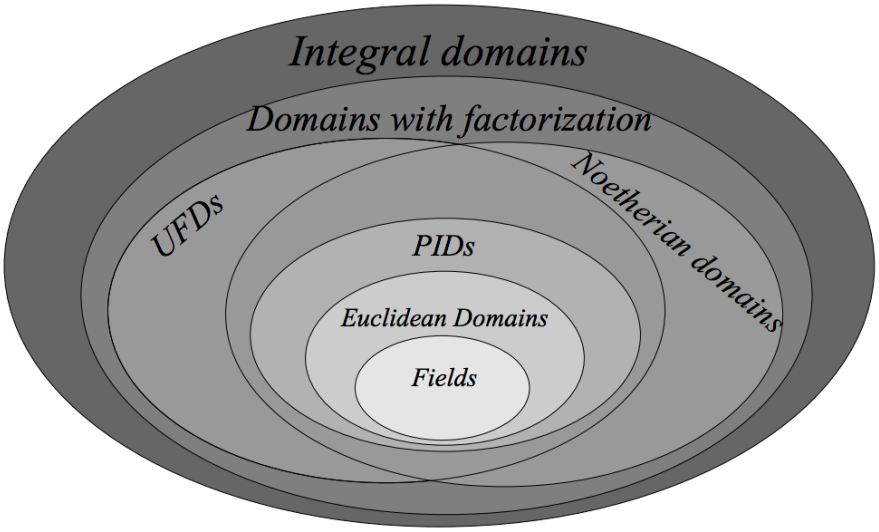
Math 28B: Introduction to Rings and Fields

Typed by Hussein Hijazi

Spring 2021



Disclaimer: These notes are typeset versions of the recorded lectures and are often modified with my own exposition to help clarify and understand ideas professed in the lectures. All errors in these notes are (almost surely) mine and are thus my responsibility. The permanent link to this document is found on https://hushus46.github.io/28B-Notes

I try my best to keep the multiplication of ring elements (with the $\cdot$ operation) explicit, but sometimes I have left it out unintentionally as the notes were typed (this happens more often in earlier lectures). The spacing of nested proofs and claims can be a bit awkward; occasionally, I will go back through the notes to make it more readable.

The table of contents is set up to easily navigate between presented ideas, although I haven't been able to think of titles for everything. **Anytime** you see phrases or words in blue like this (other than literally now), it is a link to take you to some part of the notes being referenced, or an external URL. If it is a reference within the notes, you will be referred to it and will begin at the top of your screen. If there are any mathematical typos/errors or suggestions on design changes and theorem names, please do not hesitate to let me know.

Table of Contents

L1: Definitions and Examples of Rings

Definition 1.1: Rings and Fields

A **ring** R is a set with two binary operations $+, \cdot$ (addition and multiplication), i.e

$$+ : R \times R \to R$$
$$\cdot : R \times R \to R$$

such that:

(i) $(R, +)$ is an **abelian group**, i.e

- (Additive Identity) There exists a unique $0_R \in R$, such that $\forall a \in R$
$$a + 0_R = 0_R + a = a$$
- (Additive Inverse) $\forall a \in R$ there exists a unique $(-a) \in R$ such that
$$a + (-a) = (-a) + a = 0_R$$
- (Associativity) For all $a, b, c \in R$, $(a + b) + c = a + (b + c)$
- (Commutativity) For all $a, b \in R$, $a + b = b + a$

(ii) $\cdot$ is **associative**, i.e $\forall a, b, c \in R$
$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$

(iii) $\cdot$ is **distributive** over $+$, i.e $\forall a, b, c \in R$
$$a \cdot (b + c) = a \cdot b + a \cdot c$$

Now we see variations and the extension of a ring, the field:

- We say R has an **identity element**, 1_R, if there exists a $1_R \in R$ such that $\forall a \in R$
$$a \cdot 1_R = 1_R \cdot a = a$$
- We say R is **commutative** if $\forall a, b \in R$
$$a \cdot b = b \cdot a$$
- If R is a commutative ring with $1_R \neq 0_R$,then we say R is a **field** if every non-zero element has a multiplicative inverse, i.e $\forall a \neq 0 \in R, \exists\, a^{-1} \in R$ such that
$$a \cdot (a^{-1}) = (a^{-1}) \cdot a = 1_R$$

For the rest of the notes, I will omit the R subscript from the additive and multiplicative identity, unless necessary. Anyways, now we can look at some examples of rings:

Example 1.1. $(\mathbb{Z}, +, \cdot)$, The integers with the usual addition and multiplication is a ring.

Example 1.2. $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$ are fields.

Example 1.3. $(\mathbb{N}, +, \cdot)$ is **not** a ring, since there are no additive inverses.

Example 1.4. $(\mathbb{R}^3, +, \cdot)$ is **not** a ring. It has addition $\mathbf{v}, \mathbf{w} \in \mathbb{R}^3 \Rightarrow \mathbf{v} + \mathbf{w} \in \mathbb{R}^3$, but no proper multiplication operator. You can check that the cross product, $\times$, not distributive.

Definition 1.2: Unit

We say $a \in R$ is a **unit** if there exists a $b \in R$ such that $a \cdot b = b \cdot a = 1$.
Basically, a unit is an element whose multiplicative inverse is also in the ring.

Example 1.5. In $\mathbb{R}$, every element except 0 is a unit.

Example 1.6. In $\mathbb{Z}$, the only units are $\{1, -1\}$.

Now let us look at examples of rings other than the standard number types $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$:

Example 1.7. The integers modulo n are also a ring. This set is written as $\mathbb{Z}/n\mathbb{Z}$. To understand this, first define the set of multiples of an integer n as

$$n\mathbb{Z} \coloneqq \{n \cdot a | a \in \mathbb{Z}\}$$

Then,

$$\mathbb{Z}/n\mathbb{Z} \coloneqq \mathbb{Z}/\sim$$

where $\sim$ is the equivalence relation for $x, y \in \mathbb{Z}$

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

which basically means two integers are equivalent if their difference is a multiple of n. Think about it like this, if x and y are multiples of n plus the same remainder, i.e

$$x = nk + r \quad y = nl + r$$

for some $k, l \in \mathbb{Z}$ then their difference is exactly a multiple of n,

$$x - y = nk + r - (nl + r) = n(k - l) = nm$$

for $m \in \mathbb{Z}$. They are equivalent in the sense of producing the same remainder when n is divided by them. This can be written in modulo arithmetic as

$$x \equiv y \pmod{n}$$

So, $\mathbb{Z}/n\mathbb{Z}$ will contain equivalence classes of remainders when dividing any integer by n, and each of these classes contain all integers that produce such remainder

$$\mathbb{Z}/n\mathbb{Z} \coloneqq \{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{n-1}\}$$

The numbers with bars indicate the equivalence classes generated when taking the integers modulo n. For example $\mathbb{Z}/3\mathbb{Z}$ are the integers modulo 3

$$\mathbb{Z}/3\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}\}$$

where

$$\overline{0} = \{0, 3, 6, 9, \dots\}$$
$$\overline{1} = \{1, 4, 7, 10, \dots\}$$
$$\overline{2} = \{2, 5, 8, 11, \dots\}$$

Now, if $\overline{a}, \overline{b} \in \mathbb{Z}/n\mathbb{Z}$ and $a \in \overline{a}, b \in \overline{b}$ then we define

$$\overline{a} + \overline{b} = \overline{a + b}, \quad \overline{a} \cdot \overline{b} = \overline{a \cdot b}$$

This set with the two operations is a ring. (Exercise to show these operations are well defined).

Example 1.8. We can also have a rings of functions. Let R be a ring and X a set, define the set $\mathfrak{F}$

$$\mathcal{F} \coloneqq \{f : X \to R\}$$

which is the set of functions which take elements of the set X to elements of the ring R. Then

$$\begin{aligned} (f+g) :& X \to R \\ & x \mapsto f(x) + g(x) \end{aligned} \qquad \begin{aligned} (f \cdot g) :& X \to R \\ & x \mapsto f(x) \cdot g(x) \end{aligned}$$

are operations which with $\mathfrak{F}$, form a ring.

Example 1.9. Define the set of continuous functions on the closed interval $[0, 1]$

$$C[0,1] \coloneqq \{f : [0,1] \to \mathbb{R} | f \text{ continuous}\}$$

We know from calculus that if $f, g \in C[0,1]$, then $f + g$ and $f \cdot g$ are also in $C[0,1]$.
Hence, $C[0,1]$ is a ring.

Example 1.10. Sets of matrices can also be rings. Define

$$M_n(\mathbb{R}) \coloneqq \{n \times n \text{ matrices with real coefficients}\}$$

Then for matrices A, B:

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}, B = \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \cdots & b_{nn} \end{pmatrix}$$

we have

$$A + B \coloneqq \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} & \cdots & a_{1n} + b_{1n} \\ a_{21} + b_{21} & a_{22} + b_{22} & \cdots & a_{2n} + b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} + b_{n1} & a_{n2} + b_{n2} & \cdots & a_{nn} + b_{nn} \end{pmatrix}$$

$$A \cdot B \coloneqq (a_{ik} \cdot b_{ki})$$

In the product, the notation indicates that each element is the dot product of a row vector in A and a column vector in B (the variable i indicates the ith row and ith column, while the k varies to multiply the kth element of each vector). This is the usual matrix multiplication we are all aware of.
Also, the additive and multiplicative identity are

$$0 = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}, 1 = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

L2: More Examples

Let's see some basic properties of a ring R:

(i) $0 \cdot a = a \cdot 0 = 0, \quad \forall a \in R$

> ***Proof.*** Let a be in R, then:
> $$\begin{aligned} 0 = 0 + 0 \Rightarrow & 0 \cdot a = (0 + 0) \cdot a \\ \Rightarrow & 0 \cdot a = 0 \cdot a + 0 \cdot a \\ \Rightarrow & 0 \cdot a + (-0 \cdot a) = 0 \cdot a + 0 \cdot a + (-0 \cdot a) \\ \Rightarrow & 0 = 0 \cdot a \end{aligned}$$
> ■

(ii) $(-a) \cdot b = a \cdot (-b) = -(a \cdot b), \quad \forall a, b \in R$

> ***Proof.*** Let a, b be in R, then:
> $$a \cdot b + -(a \cdot b) = 0 \quad \text{(by definition)}$$
> then
> $$\begin{aligned} & a \cdot b + (-a) \cdot b = (a + (-a)) \cdot b = 0 \cdot b = 0 \\ \Rightarrow & -(a \cdot b) = (-a) \cdot b \end{aligned}$$
> ■

(iii) $(-a) \cdot (-b) = a \cdot b, \quad a, b \in R$

> ***Proof.*** Let a, b be in R, then:
> $$(-a) \cdot (-b) = -(a \cdot (-b)) = -(-(a \cdot b))$$
> But by definition we of additive inverse:
> $$-(-(a \cdot b)) + (-(a \cdot b)) = 0$$
> So
> $$(-a) \cdot (-b) = -(-(a \cdot b)) = a \cdot b$$
> ■

(iv) If R has 1, then 1 is unique and $(-a) = (-1) \cdot a$

> ***Proof.*** First, the multiplicative identity. Assume 1 and $1'$ are distinct identities. But
> $$1 = 1 \cdot 1' = 1'$$
> So, in fact, they are the same and it is unique.
> Now, by definition additive inverses are unique, so $-a = (-1) \cdot a$ must both sum with a to 0. We check
> $$a + (-1) \cdot a = 1 \cdot a + (-1) \cdot a = (1 + (-1)) \cdot a = 0 \cdot a = 0$$
> which confirms it.
> ■

Definition 2.1: Zero Divisor

We say a non-zero element $a \in R$ is a **zero divisor** if $\exists b \neq 0$ such that $a \cdot b = 0$

Example 2.1. Recall that $M_2(\mathbb{R})$ is the set of 2x2 matrices with real valued entries and $0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. Then,

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

implies $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ is a zero divsor.

Example 2.2. Let $\mathbb{Z}/6\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$. Then

$$\overline{2} \cdot \overline{3} = \overline{0}$$

implies $\overline{2}$ is a zero divisor.

Claim: If $\overline{0} \neq \overline{a} \in \mathbb{Z}/n\mathbb{Z}$ is not a zero divisor, then it is a unit.

Proof. Let $a \in \mathbb{Z}$ with $a \neq 0$ be relatively prime to n. Then Euclid's algorithm (more specifically Bezout's Identity) constructs $x, y \in \mathbb{Z}$ such that

$$a \cdot x + n \cdot y = 1 \implies \overline{a} \cdot \overline{x} = \overline{1}$$

Hence, $\overline{a}$ is a unit.
On the other hand, if $\gcd(a, n) > 1$, then let $\gcd(a, n) = d$. Hence, since n is a multiple d we can write for some $q, k \in Z$

$$n = d \cdot q \quad a = d \cdot k$$

Then,

$$\overline{a} \cdot \overline{q} = \overline{a \cdot q} = \overline{d \cdot k \cdot q} = \overline{n \cdot k} = \overline{n} = \overline{0}$$

Thus, $\overline{a}$ is a zero divisor. ■

Corollary 2.2: $\mathbb{Z}/n\mathbb{Z}$ is a field for prime n

If n is prime, then $\mathbb{Z}/n\mathbb{Z}$ is a field.

Proof. If $0 < m < n$ and n is prime, then $\gcd(m, n) = 1$. From the previous claim, this would mean every element is a unit and therefore $\mathbb{Z}/n\mathbb{Z}$ is a field. ■

Example 2.3. $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}$ are fields but $\mathbb{Z}/4\mathbb{Z}$ is not (since $\overline{2} \cdot \overline{2} = \overline{0}$, therefore $\overline{2}$ is a zero divisor and not a unit).

Claim: If $a \in R$ is a zero divisor, then it is not a unit

Proof. Let $b \neq 0$ and $a \cdot b = 0$.
Assume $\exists c \in R$ such that $a \cdot c = 1 = c \cdot a$, then

$$c \cdot a \cdot b = c \cdot (a \cdot b) = c \cdot 0 = 0$$

but similarly,

$$c \cdot a \cdot b = (c \cdot a) \cdot b = 1 \cdot b = b$$

contradicting the fact of $b \neq 0$. Hence our assumption is wrong and a is not a unit. ■

Definition 2.3: Group of Units

If R is a ring with $1 \neq 0$, we denote the set of units by

$$R^\times := \{a \in R | \exists b \in R \quad a \cdot b = b \cdot a = 1\}$$

Claim: $(R^\times, \cdot)$ is a group.

Proof. We check the properties of a group

(i) $1 \in R^\times \quad (1 \cdot 1 = 1)$

(ii) $\forall a \in \mathbb{R}^\times$, $a \cdot 1 = 1 \cdot a = a$

(iii) Associativity follows since $\cdot$ is associative in R

(iv) $\forall a \in R^\times$, by the definition of $R^\times$ there exists $b \in R$ such that

$$a \cdot b = b \cdot a = 1$$

but this is the same as

$$b \cdot a = a \cdot b = 1$$

hence b, the inverse of a, is also a unit and therefore $b \in R^\times$ ■.

A field F is a commutative ring with $1 \neq 0$ such that $F^\times = F \setminus \{0\}$

Definition 2.4: Integral Domain

We say a commutative ring R with $1 \neq 0$ is an **integral domain** if it has no zero divisors

Example 2.4. $\mathbb{Z}/4\mathbb{Z}$ is **not** an integral domain. ($\overline{2} \cdot \overline{2} = \overline{0} \implies \overline{2}$ is a zero divisor)

Example 2.5. $M_2(\mathbb{R})$ is **not** an integral domain. Then,

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

implies $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ is a zero divsor.

