

Honours Algebra - Week 5 - Equivalence Relations, The First Isomorphism Theorem & Modules

Antonio León Villares

February 2022

Contents

1	Equivalence Relations	3
1.1	Defining Equivalence Relations	3
1.1.1	Examples	3
1.1.2	Exercises (TODO)	4
1.2	Equivalence Classes	4
1.2.1	Examples	4
1.2.2	Exercises (TODO)	5
1.3	The Set of Equivalence Classes	5
1.3.1	Examples: Canonical Mappings Preserving Structure (as Homomorphisms)	6
1.3.2	Examples	7
1.3.3	Exercises (TODO)	7
1.4	Remark: A Very Important Remark At That	8
1.5	A Well-Defined Mapping	9
1.5.1	Examples	9
1.5.2	Exercises (TODO)	10
2	Factor Rings	11
2.1	Motivation 1: Equivalence Relations From Kernels	11
2.2	Motivation 2: Equivalence Relations From Ideals	12
2.3	Motivation 3: Quotients From Ideals are Rings	13
2.4	Cosets of Rings	14
2.5	Defining the Factor Ring	14
2.6	Theorem: Operations on Factor Rings	15
2.6.1	Examples	18
2.6.2	Exercises (TODO)	19
2.7	Theorem: The Universal Property of Factor Rings	20
2.8	Theorem: First Isomorphism Theorem for Rings	21
2.8.1	Examples	22
3	Modules	22
3.1	Defining Modules	23
3.1.1	Examples	24
3.1.2	Exercises (TODO)	24
3.2	Lemma: Module Hygiene	25
3.3	Module Homomorphisms	25
3.3.1	Examples	25
3.3.2	Exercises (TODO)	26

3.4	Submodules	27
3.4.1	Examples	27
3.5	Proposition: Test for a Submodule	28
3.6	Lemma: Kernel and Image as Submodules	29
3.7	Lemma: Injectivity and Kernel	30
3.8	Generating Submodules	30
3.8.1	Examples	31
3.9	Lemma: Smallest Submodule Containing a Subset	31
3.10	Lemma: Intersection of Submodules	31
3.11	Lemma: Addition of Submodules	31
3.12	Theorem: Factor Modules	31
3.12.1	Examples	32
3.13	Theorem: Factor Module Operations	33
3.14	Theorem: The Universal Property of Factor Modules	34
3.15	Theorem: First Isomorphism Theorem for Modules	35
3.16	Remark: First Isomorphism Theorem for Vector Spaces	35
3.17	Remark: First Isomorphism Theorem for Abelian Groups	35
4	Workshop	36

1 Equivalence Relations

1.1 Defining Equivalence Relations

- What is a relation?

- a **relation** R on a set X is a **subset**:

$$R \subset X \times X$$

- we describe an element $(x, y) \in R$ via:

$$xRy$$

- What is an equivalence relation?

- a **relation**, typically denoted \sim , satisfying:

1. Reflexivity

$$x \sim x$$

2. Symmetry

$$x \sim y \iff y \sim x$$

3. Transitivity

$$x \sim y \wedge y \sim z \implies x \sim z$$

1.1.1 Examples

- simple equivalence relations include:

$$x \sim y \iff x = y \quad x \sim y \iff x^2 = y^2$$

The first one is more “restrictive”, since in the second one tuples like $(x, -y)$ and $(-x, y)$ are allowed.

- **congruence modulo** m also defines an equivalence relation:

$$x \sim y \iff x \equiv y \pmod{m}$$

- $x \equiv x \pmod{m}$ (reflexivity)
- $x \equiv y \pmod{m} \iff y \equiv x \pmod{m}$ (symmetry)
- $x \equiv y \pmod{m} \wedge y \equiv z \pmod{m} \implies x \equiv z \pmod{m}$ (transitivity)

- a more interesting example is that of matrix conjugacy:

$$A \sim B \iff \exists X : B = XAX^{-1}, \quad A, X, B \in \text{Mat}(n; F)$$

- $IAI^{-1} = A \implies A \sim A$
- $B = XAX^{-1} \implies A = YBY^{-1}, \quad Y = X^{-1}$
- $B = XAX^{-1}, C = YBY^{-1} \implies C = ZAZ^{-1}, \quad Z = YX$

This relates to the notion of **similar matrices**, discussed in W2, whereby basis matrices were similar. That is, if $N = {}_B[f]_B$ and $N = {}_A[f]_A$, then N, M are similar in the sense that with $T = {}_A[id_V]_B$:

$$N = T^{-1}MT$$

1.1.2 Exercises (TODO)

1. Show that the relation \sim on $Mat(n \times m; F)$, defined by:

$$A \sim B \iff \exists P \in GL(n; F), Q \in GL(m; F) : B = PAQ$$

is an equivalence relation.

2. Show that isomorphism is an equivalence relation on finite dimensional vector spaces over a field F .

1.2 Equivalence Classes

- What is an equivalence class?

- consider a set X with **equivalence relation** \sim
- an **equivalence class** for $x \in E$ is a subset $E \subseteq X$ such that:

$$E(x) := \{z \mid x \sim z, x \in X\}$$

- What is a representative of an equivalence class?

- an element $e \in E(x)$

- What is a system of representatives?

- a subset $Z \subseteq X$
- it contains exactly **one** element from each **equivalence class** $E(x), x \in X$

- What are some properties of equivalence classes?

- the following notions are **equivalent**:
 1. $x \sim y$
 2. $E(x) = E(y)$ (this follows from (1) + symmetry)
 3. $E(x) \cap E(y) \neq \emptyset$ (this follows from (1) + reflexivity, which means that $x \in E(x), x \in E(y)$)

1.2.1 Examples

- if X is a set of students, with equivalence relation “same degree”, each equivalence class contains all students which pursue the same degree
- if $X = \mathbb{R}$, then the equivalence relation:

$$x \sim y \iff x - y \in \mathbb{Z}$$

has equivalence classes like:

$$E(1.2) = \{\dots, -2.8, -1.8, -0.8, 0.2, 1.2, 2.2, \dots\}$$

More generally, if $z \in \mathbb{Z}$, the equivalence relation tells us that:

$$y \in E(x) \implies y - x = z \implies y = x + z \implies E(x) = \{x + z \mid x \in X, z \in \mathbb{Z}\}$$

(here we have used symmetry)

- if we define:

$$x \sim y \iff x \equiv y \pmod{m}$$

then the equivalence classes are familiar:

$$E(x) = \bar{x} = \{x + mz \mid z \in \mathbb{Z}\}$$

Furthermore, if $m > 0$, a **system of representatives** will contain an element of each **equivalence class**, which can be:

$$\{0, 1, 2, \dots, m-1\}$$

where $0 \in E(0), 1 \in E(1)$, and so on. However, in general, we can pick:

$$\{a, a+1, a+2, \dots, a+m-1\}$$

where $a \in \mathbb{Z}$

1.2.2 Exercises (TODO)

1. Show that the $n \times m$ matrices over a field F in Smith-Normal Form form a system of representatives for the equivalence relation:

$$A \sim B \iff \exists P \in GL(n; F), Q \in GL(m; F) : B = PAQ$$

2. Show that the set:

$$\{F^n \mid n \in \mathbb{Z}_{\geq 0}\}$$

is a system of representatives for the equivalence relation defined by an isomorphism on finite dimensional vector spaces over a field F . Show that another system of representatives for this equivalence relation is:

$$\{F[X]_{<n} \mid n \in \mathbb{Z}_{\geq 0}\}$$

1.3 The Set of Equivalence Classes

- What is the set of equivalence classes?

- let X be a set, with equivalence relation \sim
- the **set of equivalence classes** is a **subset** of the **power set** $\mathcal{P}(X)$
- it is the set containing all equivalence classes of X :

$$(X/\sim) := \{E(x) \mid x \in X\}$$

- this is also known as the **quotient set**

- What canonical mapping arises from this definition?

*A **canonical map** is a map or morphism between objects that arises naturally from the **definition** or the **construction** of the objects. In general, it is the map which preserves the widest amount of structure, and it tends to be unique.*

- in this case, a **canonical map** is of the form:

$$can : X \rightarrow (X/\sim)$$

$$can(x) = E(x)$$

- this is a **surjection**, since each equivalence class $E(x)$ contains at least one element in X (so “worst case”, each $x \in X$ maps to a unique $E(x)$)

1.3.1 Examples: Canonical Mappings Preserving Structure (as Homomorphisms)

1. Abelian Groups

- A is an **abelian group**; B is a **subgroup** of A
- define an equivalence relation.

$$x \sim y \iff x - y \in B$$

- the equivalence classes are:

$$y - x = b \in B \implies E(x) = \{x + b \mid b \in B\}$$

(here we use the fact that the group is abelian, so $x + b = b + x$)

- the **quotient set** is $A/B \equiv A/\sim$, an **abelian group**, defined by:

$$E(x) + E(y) = E(x + y) = \{x + y + b \mid b \in B\}$$

- the canonical mapping $can : A \rightarrow A/B$ is a **surjective homomorphism**, with kernel being B (since $0 \in A/B = \{0 + b \mid b \in B\} = B$, and any element $b \in B$ will get mapped to this set)
- A/B is the **quotient abelian group** of A by the subgroup B

2. Non-Abelian Group

- G is a **group**, and H is a **normal subgroup**: that is, if $h \in H$ and $g \in G$, then:

$$ghg^{-1} \in H$$

- define an equivalence relation:

$$x \sim y \iff xy^{-1} \in H$$

- the equivalence classes are given by the **left** and **right** cosets:

$$E(x) = xH = Hx \subseteq G$$

This is because if $xy^{-1} \in H$, by symmetry, $yx^{-1} = h \in H$, so $y = hx$, meaning that $E(x) = \{hx \mid h \in H\}$. the equivalence relation is defined by

$$xy^{-1} \in H$$

. Moreover, since G is a group, and H is a normal subgroup, we know that $g^{-1}hg \in H$. Thus, if $xy^{-1} \in H$, we must also have $y^{-1}(xy^{-1})y = y^{-1}x \in H$. Hence, $y^{-1} \sim x^{-1}$, and again by symmetry, $x^{-1} \sim y^{-1} \implies x^{-1}y \in H \implies y = xh \implies E(x) = xH$.

