Advanced Ring Theory

Labix

May 12, 2024

Abstract

- Abstract Alebra by Thomas W. Judson

Contents

1 Division Rings

Division rings are very closed to being a field. They are just missing commutativity. As one can seen in Field and Galois theory, fields and field homomorphisms are rather rigid objects, so one can expect division rings to be restrictive. Indeed, in this section we will show that any finite division ring must be a field. Moreover, the only finite dimensional division algebra over $\mathbb{R}$ can only take 3 forms, namely $\mathbb{R}$, $\mathbb{C}$ or $\mathbb{H}$. In particular, they have dimension 1, 2 and 4 respectively.

1.1 Properties of Division Rings

Proposition 1.1.1

Let D be a division ring. The following are true regarding the properties of a division ring.

- The only ideals of D are (0) and D.
- If D is an division algebra, then D is a simple D-module.

Proof. Let I be a non-trivial ideal of D. Then by property of an ideal, for $x \in I \setminus \{0\}$, $x^{-1}x \in I$ so that $1 \in I$. Then for any $d \in D$, $d \cdot 1 \in I$ thus $D = I$.

Since the submodules of D are precisely the ideals of D, we conclude that D is a simple D-module. □

Lemma 1.1.2

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

- $Z(D)$ is a field and D is a $Z(D)$-algebra
- $C_D(x)$ is a division ring and a $Z(D)$-subalgebra

Proof. $Z(D)$ as a subdivision ring is also a division ring in its own right. Since $Z(D)$ consists of all commuting elements, $Z(D)$ is commutative and so is a field. Thus D is a $Z(D)$-algebra by multiplication.

It is clear that $0, 1 \in C_D(x)$. Let $a, b \in C_D(x)$. Then

$$(a-b)x = ax - bx = xa - xb = x(a-b)$$

so that $a - b \in C_D(x)$. Also $abx = axb = xab$ implies that $ab \in C_D(x)$. Finally, $ax = xa$ implies that $x = a^{-1}xa$ so that $xa^{-1} = a^{-1}x$ and that $a^{-1} \in D$. Thus $C_D(x)$ is a sub division ring. Since $C_R(x)$ contains $Z(R)$, $C_R(x)$ is thus a $Z(D)$-algebra. □

1.2 The Structure of Quaternions

Recall in Group theory that we have encountered the quaternion group. We can turn it into a vector space over $\mathbb{R}$ by allowing coefficients on the quaternion group.

Definition 1.2.1: 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 1.2.2

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 1.2.3

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

Proof. It is clear that $1, x_1, x_2, x_3, x_1x_2, x_1x_3, x_2, x_3, \dots$ 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

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

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

Proposition 1.2.4

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 1.2.5

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

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

Proof. By $\mathbb{R}$-bilinearity, we have that we have that

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

A simple calculation yields $\mathbf{h}_1\mathbf{h}_2 = -\mathbf{h}_1\cdot\mathbf{h}_2+\mathbf{h}_1\times\mathbf{h}_2$ using multiplication rules of quaternions. Thus we are done. □

Definition 1.2.6: 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 1.2.7

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

- $xx^* = \|x\|^2$
- $(xy)^* = y^*x^*$
- $\|xy\| = \|x\|\|y\|$

Proof.

- Write $x = a+b\mathbf{i}+c\mathbf{j}+d\mathbf{k}$. Then by considering the purely imaginary quaternions as a 3 dimensional vector space, we have that

$$\begin{aligned}xx^* &= \left(a^2-\begin{pmatrix}b\\c\\d\end{pmatrix}\cdot\begin{pmatrix}-b\\-c\\-d\end{pmatrix}\right)+\left(a\begin{pmatrix}b\\c\\d\end{pmatrix}-a\begin{pmatrix}b\\c\\d\end{pmatrix}-\begin{pmatrix}b\\c\\d\end{pmatrix}\times\begin{pmatrix}b\\c\\d\end{pmatrix}\right)\\ &= a^2+b^2+c^2+d^2\\ &= \|x\|^2\end{aligned}$$

- Again write $x = a_1+\mathbf{h}_1$ and $y = a_2+\mathbf{h}_2$, then by a similar method, we have that

$$\begin{aligned}y^*x^* &= (a_2a_1+\mathbf{h}_2\cdot\mathbf{h}_1)+(-a_1\mathbf{h}_2-a_2\mathbf{h}_1+\mathbf{h}_2\times\mathbf{h}_1)\\ &= (a_2a_1+\mathbf{h}_2\cdot\mathbf{h}_1)-(a_1\mathbf{h}_2+a_2\mathbf{h}_1+\mathbf{h}_1\times\mathbf{h}_2)\\ &= (xy)^*\end{aligned}$$

by using the fact that $-\mathbf{x} \times \mathbf{y} = \mathbf{y} \times \mathbf{x}$.

- Using the above two identity, we have that

$$\begin{aligned} \|xy\|^2 &= (xy)(xy)^* \\ &= xyy^*x^* \\ &= x\|y\|^2x^* \\ &= xx^*\|y\|^2 \\ &= \|x\|^2\|y\|^2 \end{aligned}$$

And so we are done. □

Proposition 1.2.8

$\mathbb{H}$ 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 $\frac{x^*}{\|x\|}$ for x. □

Similar to the real and complex counter part, we can form all kinds of special groups for quaternions, beginning with the unitary group.

Definition 1.2.9: The Quaternionic Unitary Group

Define the quaternionic unitary group to be the subgroup

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

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

Note that this is different from the quaternion group since the quaternion group only consists of the basis vectors and their inverses.

Proposition 1.2.10

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. Define $\phi : \mathbb{R}_+^\times \times U(\mathbb{H}) \to \mathbb{H}$ by $\phi(r, x) = rx$. It is clear that this is a group homomorphism. Moreover, its kernel is trivial since scalar multiplication is equal to 0 if and only if $x = 0$. Also it is surjective. Indeed any vector x can be written as $\|x\|\frac{x}{\|x\|}$ where $\frac{x}{\|x\|}$ now lies in the unitary group. Thus ϕ is a bijective homomorphism. □

By writing every quaternion group as a scalar multiplied by an element of the unitary group, we obtain a polar coordinate representation similar to that of the complex numbers in terms of the argument and magnitude.

Proposition 1.2.11: 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

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

Proof. If $q = a + b\mathbf{x}$ then notice that q lies in the two dimensional $\mathbb{R}$-subalgebra $\mathbb{R}(x) = \mathbb{R} + \mathbb{R}\mathbf{x}$. This is isomorphic to $\mathbb{C}$ so in particular, all partial sums

$$\sum_{k=0}^{n} \frac{\mathbf{x}^n}{n!}$$

also lie in $\mathbb{R}(x) \cong \mathbb{C}$ and quaternionic Euler's formula follows from the usual Euler's formula. □

However, note that in general since quaternions do not commute, $e^{X+Y} \neq e^X e^Y$. This is true only if $X, Y \in \mathbb{R}(x)$. This is because then $XY = YX$ so that $e^{X+Y} = e^X e^Y$.

Proposition 1.2.12: 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

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

Proof. We have that

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

and so we are done. □

1.3 3D Rotations using Quaternions

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

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

Proposition 1.3.1

Let $M \in \text{SO}_3(\mathbb{R})$ 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 $\mathbb{R}^2$.

Proof. Since M is a bijective linear transformation, M has at least 1 real eigenvector $\mathbf{v}$ with eigenvalue $\alpha \in \mathbb{R}$. Note that since M is also in the special orthogonal group, $a = \pm 1$. Let W be the plane orthogonal to $\mathbf{v}$. Note that $M\mathbf{w} \in W$ for any $\mathbf{w} \in W$ because M is bijective and that

$$\mathbf{v} \cdot M\mathbf{w} = M(\alpha^{-1}\mathbf{v}) \cdot (M\mathbf{w}) = \alpha^{-1}\mathbf{v} \cdot \mathbf{w} = 0$$

so that $M\mathbf{w} \in W$. Thus the linear transformation of M restricted to W is an orthogonal transformation. But orthogonal transformations in $\mathbb{R}^2$ is exactly given by R_α for some angle α, or a reflection S_α along an angle.

If $\alpha = 1$, we must have that M restricted to the orthogonal plane is a rotation R_α. Then we are done by choosing the ordered basis $\mathbf{v}$ and any orthonormal basis e_2 and e_3 of W. If $\alpha = -1$, then M restricted to the orthogonal plane is a reflection S_α. But S_α then has eigenvalues 1 and -1. We can then return to the start of the proof and choose the eigenvector corresponding to the eigenvalue 1. Thus then we will arrive at the case of $\alpha = 1$. □

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. This is more compact than the usual notations.

Lemma 1.3.2

Let $\mathbf{x} \in \mathbb{H}_0$ 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 $\mathbf{w} \in \mathbb{H}_0$.