Example 2.6. $\mathbb{Z}$ is an integral domain,

Proposition 2.5: Cancellation Law

Let R be a ring and $a, b, c \in R$.
Suppose a is not a zero divisor, then

$$ab = ac \implies b = c$$

Proof. If $a \neq 0$, then $a \cdot (b - c) = 0$. Since we supposed a is not a zero divisor then it must be

$$b - c = 0 \implies b = c$$

■

Example 2.7. To show why a must **not** be a zero divisor, consider $\mathbb{Z}/4\mathbb{Z}$. We have $\overline{2} \cdot \overline{2} = \overline{0}$ and $\overline{2} \cdot \overline{0} = \overline{0}$. So

$$\overline{2} \cdot \overline{2} = \overline{2} \cdot \overline{0}$$

but

$$\overline{2} \neq \overline{0}$$

Corollary 2.6: Finite integral domain is field

If R is a finite (as a set) integral domain then R is a field

Proof. Fix $a \in R$ and $a \neq 0$. Then define a map

$$\begin{aligned} f_a : R &\to R \\ x &\mapsto a \cdot x \end{aligned}$$

Claim: f_a is an injective map by cancellation

> ***Proof.*** Suppose $f_a(x) = f_a(y)$, then
>
> $$a \cdot x = a \cdot y \implies x = y$$
>
> hence, it is injective. ■

By the Pigeonhole Principle f_a is also surjective. This bijection implies that there exists $x \in R$ such that $a \cdot x = 1$. Hence, a is a unit and is an element of the group of units, i.e $a \in R^\times$.
Since every non-zero a is shown to be in $R^\times$ this way, they are all units, and hence R is a field (since every element in the ring has a multiplicative inverse). ■

Definition 2.7: Subring

A subring S of a ring R is a subgroup that is closed under multiplication. That is $S \subset R$ such that $\forall a, b \in S$,

$$\left.\begin{array}{ll} \text{(i) } a+b \in S & \text{(closure under } +) \\ \text{(ii) } 0 \in S & \text{(additive identity)} \\ \text{(iii) } -a \in S & \text{(additive inverse)} \end{array}\right\} S \text{ is a subgroup}$$
$$\text{(iv) } a \cdot b \in S \quad \text{(closure under } \cdot)$$

Proposition 2.8: Subring Criterion

If $S \subset R$ is a subset of a ring such that $\forall a, b \in S$

(i) $S \neq \emptyset$
(ii) $a - b \in S$
(iii) $a \cdot b \in S$

then S is a subring.

Proof. Suppose $a, b \in S$ and the conditions above are true, then

(i) $a - a = 0 \in S$
(ii) $0 - a = -a \in S$
(iii) $a - b = a + (-b) \in S$
(iv) $a \cdot b \in S$

thus satisfying the definition of a subring. ■

Example 2.8. $\mathbb{Z} \subset \mathbb{Q}, \mathbb{Q} \subset \mathbb{R}, \mathbb{Z} \subset \mathbb{R}$ are all subrings.

Example 2.9. $2\mathbb{Z} \subset \mathbb{Z}$ is a subring and more generally $n\mathbb{Z} \subset \mathbb{Z}$ is a subring.

Example 2.10. $C[0,1] \subset \mathcal{F} \coloneqq \{f : [0,1] \to \mathbb{R}\}$ is a subring.

Definition 2.9: Subfield

If F is a field and $F' \subset F$ is a subring such that

(i) $1 \in F'$
(ii) $\forall a \in F', a^{-1} \in F'$

then we say F' is a **subfield** of F.

Warning: Not all subrings of fields are subfields! (e.g $\mathbb{Z} \subset \mathbb{R}$)

Claim: If $R \subset F$ is a subring of a field with $1 \in R$, then R is an integral domain.

L3: Ring Homomorphisms

Polynomial Rings

Fix a commutative ring R with 1 (e.g. $R = \mathbb{Z}, R = \mathbb{Q}$, etc) Let X be an indeterminate (this means X is just a symbol without an exact representation, compared to to when you think x is a variable representing a number). Read more about it here!

Definition 3.1: Polynomial in a ring

A **polynomial** in X with coefficients in R is a formal, finite sum

$$a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0, \quad a_i \in R, i \in \{0, \ldots, n\}$$

Note: If $a_n \neq 0$ and $a_m = 0, \quad \forall m > n$. Then we say the **degree** of the polynomial is n. If $a_k = 1$, we often omit it from the notation, e.g

$$X^2 + 2$$

has a 1 "missing" infront of X^2.
If $a_n = 1$, we say the polynomial is **monic**

Definition 3.2: Ring of Polynomials and Constant Polynomial

The **set of polynomials** in X w/ coefficients in R is denoted

$$R[X] \coloneqq \{a_n X^n + \cdots + a_0 | a_i \in R\}$$

If the degree of $p \in R[X]$ is zero, we say p is a **constant** polynomial.

Observe that there is an obvious inclusion map from a ring into the ring of polynomials, by taking each element $a \in R$ to the constant polynomial $a \in R[X]$.

$$R \to R[X]$$
$$a \mapsto a$$

Claim: $R[X]$ is a ring.

Proof. We check the ring properties
(i) Closure under addition

$$\begin{aligned}&(a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0) + (b_n X^n + b_{n-1} X^{n-1} + \cdots + b_1 X + b_0)\\ =&(a_n + b_n) X^n + (a_{n-1} + b_{n-1}) X^{n_1} + \cdots + (a_1 + b_1) X + (a_0 + b_0)\end{aligned}$$

(ii) Closure under multiplication

$$\begin{aligned}&(a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0) \cdot (b_n X^n + b_{n-1} X^{n-1} + \cdots + b_1 X + b_0)\\ &= (a_0 \cdot b_0) + (a_1 \cdot b_0 + a_0 \cdot b_1) X + (a_2 \cdot b_0 + a_1 \cdot b_1 + a_0 \cdot b_2) X^2\\ &\qquad + \cdots + \left(\sum_{k=0}^{l} a_k \cdot b_{l-k} \right) X^l + \cdots + (a_n \cdot b_m) X^{n+m}\end{aligned}$$

■

Example 3.1. $\mathbb{Z}[X], \mathbb{Q}[X], \mathbb{Z}/3\mathbb{Z}[X]$, which are rings of polynomials with coefficients in different number systems. In particular, we may write $\mathbb{Z}/3\mathbb{Z}$ coefficients without the "overbar" notation,

$$X + 2, X^3 + 2X^2 + 1 \in \mathbb{Z}/3\mathbb{Z}[X]$$

Factoring polynomials depends on the coefficient ring. For example

$$X^2 - 2 \in \mathbb{Z}[X]$$
$$X^2 - 2 = (X + \sqrt{2}) \cdot (X - \sqrt{2}) \in \mathbb{R}[X]$$

Here we can see that $X^2 - 2$ can not be factored further in the integers, but in the real numbers it can.
Similarly, $X^2 + 1 \in \mathbb{Z}[X], X^2 + 1 \in \mathbb{R}[X]$. These polynomials doesn't factor in either ring, but it does factor in $\mathbb{C}[X]$

$$X^2 + 1 = (X + i)(X - i)$$

it also factors in $\mathbb{Z}/2\mathbb{Z}[X]$

$$X^2 + 1 = (X + 1)(X + 1) \pmod 2$$

Because $X^2 + 2X + 1 \equiv X^2 + 1 \pmod 2$

Proposition 3.3: $R[X]$ is an integral domain

Let R be an integral domain and $p(X), q(X) \in R[X]$
(i) $\deg(p(X) \cdot q(X)) = \deg p(X) + \deg q(X)$.
(ii) $R[X]^\times = R^\times$
(iii) $R[X]$ is an integral domain

Proof.
(i) The leading term is

$$(a_n \cdot b_m)X^{n+m}$$

Since R is an integral domain and $a_n, b_m \neq 0$. Then $a_n \cdot b_m \neq 0$ (This also proves (iii))
(ii) Suppose $p(X) \in R[X]^\times$, say $p(X) \cdot q(X) = 1$.
Then

$$\deg(p \cdot q) = \deg(1) = 0 \implies \deg(p) + \deg(q) = 0 \implies \deg(p) = \deg(q) = 0 \implies p(X) \in R$$

i.e $p(X)$ is a constant polynomial whose constant coefficient, say p, is from the ring R.
Hence, since $p(X)$ is a unit, so is p. ■

Example 3.2. Consider $2X^2 + 1, 2X^5 + 3X \in \mathbb{Z}/4\mathbb{Z}[X]$

$$(2X^2 + 1) \cdot (2X^5 + 3X) = 2 \cdot 2X^7 + \text{ lower terms} = 0 \cdot X^7 + \text{ lower terms}$$

This implies

$$\deg\left((2X^2 + 1) \cdot (2X^5 + 3X)\right) < \deg(2X^2 + 1) + \deg(2X^5 + 3x)$$

When R isn't an integral domain, the degree of the product of polynomials can be less than

the degree of their sum (in general, the degree is at most the sum).

Ring Homomorphisms

Definition 3.4: Ring Homomorphism and Isomorphism

Let R, S be rings. A **ring homomorphism** is a map $f : R \to S$ such that
(i) $f(a +_R b) = f(a) +_S f(b)$ (**Group homomorphism**)
(ii) $f(a \cdot_R b) = f(a) \cdot_S f(b)$
If f is a bijective ring homomorphism, we say it is a **ring isomorphism**.
We say, in this case R is **isomorphic** to S as rings and write

$$R \cong S$$

Definition 3.5: Kernel

The **kernel** of a ring homomorphism $f : R \to S$ is the subset

$$\operatorname{Ker} f \coloneqq f^{-1}(0_S) \subset R$$

Proposition 3.6: $\operatorname{Ker} f$ **is an ideal**

Let R, S be rings and $f : R \to S$ a homomorphism, then
(i) $\operatorname{Im} f \subset S$ is a subring
(ii) $\operatorname{Ker} f \subset R$ is a subring
where Im is the image of f and Ker is the kernel.
Moreover, if $r \in R$, $a \in \operatorname{Ker} f$ then $r \cdot a \in \operatorname{Ker} f$.
(this is a stronger property of the kernel, which shows it is more than just a subring, since it is also closed under multiplication with elements from outside the kernel, in particular from the ring).

Both proofs rely on using the Subring Criterion Test mentioned in Lecture 2.

Proof (i). First, we check show that it is non empty.
Claim: $f(0_R) = 0_S$ and in particular $\operatorname{Im} f \neq \emptyset$.

> ***Proof.*** By definition of ring homomorphism
> $$f(0_R) = f(0_R + 0_R) = f(0_R) + f(0_R) \implies 0_s = f(0_R)$$
> Where we have subtracted (in S) $f(0_R)$ from both sides. ■

Suppose now $f(a), f(b) \in \operatorname{Im} f$, then

$$f(a) \cdot f(b) = f(a \cdot b) \in \operatorname{Im} f$$

which shows the product is also in the image.

Finally, whats left to show is that the difference is also in the image. To see $f(a) - f(b) \in \operatorname{Im} f$, it suffices to see that $-f(b) = f(-b)$.

Claim: $-f(b) = f(-b)$

> ***Proof.*** Again using the ring homomorphism definition
> $$0 = f(0_R) = f(b + (-b)) = f(b) + f(-b) \implies f(-b) = -f(b)$$ ■

Therefore, with the subring criterion satisfied, then $\operatorname{Im} f$ is a subring in S. ■

Proof (ii). Since $f(0_R) = 0_S \implies 0_R \in \operatorname{Ker} f$, hence $\operatorname{Ker} f$ is nonempty.
Suppose $a, b \in \operatorname{Ker} f$, then

$$f(a - b) = f(a) - f(b) = 0 - 0 = 0 \implies a - b \in \operatorname{Ker} f$$

and

$$f(a \cdot b) = f(a) \cdot f(b) = 0 \cdot 0 = 0 \implies a \cdot b \in \operatorname{Ker} f$$

Hence, $\operatorname{Ker} f$ is a subring in R.
Now suppose $r \in R$

$$f(r \cdot a) = f(r) \cdot f(a) = f(r) \cdot 0 = 0$$

which proves the additional property. ■

Example 3.3. Consider the map which takes even numbers to 0 and odd numbers to 1.

$$\begin{aligned} f : \mathbb{Z} &\to \mathbb{Z}/2\mathbb{Z} \\ a &\mapsto a \pmod 2 \end{aligned}$$

Check the possible situations (these show the sums and products follow the homomorphism properties)

Addition	$\overline{0} + \overline{0} = \overline{0}$	even + even = even
	$\overline{0} + \overline{1} = \overline{1}$	even + odd = odd
	$\overline{1} + \overline{1} = \overline{0}$	odd + odd = even

Multiplication	$\overline{0} \cdot \overline{0} = \overline{0}$	even $\cdot$ even = even
	$\overline{0} \cdot \overline{1} = \overline{0}$	even $\cdot$ odd = even
	$\overline{1} \cdot \overline{1} = \overline{1}$	odd $\cdot$ odd = odd

Therefore $\operatorname{Ker} f = \{\text{evens}\} = 2\mathbb{Z}$ and observe that

$$f^{-1}(\overline{1}) = \{\text{odds}\} = 1 + 2\mathbb{Z} = \{1 + 2n | n \in Z\} = 1 + \operatorname{Ker} f$$

Example 3.4. The following is a non-example. Consider

$$\begin{aligned} f_n : \mathbb{Z} &\to \mathbb{Z} \\ a &\mapsto n \cdot a \end{aligned}$$

Then

$$f_n(a + b) = n \cdot (a + b) = n \cdot a + n \cdot b = f_n(a) + f_n(b)$$

But

$$f_n(a \cdot b) = n(a \cdot b) \stackrel{?}{=} n^2(a \cdot b) = (n \cdot a) \cdot (n \cdot b) = f_n(a) \cdot f_n(b)$$

So f_n is a ring homomorphism if and only if $n^2 = n$ (i.e $n = 0, 1$). f_0 is the constant map zero and f_1 is the identity.
Therefore $f_2, f_3, \ldots$ are **NOT** ring homomorphisms. In particular, it shows that a group homomorphism is not necessarily a ring homomorphism.

Example 3.5. Here is a polynomial homomorphism which maps a polynomial to its own constant term

$$\begin{aligned} \phi :& \mathbb{R}[X] \to \mathbb{R} \\ & p(X) \mapsto p(0) \end{aligned}$$

This can easily be checked

$$\begin{aligned} \phi(p+q) &= (p+q)(0) = p(0) + q(0) = \phi(p)\phi(q) \\ \phi(p \cdot q) &= (p \cdot q)(0) = p(0) \cdot q(0) = \phi(p) \cdot \phi(q) \end{aligned}$$

Its kernel (which are polynomials who have 0 as a root) can be written

$$\mathrm{Ker}\{p \in \mathbb{R}[X] \,|\, p(0) = 0\} = \{p \in R[X] \,|\, p(X) = X \cdot p'(X) \text{ for some } p' \in \mathbb{R}[X]\}$$

(p' is not the derivative, just another polynomial).

Question: What about

$$\begin{aligned} \phi_1 :& \mathbb{R}[X] \to \mathbb{R} \\ & p(X) \mapsto p(1) \end{aligned}$$

L4: Quotient Rings

Recall that given a ring homomorphism $f : R \to S$, the kernel of f, $\operatorname{Ker} f$, is a subring of R.

Definition 4.1: Coset and Quotient Ring

Given a ring homomorphism $f : R \to S$, let $I = \operatorname{Ker} f$ and $r \in R$.
The **coset** of $r \in R$ with respect to f (or w.r.t I) is the set

$$r + I \coloneqq \{r + x | x \in I = \operatorname{Ker} f\}$$

The **quotient ring** of R by I is the set

$$R/I \coloneqq \{r + I | r \in R\}$$

Proposition 4.2: Coset space is a ring

Given a ring homomorphism $f : R \to S$ with $I = \operatorname{Ker} f$, the quotient ring R/I is a ring with operations

$$(r + I) + (s + I) \coloneqq (r + s) + I$$
$$(r + I) \cdot (s + I) \coloneqq (r \cdot s) + I$$

Note: If I is understood, we will often write $\overline{r}$ for $r + I$, e.g

$$(r + I) + (s + I) = (r + s) + I$$

becomes

$$\overline{r} + \overline{s} = \overline{r + s}$$

Lemma 4.3

If $r, s \in R$ and $(r + I) \cap (s + I) \neq \emptyset$, then $r + I = s + I$

Proof. Suppose $x \in (r + I) \cap (s + I)$, then

$$x \in r + I \implies x = r + a, a \in I$$
$$x \in s + I \implies x = s + b, a \in I$$

These together lead to three equivalent equations

$$r + a = s + b \iff r = s + (b - a) \iff s = r + (a - b)$$

Since $I \subset R$ is a subring then we know $b - a, a - b \in I$. Then the previous equations imply

$$r \in s + I,\ s \in r + I$$

Now take any element $c \in I$, then

$$r + c = (s + (b - a)) + c = s + (b - a + c) \in s + I \implies r + I \subset s + I$$

where the last implication comes from the fact that $b - a + c$ are elements in I and as such their combination is as well.
With similar logic we see that

$$s + c = (r + (a - b)) + c = r + (a - b + c) \in r + I \implies s + I \subset r + I$$

Hence, $r + I = s + I$. ■

Example 4.1. Let f be the homomorphism from the integers to the integers mod 2, i.e

$$\begin{aligned} f :& \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \\ & n \mapsto n \bmod 2 \end{aligned}$$

Immediately we know that the kernel is the set of even integers, Ker $f = 2\mathbb{Z}$.
Consider the coset of $1 \in Z$ which is $1 + 2\mathbb{Z}$, then

$$1 + 2\mathbb{Z} = 3 + 2\mathbb{Z} = -7 + 2\mathbb{Z} = 29 + 2\mathbb{Z}$$

where the equivalence follows from Lemma 4.1.