- the quotient set $G/\sim \equiv G/H$ is the group with operations:

$$E(x)E(y) = E(xy)$$

- the canonical **surjective homomorphism** $can : G \rightarrow G/H$ has kernel H , since $hH = Hh = H$, so $\forall h \in H, can(h) = H$, and H is the identity element in G/H
- this relates to **Lagrange's Theorem**, which states that:

$$|G| = |G/H||H|$$

which is proved by noting that each coset $E(x)$ has exactly $|H|$ elements (since it is given by $xH = Hx$), and that G is the disjoint union of $|G/H|$ cosets (the union is disjoint because otherwise we'd have elements belonging to more than 1 equivalence classes; there are $|G/H|$ cosets because G/H is the set of all cosets).

-
- G/H is the **quotient group** of G by the normal subgroup H

3. F-Vector Spaces

- let V be a **F-Vector Space**, with subspace W
- define an equivalence relation:

$$x \sim y \iff x - y \in W$$

- as in the first case, the equivalence classes are:

$$y - x = w \implies E(x) = \{x + w \mid w \in W\} = x + W$$

- the **quotient set** is an **F-Vector Space** with:

$$\lambda E(x) = E(\lambda x)$$

- the canonical **surjective homomorphism** $can : V \rightarrow V/W$ has kernel W (same reason as in case (1))
- by the exercise below, we can show that if V is finite-dimensional:

$$\dim(V/W) = \dim(V) - \dim(W)$$

- V/W is the **quotient vector space** of V by the subspace W

1.3.2 Examples

- if \sim defines the congruence equivalence relation, modulo m , then:

$$(\mathbb{Z}/\sim) = \mathbb{Z}_m$$

This is easy to see, since as discussed above, the equivalence classes of \sim are the sets $\bar{0}, \bar{1}, \dots, \overline{m-1}$, and the set of all these elements is precisely \mathbb{Z}_m

1.3.3 Exercises (TODO)

1. Let $R = F$ be a field, V and F -vector space, and $W \subseteq V$ a subspace of V . The quotient V/W is the **quotient vector space**, and $can : V \rightarrow V/W$ is a linear mapping. Assume that $\dim V = m < \infty$. By the **Dimension Estimate for Vector Subspaces**, $\dim W = n \leq m$. Let:

$$\{\underline{v}_1, \dots, \underline{v}_n\}$$

be a basis for W . Using the **Steinitz Exchange Theorem**, we can extend it to a basis of V :

$$\{\underline{v}_1, \dots, \underline{v}_n, \underline{v}_{n+1}, \dots, \underline{v}_m\}$$

Show that:

$$\{\underline{v}_{n+1} + W, \dots, \underline{v}_m + W\}$$

is a basis for the vector space V/W . Hence, deduce that:

$$\dim(V/W) = \dim V - \dim W$$

1.4 Remark: A Very Important Remark At That

Consider \sim as an equivalence relation on X , and let $f : X \rightarrow Z$ be a mapping, such that:

$$x \sim y \implies f(x) = f(y)$$

In other words, whatever the equivalence relation is, it is such that all elements in the same **equivalence class** are mapped to the same value under f

Then, there exists a **unique** mapping:

$$\bar{f} : (X / \sim) \rightarrow Z$$

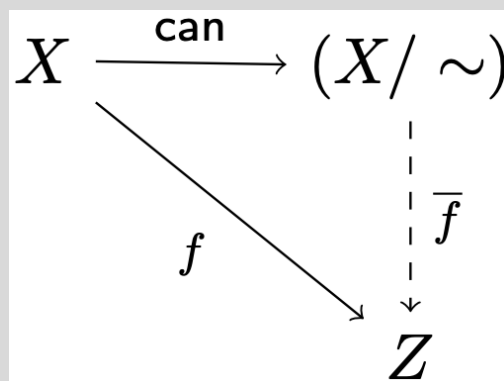
This mapping is simple to define:

$$\bar{f}(E(x)) = f(x)$$

such that:

$$f = \bar{f} \circ \text{can}$$

This can be summarised by the following diagram:



This is known as the **universal property of the set of equivalence classes**

A more interesting case occurs when

$$f : X \rightarrow Z$$

is **any** mapping, and we define:

$$x \sim y \iff f(x) = f(y)$$

Then, we will have that:

$$\bar{f} : (X / \sim) \rightarrow \text{im } f$$

is a **bijection**. This bijection is a prelude to the **First Isomorphism Theorem**.

1.5 A Well-Defined Mapping

- When is a mapping well-defined?

– consider a mapping:

$$g : (X / \sim) \rightarrow Z$$

– g is **well-defined** if there exists a mapping:

$$f : X \rightarrow Z$$

such that:

$$x \sim y \implies f(x) = f(y)$$

– here we recognise $g = \bar{f}$

- Why are well-defined mappings important?

- they **solidify** the notion of **equivalence**
- they ensure that elements in the **same equivalence class** are mapped to the **same** value
- this means that equivalent elements in X are the same in Z
- more on this in [Proof-Wiki](#)

1.5.1 Examples

- recall the equivalence relation:

$$a \sim b \iff a - b \in \mathbb{Z}$$

with equivalence classes:

$$E(a) = \{\dots, a - 2, a - 1, a, a + 1, a + 2, \dots\}$$

Further consider:

$$f : \mathbb{R} \rightarrow \mathbb{R} \quad f(x) = \cos(x)$$

$$g : \mathbb{R} \rightarrow \mathbb{R} \quad f(x) = \cos(2\pi x)$$

Then, f is **not** well-defined, since:

$$0 \sim 1 \quad f(0) = 1 \neq f(1)$$

However, g is well-defined. Indeed:

$$a \sim b \implies a = b + z, z \in \mathbb{Z}$$

So:

$$g(a) = \cos(2\pi a) = \cos(2\pi b + 2\pi z) = \cos(2\pi b) = g(b)$$

where we exploit the fact that \cos is 2π periodic. Moreover, we can define:

$$\bar{g} : (\mathbb{R} / \sim) \rightarrow \mathbb{R}$$

via:

$$\bar{g}(E(a)) = g(a) = \cos(2\pi a)$$

1.5.2 Exercises (TODO)

1. Define a relation \sim on $\mathbb{X} \times \mathbb{N}$ by:

$$(x, y) \sim (a, b) \iff x + b = y + a$$

- (a) Show that \sim is an equivalence relation
- (b) Let $\bar{\mathbb{N}} = (\mathbb{N} \times \mathbb{N} / \sim)$. Show that addition on \mathbb{N} induces a *well-defined* addition on $\bar{\mathbb{N}}$
- (c) Show that with this addition, $\bar{\mathbb{N}}$ is an abelian group
- (d) Show that

$$nat : \mathbb{N} \rightarrow \bar{\mathbb{N}}$$

is an additive mapping, where:

$$nat(a) = E((a + n, n)), \forall n \in \mathbb{N}$$

That is:

$$nat(a + b) = nat(a) + nat(b)$$

- (e) Show that $\bar{\mathbb{N}}$ is *isomorphic* as a group to $(\mathbb{Z}, +)$

2 Factor Rings

2.1 Motivation 1: Equivalence Relations From Kernels

We just showed that **mappings between sets** generate **equivalence relations**. In particular, consider a **ring homomorphism**:

$$f : R \rightarrow S$$

We can define an **equivalence relation** on R :

$$x \sim y \iff f(x) = f(y)$$

By properties of homomorphism:

$$\begin{aligned} x \sim y &\iff f(x) = f(y) \\ &\iff f(x) - f(y) = 0_S \\ &\iff f(x - y) = 0_S \\ &\iff x - y \in \ker(f) \end{aligned}$$

This then defines the **equivalence classes** via:

$$y - x = k \in \ker(f) \implies y = x + k$$

so in particular:

$$E(x) = x + \ker(f) = \{x + k \mid k \in \ker(f)\}$$

2.2 Motivation 2: Equivalence Relations From Ideals

In fact, all the above generalises easily to **ideals**:

If I is an ideal of a ring R , and $f : R \rightarrow S$, then the following is an equivalence relation:

$$r_1 \sim r_2 \iff r_1 - r_2 \in I$$

1. $r_1 - r_1 = 0_R \in I \iff r_1 \sim r_1$ (since 0 is always part of an ideal).
Hence, **reflexivity** holds.

2. if $r_1 \sim r_2$, then:

$$r_1 - r_2 \in I$$

Since ideals are closed under subtraction, it follows that:

$$-(r_1 - r_2) = r_2 - r_1 \in I$$

so we have $r_2 \sim r_1$. Thus, **symmetry** holds.

3. if $r_1 \sim r_2$ and $r_2 \sim r_3$, then:

$$r_1 - r_2 \in I$$

$$r_2 - r_3 \in I$$

Ideals are closed under subtraction/addition, so:

$$(r_1 - r_2) + (r_2 - r_3) = r_1 - r_3 \in I$$

so we have $r_1 \sim r_3$. Thus, **transitivity** holds.

As above, the equivalence classes then become:

$$E(r_1) = r_1 + I = \{r_1 + i \mid i \in I\}$$

and the **quotient of R by I** (the set of **all equivalence classes**) is:

$$R/I$$

We have constructed R/I . We now go back, and discover that it is a ring.