Proof. Choose $\mathbf{y} \in \mathbb{H}_0$ an orthogonal vector to $\mathbf{x}$ that is a unit vector. Let $\mathbf{z} = \mathbf{x} \times \mathbf{y}$. By proposition 5.1.5, we have that $\mathbf{x}^2 + \mathbf{y}^2 + \mathbf{z}^2 = -1$ and

$$\begin{aligned} \mathbf{xy} &= -\mathbf{yx} = \mathbf{z} \\ \mathbf{yz} &= -\mathbf{zy} = \mathbf{x} \\ \mathbf{zx} &= -\mathbf{xz} = \mathbf{y} \end{aligned}$$

so that $\mathbf{x}$, $\mathbf{y}$, $\mathbf{z}$ forms a basis for $\mathbb{H}_0$. It suffices to check the equation on basis vectors since the rotation is a linear map. Notice that $e^{-\theta\mathbf{x}} = \cos(\theta) - \mathbf{x}\sin(\theta)$. Now we have that

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

Now also,

$$\begin{aligned} e^{\theta\mathbf{x}}\mathbf{y}e^{-\theta\mathbf{x}} &= (\cos(\theta) + \mathbf{x}\sin(\theta))\mathbf{y}(\cos(\theta) - \mathbf{x}\sin(\theta)) \\ &= (\mathbf{y}\cos(\theta) + \mathbf{z}\sin(\theta))(\cos(\theta) - \mathbf{x}\sin(\theta)) \\ &= ((\cos(\theta))^2 - (\sin(\theta))^2)\mathbf{y} + (2\cos(\theta)\sin(\theta))\mathbf{z} \\ &= \mathbf{y}\cos(2\theta) + \mathbf{z}\sin(2\theta) \\ &= R_{\mathbf{x}}^{2\theta}(\mathbf{y}) \end{aligned}$$

Finally we have that

$$\begin{aligned} e^{\theta\mathbf{x}}\mathbf{z}e^{-\theta\mathbf{x}} &= (\cos(\theta) + \mathbf{x}\sin(\theta))\mathbf{z}(\cos(\theta) - \mathbf{x}\sin(\theta)) \\ &= (\mathbf{z}\cos(\theta) - \mathbf{y}\sin(\theta))(\cos(\theta) - \mathbf{x}\sin(\theta)) \\ &= ((\cos(\theta))^2 - (\sin(\theta))^2)\mathbf{z} - (2\cos(\theta)\sin(\theta))\mathbf{y} \\ &= \mathbf{z}\cos(2\theta) - \mathbf{y}\sin(2\theta) \\ &= R_{\mathbf{x}}^{2\theta}(\mathbf{z}) \end{aligned}$$

and so we conclude. □

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

Theorem 1.3.3

The conjugation action map

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

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.

2 Division Algebras

A division algebra is an algebra such that the underlying ring is a division ring. When it is also a field, we have seen in Field and Galois theory that they are well understood. We now study division algebras over $\mathbb{R}$ and $\mathbb{C}$.

2.1 Amitsur-Schur Lemma

Recall that we say $a \in \mathbb{F}$ a field is an algebraic element over $\mathbb{F}$ if there exists some polynomial in $f \in \mathbb{F}[x]$ for which $f(a) = 0$. Moreover, the minimal polynomial μ_a is monic and of smallest degree amongst all f for which $f(a) = 0$.

Theorem 2.1.1: Amitsur-Schur Lemma

Let A be an $\mathbb{F}$-algebra for $\mathbb{F}$ a field, such that A has vector space dimension less than $|\mathbb{F}|$. If M is a simple left A-module, then every element of the division $\mathbb{F}$-algebra $\text{End}_A(M)$ is algebraic.

Proof. By Schur's Lemma II, $D = \text{End}_A(M)$ is a division ring. Clearly, D is an $\mathbb{F}$-algebra by defining the ring homomorphism $\phi : \mathbb{F} \to D$ by $\phi(\alpha)(m) = \alpha m$. Then the dimensions of the three vector spaces satisfy

$$\dim_{\mathbb{F}}(D) \leq \dim_{\mathbb{F}}(M) \leq \dim_{\mathbb{F}}(A) < |\mathbb{F}|$$

Indeed, suppose that $x \in M$ is non-zero. Consider the map $\pi : A \to M$ defined by $\pi(a) = ax$. Since π is not the zero map and M is simple, by Shur's lemma I we know that $\text{im}(\pi) = M$. By the firs isomorphism theorem, we have that $M \cong \frac{A}{\ker(\pi)}$ and thus the second inequality in dimensions hold. For the first inequality, the linear map $\omega_x : D \to M$ defined by $\omega_x(d) = xd$ is injective because M is simple.

Any element $\alpha \in \mathbb{F} \subseteq D$ is clearly algebraic: Just choose $\mu_\alpha(x) = x - \alpha$. Now consider $d \in D \setminus \mathbb{F}$. Then for each $\alpha \in \mathbb{F}$, the element $d - \alpha$ is non-zero. Since D is a division ring, we get $|\mathbb{F}|$ number of non-zero elements $(d - \alpha)^{-1}$. Their number exceeds the dimension of D. Hence we have a non-trivial linear dependence

$$\sum_{i=1}^{k} \beta_i (d - \alpha_i)^{-1} = 0$$

for any $k \geq 1$. All elements $d - \alpha_i$ commutes because $\alpha_i \in \mathbb{F} \subseteq Z(D)$. Furthermore, $d - \alpha_i$ commutes with $(d - \alpha_j)^{-1}$ because

$$\begin{aligned} ab = ba &\implies ab^{-1} = b^{-1}bab^{-1} = b^{-1}abb^{-1} = b^{-1}a \\ &\implies a^{-1}b^{-1} = b^{-1}a^{-1} \end{aligned}$$

Thus we can apply the usual calculations with fractions:

$$0 = \sum_{i=1}^{k} \beta_i \frac{1}{d - \alpha_i} = \frac{f(d)}{(d - \alpha_1) \cdots (d - \alpha_k)}$$

where $f(d) = \sum_{j=1}^{k} \prod_{i=1}^{k} \frac{\beta_j}{x - \alpha_j}(x - \alpha_i)$. Multiplying by the denominator, we get $f(d) = 0$. Notice that

$$f(\alpha_1) = \beta_1(\alpha_1 - \alpha_2) \cdots (\alpha_1 - \alpha_k) \neq 0$$

so that $f(x) \neq 0$ and thus d is algebraic. □

The following statement is core to the entire theory of Groups and Representations.

Corollary 2.1.2

Let A be a countable generated $\mathbb{C}$-algebra. Let M is a simple left A-module. Then $\text{End}_A(M) = \mathbb{C}$.

Proof. The dimension of A is countable since A is a quotient of $\mathbb{C}\langle X \rangle$ by proposition 3.3.3. Since M is simple, it is isomorphic to A/L for some left ideal L. Hence the dimension of M over $\mathbb{C}$ is also countable. This implies that $\dim_{\mathbb{C}}(\text{End}_{\mathbb{C}}(M))$ is countable, and so is the dimension of its subalgebra $\text{End}_A(M)$. But $\mathbb{C}$ is uncountable. Thus every $f \in \text{End}_A(M)$ is algebraic by the Amitsur-Schur lemma. By the fundamental theorem of algebra, the $\mathbb{C}$ is algebraically closed so that the minimal polynomial of f, which is irreducible, has degree 1. Thus the minimal polynomial has root $f \in \mathbb{C}$. □

2.2 Division Rings over Real and Complex Numbers

Proposition 2.2.1

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 2.2.2

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 $\mathbb{R} = D$. □

In order to proof the grand result, we need the notion of the trace map from Linear Algebra.

Definition 2.2.3: Trace Map

Let D be a real division algebra of finite dimension over $\mathbb{R}$. Define the trace map $\text{Tr}_D : D \to \mathbb{R}$ by

$$\text{Tr}_D(a) = \text{Tr}(L_a)$$

where $L_a : D \to D$ is the left multiplication map $L_a(d) = ad$.

Lemma 2.2.4

Let A be a finite dimensional algebra over a field $\mathbb{F}$. If $a \in A$ then the minimal polynomial of L_a is equal to μ_a.

Proof. Notice that we have $L_a^n(b) = a^n b = L_{a^n}(b)$ so that

$$f(L_a)(b) = f(a)b = L_{f(a)}(b)$$

for each polynomial $f(x)$ and $b \in A$. If $f(a) = 0$, then $f(L_a) = 0$. If $f(L_a) = 0$, then $f(a) = f(a) \cdot 1 = f(L_a)(1) = 0$. Thus the minimal polynomial of L_a and a are the same. □

Theorem 2.2.5: Frobenius Theorem

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

Proof. Let D be a finite dimensional division algebra over $\mathbb{R}$.