Lemma 4.4

If

$$\begin{aligned} r + I &= r' + I \\ s + I &= s' + I \end{aligned}$$

then

$$\begin{aligned} (r + s) + I &= (r' + s') + I \\ (r \cdot s) + I &= (r' \cdot s') + I \end{aligned}$$

i.e, $+, \cdot$ are well-defined in R/I

Proof. Let $r, r', s, s' \in R$, then

$$\begin{aligned} r + I = r' + I &\implies r = r' + x,\ x \in I \\ s + I = s' + I &\implies s = s' + y,\ y \in I \end{aligned}$$

Then their sum

$$r + s = (r' + x) + (s' + y) = (r' + s') + (x + y) \implies r + s \in (r' + s') + I$$

On the other hand $r + s = r + s + 0 \in (r + s) + I$, hence

$$[(r + s) + I] \cap [(r' + s') + I] \neq \emptyset$$

By Lemma 4.1, it is immediate that

$$(r + s) + I = (r' + s') + I$$

Similarly,

$$r \cdot s = (r' + x) \cdot (s' + y) = r's' + r'y + xs' + xy \in r' \cdot s' + I$$

■

Observe that R/I consists of the equivalence classes in R of the equivalence relation given by

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

Proof of Prop 4.1.
We check that the quotient is a ring

$\overline{0} + \overline{a} = \overline{0+a} = \overline{a} = \overline{a+0} = \overline{a} + \overline{0}$ ($\overline{0} \in R/I$ is the additive identity)

$\overline{a} + \overline{(-a)} = \overline{a + (-a)} = \overline{0} = \overline{(-a) + a} = \overline{(-a)} + \overline{a}$

$\overline{a} + (\overline{b} + \overline{c}) = \overline{a} + (\overline{b+c}) = \overline{a + (b+c)} = \overline{(a+b) + c} = \overline{(a+b)} + \overline{c} = (\overline{a} + \overline{b}) + \overline{c}$

$\overline{a} \cdot (\overline{b} \cdot \overline{c}) = \overline{a} \cdot (\overline{bc}) = \overline{a \cdot (b \cdot c)} = \overline{(a \cdot b) \cdot c} = \overline{ab} \cdot \overline{c} = (\overline{a} \cdot \overline{b}) \cdot \overline{c}$

$\overline{a} \cdot (\overline{b} + \overline{c}) = \overline{a} \cdot (\overline{b+c}) = \overline{a \cdot (b+c)} = \overline{a \cdot b + a \cdot c} = \overline{ab} + \overline{ac} = \overline{a} \cdot \overline{b} + \overline{a} \cdot \overline{c}$ ■

Definition 4.5: Ideal

Let R be a ring and $I \subset R$.
We say I is a

(i) **Left ideal** if I is a subring such that for all $a \in R, x \in I$

$$a \cdot x \in I$$

(ii) **Right ideal** if I is a subring such that for all $a \in R, x \in I$

$$x \cdot a \in I$$

(iii) **Ideal** if I is both a left and right ideal (sometimes called a **two-sided ideal**).

Observe that if $f : R \to S$ is a ring homomorphism then $\operatorname{Ker} f$ is an ideal in R.
Note: We may define R/I for **any** ideal $I \subset R$, whether or not $I = \operatorname{Ker} f$ for some ring homomorphism $f : R \to S$.

Theorem 4.6: The First Isomorphism Theorem

If $f : R \to S$ is a ring homomorphism and $I = \operatorname{Ker} f$. Then

$$R/I \cong \operatorname{Im} f$$

as rings.

Proof. We first prove a smaller claim.
Claim: If $r \in R$, then

$$r + I = f^{-1}(f(r)) = \{x \in R | f(x) = f(r)\}$$

(Here f^{-1} is the preimage, not the inverse).

> ***Proof.*** If $a \in I$, then
> $$f(r+a) = f(r) + f(a) = f(r) \implies r + a \in f^{-1}(f(r)) \implies r + I \subset f^{-1}(f(r))$$
> Similarly, if $x \in f^{-1}(f(r))$, then
> $$f(r) = f(x) \implies f(r) - f(x) = 0 \implies f(r - x) = 0$$
> This last equality means $r - x$ (and $x - r$) $\in \operatorname{Ker} f$, hence
> $$x - r \in \operatorname{Ker} f \implies x = r + (x - r) \in r + I \implies f^{-1}(f(r)) \subset r + I$$
> Therefore, both inclusions are proved and $r + I = f^{-1}(f(r))$. ■

There is a bijective map

$$\begin{aligned} \overline{f} : & R/I \to \operatorname{Im} f \\ & \overline{r} \mapsto f(r) \end{aligned}$$

The point being that $\overline{r}$ is independent of the representative $r \in R$. ■

Theorem 4.7: Canonical quotient map is surjective

If $I \subset R$ is an ideal, then the **quotient map**

$$\begin{aligned} f : & R \to R/I \\ & r \mapsto \overline{r} \end{aligned}$$

is a surjective ring homomorphism with $\operatorname{Ker} f = I$

Proof. Firstly, f is clearly surjective because every element of $r \in R$ will be an element of its own equivalence class. It remains to show that this is a homomorphism.

$$f(a + b) = \overline{a + b} = \overline{a} + \overline{b} = f(a) + f(b)$$
$$f(a \cdot b) = \overline{a \cdot b} = \overline{a} \cdot \overline{b} = f(a) \cdot f(b)$$

For the kernel, by definition of the map $f(a) = \overline{a}$, but if we also have that $f(a) = \overline{0}$ then by definition of equivalence classes $\overline{a} = \overline{0}$ because if $a \sim 0$ then $\overline{a} = \overline{0}$.
Therefore $a \in I = \operatorname{Ker} f$. ■

Example 4.2. For any integer $n \in \mathbb{Z}$, we have that

$$n\mathbb{Z} = \{nx | x \in \mathbb{Z}\}$$

is an ideal in $\mathbb{Z}$.
Furthermore, the quotient ring of $\mathbb{Z}$ by $n\mathbb{Z}$ is exactly the ring $\mathbb{Z}/n\mathbb{Z}$.

Example 4.3. Let $R = \mathbb{Z}[X]$ and define

$$I \coloneqq \{p(X) \in R | \text{ all nonzero terms have degree at least } 2\}$$

e.g $7X^2 + 3X^3 + 10X^9 \in I$

Note: $0 \in I$ because it has **no** terms with non-zero coefficient.
Exercise: Prove that I is an ideal. Now consider two polynomials $p(X), q(X) \in R$ and $\overline{p(X)} = \overline{q(X)}$, then by definition of equivalence, $p - q \in I$.
So $p - q$ consists of terms of *at least* degree 2, i.e the degree 0 and degree 1 parts of p, q agree, e.g

$$5 + X + 7X^3 = 5 + X - 21X^5 + 7X^{19}$$

This implies that the polynomials of degree at most 1 represent *distinct* cosets in R/I, e.g

$$5 + X,\ -7 + 2X,\ 11 - 4X$$

Therefore, there is a bijection between

$$R/I \iff \{a + bX | a, b, \in \mathbb{Z}\}$$

Observe that R/I has zero divisors: $\overline{x} \cdot \overline{X} = \overline{X^2} = \overline{0}$.

Example 4.4. Let R be a ring and X a non-empty set.
Consider the ring

$$\mathcal{F}(X, R) \coloneqq \{f : X \to R\}$$

For a fixed element $a \in X$, the **evaluation map** at a is

$$\begin{aligned} \mathrm{Ev}_a : \mathcal{F}(X, R) &\to R \\ f &\mapsto f(a) \end{aligned}$$

Exercise: Ev_a is a ring homomorphism.
Moreover, Ev_a is a *surjective* ring homomorphism and

$$\mathrm{Ker}(\mathrm{Ev}_a) \coloneqq \{f \in \mathcal{F}(X, R) | f(a) = 0\}$$

In particular, by the First Isomorphism Theorem we have

$$\mathcal{F}(X, R)/\mathrm{Ker}(\mathrm{Ev}_a) \cong R$$

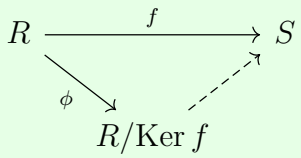
L5: Isomorphism Theorems

Theorem 5.1: The First Isomorphism Theorem

If $f : R \to S$ is a ring homomorphism and $I = \operatorname{Ker} f$. Then

$$R/I \cong \operatorname{Im} f$$

as rings.



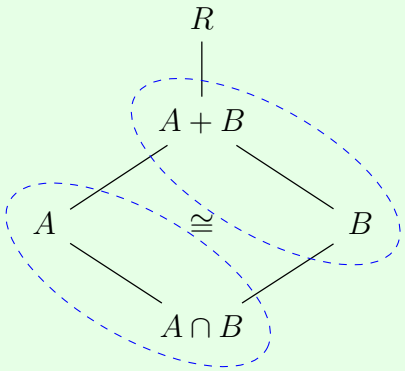
Theorem 5.2: The Second Isomorphism Theorem

Let $A \subset R$ be a subring and $B \subset I$ an ideal.
Then

$$A + B \coloneqq \{a + b \mid a \in A, b \in B\}$$

is a subring of R and $A \cap B$ is an ideal of A and

$$(A + B)/B \cong A/(A \cap B)$$



Proof of 5.2.
Let $A \subset R$ be a subring and $B \subset I$ an ideal.
It is **Easy to check** that $A + B$ is a subring and $A \cap B$ is an ideal in A.
Now we want to find an isomorphism

$$(A + B)/B \longrightarrow A/(A \cap B)$$

Idea: Use the First Isomorphism Theorem, i.e we want to find a surjective homomorphism

$$f\colon A + B \to A/(A \cap B)$$

such that $\operatorname{Ker} f = B$.

Define a map

$$\phi\colon A+B \to A/(A\cap B)$$
$$a+b \mapsto a+A\cap B$$

which can be shown to be homomorphism if it is well defined. Generally, if $x \in A+B$, there are many ways to express $x \in A+B$, i.e there may exist, $a, a' \in A$ and $b, b' \in B$ such that

$$x = a+b = a'+b'$$

So is $\phi(x) = a + A\cap B$ or $\phi(x) = a' + A\cap B$?
This is not a problem so long as $a+A\cap B = a'+A\cap B$. In other words, if $a-a' \in A\cap B$ BUT

$$a+b = a'+b' \implies \underbrace{a-a'}_{\in A} = b'-b \in B \implies a-a' \in A\cap B$$

We also need to check that ϕ is surjective.
Clearly, if $a+A\cap B \in A/(A\cap B)$, then say $a \in A$ and is a representative for $a+A\cap B$.
Then, $a+0 \in A+B$ and $\phi(a) = a+A\cap B$.
Finally, we must check that

$$\operatorname{Ker}\phi = B$$

If $a+b \in \operatorname{Ker}\phi$ then $\phi(a+b) = 0+A\cap B$ and so

$$a \in A\cap B \implies a \in B \implies \operatorname{Ker}\phi \subset B$$

On the other hand, if $b \in B \subset A+B$, then we can write it as $b = 0+b$ and so

$$\phi(b) = 0+A\cap B \implies b \in \operatorname{Ker}\phi \implies B \subset \operatorname{Ker}\phi$$

Therefore, $\operatorname{Ker}\phi = B$. ■

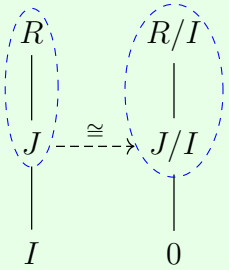
Theorem 5.3: The Third Isomorphism Theorem

Let $I, J \subset R$ be ideals $I \subset J$.
Then

$$J/I \coloneqq \{a+I \in R/I \mid a \in J\}$$

(the cosets of R/I whose representatives are in J or similarly the restriction of the quotient map from R to R/I to the domain J) is an ideal in R/I and

$$(R/I)/(J/I) \cong R/J$$



Proof of 5.3.
Let $I \subset J \subset R$ be ideals.
Then we want to show, $J/I \subset R/I$ is an ideal and

$$(R/I)/(J/I) \cong R/J$$

Check: J/I is an ideal in R/I.
Then define a map

$$\phi\colon R/I \to R/J$$
$$a + I \mapsto a + J$$

Observe that if $a \in J$, then $\phi(a + I) = a + J = J = \overline{0}$
ϕ is also clearly surjective: Pick any representative $a \in R$ for $a + J$, then

$$\phi(a + I) = a + J$$

It remains to be shown that $\operatorname{Ker}\phi = J/I$ as follows:
If $a + I \in \operatorname{Ker}\phi$ then $\phi(a + I) = a + J = 0 + J = J$ which implies

$$a \in J \implies a + I \in J/I \implies \operatorname{Ker}\phi \subset J/I$$

If $a \in J$, then $\phi(a + I) = a + J = J$ which implies

$$a + I \in \operatorname{Ker}\phi \implies \operatorname{Ker}\phi \supset J/I$$

and therefore $\operatorname{Ker}\phi = J/I$. ■

Theorem 5.4: The Fourth Isomorphism Theorem

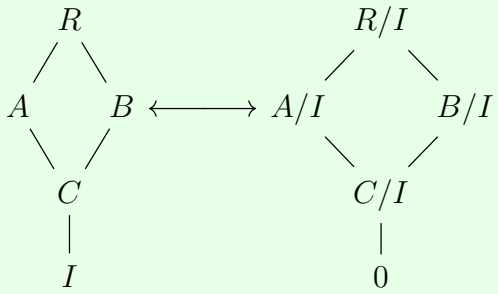
Let $I \subset R$ be an ideal.
Then the correspondence

$$I \subset A \subset R \longleftrightarrow A/I \subset R/I$$

is a bijection between

$$\{\text{subrings of } R \text{ containing } I\} \longleftrightarrow \{\text{subrings of } R/I\}$$

Moreover, $A \subset R$ is an ideal *iff* A/I is an ideal in R/I.



Definition 5.5: Ideal Generation, Principal and Finitely Generated Ideal

Let R be a ring, with $1 \neq 0$ and let $A \subset R$ be any subset.
The **ideal generated by** A is

$$A \subset (A) \subset R$$

i.e, the smallest ideal of R containing A.
If an ideal I is generated by a single element set, then we say I is a **principal ideal**.
If I is generated by a finite set then we say I is a **finitely generated ideal**.

Note: Instead of writing $I = (\{a\})$ for a principal ideal, we often omit the set notation and just write

$$I = (a)$$

Similarly, we will write $I = (a_1, \ldots, a_n)$ for finitely generated ideals.

Proposition 5.6: Minimality of ideal generated by a set

For any subset $A \subset R$ and ideals $I \subset R$ such that $A \subset I$, we have

$$(A) = \bigcap_{\substack{I \subset R \\ A \subset I}} I$$

Proof.
Observe that $R \subset R$ and is always an ideal of itself which implies that there always exists an ideal containing A (at least R)

$$\{A \subset I \subset R\} \neq \emptyset$$

First check that $(A) \subset \bigcap_{\substack{I \subset R \\ A \subset I}} I$
Suppose, for a contradiction, $A \subset I$ and $(A) \not\subset I$, then
(i) $(A) \cap I \subsetneq (A)$ (proper subset otherwise $(A) \subset I$)
(ii) $A \subset (A)$ and $A \subset I \implies A \subset (A) \cap I$
(iii) $(A) \cap I$ is an ideal (second isomorphism theorem).
Therefore there is an ideal containing A (i.e $(A) \cap I$) that is smaller than (A), which is contradictory the definition of (A). Hence

$$(A) \subset \bigcap_{\substack{I \subset R \\ A \subset I}} I$$

Now check that $\bigcap_{\substack{I \subset R \\ A \subset I}} I \subset (A)$
We have that

$$\bigcap_{\substack{I \subset R \\ A \subset I}} I$$

is an ideal and therefore $A \subset \bigcap I$ which implies

$$\bigcap_{\substack{I \subset R \\ A \subset I}} I \subset (A)$$

because (A) is an ideal. Therefore,

$$(A) = \bigcap_{\substack{I \subset R \\ A \subset I}} I$$

■

L6: More on Ideals

Let R be a ring with $1 \neq 0$.
Recall that if $A \subset R$, then

$$(A) = \bigcap_{\substack{I \subset R \text{ ideals} \\ A \subset I}} I$$

Definition 6.1: Ring Multiplication

For fixed sets $A, B \subset R$, we define **ring multiplication** as

$$A \cdot B \coloneqq \{a_1 b_1 + \cdots + a_n b_n \mid a_1, \ldots, a_n \in A,\ b_1, \ldots, b_n \in B,\ n \in \mathbb{N}\}$$

Proposition 6.2: Characterization of ideal generated by a set

If $A \subset R$ is any subset, then:
(i) $R \cdot A$ is the left ideal generated by A
(ii) $A \cdot R$ is the right ideal generated by A
(iii) $R \cdot A \cdot R$ is the (two-sided) ideal generated by A

Note: If
- $A = \emptyset$, then we say $RA = AR = RAR = \{0\}$
- R is commutative, then $RA = AR = RAR$.