2.3 Motivation 3: Quotients From Ideals are Rings

R/I is the set of all equivalence classes, constructed from the **equivalence relation**:

$$r_1 \sim r_2 \iff r_1 - r_2 \in I$$

But if we think about it, this equivalence relation was originally defined as:

$$r_1 \sim r_2 \iff f(r_1) = f(r_2)$$

But now recall, such an equivalence relation lead to the following bijection:

$$\bar{f} : (R/I) \rightarrow \text{im}(f)$$

$$\bar{f}(E(r)) = f(r)$$

The existence of this bijection tells us that, since $\text{im}(f)$ is a **subring** of S , we should expect that R/I should also have a ring-like structure, since we have a one-to-one correspondance between elements in R/I and a subring (in fact, if \bar{f} is an **isomorphism**, R/I would indeed be **isomorphic** to the subring $\text{im}(f)$).

So if we have R/I as a ring, we better endow it with **addition** and **multiplication**:

$$E(r_1) + E(r_2) = E(r_1 + r_2)$$

$$E(r_1 r_2) = E(r_1) E(r_2)$$

This section focuses on formalising the notion of R/I as a **factor ring**, defines the **Universal Property of Factor Rings** results, and has a grand finale in the **First Isomorphism Theorem**.

2.4 Cosets of Rings

- What is a coset of a ring?

- let R be a ring, and I an ideal of R
- the **coset of x with respect to I in R** is the subset of R :

$$x + I = \{x + i \mid i \in I\}$$

- cosets in **rings** are special cases of cosets in **groups**

- Are cosets equivalence classes?

- as we saw above,

$$x \sim y \iff x - y \in I$$

defines an equivalence class:

$$E(x) = x + I$$

- so **cosets** are **equivalence classes**

- Given 2 cosets, how can they be related?

- we saw that if $x \sim y$, then:

$$E(x) = E(y) \quad E(x) \cap E(y) \neq \emptyset$$

- hence, depending on whether $x \sim y$, 2 cosets $x + I$ and $y + I$ are related in one of 2 ways:

- * $x + I = y + I$
- * or $(x + I) \cap (y + I) = \emptyset$

2.5 Defining the Factor Ring

- What is a factor ring?

- let:

- * R be a ring
- * I be an ideal of R
- * \sim the equivalence relation on R :

$$x \sim y \iff x - y \in I$$

- the **factor ring of R by I** is nothing but the **quotient of R by I**
- hence, the factor ring is R/I :
 - the set of **equivalence classes** under \sim
 - the set of **cosets** of I in R

2.6 Theorem: Operations on Factor Rings

For the **factor ring** to be a ring, we need to provide ring operations.

Let R be a **ring**, and I an **ideal**.

Then, R/I is a **ring**, with **addition** defined as:

$$(x + I) + (y + I) = (x + y) + I, \forall x, y \in R$$

and **multiplication** defined as:

$$(x + I) \cdot (y + I) = xy + I, \forall x, y \in R$$

[Theorem 3.6.4]

For the proof we need to be careful, and show that:

- R/I is an **abelian** group under **addition**
- addition is **well-defined**
- R/I is a **monoid** under **multiplication**
- multiplication is **well-defined**
- R/I satisfies the **distributive axioms**

This proves that R/I is a ring. It is important to emphasise the need to show that the operations are **well-defined**:

Consider $R = \mathbb{Z}$ and $I = 15\mathbb{Z} = \{15z \mid z \in \mathbb{Z}\}$. The **equivalence classes**, as discussed, are of the form:

$$E(r) = \{r + 15z \mid z \in \mathbb{Z}\}$$

The factor ring is our well known:

$$\mathbb{Z}/15\mathbb{Z} = \mathbb{Z}_{15}$$

Now, consider the following products:

$$E(7) \cdot E(9) = E(63) \quad E(22) \cdot E(9) = E(198)$$

Now, we know that 22 and 7 are congruent modulo 15, so obviously $E(7) = E(22)$ (they are the same equivalence class). The question now becomes: are $E(63)$ and $E(198)$ congruent modulo 15? How can we be sure? This is the importance of having **well-defined** operations: we are working over **equivalence classes**, so we need to ensure that any arithmetic we do doesn't depend of our choice of **representative** of the equivalence class.

In this example, any arithmetic we do shouldn't depend on the number we choose (i.e 7 and 22), but rather the **remainder** when dividing by 15.

Proof. **1. Addition is Well-Defined**

To show that addition is well-defined, we need to show that if $x, x', y, y' \in R$ and:

$$E(x) = E(x') \quad E(y) = E(y')$$

(we use $E(x)$ instead of $x + I$ for ease of reading and writing) then:

$$E(x) + E(y) = E(x') + E(y')$$

Notice, by how addition is defined, this is equivalent to showing that:

$$E(x + y) = E(x' + y')$$

which is equivalent to showing that the two are the **same equivalence class**. In other words, we need to show that:

$$(x + y) \sim (x' + y') \implies (x + y) - (x' + y') \in I$$

We consider:

$$(x + y) - (x' + y') = (x - x') + (y - y')$$

By assumption, $E(x) = E(x')$, so $x \sim x'$, so $x - x' \in I$. Similarly, $y \sim y'$, so $y - y' \in I$. Since ideals are closed under addition/subtraction, it is clear that:

$$(x - x') + (y - y') \in I$$

Hence, addition is well-defined.

2. R/I is an Abelian Group Under Addition

(a) Existence of Identity

$$E(0) + E(x) = E(0 + x) = E(x) = E(x + 0) = E(x) + E(0)$$

(b) Existence of Inverse

$$E(-x) + E(x) = E(-x + x) = E(0) = E(x - x) = E(x) + E(-x)$$

(c) Associativity

$$(E(x) + E(y)) + E(z) = E(x + y) + E(z) = E(x + y + z) = E(x) + E(y + z) = E(x) + (E(y) + E(z))$$

(d) Closure This follows directly from the definition of addition.

(e) Abelian

$$E(x) + E(y) = E(x + y) = E(y + x) = E(y) + E(x)$$

(using commutativity of R under addition)

Hence, R/I is an abelian group under addition.

3. Multiplication is Well-Defined Again ,consider x, x', y, y' with:

$$E(x) = E(x') \quad E(y) = E(y')$$

we need to show that:

$$E(x)E(y) = E(x')E(y')$$

Since $E(x) = E(x')$, we know that:

$$x \sim x' \implies x - x' \in I \implies x = x' + i, i \in I$$

Similarly:

$$y = y' + j, j \in I$$

Hence:

$$\begin{aligned} E(x)E(y) &= E(xy) \\ &= E((x' + i)(y' + j)) \\ &= E(x'y' + x'j + iy' + ij) \\ &= E(x'y') + E(x'j) + E(iy') + E(ij) \end{aligned}$$

Now, notice that:

$$E(x'j) = E(iy') = E(ij) = E(0)$$

Since $ij, iy', x'j \in I$ (since multiplying elements in R by elements in I produces elements in I), then:

$$ij - 0 \in I \quad iy' - 0 \in I \quad x'j - 0 \in I$$

So $ij \sim iy' \sim x'j \sim 0$, from which $E(x'j) = E(iy') = E(ij) = E(0)$ follows. Hence, we have shown that:

$$E(x)E(y) = E(x'y') = E(x')E(y')$$

so multiplication is well-defined.

4. R/I is a Monoid Under Multiplication

(a) **Closure** This follows directly from the definition of multiplication.

(b) **Associativity**

$$(E(x)E(y))E(z) = E(xy)E(z) = E(xyz) = E(x)E(yz) = E(x)(E(y)E(z))$$

(c) **Existence of Identity**

$$E(x)E(1) = E(x \cdot 1) = E(x) = E(1 \cdot x) = E(1)E(x)$$

Hence, R/I is a monoid under multiplication.

5. R/I Satisfies Distributivity

$$E(x)(E(y)+E(z)) = E(x)E(y+z) = E(x(y+z)) = E(xy+xz) = E(xy)+E(xz) = E(x)E(y)+E(x)E(z)$$

Hence, by all of the above, R/I is a ring, with **well-defined** operations. □

2.6.1 Examples

- this is another way of seeing that $\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m$ is a **ring**
- consider the ring $R = \mathbb{F}_2[X]$ (the ring of polynomials with coefficients 0 or 1), and the following 2 ideals:

$$I = {}_R\langle X^2 \rangle = \{pX^2 \mid p \in R\}$$

$$J = {}_R\langle X^2 + X + 1 \rangle = \{p(X^2 + X + 1) \mid p \in R\}$$

How do we describe R/I and R/J ?