Step 1: $D = \mathbb{R} \oplus \ker(\text{Tr}_D)$.
The trace map is defined to be linear over the components of the matrix. Moreover, the second one follows from the fact that $L_a : D \to D$ is given by the matrix aI_n. Finally, it is clear that the kernel of the trace map is $n-1$ dimensional. Moreover it is surjective and that $\mathbb{R} \cap \ker(\text{Tr}_D) = 0$.

Step 2: If $a \in \ker(\text{Tr}_D)$ then $a^2 \in \mathbb{R}$ and $a^2 \leq 0$.
Now let $a \in D$ lie in the kernel. If $a \in \mathbb{R}$ then since D is the direct sum of $\mathbb{R}$ and the kernel, we must have that $a = 0$. So suppose that $a \notin \mathbb{R}$. Then since any irreducible polynomial in $\mathbb{R}[x]$ must either be linear or quadratic with discriminant less than 0. Since $a \notin \mathbb{R}$, the minimal polynomial μ_a of a must be quadratic:

$$\mu_a(x) = x^2 + \alpha x + \beta$$

where $\alpha^2 - 4\beta < 0$. By the above corollary, L_a also has μ_a as the minimal polynomial. The characteristic polynomial $c_{L_a}(x)$ of L_a has the same roots as μ_a. Since μ_a is irreducible, c_{L_a} must be a power of μ_a. It follows that

$$c_{L_a}(x) = \mu_a(x)^{n/2} = (x^2 + \alpha x + \beta)^{n/2} = x^n + \frac{n\alpha}{2}x^{n-1} + \cdots + \beta^{n/2}$$

From Linear Algebra, we know that the trace appears as the first coefficient of the characteristic polynomial. By definition of $\ker(\text{Tr}_D)$, we have that $\text{Tr}_D(a) = 0$. It follows that $\alpha = 0$, $\beta > 0$ and $\alpha^2 + \beta = 0$. Thus $\alpha^2 = -\beta < 0$. We then conclude that $a^2 \leq 0$.

Write $D_0 = \ker(\text{Tr}_D)$. We now have a function $q : D_0 \to \mathbb{R}$ defined by

$$q(a) = -a^2$$

This is a positive definite quadratic form. We can polarize it to obtain $\tau : D_0 \times D_0 \to \mathbb{R}$ defined by

$$\tau(a, b) = -\frac{1}{2}(ab + ba)$$

Step 3: (D_0, τ) is a finite dimensional Euclidean space.
It is clear that τ is symmetric since $\tau(a, b) = \tau(b, a)$. τ is bilinear since

$$\begin{aligned} \tau(a + b, c) &= -\frac{1}{2}((a + b)c + c(a + b)) \\ &= -\frac{1}{2}(ac + ca) - \frac{1}{2}(bc + cb) \\ &= \tau(a, c) + \tau(b, c) \end{aligned}$$

and the property that $\tau(\lambda a, b) = \lambda\tau(a, b)$ for $\lambda \in \mathbb{R}$ is clear. Thus τ is a bilinear form. It is positive definite by step 2 since $\tau(a, a) = -a^2 > 0$.

By Gram-schimdt, we obtain an orthonormal basis for D_0, namely $e_1, \dots, e_{n-1}$.

Step 4: $e_i^2 = -1$ and $e_i \cdot e_j = -e_j \cdot e_i$ for all $1 \leq i \neq j \leq n-1$. Also, $e_k = \pm(e_i \cdot e_j)^{-1}$ for $1 \leq i < j < k \leq n-1$.

As the basis is orthonormal, we have that $\tau(e_i, e_i) = 1$ and $\tau(e_i, e_j) = 0$ for all $i \neq j$. The results then follow from the definition of τ. Also, let $u = e_ie_je_k$. We have that

$$\begin{aligned} u^2 &= (e_ie_j)e_ke_ie_je_k \\ &= -e_j(e_ie_k)e_ie_je_k \\ &= e_je_k(e_ie_i)e_je_k \\ &= -(e_je_k)e_je_k \\ &= e_je_je_ke_k \\ &= 1 \end{aligned}$$

Thus $u^2 = 1$ implies $(u-1)(u+1) = 0$. Since D is a division algebra, $e_ie_je_k = u = \pm 1$. Hence we conclude.
Step 5: Conclusion.
By analzing the dimension n, we have the following:

- If $n = 1$, then we must have $D = \mathbb{R}$.
- If $n = 2$, then $e_1^2 = 1$ so that $D \cong \mathbb{C}$.
- If $n = 3$, then it is impossible by proposition 5.4.2.
- If $n = 4$, then $D = \mathbb{R} \oplus \mathbb{R}e_1 \oplus \mathbb{R}e_2 \oplus \mathbb{R}e_3$. Let $i = e_1$, $j = e_2$ and $k = e_1e_2$. Then by step 4, we have that $i^2 = j^2 = k^2 = -1$ and $ijk = kk = -1$. Thus $D \cong \mathbb{H}$.
- If $n = 5$, then it is impossible by step 4. Indeed we have that $e_3 \pm (e_1e_2)^{-1}$ and $e_4 = \pm(e_1e_2)^{-1}$ so that $e_4 = \pm e_3$. This contradicts the fact that $e_1, \dots, e_{n-1}$ is a basis.

□

Together with Amitsur-Schur lemma, we can prove a stronger statement.

Theorem 2.2.6

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

Proof. Let D be a countable generated $\mathbb{R}$-division algebra. Then D is a simple module and $\text{End}_D(D) \cong D$ by lemma 2.4.3. Moreover, by Amitsur-Schur lemma, every element $d \in D$ is algebraic. The algebra $\mathbb{R}(d)$ generated by d is a finite dimensional field. If $d \notin \mathbb{R}$, then by Frobenius theorem, $\mathbb{R}(d) \cong \mathbb{C}$ and the minimal polynomial is quadratic. Write it as $\mu_d = x^2 + \alpha_d x + \beta_d$. If $\mathbb{R}(d) = D$, then we are done.

If $\mathbb{R}\langle d\rangle \neq D$, pick $c \in D \setminus \mathbb{R}\langle d\rangle$. Then subalgebra $A = \mathbb{R}(c, d)$ generated by d and c is a division algebra because each element $r \notin R$ can be inverted from $r^2 + \alpha_r + \beta_r = 0$. Indeed we have that $(r + \alpha_r)r = -\beta_r$ so that $r^{-1} = -\beta_r^{-1}(r + \alpha_r)$. Note that $\beta_r \neq 0$ since $\mu_r(x)$ is irreducible.

Now we have that

$$(c+d)^2 + \alpha_{c+d}(c+d) + \beta_{c+d} = c^2 + cd + dc + d^2 + \alpha_{c+d}(c+d) + \beta_{c+d}$$

This is the minimal polynomial of $c + d$, and so it is 0. It follows that

$$\begin{aligned} dc &= -c^2 - cd - d^2 - \alpha_{c+d}(c+d) - \beta_{c+d} \\ &= \alpha_c c + \beta_c - cd + \alpha_d d + \beta_d - \alpha_{c+d}(c+d) - \beta_{c+d} \end{aligned}$$

Thus every element of $\mathbb{R}\langle c, d\rangle$ is an $\mathbb{R}$-linear combination of $1, c, d, cd$. By Frobenius theorem, we have that $\mathbb{R}\langle c, d\rangle \cong \mathbb{H}$. If $\mathbb{R}\langle c, d\rangle = D$ then we are done.

Suppose that $\mathbb{R}\langle c, d\rangle \neq D$. Pick $b \in D \setminus \mathbb{R}\langle c, d\rangle$. Consider the subalgebra $\mathbb{R}\langle b, c, d\rangle$ generated by b, c, d. By the same argument as above, $\mathbb{R}\langle b, c, d\rangle$ is a division algebra. By the argument with the minimal polynomials of b, r and $b + r$ for some $r \in \mathbb{R}\langle c, d\rangle$, we can write every element as an $\mathbb{R}$-linear combination of $1, c, d, cd, b, cb, db$ and cdb. Thus $\mathbb{R}\langle b, c, d\rangle$ is a finite dimensional division algebra over $\mathbb{R}$ of dimension at least 5. This contradicts Frobenius theorem. □

However this is no longer true for division algebras over $\mathbb{R}$ of uncountable dimension. For example, the ring of Laurent series $\mathbb{R}((x))$, $\mathbb{C}((x))$ and $\mathbb{H}((x))$ are all examples of such.