Proof. We will only check for the left ideal, the others follow similarly.
First the subring criterion for $RA \subset R$
(i) $0 = 0 \cdot a \in RA \implies RA \neq \emptyset$
(ii) Let $x, y \in RA$, then there exist

$$r_1, \ldots r_n \in R,\ a_1, \ldots, a_n \in A$$
$$r'_1, \ldots r'_m \in R,\ a'_1, \ldots, a'_m \in A$$

such that

$$x = r_1 a_1 + r_2 a_2 + \cdots + r_n a_n$$
$$y = r'_1 a'_1 + r'_2 a'_2 + \cdots + r'_m + a'_m$$

then

$$\begin{aligned} x - y &= (r_1 a_2 + \cdots + r_n a_n) - (r'_1 a'_1 + \cdots + r'_m a'_m) \\ &= r_1 a_1 + \cdots + r_n a_n + (-r'_1) a'_1 + \cdots + (-r'_m) a'_m \in RA \end{aligned}$$

and

$$\begin{aligned} xy &= (r_1 a_2 + \cdots + r_n a_n) \cdot (r'_1 a'_1 + \cdots + r'_m a'_m) \\ &= (r_1 a_1 r'_1) a'_1 + \cdots + (r_1 a_1 r'_m) a'_m \\ &\quad + \vdots \\ &\quad + (r_n a_n r'_1) a'_1 + \cdots + (r_n a_n r'_m) a'_m \in RA \end{aligned}$$

Then RA is a subring.
To see RA is an ideal: Let $r \in R, x \in RA$ as above.

$$r \bullet x = r \bullet (r_1 a_2 + \cdots + r_n a_n) = (rr_1)a_1 + \cdots + (rr_n)a_n \in RA$$

Moreover

$$A \subset RA \quad (1 \in R \implies \forall a \in A,\, 1 \bullet a = a \in RA)$$

So RA is an ideal containing A i.e

$$(A) \subset RA$$

On the other hand, if I is a left ideal such that $A \subset I$, then $a \in A, r \in R \implies r \bullet a \in I$ which implies for any finite list $r_1, \ldots, r_n \in R$, $a_1, \ldots, a_n \in A$

$$r_1 a_1, \ldots, r_n a_n \in I \implies r_1 a_1 + \cdots + r_n a_n \in I \implies RA \subset I$$

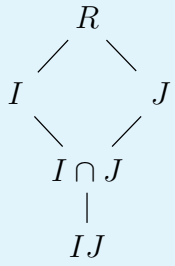
and since (A) is a left ideal, we have

$$RA = (A)$$

and specifically this is the smallest ideal needed to contain A. ■

Proposition 6.3: $I \bullet J \subset I \cap J$

If $I, J \subset R$ are ideals, then $I \bullet J$ is an ideal, $I \bullet J \subset I \cap J$.



Note: $I \bullet I = I^2, \ldots, \underbrace{I \bullet I \bullet \ldots \bullet I}_{n-\text{times}} = I^n$

Example 6.1. Consider $2\mathbb{Z}, 3\mathbb{Z} \subset Z$, then

$$2\mathbb{Z} \bullet 3\mathbb{Z} = \left\{ \sum_{k=1}^{n} 2a_k \bullet 3b_k \,\middle|\, a_k, b_k \in Z \right\} = \left\{ 6 \left(\sum_{k=1}^{n} a_k \bullet b_k \right) \,\middle|\, a_k, b_k \in Z \right\} = 6\mathbb{Z}$$

and

$$2\mathbb{Z} \cap 3\mathbb{Z} = \{\underbrace{2n = 3m}_{2|m, 3|n}\} = 6\mathbb{Z}$$

In this case we have $2\mathbb{Z} \bullet 3\mathbb{Z} = 2\mathbb{Z} \cap 3\mathbb{Z}$.

Example 6.2. Consider the ring $R = \mathbb{Z}[X]$ with

$$(X) \coloneqq \{p(X) \cdot x \mid p(X) \in R\}$$
$$(X^2) \coloneqq \{q(X) \cdot x^2 \mid q(X) \in R\}$$

Then

$$\begin{aligned}(X) \cdot (X^2) &= \{(p_1(X) \cdot X) \cdot (q_1(X) \cdot X^2) + \cdots + (p_n(X) \cdot X) \cdot (q_n(X) \cdot X^2)\} \\ &= \{(p_1 \cdot q_1(X) + \cdots + p_n \cdot q_n(X)) \cdot X^3\} = (X^3)\end{aligned}$$

On the other hand, since multiples of X^2 are also multiples of X, we get

$$(X) \cap (X^2) = (X^2)$$

and so

$$(X) \cdot (X^2) = (X^3) \subsetneq (X) \cap (X^2) = (X^2)$$

Since a multiple of X^3 is a multiple of X^2 but there is no multiple of X^3 which is equal to aX^2 for nonzero $a \in R$.

Large Ideals in R and Arithmetic in R

Assume R is a commutative ring w/ $1 \neq 0$.
If $a \in R$, then

$$(a) = \{ra \mid a \in R\} \quad \text{(the "multiples" of a)}$$

e.g. $2\mathbb{Z} = \{2n \mid n \in Z\} = (2)$
Note: We sometimes write

$$(a) = R \cdot a = a \cdot R$$

We also say that if $b \in (a)$, that a **divides** b, i.e $a \mid b$.

Claim: $b \in (a)$ *iff* $(b) \subset (a)$

> ***Proof.*** Let $b \in (a)$ then there exists $r \in R$ such that $b = r \cdot a$. In particular,
> $$c \in (b), \exists s \in R,\ c = s \cdot b = s \cdot (r \cdot a) = (s \cdot r) \cdot a \in (a) \implies (b) \subset (a)$$
> On the other hand, if $(b) \subset (a)$, then $b \in (b) \subset (a)$. ■

Definition 6.4: Prime Ideal

Let R be a commutative ring.
An ideal $P \neq R$ is called a **prime ideal** if for all $a, b \in R$ such that $a \cdot b \in P$, then either $a \in P$ or $b \in P$.

Example 6.3.

- $2\mathbb{Z}$ is prime
- $6\mathbb{Z}$ is **not** prime e.g $2 \cdot 3 = 6 \in 6\mathbb{Z}$ but $2, 3 \notin 6\mathbb{Z}$
- $\{0\} \subset \mathbb{Z}$ is prime. If $a \cdot b = 0, a, b \in \mathbb{Z}$ then either $a = 0$ or $b = 0$ (integral domain).
- $(x) \subset \mathbb{R}[x]$ is prime
- (x^2) is **not**, e.g. $x \cdot x = x^2 \in (x^2)$ but $x \notin (x^2)$.

Proposition 6.5: R integral if $\{0\}$ prime

R is an integral domain *iff* $\{0\}$ is prime

Theorem 6.6: Prime Ideal $\iff$ R/P integral domain

Assume R is commutative.
An ideal $P \subset R$ is prime *iff* R/P is an integral domain.

Proof.
$\Rightarrow$
Suppose P is prime and $\overline{a}, \overline{b} \in R/P$ such that $\overline{a} \cdot \overline{b} = \overline{0}$.
We want $\overline{a} = \overline{0}$ or $\overline{b} = \overline{0}$.
Pick representatives $a \in \overline{a}, b \in \overline{b}$. This implies $\overline{a \cdot b} = \overline{0}$, i.e $a \cdot b \in P$.
But P is prime, so either $a \in P$ or $b \in P$, i.e $\overline{a} = \overline{0}, \overline{b} = \overline{0}$.
$\Leftarrow$
If R/P is integral and $a \cdot b \in P$, then

$$\overline{a \cdot b} = \overline{0} \implies \underbrace{\overline{a} = \overline{0} \text{ or } \overline{b} = \overline{0}}_{R/P \text{ integral}} \implies a \in P \text{ or } b \in P$$

■

L7: Maximal Ideals

Let R be a commutative ring with $1 \neq 0$.

Proposition 7.1: Ideals containing units

Let $I \subset R$ an ideal
(i) $I = R$ if and only if I contains a unit.
(ii) R is a field if and only if the only ideals of R and 0 and R

Proof.
(i) If $I = R$, then $1 \in I$
Conversely, if $u \in I$ and $u \in R^\times$ say $u \cdot v = 1$, then $u \cdot v = 1 \in I$ implies, if $r \in R$, then

$$r \cdot (u \cdot v) = r \in I \implies R \subset I \implies R = I$$

(ii) If $I \subset R$ is an ideal in a field, and $\exists a \in I \setminus \{0\}$ (non-zero element of the field), then $a \in R^\times$ (since it is a field) implies $I = R$ (by part (i)).
Conversely, suppose 0 and R are the only ideals in R. Let $a \in R \setminus \{0\}$ and consider $(a) \subset R$, then

$$(a) \neq 0 \implies (a) = R \underbrace{\implies}_{\text{by part (i)}} \exists u \in (a),\ u \in R^\times (\text{say } u \cdot v = 1)$$

Since $u \in (a)$, we may write $u = r \cdot a, r \in R$, then

$$(r \cdot a) \cdot v = u \cdot v = 1 = a \cdot (r \cdot v) \implies a \in R^\times \implies R \text{ is a field}$$ ■

Corollary 7.2: Homomorphism from field to ring is injective

If F is a field, then any nonzero ring homomorphism

$$f : F \to R$$

is an injective map

Proof. $\operatorname{Ker} f = 0$ or F. Because f is nonzero, we conclude that $\operatorname{Ker} f = 0$, which means f is injective since the only element that maps to 0 is 0. ■

Definition 7.3: Maximal Ideal

An ideal $M \subset R$ is called a **maximal ideal** if
(i) $M \neq R$
(ii) If $I \subset R$ is an ideal such that $M \subset I$, then $I = M$ or $I = R$

Not all rings admit maximal ideals and a given ring may admit multiple maximal ideals, e.g $2\mathbb{Z}, 3\mathbb{Z}$ are maximal ideals in $\mathbb{Z}$.

A Digression on Zorn's Lemma

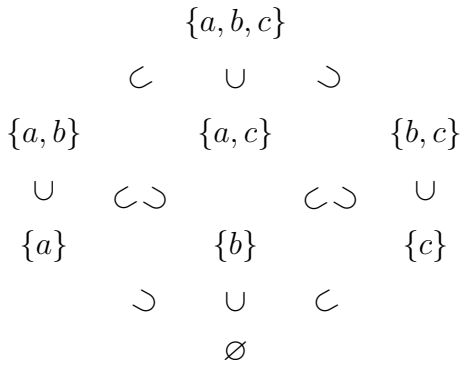
Definition 7.4: Partial Order

A **partial order** on a non-empty set A is a relation $\leq$ such that
(i) $x \leq x$ (Reflexive)
(ii) $x \leq y, y \leq x \implies x = y$ (Anti-symmetric)
(iii) $x \leq y, y \leq z \implies x \leq z$ (Transitive)

Example 7.1.
If X is any set then the power set (the set of all subsets) is written

$$\wp(X) = \{\text{subsets } U \subset X\}$$

Then inclusion is a partial order on $\wp(X)$, e.g



Definition 7.5: Poset, Chain, Upper Bound, Maximal Element

If $A, \leq$ is a **partially ordered set** (**poset**), then
(i) A subset $B \subset A$ is a **chain** if $\forall x, y \in B \implies x \leq y$ or $y \leq x$ (everything can be compared).
(ii) An **upper bound** on a subset $B \subset A$ is an element $u \in A$ such that

$$\forall b \in B, b \leq u$$

(iii) A **maximal element** of a subset $B \subset A$ is an element of $m \in B$ such that if $b \in B$ and $b \geq m$, then $b = m$.

Lemma 7.6: Zorn's Lemma

If A is a non-empty poset such that every chain admits an upper bound, then A has a maximal element.

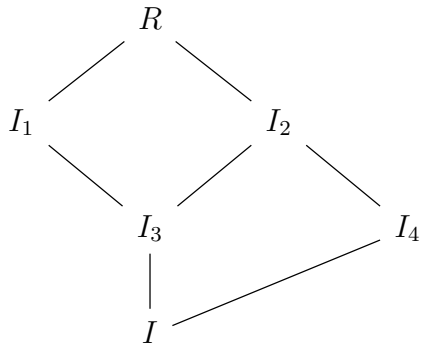
Proposition 7.7: All proper ideals contained in maximal ideal

If R is a commutative ring with $1 \neq 0$, then every proper ideal is contained in a maximal ideal

Proof.
Let $I \subsetneq R$ be a proper ideal.
Consider

$$\mathcal{S} \coloneqq \{\text{proper ideals of } R \text{ containing } I\}$$

$\mathcal{S}$ is partially ordered by inclusion



A chain of ideals in $\mathcal{S}$ is a collection of ideals

$$\mathcal{C} = \{\ldots \subset I_{-1} \subset I_0 \subset I_1 \subset I_2 \subset \ldots\}$$

and to apply Zorn's Lemma, we need to show $\mathcal{C}$ has an upper bound.
Let

$$J = \bigcup_{I_k \in C} I_k$$

Claim: J is an ideal containing I.

> ***Proof.***
> $I \subset J$ is clear, since I is contained in all the ideals $I_k \in S$. It remains to show J itself is an ideal.
> $0 \in J$ because $0 \in I_k$ for any k.
> If $a, b \in J$, then $\exists I_{k_1}, I_{k_2}$ such that $a \in I_{k_1}, b \in I_{k_2}$, so w.l.o.g say $I_{k_1} \subset I_{k_2}$, then
> $$a, b \in I_{k_2} \implies a - b \in I_{k_2} \subset J \implies a - b \in J$$
> If $r \in R$, then $r \cdot a \in I_{k_2} \subset J \implies r \cdot a \in J$.
> Hence, J is an ideal containing I. ■

Therefore J is an upper bound for $\mathcal{C}$ and we can apply Zorn's lemma.
Therefore, $\mathcal{S}$ admits a maximal element, i.e a proper ideal $M \subset R$ such that $I \subset M$.
If $M' \subset R$ is an ideal such that $M \subset M'$, then $I \subset M'$ and so

$$\underbrace{M' \in \mathcal{S}}_{M' \text{ is proper}} \implies M' = M \quad \text{or} \quad \underbrace{M' \notin \mathcal{S}}_{M' \text{ is not proper}} \implies M' = R$$

■

Theorem 7.8: M maximal in comm. $R \iff R/M$ is field

If R is a commutative ring with $1 \neq 0$, then $M \subset R$ is maximal if and only if R/M is a field.

Proof.
Using the Lattice (fourth) Isomorphism Theorem we have

$$\{\text{Ideals of } R \text{ containing } M\} \longleftrightarrow \{\text{Ideals of } R/M\}$$
$$\{M, R\} \longleftrightarrow \{0, R/M\}$$

Since, the only ideals of R/M are 0 and itself, R/M is a field by Prop 7.1 (ii). ■

Recall: $P \subset R$ is prime if and only if R/P is an integral domain.

Corollary 7.9: Maximal ideals are prime

Maximal ideals are prime.

Proof.
If M is maximal then R/M is a field. Therefore, R/M is an integral domain and hence M is prime. ■

Example 7.2.
$n\mathbb{Z} \subset \mathbb{Z}$ is maximal if and only if $\mathbb{Z}/n\mathbb{Z}$ is a field, i.e n is prime.
So in $\mathbb{Z}$ we have

$$\{\text{prime ideals}\} = \{\text{maximal ideals}\}$$

Example 7.3.
The ideal generated by x, $(x) \subset \mathbb{Z}[x]$ is prime (check).
However, it is not maximal as $(x) \subset (2, x)$, but $1 \notin (2, x)$ and therefore $(2, x) \subsetneq \mathbb{Z}[x]$. So, in this case prime ideals are not necessarily maximal.

Example 7.4.
$(x) \subset \mathbb{R}[x]$ is maximal.

$$\mathbb{R}[x]/(x) \cong \mathbb{R}$$

and recall $\mathbb{R}$ is a field.