1. Elements in the Factor Rings

(a) **Elements in R/I** For $p \in R$, We denote:

$$E_I(p) = p + I$$

Then, we can consider the equivalence classes, given by the relation:

$$p_1 \sim p_2 \iff p_1 - p_2 \in I$$

that is $p_1 \sim p_2$ if $p_1 - p_2$ has X^2 as a factor. Consider the constant polynomials first (only 2 of them)

$$E_I(0) = \{i \mid i \in I\} \quad E_I(1) = \{1 + i \mid i \in I\}$$

Clearly, $0 \not\sim 1$, since $0 - 1 = 1$ (we operate in \mathbb{F}_2) which is not divisible by X^2 . Hence, $E_I(0)$ and $E_I(1)$ are different equivalence classes. Now considering linear polynomials:

$$E_I(X) = \{X + i \mid i \in I\} \quad E_I(X + 1) = \{X + 1 + i \mid i \in I\}$$

Then:

- $X - 0 \notin I$
- $X - 1 \notin I$
- $(X + 1) - 0 \notin I$
- $(X + 1) - 1 \notin I$
- $(X + 1) - X \notin I$

Hence, we have 2 more equivalence classes:

$$E_I(X) \quad E_I(X + 1)$$

Now, consider a polynomial $p \in R$ with $\deg(p) \geq 2$. We can factorise it as:

$$p(X) = q(X)X^2 + r(X)$$

such that $\deg(r) < \deg(X^2) = 2$. Then notice that:

$$p - r = qX^2 \in I \implies p \sim r$$

Thus, any polynomial is in the equivalence class of its remainder. Since the remainder r has degree 0 or 1, it means that p is in one of $E_I(0), E_I(1), E_I(X), E_I(X + 1)$. Thus:

$$(R/I) = \{E_I(0), E_I(1), E_I(X), E_I(X + 1)\}$$

(b) **Elements in R/J** Working in a similar, we will see that:

$$(R/J) = \{E_J(0), E_J(1), E_J(X), E_J(X + 1)\}$$

2. Behaviour of Elements We have reduced the elements of R/I to a set of 4 elements. We now need to see how they interact with each other through a multiplication table:

	$E_I(0)$	$E_I(1)$	$E_I(X)$	$E_I(X + 1)$
$E_I(0)$	$E_I(0 \cdot 0) = E_I(0)$	$E_I(0 \cdot 1) = E_I(0)$	$E_I(0 \cdot X) = E_I(0)$	$E_I(0 \cdot (X + 1)) = E_I(0)$
$E_I(1)$	$E_I(1 \cdot 0) = E_I(0)$	$E_I(1 \cdot 1) = E_I(1)$	$E_I(1 \cdot X) = E_I(X)$	$E_I(1 \cdot (X + 1)) = E_I(X + 1)$
$E_I(X)$	$E_I(X \cdot 0) = E_I(0)$	$E_I(X \cdot 1) = E_I(X)$	$E_I(X^2) = E_I(0)$	$E_I(X^2 + X) = E_I(X)$
$E_I(X + 1)$	$E_I((X + 1) \cdot 0) = E_I(0)$	$E_I((X + 1) \cdot 1) = E_I(X + 1)$	$E_I(X^2 + X) = E_I(X)$	$E_I(X^2 + 2X + 1) = E_I(1)$

Table 1: Here we use facts like $X^2 \sim 0$ and $X^2 + X \sim X$ to simplify. Also, don't forget that $2 = 0$ in \mathbb{F}_2 .

	$E_J(0)$	$E_J(1)$	$E_J(X)$	$E_J(X + 1)$
$E_J(0)$	$E_J(0 \cdot 0) = E_J(0)$	$E_J(0 \cdot 1) = E_J(0)$	$E_J(0 \cdot X) = E_J(0)$	$E_J(0 \cdot (X + 1)) = E_J(0)$
$E_J(1)$	$E_J(1 \cdot 0) = E_J(0)$	$E_J(1 \cdot 1) = E_J(1)$	$E_J(1 \cdot X) = E_J(X)$	$E_J(1 \cdot (X + 1)) = E_J(X + 1)$
$E_J(X)$	$E_J(X \cdot 0) = E_J(0)$	$E_J(X \cdot 1) = E_J(X)$	$E_J(X^2) = E_J(X + 1)$	$E_J(X^2 + X) = E_J(1)$
$E_J(X + 1)$	$E_J((X + 1) \cdot 0) = E_J(0)$	$E_J((X + 1) \cdot 1) = E_J(X + 1)$	$E_J(X^2 + X) = E_J(1)$	$E_J(X^2 + 2X + 1) = E_J(X)$

Table 2: Here we use facts like $X^2 \sim X + 1$ (since $X^2 - (X + 1) = X^2 - X - 1 = X^2 + X + 1 \in J$ and $X^2 + X \sim 1$ (since $X^2 + X - 1 = X^2 + X + 1 \in J$) to simplify. Also, don't forget that $2 = 0$ in \mathbb{F}_2 .

Now notice: in R/J every non-zero element has an inverse, so R/J is a **field** with 4 elements. On the other hand, R/I is **not**, since it has a **zero-divisor** (for example $E_I(X)$).

2.6.2 Exercises (TODO)

1. Let R be a ring, and I an ideal of R . Show that if R is commutative, then so is R/I .
2. Let R be a ring, and I an ideal of R . Show that R/I is a non-zero ring if and only if $I \neq R$.
3. Let R be a ring, and I a *proper* ideal of R (so $I \neq R$). Show that if $r \in R^\times$, then $E(r) \in (R/I)^\times$, and $(E(r))^{-1} = E(r^{-1})$.

2.7 Theorem: The Universal Property of Factor Rings

In the **Very Important Remark** (1.4) (the **universal property of the set of equivalence classes**, we showed how there are 2 ways to go between sets X, Z : one that is direct ($f : X \rightarrow Z$) and one that is indirect ($g : X \rightarrow X/\sim \rightarrow Z$, with $g = \bar{g} \circ \text{can}$, where \bar{g} is a unique mapping $\bar{g}(E(r)) = f(r)$). This theorem considers the same case, but adapted to **rings**.

Let R be a **ring**, and I an **ideal** of R .

1. The **canonical mapping**:

$$\text{can} : R \rightarrow (R/I) \quad \text{can}(r) = E(r), \forall r \in R$$

is a **surjective ring homomorphism**, with **kernel**:

$$\ker(\text{can}) = I$$

2. If:

$$f : R \rightarrow S$$

is a **ring homomorphism** and:

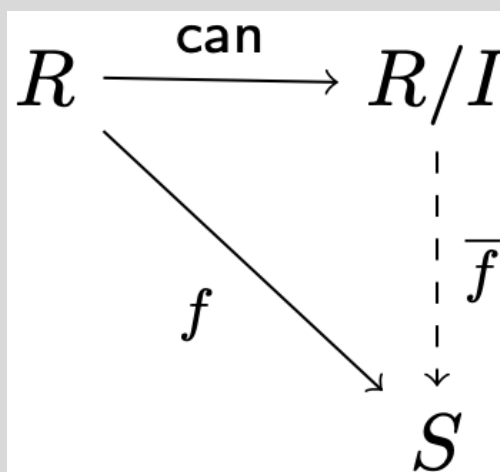
$$f(I) = \{0_S\}$$

so that $I \subseteq \ker(f)$, then there is a **unique ring homomorphism**:

$$\bar{f} : (R/I) \rightarrow S$$

such that:

$$f = \bar{f} \circ \text{can}$$



[Theorem 3.6.7]

Proof. 1. **The Canonical Mapping is a Surjective Ring Homomorphism With Kernel I**

- (a) **Surjective Mapping** This easy to see. Any $E(r)$ is produced by at least one element in R . By the pigeonhold principle, every possible $E(r)$ must be mapped to by some element in R .
- (b) **The Kernel is I** If $i \in I$, then by properties of ideals:

$$i - 0_R \in I \implies i \sim 0 \implies E(i) = E(0) = 0_{R/I}$$

Any other $i \notin I$ won't have an equivalence relation with 0_R . Hence, $\ker(\text{can}) = I$.

- (c) **The Mapping is a Ring Homomorphism** This follows from how **addition** and **multiplication** are defined in the **factor ring R/I** :

$$\text{can}(x) + \text{can}(y) = E(x) + E(y) = E(x + y) = \text{can}(x + y)$$

$$\text{can}(x)\text{can}(y) = E(x)E(y) = E(xy) = \text{can}(xy)$$

2. Existence of Unique Ring Homomorphism \bar{f}

- (a) **Existence of Unique Mapping \bar{f}** Since $f(I) = \{0_S\}$, then:

$$f(E(x)) = \{f(x + i) \mid i \in I\} = \{f(x) + f(i) \mid i \in I\} = \{f(x)\}$$

Define:

$$\bar{f}(E(x)) = f(x)$$

such that:

$$f(E(x)) = \{\bar{f}(E(x))\}$$

Then, \bar{f} is the only mapping satisfying $f = \bar{f} \circ \text{can}$.

- (b) **\bar{f} is a Ring Homomorphism**

$$\bar{f}(E(x) + E(y)) = \bar{f}(E(x + y)) = f(x + y) = f(x) + f(y) = \bar{f}(E(x)) + \bar{f}(E(y))$$

$$\bar{f}(E(x)E(y)) = \bar{f}(E(xy)) = f(xy) = f(x)f(y) = \bar{f}(E(x))\bar{f}(E(y))$$

□

2.8 Theorem: First Isomorphism Theorem for Rings

Let R and S be **rings**.

Then, every **ring homomorphism**:

$$f : R \rightarrow S$$

induces a **ring isomorphism**:

$$\bar{f} : (R/\ker(f)) \rightarrow \text{im}(f)$$

This **isomorphism** is nothing but:

$$\bar{f}(r + \ker(f)) = f(r)$$

[Theorem 3.6.9]

Proof. Notice, $\ker(f)$ is an ideal, so R/I is a ring; similarly, $\text{im}(f)$ is a subring, so a **ring**. Moreover, by definition of the kernel, we must have that $f(\ker(f)) = \{0_S\}$. Hence, by the **universal property of factor rings**, we have that \bar{f} is a homomorphism.

Clearly, it is also **surjective** (each $f(r) \in \text{im}(f)$ is produced by at least one element in each equivalence class $r + \ker(f)$).

Moreover, $\ker(\bar{f}) = 0 + \ker(f) = \ker(f)$ (recall $0 + \ker(f)$ is nothing but $E(0)$). If $E(r) = \ker(f)$, clearly $\bar{f}(E(r)) = f(r) = 0_S$, by definition of the kernel. No other equivalence class achieves this. Hence, since the kernel only contains the additive identity, the homomorphism must be **injective**.