2.3 Finite Division Rings

Corollary 2.3.1

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
- $|D| = p^{nm}$

Proof. We know that $Z(D)$ is a field. Since D is finite, $Z(D)$ is finite. Every finite field is of the form $\mathbb{F}_{p^n}$ from Field and Galois theory. Since D is a $Z(D)$-algebra and D is finite, we must have $\dim_{Z(D)} D$ is finite. The final point also follows. □

Proposition 2.3.2

Let D be a finite division ring and $\dim_{Z(D)}(D) = m$ for $Z(D) \cong \mathbb{F}_{p^n}$ for some prime p and $n \in \mathbb{N} \setminus \{0\}$. Then there exists positive integers $d_1, \dots, d_k$ such that $d_i | m$, $d_i < m$ and

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

Proof. The group $D^\times$ acts on D by conjugation. By the class equation, we have that

$$q^m = |D| = |Z(R)| + \sum_{i=1}^{k} |\text{Orb}_{D^\times}(x_i)|$$

for $Z(R), \text{Orb}_{D^\times}(x_1), \dots, \text{Orb}_{D^\times}(x_k)$ the distinct orbits of the action.

If D is a field, then $Z(D) = D$ and $m = 1$. All orbits moreover have size 1 since D is commutative. Thus we have that $q = q$ for the identity.

Now suppose that D is not a field. There exists orbits of size greater than 1 since in general. $xyx^{-1} \neq y$. Thus $k \geq 1$. Let $\text{Orb}_{D^\times}(y_1), \dots, \text{Orb}_{D^\times}(y_k)$ be the distinct orbits of size at least 2. Notice that

$$\begin{aligned} \text{Stab}_{D^\times}(y_i) &= \{g \in D^\times \mid g y_i g^{-1} = y_i\} \\ &= \{g \in D^\times \mid g y_i = y_i g\} \\ &= C_D(y_i) \setminus \{0\} \end{aligned}$$

Since $C_D(y_i)$ is a division algebra, its dimension d_i must be finite since D is finite. It is also strictly less than m since $C_D(y_i)$ is a $Z(R)$-subalgebra of D. The orbit stabilizer theorem together with the class equation gives

$$\begin{aligned} q^m &= |D| \\ &= |Z(R)| + \sum_{i=1}^{k} |\text{Orb}_{D^\times}(x_i)| \\ &= q + \sum_{i=1}^{k} \frac{|D^\times|}{|C_D(y_i) \setminus \{0\}|} \\ &= q + \sum_{i=1}^{k} \frac{q^m - 1}{q^{d_i} - 1} \end{aligned}$$

and so we conclude. □

Theorem 2.3.3: Little Wedderburn's Theorem

A finite division ring is a field.

Proof. Firstly, the function $h(x) = \frac{x^m - 1}{x^{d_i} - 1}$ is a polynomial since d_i divides m. Any factor $x - \zeta^k$ where $\zeta = e^{2\pi i/m}$ of the cyclotomic polynomial $\Psi_m(x)$ divides $x^m - 1$ but not $x^{d_i} - 1$ and hence it divides $h(x)$. Thus $\Psi_m(x)$ divides $h(x)$ and $\Psi_m(q)$ divides the right hand side of

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

Hence $\Psi_m(q)$ divides $q - 1$. But this is a contradiction since $|\Psi_m(q)| > q - 1$. Indeed, we have that

$$\begin{aligned} |\Psi_m(q)| &= \prod_{t=1, \gcd(t,m)=1}^{m-1} |q - \zeta^t| \\ &> (q-1)^{\deg(\Psi_m(x))} \\ &\geq q - 1 \end{aligned}$$

where the first inequality $|q - \zeta^t| > q - 1$ is clear since $\zeta^t \neq 1$ and on the complex plane, $q - 1$ is the distinct from the real point q to 1 and $|q - \zeta^t|$ is the distance from q to ζ^t which is on the unit circle and thus is further away from q than 1. □

3 Semisimplicity

Simple modules are easy to understand since they have minimal internal structure. Semisimple modules are the next best modules one can consider. Artin-Wedderburn theorem at the very end not only gives a decomposition of semisimple rings using matrix rings over division rings, it also shows that semisimplicity does not depend on the left / right module structure.

3.1 Semisimple Modules

Definition 3.1.1: Semisimple Modules

Let R be a ring. A left R-module M is semisimple if

$$M = \bigoplus_{i\in I} S_i$$

is a direct sum of simple modules S_i.

Definition 3.1.2: Socle of a Module

Let M be a left R-module. The socle of M is defined by

$$\text{soc}(M) = \sum_{\substack{S \text{ is a simple} \\ \text{submodule}}} S$$

Lemma 3.1.3

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

Proof. Suppose that M is semisimple. Then M is a direct sum of simple submodules so that $M = \text{soc}(M)$. Now suppose that $\text{soc}(M) = M$. Suppose that $M = \sum_{i\in I} S_i$ is the internal direct product of some submodules of M. Consider the poset

$$\mathcal{P} = \left\{ X \subseteq I \;\middle|\; \sum_{i\in X} S_i \text{ is a direct sum} \right\}$$

ordered by inclusion. In particular, recall from Rings and Modules that $X \in \mathcal{P}$ if and only if $\phi : \bigoplus_{i\in X} S_i \to M$ defined by $\phi\left((m_i)_{i\in X}\right) = \sum_{i\in X} m_i$ is injective. The kernel of ϕ is given by

$$\begin{aligned} \ker(\phi) &= \left\{ (m_i)_{i\in X} \mid \sum_{i\in X} m_i = 0 \right\} \\ &= \left\{ (m_i)_{i\in X} \;\middle|\; \text{for all } i_1, \dots i_k \in X \text{ we have } m_{i_1} + \dots + m_{i_k} = 0 \right\} \end{aligned}$$

The kernel being trivial is equivalent to the condition that for all $i_1, \dots, i_k \in X$ and all $m_{i_t} \in S_{i_t}$, we have $m_{i_1} + \dots + m_{i_k} = 0$ implies $m_{i_1} = \dots = m_{i_k} = 0$. Let $\mathcal{C}$ be a chain in $\mathcal{P}$. It is clear that $T = \bigcup_{Z\in\mathcal{C}} Z$ is an upper bound of $\mathcal{C}$. Indeed if the above condition fails, then it fails on some finitely many elements x_i which are contained in $X \subseteq Z \subseteq T$. By Zorn's lemma, $\mathcal{P}$ has a maximal element J. We know that $N = \sum_{i\in J} S_i$ is a direct sum. It remains to show that $N = M$. If this is false, then there exists S_k not a subset of N. In particular, $k \neq J$. Consider the set $J \cup \{k\}$. In particular the above condition fails and such a failure must contain a non-zero element $x_k \in S_k$ since the condition holds before k was introduced to J. Then $x_k = -\sum_{j\neq k} x_j \in N$ and $N \cap S_k$ is non-zero. Since S_k is simple, $N \cap S_k = S_k$ and thus $N \supseteq S_k$, which is a contradiction. □

Corollary 3.1.4

A quotient module of a semisimple module is semisimple.

Proof. Suppose that M is semisimple. Then $M = \bigoplus_{i\in I} S_i$ where S_i are simple modules. Consider a quotient M/N and the quotient homomorphism $\psi : M \to M/N$. Clearly, $M/N = \psi(M) = \sum_{i\in I} \psi(S_i)$ and each $\psi(S_i)$ is either 0 or simple. Then $\text{soc}(M/N) = M/N$ and M/N is semisimple. □

Lemma 3.1.5

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

Proof. Suppose that M is semisimple. Then $M = \bigoplus_{i\in I} S_i$ for S_i simple submodules of M. Define

$$M_i = \bigoplus_{j\in I\setminus\{i\}} S_j$$

for each $i \in I$. Since $M/M_i \cong S_i$, we have that M_i is cosimple. Then

$$\text{rad}(M) = \bigcap_{\substack{N\leq M\\ N \text{ is cosimple}}} N \subseteq \cap_{i\in I} M_i = 0$$

Thus $\text{rad}(M) = 0$. □

Theorem 3.1.6

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

Proof. Lemma 2.5.4 proves one direction. So suppose that $\text{rad}(M) = 0$. Then we obtain a descending chain using intersections of cosimple submodules

$$N_1 \supseteq N_1 \cap N_2 \supseteq \cdots \text{rad}(M) = 0$$

Since M is Artinian, the chain stops after finitely many steps. Then this gives us finitely many cosimple modules N_i such that

$$N_1 \cap \cdots \cap N_k = 0$$

Consider the following homomorphism of R-modules $\psi : M \to \prod_{i=1}^k \frac{M}{N_i}$ defined by the individual projection homomorphism. It is injective since its kernel if $N_1 \cap \cdots \cap N_k = 0$. Since there are only finitely many submodules, together with surjectivity we have that

$$M \cong \psi(M) \cong \bigoplus_{i=1}^k \frac{M}{N_i}$$

Thus M is semisimple. □

Corollary 3.1.7

Let R be a ring. Then R is semisimple if and only if R is left artinian and $J(R) = 0$.

Proof. Direct from the above theorem. □

3.2 Maschke's Theorem

For Maschke's theorem, we would need an equivalent definition of semisimplicity of modules.