L8: Maximal Ideals and Ring of Fractions

Recall: $(X) \subset \mathbb{Z}[X]$ is prime, but $(X) \subsetneq (2, X)$, so it not maximal.
$(X) \in \mathbb{R}[X]$ is maximal because $\mathbb{R}[X]/(X) \cong \mathbb{R}$ is a field

Example 8.1. Let $a \in \mathbb{R}$. We defined the evaluation homomorphism before:

$$\begin{aligned} \mathrm{Ev}_a \colon \mathbb{R}[X] &\to \mathbb{R} \\ p(X) &\mapsto p(a) \end{aligned}$$

Observe that Ev_a is in fact surjective. Then

$$\mathbb{R}[X]/\mathrm{Ker}(\mathrm{Ev}_a) \cong \mathbb{R} \implies \mathrm{Ker}(\mathrm{Ev}_a) \text{ is a maximal ideal}$$

Denote the set of polynomials with real coefficients which have a as a root as

$$M_a \coloneqq \mathrm{Ker}(\mathrm{Ev}_a)$$

Claim: $M_a = (X - a)$ (e.g $M_0 = (X)$)

Proof.
If $p(X) \in (X - a)$ then we may write $p(X) = q(X) \cdot (X - a)$, $q(X) \in \mathbb{R}[X]$, then

$$\mathrm{Ev}_a(p(X)) = p(a) = q(a) \cdot (a - a) = 0 \implies p(X) \in M_a \implies (X - a) \subset M_a$$

Conversely, suppose $p(X) \in M_a = \mathrm{Ker}(\mathrm{Ev}_a)$. Let $p(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$, then you can check with polynomial division that $X - a$ divides $p(X)$ with remainder exactly $p(a)$ which is 0, hence $X - a$ is a factor of $p(X)$ [obviously, if $p(X)$ is a polynomial with a root at $X = a$, then $X - a$ is a factor], and we can write

$$\frac{p(X)}{X - a} = q(X)$$

therefore,

$$p(X) = q(X) \cdot (X - a) \implies p(X) \in (X - a) \implies M_a \subset (X - a)$$

and hence $M_a = (X - a)$. ■

Q: Is every maximal ideal of $\mathbb{R}[X]$ of the form M_a?
For example, in $\mathbb{Z}$, the {maximal ideals} = {prime ideals} but we saw above that in $\mathbb{Z}[X]$ there exist prime ideals that are not maximal.
Two standard questions:
(1) What are the primes?
(2) What are the maximal ideals?

Claim: Consider $I = (X^2 + 1)$, then $I \subset \mathbb{R}[X]$ is a maximal ideal.

Proof. We have that

$$\mathbb{R}[X] = \{a_0 + a_1X + a_2X^2 + a_3X^3 + \cdots + a_nX^n | a_k \in \mathbb{R},\ k = 0, 1, 2, \ldots n\}$$

What does $\overline{X^n}$ look like in $\mathbb{R}[X]/(X^2 + 1)$? We can deduce from the zero coset of the ideal:

$$X^2 + 1 \in (X^2 + 1) \implies \overline{X^2 + 1} = \overline{0} \implies \overline{X^2} = \overline{-1} \in \mathbb{R}[X]/I$$

Furthermore

$$X^3 = X \cdot X^2 \implies \overline{X^3} = \overline{X} \cdot \overline{(-1)} \in \mathbb{R}[x]/I$$
$$X^4 = X^2 \cdot x^2 \implies \overline{X^4} = \overline{(-1)} \cdot \overline{(-1)} \in \mathbb{R}[X]/I$$

Therefore, since all powers of X greater than 2 can be deconstructed into products of -1 and X, we can collapse the cosets of the quotient to a convenient form:

$$\mathbb{R}[X]/I = \{\overline{a_0 + a_1 X} \mid a_0, a_1 \in \mathbb{R}\}$$

with the rule $\overline{X} \cdot \overline{X} = \overline{-1}$.
This should be familiar and there is a ring isomorphism

$$\begin{aligned} \mathbb{R}[X]/I &\to \mathbb{C} \\ \overline{1} &\mapsto 1 \\ \overline{X} &\mapsto i \end{aligned}$$

and since the quotient ring is isomorphic to the field $\mathbb{C}$, I is maximal. ■

Claim: $(X^2 + 1)$ is **not** maximal in $\mathbb{C}[X]$

Proof. We know that $X + i, x - i \in \mathbb{C}[X]$ and

$$(X + i)(X - i) = X^2 + 1 \in (X^2 + 1)$$

But $X + i, X - i \notin (X^2 + 1)$ therefore $(X^2 + 1)$ is not prime in $\mathbb{C}[X]$ and consequently is not maximal. ■

Observe if $a \in R \subset S$ Then

$$\begin{aligned} (a)_R &= \{r \cdot a | r \in R\} \\ &\cap \\ (a)_S &= \{s \cdot a | s \in S\} \end{aligned}$$

can have different properties as ideals, e.g

$$\underbrace{(X) \subset \mathbb{Z}[X]}_{\text{prime}} \longrightarrow \underbrace{(x) \subset \mathbb{R}[X]}_{\text{maximal}}$$
$$\underbrace{(X^2 + 1) \subset \mathbb{R}[X]}_{\text{maximal}} \longrightarrow \underbrace{(X^2 + 1) \subset \mathbb{C}[X]}_{\text{not prime, not maximal}}$$

The Ring of Fractions

Q: How do we build $\mathbb{Q}$ out of $\mathbb{Z}$?
We want to add in multiplicative inverses like $\frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \dots$ but we can't just add them in and get a ring.
Consider

$$\mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) = \{(m, n) \mid m, n \in \mathbb{Z}, n \neq 0\}$$

and think of the elements of this set as the fractions $\frac{m}{n}$.
There are some repeats if we care about multiplication and addition like

$$\frac{1}{2} = \frac{2}{4} = \frac{3}{6}$$

We should define an equivalence relation

$$\frac{a}{b} \sim \frac{c}{d} \iff ad = bc$$

e.g $\frac{4}{6} \sim \frac{6}{9}$ because $4 \cdot 9 = 36 = 6 \cdot 6$.

Definition 8.1: Field of Rational Numbers

The **field of rational numbers** is

$$\mathbb{Q} := \left\{ \frac{m}{n} \middle| \, m, n \in \mathbb{Q},\, n \neq 0 \right\} / \sim$$

and this is a field with operations given by

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$
$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

We can also see that there is an injective ring homomorphism

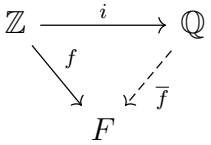
$$\mathbb{Z} \to \mathbb{Q}$$
$$n \mapsto \frac{n}{1}$$

Claim: If F is a field and there is an injective ring homomorphism

$$f : \mathbb{Z} \to F$$

Then it factors through $\mathbb{Q}$, i.e there is a ring homomorphism

$$\overline{f} : \mathbb{Q} \to F \text{ such that } f(n) = \overline{f}\left(\frac{n}{1}\right)$$



This is basically saying that if you have an injective homomorphism from Z to a field F,

then under the homomorphism the integers will have inverses $f(2) \cdot \frac{1}{2} \in F$ and one should see that this is exactly the rationals $\mathbb{Q}$ existing inside F.
Suppose R is any commutative ring with $1 \neq 0$.
Q: Can we do something similar with general rings R? i.e

$$R \times (R \setminus \{0\}) = \{(r, s) \mid r, s \in R, s \neq 0\}$$

(again, we will write (r, s) as $\frac{r}{s}$). We want to define $r^{-1} = \frac{1}{r}$, $r \neq 0$.
However, if r is a zero divisor, $r \cdot s = 0$ then in this case we want to exclude

$$\frac{1}{r} \cdot \frac{1}{s} = \frac{1}{r \cdot s} = \frac{1}{0}$$

Definition 8.2: Field of Fractions

Let R be an integral domain with $1 \neq 0$. Consider

$$R \times (R \setminus \{0\}) = \{(r, s) \mid r, s \in R, s \neq 0\}$$

Define an equivalence relation (**exercise to show it is**) by

$$\frac{a}{r} \sim \frac{b}{s} \iff a \cdot s = b \cdot r$$

There is no ambiguity in the equality of products since R is integral there are no zero zero divisors, $s, r \neq 0$.
The **field of fractions** of R is

$$Q(R) \coloneqq R \times (R \setminus \{0\})/\sim \; = \left\{ \left[\frac{a}{b}\right] \middle| \, a, b \in R,\, b \neq 0 \right\}$$

Theorem 8.3

$Q(R)$ is a field with operations

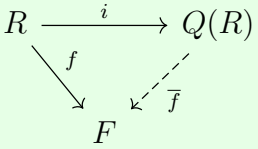
$$\frac{a}{r} + \frac{b}{s} = \frac{as + br}{rs}, \qquad \frac{a}{r} \cdot \frac{b}{s} = \frac{ab}{rs}$$

The map

$$\begin{aligned} i &: R \to Q(R) \\ r &\mapsto \frac{r}{1} \end{aligned}$$

is an injective ring homomorphism (we say R is a subring of its field of fractions).
Moreover, if F is any field such that $R \subset F$ is a subring (i.e there exists an injective ring homomorphism $f : R \to F$), then there is a ring homomorphism

$$\overline{f} : Q(R) \to F \text{ such that } f(x) = \overline{f} \circ i(x)$$



Proof. Think about it. . . ... ■

Example 8.2. $Q(\mathbb{Z}) = \mathbb{Q}$

Example 8.3. $R = \mathbb{R}[X]$ is an integral domain. The fractional field of R is the field of rational functions

$$Q(R) = \mathbb{R}(X) \coloneqq \left\{ \frac{p(X)}{q(X)} \middle| p, q \in \mathbb{R}[X],\ q \neq 0 \right\}$$

Example 8.4. If R is any integral domain with field of fractions $Q(R) = F$. Consider the integral domain $R[X]$. Then in particular $R \subset R[X]$, and $R[X] \subset Q(R[X])$ which tells us that

$$\begin{array}{ccc} R & \xrightarrow{\text{inclusion}} & F = Q(R) \\ & \searrow \quad \swarrow & \\ & Q(R[X]) & \end{array}$$

e.g $\mathbb{Z} \subset \mathbb{Z}[X]$, so in particular $\mathbb{Q} \subset Q(\mathbb{Z}[X])$.
In fact, since in $Q(\mathbb{Z}[X])$ you've added inverses to the coefficients but you also inverses to the polynomials, so you will get the field of rational functions

$$Q(\mathbb{Z}[X]) = \mathbb{R}(X)$$

Furthermore, this is generally true, as the field of fractions of $R[X]$ is going to be the rational functions with coefficients in the field of fractions of R, i.e

$$Q(R[X]) = F(X)$$

L9: The Chinese Remainder Theorem

Definition 9.1: Direct Product

Let R, S be rings.
The **direct product** of R and S is the ring

$$R \times S \coloneqq \{(r, s) | r \in R, s \in S\}$$

with ring operations

$$(r_1, s_1) + (r_2, s_2) \coloneqq (r_1 + r_2, s_1 + s_2)$$
$$(r_1, s_1) \cdot (r_2, s_2) \coloneqq (r_1 \cdot r_2, s_1 \cdot s_2)$$

More generally, if $\{R_\alpha \mid \alpha \in A\}$ is any collection of rings, then the **direct product** of the collection is the ring

$$\bigtimes_{\alpha \in A} R_\alpha \coloneqq \{(r_\alpha)_{\alpha \in A} \mid r_\alpha \in R_\alpha\}$$

with ring operations

$$(r_\alpha)_{\alpha \in A} + (s_\alpha)_{\alpha \in A} \coloneqq (r_\alpha + s_\alpha)_{\alpha \in A}$$
$$(r_\alpha)_{\alpha \in A} \cdot (s_\alpha)_{\alpha \in A} \coloneqq (r_\alpha \cdot s_\alpha)_{\alpha \in A}$$

Definition 9.2: Relatively Prime Integers

Given $a, b \in \mathbb{Z}$, we say they are **relatively prime** if the greatest common divisor is 1. Equivalently (Bezout's Identity), we say a, b are relatively prime if there exists $m, n \in \mathbb{Z}$ such that

$$am + bn = 1$$

Definition 9.3: Comaximal Ideals

In a commutative ring R with $1 \neq 0$, we say two ideals $A, B \subset R$ are **comaximal** (i.e relatively prime) if $A + B = R$. This implies there exists a sum $a + b$ such that $a + b = 1$.

Theorem 9.4: Product of pairwise comaximals is intersection

Let $A_1, \ldots, A_k \subset R$ be ideals in a commutative ring with $1 \neq 0$.
If they are pairwise comaximal then

$$A_1 \cdot A_2 \cdot \ldots \cdot A_k = A_1 \cap A_2 \cap \ldots \cap A_k$$

Proof.
We already know that

$$A_1 \cdot A_2 \cdot \ldots \cdot A_k \subset A_1 \cap A_2 \cap \ldots \cap A_k$$

It suffices to show

$$A_1 \cap A_2 \cap \ldots \cap A_k \subset A_1 \cdot A_2 \cdot \ldots \cdot A_k$$

Let's prove this for two ideals and then generalize. First, consider comaximal ideals A, B.
Let $x \in A \cap B$, then we want to show $x \in A \cdot B$
By comaximality,

$$\exists a \in A, b \in B,\ a + b = 1 \in A + B$$

In particular,

$$x = x \cdot 1 = x \cdot (a + b) = x \cdot a + x \cdot b$$

and so

$$x \in A \cap B \implies \left.\begin{array}{l} x \in A \implies x \cdot b \in A \cdot B \\ x \in B \implies x \cdot a \in A \cdot B \end{array}\right\} \implies x \cdot a + x \cdot b \in A \cdot B$$

Hence $x \in A \cdot B \implies A \cap B \subset A \cdot B$, and we can conclude

$$A \cdot B = A \cap B$$

The general case follows if we can show

$$A = A_1,\ B = A_2 \cdot A_3 \cdot \ldots \cdot A_k$$

are comaximal; we can do this with induction.
By assumption of comaximality A_1, A_i are comaximal for all $i \in \{2, \ldots, k\}$ therefore

$$\begin{aligned} &\exists x_2 \in A_1,\ y_2 \in A_2, \quad \text{s.t.} \quad 1 = x_2 + y_2 \\ &\exists x_3 \in A_1,\ y_3 \in A_3, \quad \text{s.t.} \quad 1 = x_3 + y_3 \\ &\qquad\qquad \vdots \\ &\exists x_k \in A_1,\ y_k \in A_k, \quad \text{s.t.} \quad 1 = x_k + y_k \end{aligned}$$

and this implies

$$1 = (x_2 + y_2) \cdot (x_3 + y_3) \cdot \ldots \cdot (x_k + y_k) \in A_1 + (A_2 \cdot \ldots \cdot A_k)$$

since all x's are in A_1 and all y's are in the product of the other ideals, the expanded product will have some mix of x's and some mixes of the y's. Hence, we conclude $A_1, A_2 \cdot \ldots \cdot A_k$ are comaximal. ■

Theorem 9.5: Chinese Remainder Theorem

Let $A_1, \ldots A_k \subset R$ ideals in a commutative ring with $1 \neq 0$.
The map

$$\begin{aligned} \phi \colon R &\to (R/A_1) \times (R/A_2) \times (R/A_3) \times \ldots \times (R/A_k) \\ r &\mapsto (r + A_1, r + A_2, r + A_3, \ldots, r + A_k) \end{aligned}$$

is a ring homomorphism with $\operatorname{Ker} \phi = A_1 \cap A_2 \cap \ldots \cap A_k$.
Moreover, if they are pairwise comaximal, then ϕ is surjective.

Corollary 9.6: Isomorphisms of quotient rings by product of ideals

If $A_1, \ldots, A_k \subset R$ are pairwise comaximal ideals in a commutative ring with $1 \neq 0$, then there is an isomorphism of rings (by the First Isomorphism Theorem)

$$R/(A_1 \bullet \ldots \bullet A_k) \cong R/(A_1 \cap A_2 \cap \ldots \cap A_k) \cong (R/A_1) \times (R/A_2) \times (R/A_3) \times \ldots \times (R/A_k)$$

So you can think of your quotient ring over the one ideal or over the separate components of the ideal.