Thus, \bar{f} is a bijective homomorphism - an isomorphism. □

2.8.1 Examples

- if $R = \mathbb{R}[X]$ and $I = {}_R\langle X^2 + 1 \rangle$ (the **ideal** generated by $X^2 + 1$, or in other words, the set of all polynomials with $X^2 + 1$ as a factor), then R/I is not only a **ring**, but it is **isomorphic** to the **complex numbers**

- we can **factorise** polynomials uniquely ($P = AQ + B$, with $P, Q \in R$, $\deg(B) < \deg(Q)$)
- in particular, we can write $P \in R$ as:

$$P = A(X^2 + 1) + B$$

- since $Q = X^2 + 1$, and $\deg(B) < \deg(Q)$ we must have:

$$B = a + bX, \quad a, b \in \mathbb{R}$$

- now consider the **evaluation homomorphism**:

$$f : \mathbb{R}[X] \rightarrow \mathbb{C}$$

defined by evaluation $P \in \mathbb{R}[X]$ at $\sqrt{-1}$

- clearly, $f(P) = f(B)$, since $\sqrt{-1}$ is a root of $X^2 + 1$, so:

$$f(P) = f(B) = a + b\sqrt{-1}$$

- clearly, f is surjective
- moreover, $P \in \ker(f)$ **if and only if** $a = b = 0$, which in particular means that:

$$\ker(f) = {}_{\mathbb{R}}[X]\langle X^2 + 1 \rangle$$

- by the **first isomorphism theorem for rings**, we thus have an **isomorphism**:

$$\bar{f} : ({}_{\mathbb{R}}[X] / {}_{\mathbb{R}}[X]\langle X^2 + 1 \rangle) \rightarrow \mathbb{C}$$

3 Modules

Just as **rings** are the generalisation of fields, we introduce **modules** as the generalisation of **vector spaces**.

3.1 Defining Modules

- **What is a left module?**

- a **left module** is defined over **rings**
- it consists of an **abelian group**:

$$M = (M, \dot{+})$$

armed with a mapping:

$$R \times M \rightarrow M$$

$$(r, a) \rightarrow r \cdot a$$

- **left modules** must satisfy:

$$r(a \dot{+} b) = (ra) \dot{+} (rb)$$

$$(r + s)a = (ra) \dot{+} (sa)$$

$$r(sa) = (rs)a$$

$$1_R a = a$$

- **What is an R-Module?**

- a module defined over the **ring** R

- **How do right modules differ from left modules?**

- a module in which multiplication by rings is defined via:

$$(r, a) \rightarrow a \cdot r$$

- **What is the trivial module?**

- the singleton $\{0\}$ for any ring R

- **What is a direct sum?**

- given R -modules:

$$M_1, M_2, \dots, M_n$$

their **cartesian product**:

$$M_1 \times M_2 \times \dots \times M_n$$

alongside:

$$(a_1, \dots, a_n) + (b_1, \dots, b_n) = (a_1 + b_1, \dots, a_n + b_n)$$

$$r(a_1, \dots, a_n) = (ra_1, \dots, ra_n)$$

is an R -module

- denoted:

$$M_1 \oplus M_2 \oplus \dots \oplus M_n$$

is the **direct sum**

- **How do R-Modules and F-Vector Spaces differ?**

- since modules are defined over **rings**, multiplication by R might **not** have inverses defined
- this means that if for example:

$$rm = 0$$

we can't assume that $r = 0$ or $m = 0$. For example, if:

$$R = \mathbb{Z}, \quad (M, +) = (\mathbb{Z}_4, +)$$

then:

$$2 \cdot \bar{2} = \bar{4} = \bar{0}$$

- amongst other things, this means that the notion of **linear independence** no longer makes sense in **modules**, since **linear combinations** can be 0, with not all ring scalars being 0

3.1.1 Examples

- F -vector spaces are just R -modules in which the **ring** R is a field F
- \mathbb{Z} -modules are **abelian groups**. Indeed, any abelian group M is a \mathbb{Z} -module.
- if I is an ideal of a ring R , then I is an R -module, under multiplication in the ring. In fact, R is an R -module.
 - for example, \mathbb{Z} and \mathbb{Z}_6 are both modules
 - ideals exploit the fact that if an element of $r \in R$ multiplies $i \in I$, then $ir, ri \in I$

3.1.2 Exercises (TODO)

1. Let S be a ring, and let $R = \text{Mat}(n; S)$. Let $M = S^n$. Show that M is an R -module under the operations of componentwise addition and matrix multiplication.
2. Let V be an F -vector space for some field F and let $\phi \in \text{End}(V)$ be an endomorphism of V . Show that V is an $F[X]$ -module under the operation:

$$\left(\sum_{i=0}^m a_i X^i \right) \underline{v} = \sum_{i=0}^m a_i \phi^i(\underline{v})$$

For better understanding, we are multiplying a vector \underline{v} by a polynomial with coefficients in a field. This multiplication then needs to result in a vectors in the vector space. We denote the $F[X]$ -module via V_ϕ .

As an example for this, consider:

$$R = \mathbb{C}[X] \quad (M, +) = \mathbb{C}^n$$

We can define the endomorphism ϕ as:

$$\phi(\underline{v}) = A\underline{v} \quad \underline{v} \in m, A \in \text{Mat}(n; \mathbb{C})$$

and then define ring multiplication as:

$$p(X)\underline{v} := p(A)\underline{v}, \quad p(X) \in R$$

As a concrete example, define:

$$A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

and

$$q(X) = X^2 + 2X + 3$$

Then:

$$q(A) = A^2 + 2A + 3I = \begin{pmatrix} 3 & 2 \\ 0 & 3 \end{pmatrix}$$

Such that:

$$q(X) \cdot (0 \ 1)^T = \begin{pmatrix} 3 & 2 \\ 0 & 3 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 2 \\ 3 \end{pmatrix}$$

3.2 Lemma: Module Hygiene

Let R be a ring, and M an R -module.

1. $0_R \cdot a = 0_M, \quad \forall a \in M$
2. $r0_M = 0_M, \quad \forall r \in R$
3. $(-r)a = r(-a) = -(ra), \quad \forall r \in R, a \in M$

3.3 Module Homomorphisms

- What is a module homomorphism?

- let R be a ring, and let M, N be R -modules
- a **R -homomorphism** is a mapping:

$$f : M \rightarrow N$$

satisfying:

$$f(a + b) = f(a) + f(b)$$

$$f(ra) = rf(a)$$

- What results from composing module homomorphisms?

- you obtain another **homomorphism**

- What is an **R -Module Isomorphism**?

- a **bijective** homomorphism

- What is the kernel of an R -homomorphism?

- the set:

$$\ker(f) = \{a \in M \mid f(a) = 0_N\} \subseteq M$$

- What is the image of an R -homomorphism?

- the set:

$$\operatorname{im}(f) = \{f(a) \mid a \in M\} \subseteq N$$

3.3.1 Examples

- the mapping $f(a) = 0_N$ is **always** an R -homomorphism
- if R is a field, module homomorphism are the standard **linear mappings**
- any **group** homomorphism between abelian groups is also a \mathbb{Z} -homomorphism
- consider $R = \mathbb{C}[X]$, and consider 2 modules:

$$M = \mathbb{C}_A^2 \quad N = \mathbb{C}_B^2$$

where:

$$A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \quad B = \begin{pmatrix} 2 & -1 \\ 4 & -2 \end{pmatrix}$$

We can then define a homomorphism:

$$f : \mathbb{C}_A^2 \rightarrow \mathbb{C}_B^2$$

defined by:

$$\underline{v} \rightarrow T\underline{v}, \quad \underline{v} \in M, T \in Mat(2; \mathbb{C})$$

Recall, multiplication in the module is defined by replacing each X in the polynomial in $\mathbb{C}[X]$ by the given matrix (A or B). Hence, the homomorphism is defined by:

$$f(X\underline{v}) = f(A\underline{v}) = T(A\underline{v})$$

But notice, this must be an element in N . By properties of homomorphisms:

$$f(X\underline{v}) = Xf(\underline{v}) = B(T\underline{v})$$

Hence, if T exists, it must satisfy:

$$TA = BT$$

Let:

$$T = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Then:

$$AT = \begin{pmatrix} 0 & a \\ 0 & c \end{pmatrix}$$

$$TB = \begin{pmatrix} 2a - c & 2b - d \\ 4a - 2c & 4b - 2d \end{pmatrix}$$

Hence, we have 4 variables, and 4 sets of linear equations:

$$2a - c = 0 \implies c = 2a$$

$$4a - 2c = 0 \implies c = 2a$$

$$4b - 2d = c$$

$$2b - d = a$$

Notice, the last 2 equations coincide with the fact that $c = 2a$. Overall, this system has infinitely many solutions, such that:

$$T = \begin{pmatrix} 2b - d & b \\ 4b - 2d & d \end{pmatrix}$$

3.3.2 Exercises (TODO)

1. Let F be a field, and let $V = F^2$ and $W = F^3$ be F -vector spaces. Define:

$$\phi = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \quad \psi = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

and consider the $F[X]$ -modules V_ϕ, W_ψ . Show that:

$$f : V_\phi \rightarrow W_\psi, \quad \begin{pmatrix} x \\ y \end{pmatrix} \rightarrow \begin{pmatrix} x \\ y \\ 0 \end{pmatrix}$$

$$f : W_\psi \rightarrow V_\phi, \quad \begin{pmatrix} x \\ y \\ x \end{pmatrix} \rightarrow \begin{pmatrix} z \\ 0 \end{pmatrix}$$

are $F[X]$ -homomorphisms

3.4 Submodules

- What are submodules?