Definition 3.2.1: 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 3.2.2

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.

Proof. Consider the quotient map $\psi : M \to M/N$. This restricts to a homomorphism $\overline{\psi} : L \to M/N$. This map is injective since

$$\ker(\overline{\psi}) = L \cap \ker(\psi) = L \cap N = 0$$

The map is surjective since every $m \in M$ can be written as $m = l + n$ for $l \in L$ and $n \in N$. Then

$$\psi(l) = \psi(l + n) = \psi(m) = m + N$$

so that ψ is surjective and so is $\overline{\psi}$. □

Lemma 3.2.3

A submodule of a completely reducible module is reducible.

Proof. Let N be a submodule of a completely reducible module M. Let P be a submodule of P. Then it has a direct complement

$$M = P \oplus K$$

together with the corresponding idempotents π of $\text{End}_R(M)$ and p of P for which $\pi(p + k) = p$. The image of π is equal to P, which is a subset of N. This allows us to restrict the idempotent and use proposition 6.2.4 to obtain $\phi = \pi|_N \in \text{End}_R(M)$ and

$$N = \text{im}(\phi) \oplus \ker(\phi) = P \oplus K'$$

so that we conclude. □

Lemma 3.2.4

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

Proof. Let M be a completely reducible R-module. Pick a non-zero element $x \in M$. Then left R-module homomorphism $\pi_x : R \to M$ defined by $\pi_x(r) = r \cdot x$ is non-zero because $\pi_x(1) = x \neq 0$. Since every ring has a maximal left ideal, $\ker(\pi_x)$ as an ideal also lies in some maximal ideal L. Notice that $Rx \cong \frac{R}{\ker(\pi_x)}$. This gives a surjective R-module homomorphism

$$\psi : \frac{R}{\ker(\pi_x)} \to \frac{R}{L}$$

defined by $\psi(r + \ker(\pi_x)) = r + L$. The module Rx is a submodule of M, and hence completely reducible by the above lemma. This means that there exists a submodule N of Rx such that $Rx = N \oplus \ker(\psi)$. The homomorphism $\psi|_N : N \to R/L$ is an isomorphism by proposition 6.4.2. Since R/L is simple, N is a simple submodule of M and so we conclude. □

Theorem 3.2.5

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

Proof. Suppose that M is completely reducible. By the above lemma, it is clear that $\text{soc}(M)$ is non-empty. If $M = \text{soc}(M)$ we are done. So suppose not. By complete reducibility, there exists a submodule K such that $M = \text{soc}(M) \oplus K$. Since K is a submodule of M, K is completely reducible. By the above lemma, K contains a simple submodule S. Then $S \subseteq \text{soc}(M)$, which is a contradiction.

Now assume that M is semisimple. Let $M = \bigoplus_{i \in I} S_i$ for simple modules S_i. Let N be a submodule of M. If $\psi : M \to M/N$ is the quotient homomorphism, then

$$M/N = \psi(M) = \sum_{\in I} \psi(M)$$

with each $\psi(S_i) = \frac{S_i}{S_i \cap N}$. In particular, each $\psi(S_i)$ is either zero or simple and isomorphic to S_i. Since quotient of semisimple modules are semisimple, we have that M/N is semisimple and one can choose a subset J of I indices such that

$$M/N = \bigoplus_{i \in J} S_i$$

with $\psi(S_i) \cong S_i$ for all i.

We claim that $M = N \oplus \left(\bigoplus_{i \in J} S_i\right)$. To prove it, consider the natural R-module homomorphism

$$\varphi : N \oplus \left(\bigoplus_{i \in J} S_i\right) \to M$$

defined by $\varphi(n, (s_i)_{i \in J}) = n + \sum_{i \in J} s_i$. It is injective since for $(n, (s_i)_{i \in J}) \in \ker(\varphi)$, we have $\psi(n) + \sum_{i \in J} \psi(s_i) = 0$ together with $n \in \ker(\psi)$ to imply that

$$\sum_{i \in J} \psi(s_i) = 0$$

Using the direct sum $M/N = \bigoplus_{i \in J} S_i$, we have that each $\psi(s_i) = 0$. Since $\psi : S_i \to \psi(S_i)$ is an isomorphism, we have that $s_i = 0$. This means that we have $n + \sum_{i \in J} s_i = 0$ together with $s_i = 0$ to imply that $n = 0$. So we are done with injectivity. For surjectivity, we have for each $m \in M$, we can write a finite sum $\psi(m) = \sum_{i \in J} \psi(s_i)$ for some $s_i \in S_i$ all but finitely many non-zero. Then $m - \sum_{i \in J} s_i \in \ker(\psi) = N$ and we have that

$$\varphi\left(m - \sum_{i \in J} s_i, (s_i)_{i \in J}\right) = m$$

This show that we have an isomorphism so that M is now completely reducible. □

Corollary 3.2.6

A submodule of a semisimple module is semisimple.

Proof. If M is semisimple, then M is completely reducible. Submodule of completely reducible modules are completely reducible. Then by the above theorem, the submodule is semisimple. □

Using the notion of completely reducible, we can prove that the decomposition of a semisimple module into simple modules is essentially unique.

Proposition 3.2.7

Let M be a semisimple left R-module with two decompositions

$$M = \bigoplus_{i=1}^{n} S_i \quad \text{and} \quad M = \bigoplus_{j=1}^{m} T_j$$

into simple modules. Then $n = m$ and the simple modules S_i and T_j are isomorphic up to reordering.

Proof. We proceed by induction on n. If $n = 1$, then, M is simple and we are done.

Suppose that it is true for $n - 1$. Let $K = \bigoplus_{i=1}^{n-1} S_i$. Consider the quotient homomorphism $\psi : M \to M/K$. Clearly we have that

$$\frac{M}{K} = \psi(M) = \psi\left(\sum_{j=1}^{m} T_j\right) = \sum_{j=1}^{m} \psi(T_j)$$

Then each $\psi(T_j)$ is either 0 or simple and isomorphic to T_j so that we can reduce the indexing set so that we exclude the $j \in J$ for which $\psi(T_j) = 0$. Now we have that $M = K \oplus \left(\bigoplus_{j\in J} T_j\right)$. By proposition 2.2.2, we have that S_n and $\left(\bigoplus_{j\in J} T_j\right)$ are isomorphic. Thus $\bigoplus_{j\in J} T_j$ is actually just a single element. Without loss of generality, take $J = \{m\}$. Both $\bigoplus_{i=1}^{n-1} S_i$ and $\bigoplus_{j=1}^{m-1} T_j$ are direct complements of T_m. They are isomorphic by proposition 2.2.2. By the induction hypothesis, we conclude. □

Theorem 3.2.8: Maschke's Theorem

Let G be a group, $\mathbb{F}$ a field of characteristic p. Then the group algebra $\mathbb{F}G$ is semisimple if and only if G is of finite order n with p not dividing n.

Proof. Suppose that $\mathbb{F}G$ is semisimple. Consider $\mathbb{F}$ as the trivial $\mathbb{F}G$-module defined by $g \cdot x = x$ for all $x \in \mathbb{F}$ and $g \in G$ and extend it by linearity. Then there is a homomorphism of $\mathbb{F}G$-modules $\psi : \mathbb{F}G \to \mathbb{F}$ defined by

$$\psi\left(\sum_{g\in G} \lambda_g g\right) = \sum_{g\in G} \lambda_g$$

Since $\mathbb{F}G$ is semisimple, $\ker(\psi)$ has a direct complement L. By proposition 2.2.2, and the first isomorphism theorem for modules, we have that $L \cong \mathbb{F}$. Since $L \cong \mathbb{F}$, $hx = x$ for all $h \in G$. Thus

$$\sum_{g\in G} \lambda_g (hg) = \sum_{g\in G} \lambda_g g$$

for all $h \in G$. Thus all λ_g are equal. Hence $L =\cong \mathbb{F}z$ where $z = \sum_{g\in G} g$. If G is infinite then z is not well defined. Finally, if $n = |G|$ is finite and $p \mid n$, then $\psi(z) = n = 0_{\mathbb{F}}$ and $\psi : L \to \mathbb{F}$ is not surjective, contradicting proposition 2.2.2. Thus p does not divide n.