Corollary 9.7: $\mathbb{Z}/n\mathbb{Z}$ isomorphic to quotients by prime factors

Let n be a positive integer with factorization into unique primes

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$$

then

$$\mathbb{Z}/n\mathbb{Z} \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z}) \times (\mathbb{Z}/p_2^{\alpha_2}\mathbb{Z}) \times \ldots \times (\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z})$$

Example 9.1. Here are factorizations of two integer modulo rings:

$$\mathbb{Z}/30\mathbb{Z} \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z})$$
$$\mathbb{Z}/168\mathbb{Z} \cong (\mathbb{Z}/8\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/7\mathbb{Z})$$

Proof of CRT.
We want to see

$$\phi\colon R \to (R/A_1) \times (R/A_2) \times (R/A_3) \times \ldots \times (R/A_k)$$
$$r \mapsto (r + A_1, r + A_2, r + A_3, \ldots, r + A_k)$$

(1) $\operatorname{Ker}\phi = A_2 \cap \ldots \cap A_k$
(2) If $A_1, \ldots, A_k$ are pairwise comaximal then ϕ is surjective.
We will prove these for $k = 2$ and then generalize:
(1) Let $A, B \subset R$ be ideals and

$$\phi\colon R \to (R/A) \times (R/B)$$
$$r \mapsto (r + A, r + B)$$

Let $r \in \operatorname{Ker}\phi$, then

$$\left.\begin{array}{l} r + A = 0 + A \implies r \in A \\ r + B = 0 + B \implies r \in B \end{array}\right\} \implies r \in A \cap B$$

If $r \in A \cap B$ then

$$\left.\begin{array}{l} r \in A \implies r + A = 0 + A \\ r \in B \implies r + B = 0 + B \end{array}\right\} \implies r \in \operatorname{Ker}\phi$$

(2) If A, B are comaximal then there exists $x \in A, y \in B$ such that $1 = x + y$, then

$$1 - x = y \in B \implies 1 + A = y + A$$
$$1 - y = x \in A \implies 1 + B = x + B$$

and hence

$$\phi(x) = (x + A, x + B) = (0 + A, 1 + B)$$
$$\phi(y) = (y + A, y + B) = (1 + A, 0 + B)$$

So if we have any element $(r + A, s + B) \in R/A \times R/B$ then

$$\begin{aligned}(r + A, s + B) =& (r + A, 0 + B) + (0 + A, s + B)\\ =& (r + A, r + B) \cdot (1 + A, 0 + B) + (s + A, s + B) \cdot (0 + A, 1 + B)\\ =& \phi(r) \cdot \phi(y) + \phi(s) \cdot \phi(x)\\ =& \phi(ry + sx) \implies \phi \text{ surjective}\end{aligned}$$

More generally if $A_1, \ldots, A_k \subset R$ are ideals.
Let $A = A_1$, $B = A_2 \cdot A_3 \ldots \cdot A_k$, then we have a homomorphism

$$\phi_1 \colon R \to R/A \times R/B, \quad \operatorname{Ker} \phi_1 = A_1 \cap B$$

Now by the Lattice Isomorphism Theorem $A_2/B, A_3/B, \ldots, A_k/B \subset R/B$ are ideals. Take

$$A' = A_2/B, \quad B' = (A_3/B) \cdot (A_4/B) \cdot \ldots \cdot (A_k/B) = (A_3 \cdot A_4 \cdot \ldots A_k)/B$$

Then we get a homomorphism

$$\phi_2 \colon R/B \to (R/B)/A' \times (R/B)/B', \quad \operatorname{Ker} \phi_2 = A' \cap B'$$

By the third isomorphism theorem

$$(R/B)/A' = (R/B)/(A_2/B) \cong R/A_2$$

and similarly,

$$(R/B)/B' = (R/B)/(A_3 \cdot A_4 \cdot \ldots \cdot A_k)/B \cong R/(A_3 \cdot A_4 \cdot \ldots \cdot A_k)$$

Therfore, we have

$$\hat{\phi}_2 = (\mathrm{Id}, \phi_2) \circ \phi_1 \colon R \to R/A_1 \times R/A_2 \times R/(A_3 \cdot \ldots \cdot A_k)$$

Proceeding inductively on k, we end up with

$$\phi \colon R \to R/A_1 \times R/A_2 \times \ldots \times R/A_k$$

and the surjectivity when $A_1, \ldots, A_k$ are pairwise comaximal follow essentially because $A_1, A_2, \ldots A_k$ are comaximal. ■

L10: Euclidean Domains and PIDs

Definition 10.1: Norm

Let R be an integral domain.
Any function

$$N: R \to \mathbb{Z}^+ \cup \{0\}$$

such that $N(0) = 0$ is called a **norm**.

Example 10.1. The zero norm

$$\begin{aligned} N: R &\to \mathbb{Z}^+ \cup \{0\} \\ r &\mapsto 0 \end{aligned}$$

Example 10.2. The absolute value norm on the integers

$$\begin{aligned} N: \mathbb{Z} &\to \mathbb{Z}^+ \cup \{0\} \\ n &\mapsto |n| \end{aligned}$$

Definition 10.2: Euclidean Domain, Quotient, Remainder

An integral domain R is a **Euclidean domain** if it admits a norm N such that for all $a, b \in R$ and $b \neq 0$, there exists $q, r \in R$ such that

$$a = qb + r$$

where $r = 0$ or $N(b) > N(r)$ (i.e Euclidean domains have the *familiar* division property known as the Euclidean condition).
We call q the **quotient** of a by b and r the **remainder** of a with respect to b.

What is nice about Euclidean domains is that you have the Euclidean Division Algorithm

$$\begin{aligned} a &= q_0 b + r_0 \\ b &= q_1 r_0 + r_1 \\ r_0 &= q_2 r_1 + r_2 \\ &\vdots \\ r_{n-1} &= q_{n+1} r_n \end{aligned}$$

which must terminate because by the well ordering on the non-negative integers, you are constantly reducing the size of the remainder, so you must eventually reach 0.

$$N(b) > N(r_0) > N(r_1) \cdots > N(r_n) > N(r_{n+1}) = N(0) = 0$$

Example 10.3. Fields F are Euclidean domains with any norm N.
If $a, b \in F$, $b \neq 0$, then

$$a = \underbrace{(a \cdot b^{-1})}_{\text{quotient}} \cdot b + 0$$

which means in a field, you can always divide evenly.

Example 10.4. The integers $\mathbb{Z}$ are a Euclidean domain with $N(a) = |a|$.

Example 10.5. If F is a field, the polynomial ring $F[X]$ is a Euclidean domain with norm $N(p) \coloneqq \deg(p)$. It's important to note that non-zero elements can have zero norm, as in this case, the constant polynomials have degree 0.

Proof.
Let $a(X), b(X) \in F[X]$ and $b(X) \neq 0$.
We proceed by induction on $\deg(a) = N(a)$.
If $a(X) = 0$, then $0 = 0 \cdot b(X) + 0$.
So we may assume $a(X) \neq 0$. If $\deg(a) < \deg(b)$, then

$$N(a) < N(b) \implies a(X) = 0 \cdot b(X) + a(X)$$

which verifies the Euclidean condition.
Now assume $\deg(a) \geq \deg(b)$, i.e

$$a(X) = a_m X^m + a_{n-1} X^{m-1} + \cdots + a_0$$
$$b(X) = b_n X^n + b_{n-1} X^{n-1} + \cdots + b_0$$

and since $b(X) \neq 0$ then $b_n \neq 0$ and since the coefficient ring is a field, we know $b_n^{-1} \in F$.
Let

$$a'(X) = a(X) - \frac{a_m}{b_n} X^{m-n} \cdot b(X)$$

then $\deg(a') < \deg(a)$ because we got rid of the term $a_m X^m$
By induction on $\deg(a)$ there exist $q'(X), r'(X)$ such that $N(r') < N(b)$ or $r'(X) = 0$ and

$$a' = q' \cdot b + r'$$

Hence we can write

$$a = a' + \frac{a_m}{b_n} X^{m-n} \cdot b(X)$$
$$a(X) = [q'(X) \cdot b(X) + r'(X)] + \left[\frac{a_m}{b_n} X^{m-n} b(X)\right]$$
$$= \left[q'(X) + \frac{a_m}{b_n} X^{m-n}\right] b(X) + r'(X)$$

and this also satisfies the Euclidean condition. ■

Proposition 10.3: Euclidean domains are principal

Every ideal in a Euclidean domain is principal.

Proof.
If $I \subset R$ is a non-zero ideal, consider

$$\mathcal{N} = \{N(a) \mid a \in I\} \subset \mathbb{Z}^+ \cup \{0\}$$

By the well-ordering principle, there exists $d \in I$ such that $N(d) = \min \mathcal{N}$. Clearly

$$d \in I \implies (d) \subset I$$

Conversely, suppose $a \in I$, then

$$a = q \cdot d + r$$

where $r = 0$ or $N(r) < N(d)$.
If $r = 0$, then

$$a = q \cdot d \implies a \in (d) \implies I = (d)$$

If $r \neq 0$, then $a - qd = r$. However

$$a, d \in I \implies a - qd \in I \implies r \in I$$

and because by construction $N(r) < N(d)$ this is impossible as d is the element with minimum norm. Hence, $r = 0$ and we go back to the previous situation.
Therefore, $(d) = I$. ■

Corollary 10.4: Ideals in $\mathbb{Z}$ are principal

Every ideal in $\mathbb{Z}$ is principal.

Think about it like this: in the integers, if you consider the ideal generated by 2 and 3 and you know $3 = 2 \cdot 1 + 1$, that means if 3 is in the ideal with 2, 1 must also be in the ideal. So the $(2, 3) = (1)$, so you have the whole ring. With similar logic, you can see that $(4, 6) = (2)$. This extends to the general Euclidean domain as seen in Prop 10.1, as the ideal (d) is the greatest common divisor.

Definition 10.5: Multiple, Divisor, GCD

Let R be a commutative ring with $1 \neq 0$ and $a, b \in R$ such that $b \neq 0$.

(1) We say $a \in R$ is a **multiple** of b if there exists an $r \in R$ such that

$$a = r \cdot b$$

We call b a **divisor** of a, in this case, (i.e $b \mid a$).

(2) A **greatest common divisor** of $a, b \in R$ is $d \neq 0$ such that
   (i) $d \mid a$, $d \mid b$
   (ii) If $d' \mid a$, $d' \mid b$, then $d' \mid d$.
   We write $d = \gcd(a, b)$ or sometimes just $d = (a, b)$.

Recall that $b \mid a$ if and only if $(a) \subset (b)$.

Definition 10.6: Ideal GCD

Let $I = (a, b) \subset R$, then $d \in R$ is a **greatest common divisor** $d = \gcd(a, b)$ if
(i) $I \subset (d)$
(ii) If $I \subset (d')$, then $(d) \subset (d')$.
In other words, $d \in R$ is a greatest common divisor of $a, b \in R$ if (d) is the smallest principal ideal containing (a, b).

Proposition 10.7

If $a, b \in R$ are nonzero, and $(a, b) = (d)$ then $d = \gcd(a, b)$

Theorem 10.8: GCDs exist in Euclidean domains

If R is a Euclidean domain, then greatest common divisors **always** exist

Proof.

$$\left.\begin{aligned} a &= q_0 b + r_0 \\ b &= q_1 r_0 + r_1 \\ r_0 &= q_2 r_1 + r_2 \\ &\vdots \\ r_{n-1} &= q_{n+1} r_n \end{aligned}\right\} \implies r_n = \gcd(a, b)$$

■

Definition 10.9: Principal Ideal Domain

A **principal ideal domain** (PID) is an integral domain in which every ideal is principal

Theorem 10.10: Euclidean domain is PID is Integral domain

Every Euclidean domain is a PID, i.e

$$\text{Integral domain} \supsetneq \text{PID} \supsetneq \text{Euclidean domain}$$

Theorem 10.11

Let R be a PID and $a, b \in R$ nonzero. If $(a, b) = (d)$ (this always exists in a PID), then
(1) d is a greatest common divisor of a and b.
(2) There exist $x, y \in R$ such that $d = ax + by$.
(3) d is a unique to multiplication by a unit.

Claim: $\mathbb{Z}[X]$ is an integral domain BUT in particular $(2, X)$ is not principal therefore $\mathbb{Z}[X]$ is not a PID.

Proof.
Suppose it is principal, i.e $(2, X) = (p(X))$, then

$$2 = q(X)p(X) \implies \deg p(X) = 0$$

i.e $p(X) \equiv a \in \mathbb{Z}$.
Moreover $a \mid 2$ implies $a = \pm 1, \pm 2$. Also, $(2, X) \neq \mathbb{Z}[X]$ as for example

$$3 \neq \underbrace{2p(X)}_{\text{3 is not even}} + \underbrace{X \cdot q(X)}_{\text{would need to be 0}}$$

Then, $p(X) \neq \pm 1$ otherwise $(2, X) = (1) = \mathbb{Z}[X]$. Therefore $p(X)$ must be ± 2.
But $(2, X) \neq (2)$ because $X \neq 2 \cdot q(X)$.Essentially, the issue is that 2 has no multiplicative inverse in $\mathbb{Z}$ but the coefficient of X is 1. So, nothing makes sense when $p(X) = \pm 1, \pm 2$ which means the initial assumption was false and $(2, X)$ is not principal. ■

Theorem 10.12: Nonzero primes ideals are maximal in PID

Every non-zero prime in a PID is maximal, e.g. in $\mathbb{Z}$, every prime is maximal.

Proof. Let $(p) \subset R$ be a nonzero prime in a PID.
There exists a maximal ideal $M \subset R$ such that $(p) \subset M$.
Since R is a PID, then every ideal is principal, hence

$$M = (m) \implies m \mid p \implies \exists r \in R,\ p = r \cdot m$$

Because (p) is prime either $r \in (p)$ or $m \in (p)$.
If $m \in (p)$ then $(m) = (p)$.
Suppose $r \in (p)$, say $r = s \cdot p$, $s \in R$. Then

$$p = r \cdot m = (s \cdot p) \cdot m \implies p \cdot (1 - s \cdot m) = 0$$

Since R is an integral domain and $p \neq 0$, then

$$1 - sm = 0 \implies sm = 1 \implies m \in R^{\times}$$

But then $(m) = R$, which means (m) is not maximal, by definition. This is a contradiction and hence $(p) = (m)$ is maximal. ■

Theorem 10.13: If $R[X]$ is PID then R is field

If R is a commutative ring such that $R[X]$ is a PID, then R is a field.

Proof.
Suppose $R[X]$ is a PID (in particular, an integral domain), then $R \subset R[X]$ is an integral domain. We use a clever trick

$$R[X]/(X) \cong R \implies (X) \text{ is prime} \implies (X) \text{ is maximal} \implies R \text{ is a field} \qquad \blacksquare$$

L11: Unique Factorization Domains

Definition 11.1: Irreducible/Reducible, Prime, Associate Elements

Let R be an integral domain

(i) Suppose $r \in R \setminus \{0\}$, $r \notin R^\times$.
We say r is **irreducible** if whenever $r = a \cdot b$, either $a \in R^\times$ or $b \in R^\times$.
We say r is **reducible** if it is not irreducible.

(ii) Suppose $r \in R \setminus \{0\}$, $r \notin R^\times$
We say r is **prime** if (r) is a prime ideal.
In other words, if $r \mid a \cdot b$, then either $r \mid a$ or $r \mid b$.

(iii) We say $a, b \in R$ are **associates** if there exists $u \in R^\times$ such that $a = u \cdot b$.
(If a and b generate the same principal ideal, then they are associates. Check HW3 P1)

Proposition 11.2: Prime elements in integral domain are irreducible

Any prime element in an integral domain is irreducible.

Proof. Suppose $p = a \cdot b \in R$ and (p) is a prime ideal.
Then $p \in (p)$ implies $a \in (p)$ or $b \in (p)$. W.l.o.g let $a \in (p)$.
So $\exists r \in R$ such that $a = p \cdot r$ and hence

$$p = (p \cdot r) \cdot b = p \cdot (r \cdot b)$$

Since R is an integral domain, we can cancel p, then, $1 = r \cdot b$, so $b \in R^\times$. ■

Example 11.1. It turns out to be that the converse is not true, i.e irreducible but not prime elements.
Consider the ring

$$\mathbb{Z}[\sqrt{-5}] :- \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$$

There exists a norm on this (not exactly the same as the norm for Euclidean domains), with properties

- $N(a + b\sqrt{-5}) \coloneqq a^2 + 5b^2$
- $N(x \cdot y) = N(x) \cdot N(y)$
- $N(x) = \pm 1$ if an only if $x \in \mathbb{Z}[\sqrt{-5}]^\times$

Claim: $2 + \sqrt{-5}$ is irreducible

Proof. Suppose

$$2 + \sqrt{-5} = (a + b\sqrt{-5}) \cdot (c + d\sqrt{-5})$$

Then

$$N(2+\sqrt{-5}) = 4+5 = 9 \implies N(a+b\sqrt{-5}) \mid 9 \implies N(a+b\sqrt{-5}) = \pm 1 \text{ or } \pm 3$$

Observe that if $b \neq 0$, then

$$N(a+b\sqrt{-5}) = a^2 + 5b^2 \geq 5$$

Therefore we have to assume $b = 0$ if we want the norm to be $\pm 1, \pm 3$ and so

$$b = 0 \implies N(a+b\sqrt{-5}) = N(a) = a^2$$

So the norm is a perfect square, and since the only candidates are ± 1 and ± 3, the only perfect square between them is 1 and hence

$$N(a+b\sqrt{-5}) = 1 \implies a+b\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]^\times$$

which means that $2+\sqrt{-5}$ is irreducible. ■

Claim: $2+\sqrt{-5}$ is **not** prime.

