \in R$. Denote the set of Laurent series in x by

$$R((x))$$

Lemma 1.6.2

Let R be a ring. Then $R((x))$ is also a ring. If R is a field, then $R((x))$ is also a field.

Lemma 1.6.3

The center of $\mathbb{H}((x))$ is precisely $\mathbb{R}((x))$.

2 Semisimplicity

2.1 Semisimple Modules

Definition 2.1.1: Semisimple Modules

A left R-module M is semisimple if M is a direct sum of simple modules.

Definition 2.1.2: Socle of a Module

Denote $\mathcal{SM}(M) = \{S \leq M | S \text{ is simple}\}$. A socle of a left R-module M is a submodule

$$\text{soc}(M) = \sum_{S \in \mathcal{SM}(M)} S$$

Lemma 2.1.3

A module M is semisimple if and only if $\text{soc}(M) = M$.

Corollary 2.1.4

A quotient module of a semisimple module is semisimple.

Definition 2.1.5: Completely Reducible Modules

Let M be an R-module. M is said to be completely reducible if for every submodule N of M, there exists a submodule L of M such that $M = N \oplus L$.

Proposition 2.1.6

Let M be an R-module such that $M = N \oplus L$. Then there is an isomorphism

$$L \cong \frac{M}{N}$$

of R-modules.

Lemma 2.1.7

A submodule of a completely reducible module is reducible.

Lemma 2.1.8

A non-zero completely reducible module contains a simple submodule.

Theorem 2.1.9

Let M be an R-module. Then M is semisimple if and only if M is completely reducible.

Corollary 2.1.10

A submodule of a semisimple module is semisimple.

2.2 Peirce Decomposition for Modules

Definition 2.2.1: Idempotents

Let M be a module. We say that $e \in M$ is an idempotent if $e^2 = e$.

Proposition 2.2.2

Let M be an R-module. Then there is a bijection between the set of all finite direct sum decompositions $M = \bigoplus_{i=1}^{n} M_i$ with all $M_i \neq 0$ and the set of all full orthogonal system of idempotents in $S = \mathrm{End}_R(M)$.

Note that in particular, we can also take M to just be R to get a decomposition on idempotents by ideals of R. This means that for $\{e_1, \ldots, e_n\}$ a full orthogonal system of idempotents, we have a decomposition

$$R = Re_1 \oplus \cdots \oplus Re_n$$

Theorem 2.2.3: Peirce Decompositions

A full system of orthogonal idempotents in R gives a direct sum decomposition of R and M into $\mathbb{Z}$-modules that can be written in matrix forms

$$R = \bigoplus_{i,j=1}^{n} e_i R e_j = \begin{pmatrix} e_1Re_1 & \cdots & e_1Re_n \\ \vdots & \ddots & \vdots \\ e_nRe_1 & \cdots & e_nRe_n \end{pmatrix}$$

and

$$M = \bigoplus_{i=1}^{n} e_i M = \begin{pmatrix} e_1M \\ \vdots \\ e_nM \end{pmatrix}$$

2.3 Radical

Definition 2.3.1: Cosimple

Let M be an R-module. We say that a submodule N of M is cosimple if $\frac{M}{N}$ is simple.

Lemma 2.3.2

Let M be an R-module and N a submodule of M. Then N is cosimple if and only if N is a maximal proper submodule of M.

Definition 2.3.3: Radical

Let M be an R-module. Define the radical of M to be the intersection

$$\mathrm{rad}(M) = \bigcap_{\substack{S \leq M \\ S \text{ is cosimple}}} S$$

of all cosimple submodules of M.

Lemma 2.3.4

Let M be an R-module. If M is semisimple, then $\mathrm{rad}(M) = 0$.

2.4 Artin-Wedderburn Theorem

Definition 2.4.1

A left R-module M is said to be Artinian if for every descending chain of submodules

$$N_1 \supseteq N_2 \supseteq \cdots \supseteq N_n \supseteq \cdots$$

there exists $m \in \mathbb{N}$ such that $N_n = N_m$ for all $n > m$.

Theorem 2.4.2

Let M be an Artinian left R-module. Then M is semisimple if and only if $\text{rad}(M) = 0$.

Theorem 2.4.3: Artin-Wedderburn Theorem

Let R be a ring. Then the following are equivalent characterizations of semisimplicity.

- Every left R-module is semisimple
- The regular left R-module is semisimple
- There exists $n_1, \ldots, n_k \in \mathbb{N}$ and division rings $D_1, \ldots, D_k$ such that R is isomorphic to the direct product $\prod_{i=1}^{k} M_{n_i}(D_i)$

Proof. □

Corollary 2.4.4

A ring is left semisimple if and only if it is right semisimple.

Proposition 2.4.5

The following are true regarding semisimple algebras over fields.

- A semisimple $\mathbb{C}$-algebra of at most countable dimension is isomorphic to

$$\prod_{i=1}^{k} M_{k_i}(\mathbb{C})$$

- A semisimple $\mathbb{R}$-algebra of at most countable dimension is isomorphic to

$$\prod_{i=1}^{k} M_{k_i}(\mathbb{R}) \times \prod_{i=1}^{n} M_{n_i}(\mathbb{C}) \times \prod_{i=1}^{t} M_{t_i}(\mathbb{H})$$

- A finite dimensional semisimple $\mathbb{F}_q$ algebra is isomorphic to

$$\prod_{i=1}^{k} M_{k_i}(\mathbb{F}_q^{t(i)})$$