Now suppose the contrary. Since p does not divide n, we can choose $\lambda \in \mathbb{F}$ such that $n\lambda = 1_{\mathbb{F}}$. Let N be an $\mathbb{F}G$-submodule of an $\mathbb{F}G$-module M. Then N is a vector subspace of M and so we can choose a vector space complement L such that $M = N \oplus L$ in the sense of Linear Algebra. This gives a projection map $p : M \to M$ such that $\ker(p) = L$, $\operatorname{im}(p) = N$ and $p^2 = p$ and is linear. Define $q : M \to M$ a linear map by

$$q(x) = \lambda \sum_{g\in G} g \cdot p(g^{-1}(x))$$

By definition, $N \supseteq \operatorname{im}(q)$. Moreover, for each $x \in N$, we have that $g^{-1}x \in N$ so that

$$q(x) = \lambda_{g\in G} g \cdot (g^{-1}x) = \lambda \sum_{g\in G} x = \lambda n x = x$$

Thus q is another idempotent $N = \operatorname{im}(q)$. Moreover, $q \in \text{End}_{\mathbb{F}G}(M)$ since for $x \in M$ and $h \in G$, we have that

$$\begin{aligned} q(hx) &= \lambda \sum_{g\in G} g \cdot (g^{-1}hx) \\ &= \lambda \sum_{g,k\in G, gk=h} g \cdot (kx) \\ &= \lambda \sum_{g\in G} hg \cdot (g^{-1}kx) \\ &= hq(x) \end{aligned}$$

so that $\ker(q)$ is a direct complement and so we conclude. □

3.3 Peirce Decomposition for Modules

Definition 3.3.1: Idempotents

Let R be a ring. We say that $e \in R$ is idempotent if $e^2 = e$.

Definition 3.3.2: Full System of Orthogonal Idempotents

Let R be a ring. Two idempotents e, f are orthogonal if $ef = fe = 0$. A full system of orthogonal idempotents is a finite collection of non-zero pairwise orthogonal idempotent elements $e_1, \dots, e_n \in R$ such that $e_1 + \cdots + e_n = 1$.

Such a system always exists and may not be unique up even just up to the size $n \in \mathbb{N}$. Indeed one such trivial system is to take the identity 1.

Proposition 3.3.3

Let M be an R-module. Then there is a bijection

$$\left\{ \substack{\text{Finite direct sum} \\ \text{decompositions } M=\bigoplus_{i=1}^n M_i} \right\} \overset{1:1}{\longleftrightarrow} \left\{ \substack{\text{Full orthogonal system} \\ \text{of idempotentes in } \text{End}_R(M)} \right\}$$

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 $\text{End}_R(M)$.

Proof. A decomposition $M = \bigoplus_{i=1}^n M_i$ gives a system of idempotents through its component maps $e_k : M \to M$ defined by $(x_1, \dots, x_n) \mapsto (0, \dots, 0, x_i, 0, \dots, 0)$. This map is an endomorphism since it is the composition of the projection with to M_k with the inclusion to M. It is clear that they form a full system of orthogonal idempotents for $\text{End}_R(M)$.

Now suppose that we have a full orthogonal system of idempotents $e_1, \dots, e_n$ in $\text{End}_R(M)$. Define $M_k = Me_k = \text{im}(e_k)$ for $1 \leq k \leq n$. $\phi : \bigoplus_{i=1}^n M_i \to M$ defined by $(m_1, \dots, m_n) \mapsto \sum_{i=1}^n m_i$ is surjective because each $m \in M$ can be written as

$$\begin{aligned} \text{id}_{\text{End}_R(M)}(m) &= (e_1 + \cdots + e_n)(m) \\ &= e_1(m) + \cdots + e_n(m) \\ &= \phi(e_1(m), \dots, e_n(m)) \end{aligned}$$

It is injective because if $\phi(x) = 0$ for $x = (e_1(m_1), \dots, e_n(m_n))$ implies that

$$\begin{aligned} 0 &= e_k(\phi(x)) \\ &= e_k(e_1(m_1) + \cdots + e_n(m_n)) \\ &= \sum_{i=1}^n e_k(e_i(m_i)) \\ &= e_k(m_k) \end{aligned}$$

This implies that $m_k = 0$ for $1 \leq k \leq n$ and so $x = 0$.

It is clear that these constructions are inverse functions between the stated sets. □

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 $\{e_1, \dots, e_n\}$ a full orthogonal system of idempotents, we have a decomposition

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

Definition 3.3.4: Peirce Decompositions

Let M be an R-module. A finite direct sum decomposition

$$M = \bigoplus_{i=1}^n M_i$$

arising from a full orthogonal system of idempotents are called Peirce decompositions.

For two idempotents e and f, eRf loses the structure of a ring and is just an abelian group. We give a useful interpretation of eRf as follows.

Proposition 3.3.5

Let $e, f, g \in R$ be idempotents of a ring. Then the map $\psi : eRf \to \text{Hom}_R(Re, Rf)$ defined by

$$\psi(erf) : Re \to Rf$$

to be the map $se \mapsto serf$ is an isomorphism of abelian groups such that $\psi(erf)\psi(fsg) = \psi(erfsg)$. In particular, if $e = f$, then ψ is a ring isomorphism.

By collecting all the abelian groups eRf in a matrix, we can recover the ring R itself.

Theorem 3.3.6: Two-Sided Peirce Decompositions

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

$$R = \bigoplus_{i,j=1}^{n} e_iRe_j = \begin{pmatrix} e_1Re_1 & \cdots & e_1Re_n \\ \vdots & \ddots & \vdots \\ e_nRe_1 & \cdots & e_nRe_n \end{pmatrix} \quad \text{and} \quad M = \bigoplus_{i=1}^{n} e_iM = \begin{pmatrix} e_1M \\ \vdots \\ e_nM \end{pmatrix}$$

that satisfies the following:

- If R is an $\mathbb{F}$-algebra for $\mathbb{F}$ a field, then all e_iRe_j and e_iM are $\mathbb{F}$-vector subspaces
- The multiplication in R defines the structure of a ring on each e_iRe_j. This ring is non-zero.
- The R-module action on M defines a structure of e_iRe_i-module on e_iM
- In the matrix interpretation, the multiplication in R and the R action on M satisfies the standard matrix rules

Proof. Let $e_1, \dots, e_n$ be the given full orthogonal system of idempotents of the ring R. Then by proposition 2.2.4 we obtain a finite direct sum decomposition

$$R = \bigoplus_{i=1}^{n} e_iR \quad \text{and} \quad M = \bigoplus_{i=1}^{n} e_iM$$

Each e_iR is an R-module since they are left ideals. Thus we can apply proposition 2.2.4 to obtain $e_iR = \bigoplus_{i=1}^{n} e_iRe_j$ so that we obtain the required decompositions for R and M.

Let $\lambda \in \mathbb{F}$ and $x \in e_iRe_j$. Then $x = e_iye_j$ for some $y \in R$. Then

$$\lambda x = \lambda e_iye_j = e_i(y\lambda)e_j \in e_iRe_j$$

since R is an $\mathbb{F}$-algebra. Since e_iRe_j is an abelian subgroup, it follows that e_iRe_j is an $\mathbb{F}$-vector subspace. The proof for e_iM is similar.

Multiplication in R is given by $(e_ixe_i) \cdot (e_iye_i) = e_ixye_i$ so that multiplication is closed. Moreover, $1_{e_iRe_i} = e_i$ is not equal to 0 so that the ring is non-zero.

Similarly, $(e_ixe_i) \cdot (e_im) = e_ixm \in e_iM$ so that e_iM is closed under the ring action. Thus e_iM becomes an e_iRe_i-module.

It is easy to check that multiplication defined in the matrix way makes sense. □

Note component wise multiplication only defines a group isomorphism between $R = \bigoplus_{i,j=1}^{n} e_iRe_j$ To obtain a ring isomorphism, one needs to consider multiplication as matrices.

3.4 The Matrix Rings

Recall that for a ring R, we can define the matrix ring over R by

$$M_n(R) = \left\{ \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \right\}$$

The latter section will focus on matrix rings over division rings.

Proposition 3.4.1

Let R be a ring. Then the ideals in R are in one to one correspondence with the ideals in $M_n(R)$

$$\left\{I \subseteq R \;\middle|\; I \text{ is an ideal of} R\right\} \quad \overset{1:1}{\longleftrightarrow} \quad \left\{\overline{I} \subseteq M_n(R) \;\middle|\; \overline{I} \text{ is an ideal}\right\}$$

via the following. For each I an ideal of R, $M_n(I)$ is an ideal of $M_n(R)$. For each ideal $\overline{I}$ of $M_n(R)$, the set

$$I = \{a_{11} \in R \mid (a_{ij})_{n\times n} \in \overline{I}\}$$

is an ideal in R.

Proposition 3.4.2

Let D be a division ring. Then $M_n(D)$ is both a left and right semisimple ring via the decompositions

$$M_n(D) = \bigoplus_{i=1}^{n} c_i(D) = \bigoplus_{i=1}^{n} r_i(D)$$

where

$$c_i(D) = \{M \in M_n(D) \mid M \text{ is non zero only in the } i\text{th column}\}$$

and

$$r_i(D) = \{M \in M_n(D) \mid M \text{ is non zero only in the } i\text{th row}\}$$

3.5 Artin-Wedderburn Theorem

Theorem 3.5.1: Artin-Wedderburn Theorem

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

- Every left R-module is semisimple
- The ring R as a left R-module is semisimple
- There exists $n_1, \dots, n_k \in \mathbb{N}$ and division rings $D_1, \dots, D_k$ such that R is isomorphic to the direct product $\prod_{i=1}^k M_{n_i}(D_i)$ Moreover, the decomposition in to matrix rings are unique up to reordering.