Proof. We know

$$3^2 = 9 = (2+\sqrt{-5}) \cdot (2-\sqrt{-5}) \in (2+\sqrt{-5})$$

It remains to show that 3 is not in the ideal $(2+\sqrt{-5})$, i.e $3 \notin (2+\sqrt{-5})$. If $3 = (a+b\sqrt{-5}) \cdot (2+\sqrt{-5})$, then

$$9 = N(3) = N(a+b\sqrt{-5}) \cdot N(2+\sqrt{-5}) = N(a+b\sqrt{-5}) \cdot 9 \implies N(a+b\sqrt{-5}) = 1$$

which immediately tells us $b = 0$ and $a = \pm 1$.
But $3 \neq \pm(2+\sqrt{-5})$ hence $3 \notin (2+\sqrt{-5})$ and so $2+\sqrt{-5}$ is not prime. ■

We see that in an arbitrary integral domain, the notion of primality and irreduciblity are not the same. However, there are circumstances where they are the same thing.

Proposition 11.3: Element in PID is prime iff it is irreducible

In a PID an element is prime *iff* it is irreducible.

Proof. Prop 11.2 shows prime $\implies$ irred.; it remains to show irred. $\implies$ prime.
Suppose $r \in R$ is irreducible and recall that maximal ideals are prime. Hence we will show that (r) is maximal.
Suppose $(r) \subset (m) \subsetneq R$, then

$$r \in (m) \implies \exists s \in R,\ r = s \cdot m \underbrace{\implies}_{r \text{ irreducible}} s = R^\times \text{ or } m \in R^\times$$

By assumption $(m) \subsetneq R$ and this implies

$$m \notin R^\times \implies s \in R^\times \implies r \text{ and } m \text{ associates} \implies (r) = (m)$$ ■

Example 11.2. In $\mathbb{Z}$, the irreducibles are the primes (and their negatives)

Observe that the factorization of any integer into primes is unique!

We see that irreducibility, in the natural sense, is about not being able to be split up into smaller pieces (up to a unit). Primality, while similar, is more about divisibility. We saw that 9 could be represented by fundamentally two different ideals, namely (3) and $(2+\sqrt{-5})$.

Definition 11.4: Unique Factorization Domain

A **unique factorization domain** (UFD) is an integral domain R such that for all $r \in r \setminus \{0\}$, $r \notin R^\times$

(i) $r = p_1 \cdot p_2 \cdot \ldots \cdot p_n$ for p_i irreducible.

(ii) This decomposition is unique up to associates and reordering, i.e if

$$r = q_1 \cdot \ldots \cdot q_m, \quad q_j \text{ irreducible}$$

Then after reordering, $q_i = u_i p_i, u_i \in R^\times$ and $n = m$.

Example 11.3. Fields are vacuously UFDs, because the definition of a UFD constrains non-units to certain conditions however in a field you only have units, so these constraints don't apply.

Example 11.4. $\mathbb{Z}$ is a UFD.

Example 11.5. $\mathbb{Z}[\sqrt{-5}]$ is **not** a UFD as

$$3^2 = 9 = (2+\sqrt{-5}) \cdot (2-\sqrt{-5})$$

and $3, 2 \pm \sqrt{-5}$ are irreducibles which are not associate.

Proposition 11.5: Element in UFD is prime iff it is irreducible

In a UFD, an element is prime *iff* it is irreducible.

Proof. It suffices to show once more that irreducible $\implies$ prime.
Suppose $r \in R$ is irreducible and $a \cdot b \in (r)$ i.e there exists $c \in R$ such that $a \cdot b = r \cdot c$
By unique factorization in a UFD, a, b, c have unique factorizations, i.e

$$\begin{aligned} a &= p_1 \cdot p_2 \cdot \ldots \cdot p_n, \quad p_i \text{ irreducible, unique} \\ b &= q_1 \cdot q_2 \cdot \ldots \cdot q_m, \quad q_j \text{ irreducible, unique} \\ c &= r_1 \cdot r_2 \cdot \ldots \cdot r_l, \quad r_k \text{ irreducible, unique} \end{aligned}$$

Since $a \cdot b = r \cdot c$ we have

$$p_1 \cdot p_2 \cdot \ldots \cdot p_n \cdot q_1 \cdot \ldots \cdot q_m = r \cdot r_1 \cdot r_2 \cdot \ldots \cdot r_l$$

since r is irreducible, both sides are factorizations into irreducibles. By unique factorization and w.l.o.g.

$$r = u \cdot p_1,\ u \in R^\times \implies r \mid a$$ ■

and so $a \in (r)$ which means (r) is a prime ideal (with q you get $b \in (r)$).

Proposition 11.6: Nonzero elements in UFD have GCD

Let $a, b \in R \setminus \{0\}$ in a UFD. Then there is a greatest common divisor of a, b in R.

Proof. We write for $u, v \in R^\times$ and p_i's irreducible

$$a = u \cdot p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_n^{e_n}$$
$$b = v \cdot p_1^{f_1} \cdot p_2^{f_2} \cdot \ldots \cdot p_n^{f_n}$$

We allow some exponents to be 0 ($p_i^0 = 1$) and we require $p_i \neq p_j$ if $i \neq j$ for example

$$\begin{pmatrix} 12 = 2^2 \cdot 3 \to 12 = 2^2 \cdot 3^1 \cdot 5^0 \\ 20 = 2^2 \cdot 5 \to 20 = 2^2 \cdot 3^0 \cdot 5^1 \end{pmatrix}$$

So the elements a, b can be written in terms of the same irreducibles to certain powers.
Claim:

$$d = p_1^{\min\{e_1, d_1\}} \cdot p_2^{\min\{e_2, d_2\}} \cdot \ldots \cdot p_n^{\min\{e_n, d_n\}}$$

is the gcd of a and b.

> ***Proof.*** Clearly $d \mid a$, $d \mid b$, by construction, since it's factors come from the same set of factors of a, b, namely p_i. Since d is a common divisor, it remains to show it is a greatest common divisor.
> If $c \mid a$, $c \mid b$, then we want to see that $c \mid d$. Unique factorization tells us
>
> $$c = q_1^{g_1} \cdot \ldots \cdot q_m^{g_m}, \quad q_i \text{ irreducible}, \quad q_i \neq q_j, \text{ and } g_i > 0$$
>
> Since $c \mid a$, $c \mid b$, then after (possibly) changing associates we see that the set of factors of c have to be factors of a and b, i.e
>
> $$\{q_1, \ldots, q_n\} \subset \{p_1, \ldots, p_n\}$$
>
> and since c divides both a and b then $g_i \leq \min\{e_i, f_i\}$ and thus $c \mid d$. ■

Therefore there exists a greatest common divisor of a, b in R, namely, the d we have shown. ■

L12: PIDs are UFDs and Polynomial Rings

Definition 12.1: Ascending Chains, Noetherian Ring

Let R be a commutative ring with $1 \neq 0$.
An **ascending chain** of ideals in R is a sequence

$$I_1 \subset I_2 \subset I_3 \subset \ldots \subset R$$

We say an ascending chain **stabilizes** if there exists $N \in \mathbb{N}$ such that for all $n, m \geq N$, $I_n = I_m$.
We say R satisfies the **ascending chain condition** (a.c.c.) if every ascending chain stabilizes.
If R satisfies the a.c.c., we say it is a **Noetherian ring**.

Theorem 12.2: PID is Noetherian

If R is a PID, then R is Noetherian.

Proof. Let

$$I_1 \subset I_2 \subset I_3 \subset \ldots \subset R$$

be an ascending chain in a PID.
Consider

$$I := \bigcup_{n \in \mathbb{N}} I_n$$

which is an ideal. Then since R is a PID, $I = (a)$ for some $a \in R$.
In particular,

$$a \in I = \bigcup_{n \in \mathbb{N}} I_n \implies a \in I_N$$

for some $N \in \mathbb{N}$.
But if $a \in I_N$ then we also know $(a) \subset I_N$ implying $I \subset I_N$.
But by the definition of I, we also have the containment in the other direction, i.e $I_N \subset I$, and hence we have $I = I_N$.
Furthermore the chain stops "growing" at a finite ideal I_N and so the ascending chain stabilizes

$$I = I_N = I_{N+1} = I_{N+2} = \ldots$$

Therefore, R is a Noetherian ring. ■

Theorem 12.3: PID is UFD

Every PID is a UFD.

Let R be a PID.
We want to show if $r \in R \setminus \{0\}$, $r \notin R^\times$, then r admits a **unique** expression as a product of

irreducibles.

Lemma 12.4: Existence of product of irreducibles in PID

A element r in a PID has **some** expression as a product of irreducibles

Proof.
If r is irreducible, then $r = r$ and we are done.
If not, then we can write $r = r_1 \cdot r_2$, where $r_1, r_2 \notin R^\times$. Then $r \in (r_1)$ but $(r) \neq (r_1)$ because in order for that to be the case, r_2 would have to a be a unit. Therefore, it is a proper subset i.e, $(r) \subsetneq (r_1)$.
If r_1, r_2 are irreducibles, then we are done.
If not,

$$r_1 = r_{11} \cdot r_{12}$$
$$r_2 = r_{21} \cdot r_{22}$$

where $r_{ij} \notin R^\times$, $i, j \in \{1, 2\}$. Again, $r_1 \in (r_{11})$ but (since r_{12} is not a unit) $(r_1) \neq (r_{11})$, and hence $(r) \subsetneq (r_1) \subsetneq (r_{11})$.
Since R is a PID, it is also Noetherian, and so this chain stabilizes eventually. This means we will reach a point where and $(r_{1111}) = (r_{11111})$ implying $r_{1111} = r_{11111} \cdot u$ for some unit u, and thus r_{1111} is irreducible. Hence in general r will be factored into something like

$$r = (r_{111\ldots1} \cdot r_{111\ldots2}) \cdot \ldots \cdot (r_{222\ldots1} \cdot r_{222\ldots2})$$

where each term on the right side of the inequality is irreducible. ■

Lemma 12.5: Uniqueness of product of irreducibles in PID

The factorization into irreducibles is **unique** (up to reordering and associates).

Proof.
Say the factorization into irreducibles is $r = p_1 \cdot p_2 \cdot \ldots \cdot p_n$. We proceed by induction on n.
Base Case: If $n = 1$, then $r = \underbrace{p_1}_{\text{irred.}}$ implies r is irreducible.
Suppose now r factors into a different product of irreducibles,

$$r = q_1 \cdot q_2 \cdot \ldots \cdot q_n,\ n \geq 2,\ q_i \text{ irreducible } \forall i \in \{1, \ldots, n\}$$

But then $q_1, (q_2 \cdot \ldots \cdot q_n) \notin R^\times$ (since by definition irreducibles are non-units) implying r is not irreducible, which is a contradiction.
Therefore, $r = p_1$ is the unique way to write r as the product of irreducibles when $n = 1$.
Induction Hypothesis: Now suppose if r admits a factorization into at most $n - 1$ irreducibles, then the factorization is unique.

Inductive Step: If we can write into two different factorizations

$$\begin{aligned} r &= p_1 \cdot p_2 \cdot \ldots \cdot p_n, \quad p_i\text{'s irreducible} \\ &= q_1 \cdot q_2 \cdot \ldots \cdot q_m, \quad q_j\text{'s irreducible and } m \geq n \end{aligned}$$

Then $p_1 \mid q_1 \cdot (q_2 \cdot \ldots \cdot q_m)$ and recall irreducibles are prime in a PID. Since p_1 is irreducible, it is prime and so either $p_1 \mid q_1$ or $p_1 \mid (q_2 \cdot \ldots \cdot q_n)$. W.l.o.g. assume $p_1 \mid q_1$ i.e $q_1 = u \cdot p_1$, $u \in R$.
Since q_1 is irreducible, then $u \in R^\times$ or $p_1 \in R^\times$. But p_1 is irreducible, so it can be not an element of $R^\times$, therefore $u \in R^\times$ and so p_1 and q_1 associate.
So we write

$$\begin{aligned} r = p_1 \cdot p_2 \cdot \ldots \cdot p_n &= q_1 \cdot q_2 \cdot \ldots \cdot q_m \\ &= (u \cdot p_1) \cdot q_2 \cdot \ldots \cdot q_m \end{aligned}$$

Since R is an integral domain, we can cancel p_1 from both sides to get

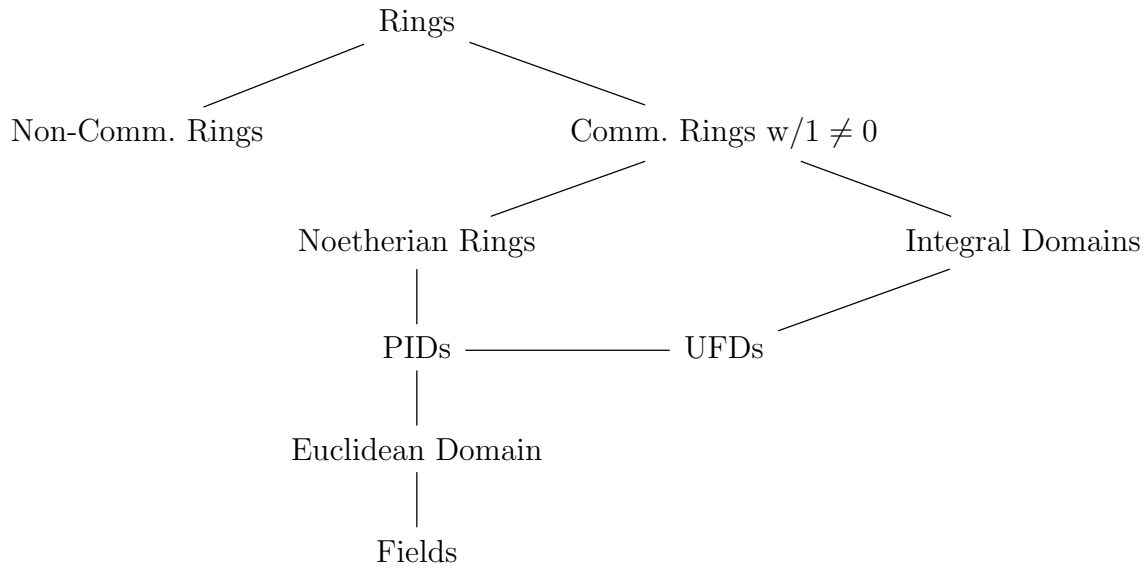
$$\underbrace{p_2 \cdot \ldots \cdot p_n}_{\text{product of (n-1) irred.}} = (u \cdot q_2) \cdot q_3 \cdot \ldots \cdot q_m$$

Now by our induction hypothesis, r admits a unique factorization into at most $(n-1)$ irreducibles, which implies the list of irreducibles on the left and right side of the equality are the same (up to associates) i.e.

$$\{(u \cdot q_2), q_3, q_4, \ldots, q_m\} = \{p_2, p_3, \ldots, p_n\}$$

and so $m = n$ and the p_i's are unique. ■

We can now see a hierarchy for the specific structures we have discussed thus far



Polynomial Rings (Again)

Let R be an commutative ring with $1 \neq 0$.
Now assume R is an integral domain and recall some facts we've already proven about :
(1) $R[X]$ is an integral domain.
(2) $R[X]^\times = R^\times$ e.g. $\mathbb{Z}[X]$, the only units are $\{\pm 1\}$.
(3) $\deg[p(X) \cdot q(X)] = \deg p(X) + \deg q(X)$
(4) The field of fractions of $R[X]$ is the field of rational functions

$$R(X) \coloneqq \left\{ \frac{p(X)}{q(X)} \middle| \; p, q \in R[X],\, q \neq 0 \right\}$$

(5) If F is a field, then $F[X]$ is a Euclidean Domain.

Corollary 12.6: $F[X]$ is PID, UFD, and Noetherian

If F is a field, $F[X]$ is a PID, UFD, and Noetherian.