- non-empty **subsets** of an R -module, which are themselves R -modules, with respect to the operations in the R -module

3.4.1 Examples

- a **submodule** of an F -vector space is a subspace
- the **submodules** of a \mathbb{Z} -module are the subgroups of its corresponding group
- the **submodules** of a ring are its ideals
- consider a field F and the $F[X]$ -module W_ψ defined using the matrix:

$$\psi = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

(recall W_ψ is an $F[X]$ -module, where its elements are in F^3 , and multiplication by a matrix $F[X]$ is defined as multiplication of $\underline{v} \in F^3$ by $F[\psi]$). Then the subspaces:

- $\langle \underline{e}_1 \rangle = \{0\}$
- $\langle \underline{e}_1, \underline{e}_2 \rangle = \{0\} \cup \{k\underline{e}_1 \mid k \in F\}$ (since $\phi \underline{e}_2 = \underline{e}_1$, and $\phi \underline{e}_1 = 0$)

are $F[X]$ -submodules of W_ψ , but $\langle \underline{e}_2 \rangle$ (since $\phi \underline{e}_2 = \underline{e}_1$, but \underline{e}_1 is not part of the generating set).

- again, consider:

$$R = \mathbb{C}[X] \quad M = \mathbb{C}_A^2$$

where multiplication by polynomials in M is defined by multiplying $\underline{v} \in M$ by:

$$A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

The question to consider is: the 1-d subspace of \mathbb{C}^2 given by:

$$L = \{\lambda(x, y) \mid \lambda \in \mathbb{C}\}$$

is definitely closed under addition and scalar multiplication; is it closed under multiplication by polynomials? That is, is it a submodule of M ? Consider $p(X) = \sum_{i=0}^n p_i X \in \mathbb{C}[X]$. Moreover, notice

that:

$$A^2 = \text{Mat}(0) \implies A^k = \text{Mat}(0), \quad \forall k \in [2, n]$$

Thus:

$$p(A) = p_0 I_2 + p_1 A = \begin{pmatrix} p_0 & p_1 \\ 0 & p_0 \end{pmatrix}$$

Hence, we ask whether:

$$p(A)(x, y) = \begin{pmatrix} p_0 & p_1 \\ 0 & p_0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} p_0 x + p_1 y \\ p_0 y \end{pmatrix} \in L$$

We thus need to find suitable x, y , such that:

$$\begin{pmatrix} p_0 x + p_1 y \\ p_0 y \end{pmatrix} = \begin{pmatrix} \lambda x \\ \lambda y \end{pmatrix}$$

Since the second entry only depends on y , we focus on that first. There are 2 cases to consider:

1. $y \neq 0$ In this case, and since \mathbb{C} is an integral domain, we must have that $p_0 = \lambda$. Thus, in the first entry:

$$p_0 x + p_1 y = \lambda x \implies \lambda x + p_1 y = \lambda x \implies p_1 y = 0$$

Now, since $y \neq 0$, this is only possible if $p_1 = 0$. But we need to consider every possible polynomial in $\mathbb{C}[X]$, so this is not possible. Hence, the only alternative is that $y = 0$.

2. $y = 0$ In this case, p_0 can be anything in \mathbb{C} . Then:

$$p_0 x + p_1 y = \lambda x \implies p_0 x = \lambda x \implies p_0 = \lambda$$

Thus, for any x , and for $y = 0$, L defines a submodule.

3.5 Proposition: Test for a Submodule

Let R be a **ring**, and M a module over R .
A subset $M' \subseteq M$ is a **submodule** if and only if:

1. $0_M \in M'$
2. $a, b \in M' \implies a - b \in M'$
3. $r \in R, a \in M' \implies ra \in M'$

[Proposition 3.7.20]

Proof. If M' is a submodule, these properties hold (since they are properties of modules). Alternatively, assume that M' satisfies the conditions. Then, recall the test of a (finite) subgroup. If G is a group, H is a subgroup if and only if:

- $H \neq \emptyset$
- $h, k \in H \implies hk^{-1} \in H$

Condition (1) means that M is not empty, and condition (2) ensures that $a - b \in M'$. Hence, M' is a subgroup of M . By (3), we know that we have:

$$R \times M' \rightarrow M'$$

The remaining properties of a module are satisfied by the fact that M' is a subset of M . Hence, M' must be a submodule. □

3.6 Lemma: Kernel and Image as Submodules

Let:

$$f : M \rightarrow N$$

*be a **module homomorphism**. Then:*

- $\ker(f)$ is a **submodule** of M
- $\text{im}(f)$ is a **submodule** of N

[Lemma 3.7.21]

Proof. 1. **The Kernel is a Submodule**

- since $f(0_M) = 0_N$, $0_M \in \ker(f)$
- if $a, b \in \ker(f)$ then:

$$f(a) - f(b) = 0_M \implies f(a - b) = 0 \implies a - b \in \ker(f)$$

- if $r \in R, a \in \ker(f)$:

$$rf(a) = r0_M = 0_M \implies f(ra) = 0_M \implies ra \in \ker(f)$$

Hence, by the test for a submodule, the kernel is a submodule.

2. **The Image is a Submodule**

- since $f(0_M) = 0_N$, $0_N \in \text{im}(f)$
- if $a, b \in \text{im}(f)$, then $\exists a', b' \in M$ such that:

$$f(a') = a \quad f(b') = b$$

But then, by properties of the homomorphism:

$$f(a' - b') = a - b$$

Since $a' - b' \in M$ (by definition of a module), it follows that $a - b \in N$

- if $r \in R, a \in \text{im}(f)$, then $\exists a' \in M$ such that:

$$f(a') = a$$

But then:

$$rf(a') = ra \implies f(ra') = ra$$

so $ra \in \text{im}(f)$

Hence, by the test for a submodule, the image is a submodule. □

3.7 Lemma: Injectivity and Kernel

Let R be a **ring**, with M, N as R -**modules**.

Let:

$$f : M \rightarrow N$$

be a **module homomorphism**. Then, f is injective **if and only if**:

$$\ker(f) = \{0_M\}$$

[Lemma 3.7.22]

Proof. This follows directly from the fact that this property is true for group homomorphisms. □

3.8 Generating Submodules

- **What is a generated module?**
 - consider a ring R , with R -module M , and a subset $T \subseteq M$
 - the **submodule of M generated by T** is the submodule:

$${}_R\langle T \rangle = \left\{ \sum_{i=1}^m r_i t_i \mid r_i \in R, t_i \in T \right\}$$

- if $T = \emptyset$, then ${}_R\langle T \rangle$ contains 0_M

- **What is a finitely generated module?**

- a **module** generated by a **finite set**:

$$M = {}_R\langle T \rangle$$

- **What is a cyclic module?**

- a **module** generated by a **single element**:

$$M = {}_R\langle t \rangle, \quad t \in M$$

3.8.1 Examples

- a **cyclic** \mathbb{Z} -module is equivalent to a **cyclic abelian group**
- the **ideal** generated by a subset T of a **commutative ring** R is equivalent to a **submodule** of R generated by T
- a **principal ideal** of R is equivalent to a **cyclic submodule** of R
- if F is a field, and W_ψ is defined as above, then w_ψ is a **cyclic** $F[X]$ -module generated by e_3
- 0_M **generates** a **cyclic submodule** $\{0_M\}$ of **any** module

3.9 Lemma: Smallest Submodule Containing a Subset

If $T \subseteq M$, then:

$${}_R\langle T \rangle$$

is the **smallest submodule** of M containing T . [Lemma 3.7.28]

3.10 Lemma: Intersection of Submodules

The **intersection** of any **collection of modules** is a **module**. [Lemma 3.7.29]

3.11 Lemma: Addition of Submodules

If M_1, M_2 are **submodules** of M , then:

$$M_1 + M_2 := \{m_1 + m_2 \mid m_1 \in M_1, m_2 \in M_2\}$$

is also a **submodule** of M . [Lemma 3.7.30]

3.12 Theorem: Factor Modules

- What are cosets in modules?

– let:

- * R be a **ring**
- * M be a **module**
- * N a **submodule** of M

– similarly to before, we can define an **equivalence relation**:

$$a \sim b \iff a - b \in N, \quad a, b \in M$$

– for $a \in M$, the **equivalence class** of this relation is the **coset of a with respect to N in M** :

$$E(a) = a + N = \{a + n \mid n \in N\}$$

- **How are factor modules defined?**

- the **factor of M by N** (or the **quotient of M by N** is the set:

$$M/N = M/\sim$$

of all cosets/equivalence classes of N in M .