Proof.

- (1) $\implies$ (2) is obvious because R is also a left R-module.
- (2) $\implies$ (1): Let M be an R-module. Choose a generating set B of M. Then M is a quotient of the free module $\bigoplus_{b\in B} Rb$. Since R is semisimple, RB is also semisimple. By corollary 6.1.4, M is also a semisimple module.
- (2) $\implies$ (3): Write the R-module R as a direct sum of simple modules $R = \bigoplus_{i\in I} S_i$. Note that the set I is finite because $1 = \sum_{i\in I} s_i$ for $s_i \in S_i$ and so we can remove the 0 in the sum to get $1 = s_1, \dots, s_m$. Then each element $r \in R$ can be written as $r = rs_1 + \dots + rs_m$. Hence $R = \bigoplus_{i=1}^m S_i$.

  Let $L_1, \dots, L_k$ be distinct simple modules among the S_i. By Schur's lemma, $D_i = \text{End}_R L_i$ is a division ring. Reorder the summands so that we can group them as following:

$$R = \underbrace{S_1 \oplus \dots \oplus S_{n_1}}_{\text{each } S_i \cong L_1} \oplus \dots \oplus \underbrace{S_{n_1+\dots+n_{k-1}+1} \oplus \dots \oplus S_m}_{\text{each } S_i \cong L_k}$$

Replace each S_i with the corresponding L_j together with lemma 2.4.3 to get

$$R \cong \text{End}_R \cong \text{End}_R \left(\underbrace{L_1 \oplus \cdots \oplus L_1}_{n_1} \oplus \cdots \oplus \underbrace{L_{i_k} \oplus \cdots \oplus L_k}_{n_k} \right) = \text{End}_R \left(\bigoplus_{j=1}^{k} L_j^{n_j} \right)$$

Now let $e_1, \dots, e_m$ be the full system of orthogonal idempotents corresponding to the above decomposition by proposition 6.2.4. Consider e_j in the jth group and e_s in the tth group. By proposition 6.2.5, we have

$$e_j R e_s \cong \text{Hom}_R(L_j, L_t) = \begin{cases} 0 & \text{if } j \neq t \\ D_j & \text{if } j = t \end{cases}$$

Then by the Peirce decomposition,

$$R = \begin{pmatrix} D_1 & \cdots & D_1 & 0 & \cdots & 0 & \cdots \\ \vdots & & \vdots & \vdots & & \vdots & \\ D_1 & \cdots & D_1 & 0 & \cdots & 0 & \cdots \\ 0 & \cdots & 0 & D_2 & \cdots & D_2 & \cdots \\ \vdots & & \vdots & \vdots & & \vdots & \\ 0 & \cdots & 0 & D_2 & \cdots & D_2 & \cdots \\ \vdots & & \vdots & \vdots & & \vdots & \end{pmatrix} = M_{n_1}(D_1) \times M_{n_2}(D_2) \times \cdots \times M_{n_k}(D_k)$$

- (3) $\implies$ (2): Let $R = \prod_{i=1}^k M_{n_i}(D_i)$. Since D_i is a division ring, we have seen that $M_{n_i}(D_i)$ is left semisimple thus their product is also left semisimple.

□

Using the matrix ring over division rings, Artin-Wedderburn theorem implies that every semisimple module is built out of these matrix rings. Moreover, semisimplicity no longer distinguishes between left and right.

Corollary 3.5.2

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

Proof. R is a right R-module if and only if it is a left R^{op}-module. Moreover $M_n(D)^{\text{op}} \cong M_n(D^{\text{op}})$. Explicitly, we have seen that each $M_n(D)$ for D a division ring is both left and right semisimple. □

It thus makes sense to just say that a ring is semisimple instead of distinguishing left and right.

Proposition 3.5.3

The following are true regarding semisimple algebras over fields.

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

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

- A semisimple $\mathbb{R}$-algebra of 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

$$\prod_{i=1}^{k} M_{k_i}(\mathbb{F}_{q^{t_i}})$$

Proof. If R is an $\mathbb{F}$-algebra that is semisimple, we have that

$$R = \prod_{i=1}^{k} M_{n_i}(D_i)$$

by Artin-Wedderburn theorem. In particular, each $M_{n_i}(D_i)$ is also an $\mathbb{F}$-algebra. Moreover, by identifying D in any one component of M_{n_i}, we can see that D is also an $\mathbb{F}$-algebra. Each D_i is a finite dimensional $\mathbb{F}$-vector space if and only if R is finite dimensional. Then we have the following.

- If $\mathbb{F} = \mathbb{C}$ then D_i can only possibly be $D_i = \mathbb{C}$
- If $\mathbb{F} = \mathbb{R}$ then D_i is either $\mathbb{R}$ or $\mathbb{C}$ or $\mathbb{H}$ by Frobenius theorem and theorem 1.4.6.
- If $\mathbb{F} = \mathbb{F}_q$ then $D_i = \mathbb{F}_{q^{t_i}}$ for some $t_i \in \mathbb{N}$ by Little Wedderburn's theorem.

Thus we conclude. □

4 Exercises

4.1 Problem Set 1

Exercise 4.1.1: Problem 1.3

Let I be an an ideal of the non-zero ring R (left, right or 2-sided), R^* its set of units. Show that I is proper if and only if $1 \notin I$. More generally, show that I is proper if and only if $I \cap R^* = \emptyset$.

Proof. Let $1 \in I$. Then for any $r \in R$, $r \cdot 1 \in I$. Thus $R = I$ and I is not proper. If I is not proper then $I = R$ and $1 \in I$.

Suppose that $I \cap R^* \neq \emptyset$. Then there exists an invertible $r \in R$ such that $r \in I$. Then $r^{-1} \cdot r \in I$ which means that $1 \in I$. Thus $I = R$. Suppose that $I = R$ is not proper. Then clearly $I \cap R^* = \emptyset$. □

Exercise 4.1.2: Problem 1.4

Let R be an integral domain. Show that $R[x]^* = R^*$.

Proof. Suppose that $f(x) = \sum_{k=0}^n a_k x^k$ is invertible. Then there exists $g(x) = \sum_{j=0}^m b_j x^j$ such that $fg = 1$ without loss of generality $b_m \neq 0$. Then we have that $a_n b_m = 0$ which implies $a_n = 0$. Inductively, for $0 \leq k \leq n-1$, if $a_n = \cdots = a_{n-k+1} = 0$, then we have

$$a_{n-k}b_m + a_{n-k+1}b_{m-1} + \cdots + a_n b_{m-k} = 0$$

which implies that $a_{n-k}b_m = 0$ so that $a_{n-k} = 0$. Now what remains is that f is a constant polynomial. Thus $f \in R^*$. Also it is clear that if $r \in R^*$ is invertible, then $r \in R[x]^*$ is also invertible since $R \subseteq R[x]$. □

Exercise 4.1.3: Problem 1.5

Let R be a ring. Prove that the rings $M_n(R[x])$ and $M_n(R)[x]$ are isomorphic.

Proof. Notice that $M_n(R[x])$ has an $R[x]$-module basis $\{E_{i,j} \mid 1 \leq i, j \leq n\}$ and hence an R-module basis $\{x^k E_{i,j} \mid 1 \leq i, j \leq n \text{ and } k \in \mathbb{N}\}$ where $E_{i,j}$ are the matrices with 1 at the (i,j)th position and 0 everywhere else. Similarly, $M_n(R)$ has R-module basis $\{E_{i,j} \mid 1 \leq i, j \leq n\}$ and hence $M_n(R)[x]$ has an R-module basis $\{x^k E_{i,j} \mid 1 \leq i, j \leq n \text{ and } k \in \mathbb{N}\}$. One can define an isomorphism by sending basis elements to basis elements from $M_n(R[x])$ to $M_n(R)[x]$. It is clearly surjectivity and injectivity. □

Exercise 4.1.4: Problem 1.8

Find the smallest positive integer x such that $x \equiv 1 \pmod 7$, $x \equiv 1 \pmod{11}$ and $x \equiv 4 \pmod{13}$.

Proof. The goal is to decompose $\mathbb{Z}$ into $\mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/13\mathbb{Z}$ via a map with kenrnel $1001\mathbb{Z}$. Since $7\mathbb{Z} + 11\mathbb{Z} = \mathbb{Z}$, using Bezout's lemma we find that $-21 + 22 = 1$. Under $7\mathbb{Z} + 13\mathbb{Z} = \mathbb{Z}$, we have that $14 - 13 = 1$. Finally under $11\mathbb{Z} + 13\mathbb{Z} = \mathbb{Z}$, we have that

$66 - 65 = 1$. Then we have that

$$
\begin{aligned}
x_1 &= (22)(-13) = -286 \\
x_2 &= (-21)(-65) = 1365 \equiv 364 \pmod{1001} \\
x_3 &= (14)(66) = 924 \equiv -77 \pmod{1001}
\end{aligned}
$$

Then $(1)x_1 + (1)x_2 + (4)x_3 = -230$ is a solution to the congruence equations. Moreover, the smallest solution in $\mathbb{N}$ is $1001 - 230 = 771$. □

Exercise 4.1.5: Problem 1.12

Let $R = M_n(\mathbb{F})$ where $\mathbb{F}$ is a field. It acts on the left on the vector space $\mathbb{F}^n$. Let $V \subseteq \mathbb{F}^n$ be a subspace.

1. Prove that $l(V) = \{X \in R \mid \ker(X) \supseteq V\}$ is a left ideal of R.
2. Pick $a \in R$. Prove that $Ra = l(\ker(a))$. (Hint: writing a in Smith Normal Form may help.)
3. Pick $a, b \in R$. Prove that $Ra + Rb = l(\ker(a) \cap \ker(b))$. (Hint: you have enough elements in Ra and Rb from the previous part, now try to find an element in $Ra + Rb$ whose kernel is $\ker(a) \cap \ker(b)$.)
4. Prove that any left ideal of R has the form $l(V)$.

Proof.

1. Let $X, Y \in l(V)$ and $v \in V$. Then $(X + Y)(v) = Xv + Yv = 0$. For any $M \in M_n(\mathbb{F})$, $(RX)(v) = R(Xv) = 0$. Thus $l(V)$ is a left ideal of R.
2. Suppose that Ca is the Smith Normal form of a, where C is an invertible matrix. Let $X \in l(\ker(a))$ and suppose that EX is the Smith Normal form of X where E is an invertible matrix. Notice that column operations are not needed since a and X are square matrices. By assumption, $\ker(X) \supseteq \ker(a)$ means that $\ker(EX) \supseteq \ker(Ca)$ and $\dim(\ker(X)) - \dim(\ker(a)) \geq 0$ Multiply a diagonal matrix D with non-zero entries on the diagonal to convert EX to have the same diagonal entries with Ca. Now apply a linear transformation T on Ca to convert the last $\dim(\ker(X)) - \dim(\ker(a))$ non-zero rows of EX to 0. Thus now we have that $DEX = TCa$. Since D and E are invertible, we have that $X = E^{-1}D^{-1}TCa$ which shows that $X \in Ra$.

   Now suppose that $Ma \in Ra$ for $M \in M_n(\mathbb{F})$. Then for any $v \in \ker(a)$, $(Ma)(v) = M(av) = 0$ shows that $\ker(Ma) \supseteq \ker(a)$ so that $\ker(Ma) \in l(\ker(a))$.
3. Suppose that $Ma + Nb \in Ra + Rb$. For $v \in \ker(a) \cap \ker(b)$, we have that $(Ma + Nb)(v) = M(av) + N(bv) = 0$ so that $Ma + Nb \in l(\ker(a) \cap \ker(b))$. Let $X \in l(\ker(a) \cap \ker(b))$. Notice that $\ker(a + b) \supseteq \ker(a) \cap \ker(b)$.

□

Exercise 4.1.6: Problem 1.14

Compute $\text{End}_{\mathbb{Z}}\mathbb{Q}$.

Proof. Let $x = \frac{a}{b} \in \mathbb{Q}$. Then $a = bx$. Suppose that $\phi \in \text{End}_{\mathbb{Z}}\mathbb{Q}$. Then $\phi(a) = \phi(bx)$. Since

$a, b \in \mathbb{Z}$ and ϕ respects the $\mathbb{Z}$-module structure, we have that

$$\begin{aligned}\phi(a) &= \phi(bx)\\ a\phi(1) &= b\phi(x)\\ \phi(x) &= \frac{a}{b}\phi(1)\\ \phi\left(\frac{a}{b}\right) &= \frac{a}{b}\phi(1)\end{aligned}$$

This means that any $\phi \in \mathrm{End}_{\mathbb{Z}}\mathbb{Q}$ is determined by where $1 \in \mathbb{Q}$ is sent to in $\mathbb{Q}$. Define $\Phi : \mathbb{Q} \to \mathrm{End}_{\mathbb{Z}}\mathbb{Q}$ by $\Phi(a) : \mathbb{Q} \to \mathbb{Q}$ defined by $x \mapsto ax$. It is clear that this is a ring homomorphism since multiplication in $\mathbb{Q}$ respects addition and multiplication is commutative. This map is surjective by the fact that any $\phi \in \mathrm{End}_{\mathbb{Z}}\mathbb{Q}$ is determined by where $1 \in \mathbb{Q}$ is sent to. It is injective since $\mathbb{Q}$ is a domain. Thus $\mathrm{End}_Z\mathbb{Q} \cong \mathbb{Q}$. □

Exercise 4.1.7: Problem 1.18

Let R be a ring. Compute the center of $M_n(R)$.

Proof. Suppose that $A \in Z(M_n(R))$. Notice that for any $E_{i,j}$ the standard basis for $M_n(R)$ over R, $AE_{i,j} = E_{i,j}A$. If $i = j$, then $AE_{i,i}$ only has a non-zero ith column. Similarly, $E_{i,i}A$ only has a non-zero ith row. In particular, this implies that for $i \neq j$, $a_{i,j} = 0$ since $AEi,i = Ei,iA$. If $i \neq j$, then $AE_{i,j}$ only has a non-zero jth column given by $\begin{pmatrix} a_{1,i} \\ \vdots \\ a_{n,i}\end{pmatrix}$ and Ei,jA only has a non-zero ith row given by $\begin{pmatrix} a_{j,1} & \cdots & a_{j,n}\end{pmatrix}$. Since $AE_{i,j} = E_{i,j}A$, we must have that $a_{i,i} = a_{j,j}$ which show that A is of the form $A = \mathrm{diag}(a, \dots, a)$. Thus

$$Z(M_n(R)) = \{A = \mathrm{diag}(a, \dots, a) \mid a \in R\}$$

□

Exercise 4.1.8: Problem 1.19

Find all idempotent in the ring $\mathbb{Z}/60\mathbb{Z}$.

Proof. Notice that $60 = 3 \times 4 \times 5$. By the Chinese Remainder theorem, we have that

$$\frac{\mathbb{Z}}{60\mathbb{Z}} \cong \frac{\mathbb{Z}}{3\mathbb{Z}} \times \frac{\mathbb{Z}}{4\mathbb{Z}} \times \frac{\mathbb{Z}}{5\mathbb{Z}}$$

The only idempotents of $\mathbb{Z}/3\mathbb{Z}$ are $0, 1$ similarly the only idempotents the other two are also $0, 1$.

We will construct the ring isomorphism $\phi : \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \to \mathbb{Z}/60\mathbb{Z}$. Using the fact that $3\mathbb{Z} + 4\mathbb{Z} = \mathbb{Z}$, we have that $-3 + 4 = 1$, for $3\mathbb{Z} + 5\mathbb{Z} = \mathbb{Z}$ we have $-9 + 10 = 1$. Finally for $4\mathbb{Z} + 5\mathbb{Z} = \mathbb{Z}$, we have that $-4 + 5 = 1$. Let $x_1 = (4)(10) = 40$. Let $x_2 = (-3)(5) = -15 \equiv 45 \pmod{60}$ and $x_3 = (-9)(-4) = 36$. Then we have that $\phi(a, b, c) = (40a + 45b + 36c)$. There are eight idempotents in $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ given by a combination of 0 and 1 in each factor of the product ring. Each of these correspond to an element in $\mathbb{Z}/60\mathbb{Z}$ as follows:

1. $(0, 0, 0)$ corresponds to $0 \in \mathbb{Z}/60\mathbb{Z}$
2. $(0, 0, 1) \mapsto 36 \in \mathbb{Z}/60\mathbb{Z}$
3. $(0, 1, 0) \mapsto 45 \in \mathbb{Z}/60\mathbb{Z}$

4. $(0, 1, 1) \mapsto 21 \in \mathbb{Z}/60\mathbb{Z}$
5. $(1, 0, 0) \mapsto 40 \in \mathbb{Z}/60\mathbb{Z}$
6. $(1, 0, 1) \mapsto 16 \in \mathbb{Z}/60\mathbb{Z}$
7. $(1, 1, 0) \mapsto 25 \in \mathbb{Z}/60\mathbb{Z}$
8. $(1, 1, 1) \mapsto 1 \in \mathbb{Z}/60\mathbb{Z}$

and so we conclude. □