3.12.1 Examples

Let $R = \mathbb{R}$, $M = \mathbb{R}^4$ and:

$$N = \{(x_1, x_2, x_3, x_4) \mid x_1 = 2x_3, x_2 = 4x_4\}$$

What is M/N ? We know its an R module over a field, so M/N is a vector space. First, lets consider what the bases of M, N are. For N its simple:

$$\{(2, 0, 1, 0), (0, 4, 0, 1)\}$$

For M , we can extend the basis for N :

$$\{(2, 0, 1, 0), (0, 4, 0, 1), (1, 0, 0, 0), (0, 1, 0, 0)\}$$

Indeed, this is a basis, since the vectors are linearly independent, and:

$$(x_1, x_2, x_3, x_4) = x_3(2, 0, 1, 0) + x_4(0, 4, 0, 1) + (x_1 - 2x_3)(1, 0, 0, 0) + (x_2 - 4x_4)(0, 1, 0, 0)$$

Now, recall that:

$$a \sim b \iff a - b \in N$$

We claim that a basis for M/N is given by:

$$\{(1, 0, 0, 0) + N, (0, 1, 0, 0) + N\}$$

For this we need 2 things:

1. **Generation** Take any element in M/N :

$$(x_1, x_2, x_3, x_4) + N$$

Then, it is clear that:

$$((x_1, x_2, x_3, x_4) + N) - (((x_1 - 2x_3)(1, 0, 0, 0) + N) + ((x_2 - 4x_4)(0, 1, 0, 0) + N)) = (x_3(2, 0, 1, 0) + N) + (x_4(0, 4, 0, 1) + N)$$

But notice, $\{(2, 0, 1, 0), (0, 4, 0, 1)\}$ is a basis for N , so:

$$((x_1, x_2, x_3, x_4) + N) - (((x_1 - 2x_3)(1, 0, 0, 0) + N) + ((x_2 - 4x_4)(0, 1, 0, 0) + N)) \in N$$

or in other words, $(x_1, x_2, x_3, x_4) + N$ and $((x_1 - 2x_3)(1, 0, 0, 0) + N) + ((x_2 - 4x_4)(0, 1, 0, 0) + N)$ are equivalent in the cosets, so:

$$(x_1, x_2, x_3, x_4) + N = ((x_1 - 2x_3)(1, 0, 0, 0) + N) + ((x_2 - 4x_4)(0, 1, 0, 0) + N)$$

Hence, any element in M/N is generated by our claimed basis.

2. **Linear Independence** It is clear that if:

$$(\alpha(1, 0, 0, 0) + \beta(0, 1, 0, 0)) + N = (0, 0, 0, 0) + N$$

we can only have $\alpha = \beta = 0$, so the generating set is linearly independent.

3.13 Theorem: Factor Module Operations

Let R be a ring, and let M, N be R -modules. For $a, b \in M$ and $r \in R$. For the **factor module** M/N , define **addition** via:

$$(a + N) + (b + N) = (a + b) + N \quad E(a) + E(b) = E(a + b)$$

and **multiplication** via:

$$r(a + N) = (ra) + N$$

[Theorem 3.7.31]

Proof. As before, we need to show that not only M/N is a module, but also that **addition** and **multiplication** are **well-defined**.

Addition is well-defined, since additively, modules are abelian groups, so the proof for **factor rings** applies.

For multiplication, consider $a, b \in M$, such that:

$$E(a) = E(b)$$

We need to show that:

$$rE(a) = rE(b)$$

By properties of modules, this means that $a \sim b \implies a - b \in N$. Again by properties of modules, $r(a - b) \in N \implies ra - rb \in N$. Hence:

$$E(ra) = E(rb) \iff rE(a) = rE(b)$$

Thus, multiplication is **well-defined**.

Lastly, we check that addition defines a group:

- $E(0) + E(a) = E(0 + a) = E(a) = E(a + 0) = E(a) + E(0)$
- $E(a) + E(-a) = E(a - a) = E(0)$

Hence, M/N is indeed a module.

□

3.14 Theorem: The Universal Property of Factor Modules

Let R be a **ring**, with L and M as R -modules. Let N be a **submodule** of M .

Then:

1. The **canonical mapping**:

$$\text{can} : M \rightarrow M/N$$

$$\text{can}(a) = E(a) = a + N, \quad \forall a \in M$$

is a **surjective R -module homomorphism**, with:

$$\ker(\text{can}) = N$$

2. If:

$$f : M \rightarrow L$$

is an **R -homomorphism** with:

$$f(N) = \{0_L\}$$

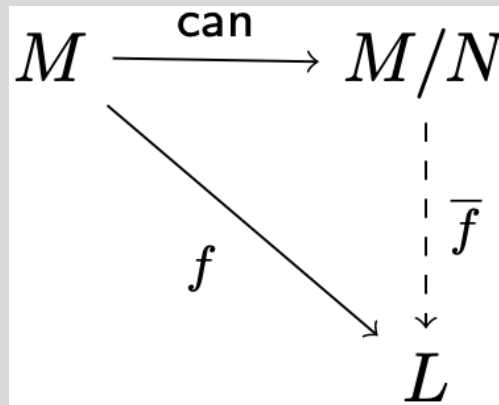
(so then $N \subseteq \ker(f)$), then there is a **unique homomorphism**:

$$\bar{f} : M/N \rightarrow L$$

$$\bar{f}(E(a)) = f(a), \quad \forall a \in M$$

such that:

$$f = \bar{f} \circ \text{can}$$



[Theorem 3.7.32]

Proof. The proof is completely analogous to the proof of the **universal property of factor rings** (2.7) □

3.15 Theorem: First Isomorphism Theorem for Modules

Let R be a **ring**, and let M, N be R -**modules**
Then, every R -**homomorphism**:

$$f : M \rightarrow N$$

induces an R -**isomorphism**:

$$\bar{f} : (M/\ker(f)) \rightarrow \text{im}(f)$$

[Theorem 3.7.33]

Proof. Again, completely analogous to that of the **first isomorphism theorem for rings** (2.8) □

3.16 Remark: First Isomorphism Theorem for Vector Spaces

If we pick $R = F$ to be a field, then the above gives us the **First Isomorphism Theorem for Vector Spaces**.

Similarly to before, we can show that:

$$\dim(M/\ker(f)) = \dim(M) - \dim(\ker(f))$$

Moreover, due to the isomorphism $\bar{f} : (M/\ker(f)) \rightarrow \text{im}(f)$ we know that:

$$\dim(M/\ker(f)) = \dim(\text{im}(f))$$

which gives us another proof of the **rank-nullity theorem**. [Remark 3.7.34]

3.17 Remark: First Isomorphism Theorem for Abelian Groups

If we pick $R = \mathbb{Z}$, then the above gives us the **First Isomorphism Theorem for Abelian Groups**, a special case of the **First Isomorphism Theorem for Groups**. [Remark 3.7.35]

1. Let N, K be submodules of an R -module M . Show that K is a submodule of $N + K = \{b + c \mid b \in N, c \in K\}$ and $N \cap K$ is a submodule of N . Show further that:

$$\frac{N + K}{N} \cong \frac{N}{N \cap K}$$

This is the *Second Isomorphism Theorem for Modules*

2. Let N, K be submodules of an R -module M , where $K \subseteq N$. Show that N/K is a submodule of M/K , and that:

$$\frac{M/K}{N/K} \cong M/N$$

This is the *Third Isomorphism Theorem for Modules*

4 Workshop

1. True or false. Although \mathbb{Q} is not algebraically closed, the set:

$$\mathbb{Q}[\sqrt{-1}] = \{a + b\sqrt{-1} \mid a, b \in \mathbb{Q}\}$$

(a subset of \mathbb{C}) is algebraically closed.

This is false. Consider $X^2 - 2$. This only has roots $X = \pm\sqrt{2}$, but neither of these roots are in $\mathbb{Q}[\sqrt{-1}]$, so this field isn't algebraically closed.

2. Define an equivalence relation \sim on \mathbb{R} by:

$$x \sim y \text{ if and only if } x - y \in \mathbb{Z}$$

Let $E(x)$ denote the equivalence class containing $x \in \mathbb{R}$. Which of the following operations are well-defined where $x, y \in \mathbb{R}$?

(a) $E(x) \rightarrow e^{2\pi\sqrt{-1}x}$

Assume that $x \sim y$ (that is, $E(x) = E(y)$). When $\exists z \in \mathbb{Z}$ such that $y = x + z$. Then, this mapping is well defined if:

$$e^{2\pi\sqrt{-1}x} = e^{2\pi\sqrt{-1}y}$$

We compute:

$$e^{2\pi\sqrt{-1}y} = e^{2\pi\sqrt{-1}(x+z)} = e^{2\pi\sqrt{-1}x} e^{2\pi\sqrt{-1}z} = e^{2\pi\sqrt{-1}x}$$

where we use the fact that $z \in \mathbb{Z}$ and so $e^{2\pi\sqrt{-1}z} = 1$

(b) $(E(x), E(y)) \rightarrow E(x + y)$

This mapping is well defined if we can show that:

$$(E(x), E(y)) = (E(x'), E(y')) \implies E(x + y) = E(x' + y')$$

Notice:

$$E(x) = E(x') \implies x - x' = z \in \mathbb{Z}$$

$$E(y) = E(y') \implies y - y' = w \in \mathbb{Z}$$

Now, consider:

$$(x + y) - (x' + y') = (x - x') + (y - y') = z + w \in \mathbb{Z}$$

Thus:

$$(x + y) - (x' + y') \in \mathbb{Z} \implies E(x + y) = E(x' + y')$$

$$(c) (E(x), E(y)) \rightarrow E(xy)$$

Operating similarly as above, consider:

$$xy - x'y'$$

If this difference is an integer, then $E(xy) = E(x'y')$, where:

$$E(x) = E(x') \implies x - x' = z \in \mathbb{Z}$$

$$E(y) = E(y') \implies y - y' = w \in \mathbb{Z}$$

Thus:

$$x'y' = (x + z)(y + w) = xy + zy + zw + xw$$

Hence:

$$xy - x'y' = -(zy + xw + zw)$$

This need not be an integer. For example, picking rational x, y can ensure this. Indeed, if $x = \frac{3}{2}$ and $y = \frac{1}{2}$, then $x - y \in \mathbb{Z}$. Then:

$$\left(E\left(\frac{1}{2}\right), E\left(\frac{1}{2}\right) \right) \rightarrow E\left(\frac{1}{4}\right)$$

but

$$\left(E\left(\frac{3}{2}\right), E\left(\frac{1}{2}\right) \right) \rightarrow E\left(\frac{3}{4}\right)$$

and:

$$E\left(\frac{3}{4}\right) \neq E\left(\frac{1}{4}\right)$$

since:

$$\frac{3}{4} - \frac{1}{4} = \frac{1}{2} \notin \mathbb{Z}$$

3. **Let:**

$$I = \mathbb{C}[X] \langle X^2 + 1 \rangle$$

the principal ideal of $\mathbb{C}[X]$ generated by $X^2 + 1$. Is the factor ring $\mathbb{C}[X]/I$ an integral domain?

This question relies on having a strong understanding of all the concepts involved.

- *I is the ideal containing all the polynomials which have $X^2 + 1$ as a factor*
- *$\mathbb{C}[X]/I$ is a quotient ring, with 0 element $E(0)$ given by I : that is, $E(0)$ is the set of polynomials with $X^2 + 1$ as a factor*
- *an **integral domain** is a non-zero commutative ring that has no zero-divisors; that is, multiplying non-zero elements together never produces the 0 element*

This claim is False. This is because we can find non-zero elements in $\mathbb{C}[X]/I$ which when multiplied produce $E(0)$.

Notice, we can write:

$$X^2 + 1 = (X + \sqrt{-1})(X - \sqrt{-1})$$

This means that:

$$E(X + \sqrt{-1})E(X - \sqrt{-1}) = E(X^2 + 1) = E(0)$$

We just need to show that neither of the two are 0. This is clear, since these are both polynomials of degree 1. The ideal I contains only elements of degree at least 2 (since they are obtained by multiplying non-zero polynomials by $X^2 + 1$, and since \mathbb{C} is an integral domain, if $P = Q(X)(X^2 + 1)$ then $\deg(P) = \deg(Q) + 2 \geq 2$). Hence, $E(X + \sqrt{-1}) \neq E(0), E(X - \sqrt{-1}) \neq E(0)$.

4. Let $n \in \mathbb{Z}$ with $n \geq 2$ and let $I = {}_{\mathbb{Z}[X]}\langle n, X \rangle$, an ideal of $\mathbb{Z}[X]$. Show that $\mathbb{Z}[X]/I$ is isomorphic to \mathbb{Z}_n

We need to realise 2 things:

- *I is an ideal generated by using combinations of the constant polynomial n and the linear polynomial X*
- *to show the isomorphic nature of the 2 rings, we first need to come up with a ring homomorphism ($f : \mathbb{Z}[X] \rightarrow \mathbb{Z}_n$) which must be surjective, so that $\text{im}(f) = \mathbb{Z}_n$. Then, if we can show that $I = \ker(f)$ then f leads to an isomorphism from $\mathbb{Z}[X]/I$ to \mathbb{Z}_n .*

$\mathbb{Z}[X]$ is the ring of polynomials with integer coefficients. It makes intuitive sense to define a mapping:

$$f(a_n X^n + \dots + a_0) = \overline{a_0}$$

We verify that it is a ring homomorphism. Consider 2 polynomials:

$$P(X) = \sum_{i=0}^n a_i X^i \quad P(X) = \sum_{i=0}^n b_i X^i$$

Then:

$$f(P + Q) = f\left(\sum_{i=0}^n (a_i + b_i) X^i\right) = \overline{a_i + b_i} = \overline{a_i} + \overline{b_i} = f(P) + f(Q)$$

$$f(PQ) = \overline{a_i b_i} = \overline{a_i} \overline{b_i} = f(P)f(Q)$$

Moreover, f is clearly surjective, since if $\bar{x} \in \mathbb{Z}_n$ then the constant polynomial $P(X) = x$ is such that:

$$f(P) = \bar{x}$$

The final step is to show that $I = \ker(f)$. It is clear that $I \subseteq \ker(f)$, since:

$$f(n) = \bar{n} = \bar{0}$$

$$f(X) = f(X + 0) = \bar{0}$$

Now, suppose that:

$$P(X) = \sum_{i=0}^n a_i X^i \quad P(X) = \sum_{i=0}^n b_i X^i \in \ker(f)$$

This means that:

$$a_0 = nz, \quad z \in \mathbb{Z}$$

since then $f(nz) = \bar{0}$. But then:

$$P(X) = nz + X \left(\sum_{i=0}^{n-1} a_{i+1} X^i \right)$$

so clearly:

$$P(X) \in I \implies \ker(f) \subseteq I$$

Hence, $I = \ker(f)$. Then, by the first isomorphism Theorem we have that:

$$\mathbb{Z}[X]/\ker(f) \cong \text{im}(f) \implies \mathbb{Z}[X]/I \cong \mathbb{Z}_n$$

5. Let V be the real vector space of polynomials $\mathbb{R}[X]_{<4}$ of degree less than 4. Let:

$$U = \{P \in V \mid P(3) = 0\}$$

(a) Show that U is a subspace of V .

We check the 3 properties of a subspace:

① Contains 0 Element

If $P(X) = 0$, then clearly $P(3) = 0$, so $0 \in U$.

② Closed Under Addition

Let $P(X), Q(X) \in U$. Then:

$$(P + Q)(3) = P(3) + Q(3) = 0 \implies P + Q \in U$$

③ Closed Under Scalar Multiplication

Let $P(X) \in U, \lambda \in \mathbb{R}$. Then:

$$(\lambda P)(3) = \lambda P(3) = 0 \implies \lambda P \in U$$

Hence, it follows that U is a subspace of V .

(b) Find a basis for U and extend it to a basis for V . Express $P \in V$ explicitly in terms of this basis.

When I did this, as a basis I picked:

$$\{(X - 3), (X - 3)^2, (X - 3)^3\}$$

which certainly worked, but it makes the calculations a bit harder. The solutions pick a simpler basis, so I will use their answers below.

As a basis we can pick:

$$\{(X - 3), X(X - 3), X^2(X - 3)\} = \{X - 3, X^2 - 3X, X^3 - 3X^2\}$$

Clearly, each element is linearly independent (they differ by factors of X). Intuitively, it will span, since any linear combination of these will have 3 as a root. In particular, consider $P \in U$, then, we can write:

$$\begin{aligned} P(X) &= (aX^2 + bX + c)(X - 3) \\ &= aX^3 - 3aX^2 + bX^2 - 3bX + cX - 3c \\ &= a(X^3 - 3X^2) + b(X^2 - 3X) + c(X - 3) \end{aligned}$$

so the set is spanning.

Again, it is intuitive that to produce a basis of P , we just need control over the constant term (since the current basis already “handles” all the powers of X , except for 0). Hence, for P , we consider the basis:

$$\{1, X - 3, X^2 - 3X, X^3 - 3X^2\}$$

Now, consider $P \in V$. Then:

$$\begin{aligned} P &= aX^3 + bX^2 + cX + d \\ &= aX^3 - 3aX^2 + 3aX^2 + bX^2 + cX + d \\ &= a(X^3 - 3X^2) + (3a + b)X^2 + cX + d \\ &= a(X^3 - 3X^2) + (3a + b)X^2 - 3(3a + b)X + 3(3a + b)X + cX + d \\ &= a(X^3 - 3X^2) + (3a + b)(X^2 - 3X) + (9a + 3b + c)X + d \\ &= a(X^3 - 3X^2) + (3a + b)(X^2 - 3X) + (9a + 3b + c)X - 3(9a + 3b + c) + 3(9a + 3b + c) + d \\ &= a(X^3 - 3X^2) + (3a + b)(X^2 - 3X) + (9a + 3b + c)(X - 3) + (27a + 9b + 3c + d) \end{aligned}$$

So we can see that this basis is LiD and spans V , as required.

Using my basis, these calculations were a true pain, but I got very similar results (albeit not checked, so just stick to the above).

(c) **Write down a basis for V/U .**

This is very similar to an exercise for the notes, which tells us that the basis for V/U is obtained by applying the canonical mapping to the elements used to extend U to V .

We claim that:

$$\{1 + U\}$$

is a basis for V/U .

To verify this, consider $P + U \in V/U$. In particular, by the exercise above, we know that we can find $a, b, c, d \in \mathbb{R}$ such that:

$$P = a(X^3 - 3X^2) + b(X^2 - 3X) + c(X - 3) + d = (X - 3)(aX^2 + bX + c) + d$$

Then, it is clear that:

$$P + U = d + U = d(1 + U)$$

Hence, the basis spans V/U . Moreover, it contains a single element, so it is linearly independent.

(d) **Write down the matrix that represents the canonical mapping:**

$$can : V \rightarrow V/U$$

which sends P to $P + U$, in terms of the (ordered) basis $\{X^3, X^2, X, 1\}$ of V , and the one you chose in (3) for V/U .

We have that $(1 + U)$ is the basis vector of V/U . Recall, the representing matrix of the mapping is defined by the coefficients used to write $can(P)$ in terms of $(1 + U)$. Notice, in part b), we showed that:

$$P(X) = aX^3 + bX^2 + cX + d$$

can be written as:

$$P(X) = a(X^3 - 3X^2) + (3a + b)(X^2 - 3X) + (9a + 3b + c)(X - 3) + (27a + 9b + 3c + d)$$

This is great, since then:

$$can(P) = P + U = (27a + 9b + 3c + d) + U$$

Hence, we compute:

$$can(1) = 1 + U = 1(1 + U)$$

If we set $c = 1$, and everything else to 0:

$$can(X) = X + U = 3 + U = 3(1 + U)$$

If we set $b = 1$, and everything else to 0:

$$can(X^2) = X^2 + U = 9 + U = 9(1 + U)$$

If we set $a = 1$, and everything else to 0:

$$can(X^3) = X^3 + U = 27 + U = 27(1 + U)$$

Hence, we get that the representing matrix is:

$${}_{\{1+U\}}[can]_{\{X^3, X^2, X, 1\}} = \begin{pmatrix} 27 & 9 & 3 & 1 \end{pmatrix}$$