(6) Let $I \subset R$ be an ideal and R a commutative ring (not necessarily integral) and consider the ideal generated by I in $R[X]$, i.e.

$$(I) \coloneqq I[X] \coloneqq \{p(X) \in R[X] \mid \text{coeffs. are in } I\}$$

Then

$$R[X]/(I) \cong (R/I)[X]$$

Proof.
Consider the map

$$\phi : R[X] \to (R/I)[X]$$
$$a_0 + a_1 X + \cdots + a_n X^n \mapsto \overline{a_0} + \overline{a_1} X + \overline{a_2} X^2 + \cdots + \overline{a_n} X^n$$

for example

$$\phi : \mathbb{Z}[X] \to (\mathbb{Z}/3\mathbb{Z})[X]$$
$$1 + 2X + 4X^3 \mapsto \overline{1} + \overline{2}X + \overline{4}X^3 = \overline{1} + \overline{2}X + X^3$$

"Clearly" ϕ is a surjective ring homomorphism, so

$$(R/I)[X] \cong R[X]/\operatorname{Ker}\phi$$

But the kernel is exactly the set of polynomials with coefficients that are zero (i.e. in the ideal), hence $\operatorname{Ker}\phi \coloneqq \{a_0 + a_1 X + \cdots + a_n X^n \mid a_i \in I\} = (I)$. ■

Example 12.1. Consider $3\mathbb{Z} \coloneqq \{0, 3, -3, 6, -6, \dots\}$ and

$$(3\mathbb{Z}) \coloneqq \{a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n \mid a_i \in 3\mathbb{Z}\} \implies \mathbb{Z}[X]/(3\mathbb{Z}) \cong (\mathbb{Z}/3\mathbb{Z})[X]$$

e.g $1 + 2X + 4X^3 = 1 + 2X + X^3 + \underbrace{3X^3}_{\in(3\mathbb{Z})}$; so we can think about the coefficients in either ring

$$\underbrace{1, 2, 4}_{\in\mathbb{Z}} \to \underbrace{\overline{1}, \overline{2}, \overline{1}}_{\in\mathbb{Z}/3\mathbb{Z}}$$

Corollary 12.7

If $I \subset R$ is prime, then $(I) \subset R[X]$ is prime.

Theorem 12.8: $F[X]$ satisfies unique euclidean condition

If $a(X), b(X) \in F[X]$ where F is a field. Then there exist **unique** $q(X), r(X) \in F[X]$ such that $\deg(r(X)) < \deg(b(X))$ (or $r(X) = 0$) for which

$$a(X) = q(X) \cdot b(X) + r(X)$$

Note: The point of the above theorem being that elements in $F[X]$ have unique quotients and remainders, which doesn't always happen in a general Euclidean domain as $\mathbb{Z}$ is a Euclidean Domain with $N(n) = |n|$, e.g

$$7 = 3 \cdot 2 + 1 \quad N(1) = 1 < N(2)$$
$$7 = 4 \cdot 2 - 1 \quad N(-1) = 1 < N(2)$$

Proof.
Suppose $a(X) = q(X) \cdot b(X) + r(X) = q'(X) \cdot b(X) + r'(X)$, then

$$r(X) = a(X) - q(X) \cdot b(X)$$
$$r'(X) = a(X) - q'(X) \cdot b(X)$$

and $\deg(r), \deg(r') < \deg(b)$ (or they're both 0 but then obviously they are unique). Consider

$$r(X) - r'(X) = q'(x) \cdot b(X) - q(X) \cdot b(X) = [q'(X) - q(X)] \cdot b(X)$$

Assume $q' - q \neq 0$ and $b \neq 0$, then since Euclidean domains are integral we have

$$\deg[(q' - q) \cdot b] = \deg(q' - q) + \deg(b)$$

but also $(q' - q) \cdot b = r - r'$ for which we know

$$\deg[r - r'] < \deg b$$

and hence a contradiction arises and it must be that $q' - q = 0$ and so

$$q' - q = 0 \implies q' = q \implies r = r'$$ ■

The idea here behind this theorem and proof being that in regular Euclidean domains adding or subtracting alters the value of a norm while in polynomial rings, which has norm as the degree of the polynomial, it doesn't. This can be seen by considering that in the integers, if you start with 8 and subtract off 1, the norm is now 7, but in the polynomial ring if you start with a polynomial of degree 8 and subtract off a polynomial of strictly less degree (possibly even the same degree) then the norm (degree) does not change.

Corollary 12.9

Suppose F, K are fields with $F \subset K$ and $a(X), b(X) \in F[X]$.
Then the quotient and remainder polynomials of a by b are independent of field.

Proof. There exist $q(X), r(X) \in F[X]$ and $Q(X), R(X) \in K[X]$ with $\deg r < \deg b$ and $\deg R < \deg b$, such that

$$a(X) = q(X) \cdot b(X) + r(X) \quad a(X) = Q(X) \cdot b(X) + R(X)$$

But by the previous theorem, there is uniqueness since $q, r \in K[X]$ it must mean that

$$q(X) = Q(X) \quad r(X) = R(X)$$ ■

Corollary 12.10

For fields F, K with $F \subset K$, $b(X) \,|\, a(X)$ in $K[X]$ *iff* $b(X) \,|\, a(X)$ in $F[X]$

Example 12.2.

$$(X-1) \,|\, X^2 - 1 \text{ in } \mathbb{R}[X] \text{ and so also in } \mathbb{C}[X]$$

However note the case where $b(X) \,|\, a(X)$ in $K[X]$ but not in $F[X]$ e.g.

$$(X-i) \,|\, X^2 + 1 \text{ in } \mathbb{C}[X] \text{ but not } \mathbb{R}[X]$$

Since $X^2 + 1$ has no non-trivial factors in $\mathbb{R}[X]$.

Definition 12.11: Multivariable Polynoimal Ring

Let R be a commutative ring with $1 \neq 0$.
The **polynomial ring in the variables $X_1, \ldots, X_n$ with coefficients in R** is defined inductively as

$$R[X_1, X_2, \ldots, X_n] \coloneqq R[X_1, X_2, \ldots, X_{n-1}][X_n]$$

Concretely, think of $R[X_1, \ldots, X_n]$ as finite sums of **monomials**, i.e

$$aX_1^{d_1} X_2^{d_1} \ldots X_n^{d_n}, \quad d_i \in \mathbb{Z},\ d_i \geq 0$$

e.g

$$1 + 2XY + Y^2, 2X - 7X^3y + 2XY^4 + 1 \in \mathbb{Z}[X, Y]$$

Definition 12.12: Multi-Degree

The **degree** of a monomial

$$aX_1^{d_1} X_2^{d_1} \ldots X_n^{d_n}$$

is $d = d_1 + d_2 + \cdots + d_n$.
The **multi-degree** is $(d_1, d_2, d_3, \ldots, d_n)$.
The **degree** of a polynomial is the highest degree of any monomial in it.

Proposition 12.13

Let R be an integral domain and

$$p(X_1, \ldots, X_n), q(X_1, \ldots, X_n) \in R[X_1, X_2, \ldots, X_n] \setminus \{0\}$$

then

(1) $R[X_1, X_2, \ldots, X_n]$ is an integral domain.
(2) $R[X_1, X_2, \ldots, X_n]^\times = R^\times$
(3) $\deg[p \cdot q] = \deg p + \deg q$

L13: Polynomial Rings over UFDs

Lemma 13.1: Gauss's Lemma

Let R be a UFD and F its field of fractions. Let $p(X) \in R[X]$, then if $p(X)$ is reducible in $F[X]$ then $p(X)$ is reducible in $R[X]$.
Explicitly, if $p(X) = A(X) \cdot B(X)$ and $A \cdot B \in F[X]$, then there exist $r, s \in F$ such that

$$r \cdot A(X) = a(X) \in R[X], \quad s \cdot B(X) = b(X) \in R[X]$$

and $p(X) = a(X) \cdot b(X)$.

Observe that $F[X]^\times = F$, i.e the constant polynomials. Then since $p(X)$ is reducible, $A(X)$ and $B(X)$ are non-units, and hence

$$A(X), B(X) \notin F[X]^\times \implies \deg A, \deg B \geq 1$$

Example 13.1. Consider the polynomial

$$15X^2 + 13X + 2 = \underbrace{\left(\frac{5}{2}X + \frac{5}{3}\right)}_{A(X)} \cdot \underbrace{\left(6X + \frac{6}{5}\right)}_{B(X)}$$

Then see that by looking to clear the denominators of $A(X)$ and $B(X)$ we get,

$$\begin{aligned} 2 \cdot 3 \cdot 5(15X^2 + 13X + 2) &= \left[2 \cdot 3 \cdot \left(\frac{5}{2}X + \frac{5}{3}\right)\right] \cdot \left[5 \cdot \left(6X + \frac{6}{5}\right)\right] \\ &= (15X + 10) \cdot (30X + 6) \end{aligned}$$

Now we have factored the a multiple of our polynomial, so we get back to the original polynomial by dividing $2 \cdot 3 \cdot 5$ in such a way that we redistribute where they end up

$$\begin{aligned} 15X^2 + 13X + 2 &= \left[\underbrace{\frac{2 \cdot 3}{5}}_{r} \underbrace{\left(\frac{5}{2}X + \frac{5}{3}\right)}_{A(X)}\right] \cdot \left[\underbrace{\frac{5}{2 \cdot 3}}_{s} \underbrace{\left(6X + \frac{6}{5}\right)}_{B(X)}\right] \\ &= (\underbrace{3X + 2}_{a(X)}) \cdot (\underbrace{5X + 1}_{b(X)}) \end{aligned}$$

Proof.
Write out the polynomials $A(X), B(X)$ where $\deg A(X) = n$ is not necessarily equal to $\deg B(X) = m$,

$$\begin{aligned} A(X) &= \frac{a_0}{\alpha_0} + \frac{a_1}{\alpha_1}X_1 + \cdots + \frac{a_n}{\alpha_n}X^n \\ B(X) &= \frac{b_0}{\beta_0} + \frac{b_1}{\beta_1}X_1 + \cdots + \frac{b_m}{\beta_m}X^m \end{aligned}$$

We want to clear out the denominators, so let

$$\left.\begin{aligned}\alpha &= \alpha_0\alpha_1\dots\alpha_n\\ \beta &= \beta_0\beta_1\dots\beta_m\end{aligned}\right\} d = \alpha\bullet\beta$$

(1) Since R is an integral domain and none of the α_i's and β_i's can be 0 (as they are in denominators of fractions), so $\alpha, \beta, d \neq 0$
(2) Now after clearing out the denominators, denote the new polynomials

$$\begin{aligned}\alpha\bullet A(X) &= a'(X)\\ \beta\bullet B(X) &= b'(X)\end{aligned} \quad \in R[X]$$

For example

$$\underbrace{(2\bullet 3)}_{\alpha}\bullet\underbrace{\left(\frac{5}{2}X+\frac{5}{3}\right)}_{A(X)} = \underbrace{15X+10}_{a'(X)}$$

$$\underbrace{5}_{\beta}\bullet\underbrace{\left(6X+\frac{6}{5}\right)}_{B(X)} = \underbrace{30X+6}_{b'(X)}$$

Therefore $d\bullet p(X) = a'(X)\bullet b'(X)$.
Write $d = q_1\bullet q_2\bullet\ldots\bullet q_k$, where q_i is irreducible $\forall i\in\{1,\dots,k\}$. Then $(q_i)\subset R$ is prime, hence

$$R[X]/q_iR[X] \cong (R/(q_i))[X] \text{ is an integral domain}$$

Furthermore,

$$q_i \mid d \implies \overline{d\bullet p(X)} = \overline{0}\in(R/(q_i))[X] \implies \overline{a'(X)}\bullet\overline{b'(X)} = \overline{0}$$

Since $a'(X)$ or $b'(X)$ are equal to the 0 coset, then it is equivalent to say $a'(X)$ or $b'(X)$ are in $q_iR[X]$ (the ideal being modded out). In other words, whichever of the two is equal to $\bar{0}$ will have q_i as a factor of the numerators of their coefficients. Therefore

$$\frac{1}{q_i}\bullet a'(X) \text{ or } \frac{1}{q_i}\bullet b'(X)\in R[X]$$

Now assuming w.l.o.g. it is $a'(X)$ which has q_i then

$$\frac{d}{q_i}\bullet p(X) = \underbrace{\left[\frac{1}{q_i}\bullet a'(X)\right]}_{\in R[X]}\bullet\underbrace{b'(X)}_{\in R[X]}$$

If we continue doing this process for all the irreducibles that appear in the factorization of d, then eventually we will clear all of d on the left, and at each stage we are ending up with polynomials in $R[X]$. So, in the end we get

$$p(X) = \underbrace{a(X)}_{\in R[X]}\bullet\underbrace{b(X)}_{\in R[X]}$$

■

Going back to the previous example, what we were doing is

$$\begin{aligned} 30 \cdot p(X) &= (15X+10)\cdot(30X+6) \\ 15 \cdot p(X) &= (15X+10)\cdot(15X+3) \\ 3 \cdot p(X) &= (3X+2)\cdot(15X+3) \\ p(X) &= (3X+2)\cdot(5X+1) \end{aligned}$$

To rephrase Gauss's Lemma in the form of its contrapositive:
If $p(X)$ is irreducible in $R[X]$, then it is **still** irreducible in $F[X]$. The point being that if R is a UFD and F is its field of fractions, knowing that $p(X)$ is irreducible in $R[X]$ and adding structure to reach $F[X]$ isn't enough structure to make $p(X)$ reducible.

Q: Are there any irreducibles in $F[X]$ that **are not** irreducible in $R[X]$?
Recall that if F, K are fields with $F \subset K$ then

$$p(X) \text{ irreducible } \in F[X] \iff p(X) \text{ irreducible } \in K[X]$$

So in a more general setting with fields, it is not the case. So let us to continue consider our case where R is a UFD, to which the answer is yes.

Example 13.2. $7X$ is reducible in $\mathbb{Z}[X]$ as 7 and X are non-units. But $7 \in \mathbb{Q}^\times$, so $7, X$ do not constitute a reduction of $7X$ in $\mathbb{Q}[X]$. Now it could be the case that $7X$ is reducible in another way not involving 7 and X, but we can prove in fact that there **isn't** a way of writing $7X$ as the product of two irreducibles in $\mathbb{Q}[X]$.

Proof.
$7X$ is associate to X (only differ by a unit) and notably $\mathbb{Q}[X]/(X) \cong \mathbb{Q}$ and since $\mathbb{Q}$ is a field, then

$$(X) \text{ is maximal} \implies (X) \text{ is prime} \implies X \text{ is irreducible} \implies 7X \text{ is irreducible}$$

where the last implication is since 7 is associate to X then since 7 is a unit and X is irreducible (hence not a unit), $7X$ is irreducible. ■

In fact, we see that by shifting to the field of fractions, one of the elements in $7X$ became a unit, namely 7. As a corollary to Gauss's Lemma, we will see how situations like this are the only things that turn from irreducibles to units as one goes to the field of fractions.

Corollary 13.2

Let R be a UFD and F its field of fractions. If

$$p(X) = a_0 + a_1X + \cdots + a_nX^n \in R[X]$$

and $\gcd(a_0, a_1, \ldots, a_n) = 1$. Then

$$p(X) \text{ irreducible } \in R[X] \iff p(X) \text{ irreducible } \in F[X]$$

Note: $\gcd(a_0, a_1, \ldots, a_n) = 1$ means we cannot factor out a non-unit from the coefficients, i.e. we cannot write

$$p(X) = d \cdot p'(X), \quad d \in R \setminus R^\times, \quad \deg p = \deg p'$$

Proof.
This will be proved by contrapositives.
$\Longleftarrow$
In this direction, it is to show that if $p(X)$ is reducible in $R[X]$ then it is reducible in $F[X]$.
Suppose $p(X) \in R[X]$ is reducible in $R[X]$ and $\gcd(a_0, a_1, \ldots, a_n) = 1$. That is, suppose

$$p(X) = a(X) \cdot b(X), \quad a(X), b(X) \notin R[X]^\times$$

Then since $\gcd(a_0, a_1, \ldots, a_n) = 1$ the note in the statement of the corollary essentially says $a(X), b(X)$ are non-constant polynomials because you can not factor out of $p(X)$ a constant non-unit. So in fact that means $\deg a, \deg b \geq 1$.
However, we know $F[X]^\times$ is exactly $F^\times$, the non-zero constant polynomials. Hence $a(X), b(X) \in F[X]$ are not units in $F[X]$ and so $p(X)$ is reducible in $F[X]$.
The other direction, $\Longrightarrow$, is the contrapositive of Gauss's Lemma. ■

Theorem 13.3: R UFD $\Longleftrightarrow$ $R[X]$ UFD

R is a UFD if and only if $R[X]$ is a UFD.

Proof.
$\Longleftarrow$
If $R[X]$ is a UFD, then since $R \subset R[X]$ is a subring then R is also a UFD.
$\Rightarrow$
Suppose that R is a UFD and F is its field of fractions. We can write

$$p(X) = a_0 + a_1 X + \cdots + a_n X^n \in R[X]$$

The goal is to uniquely factor $p(X)$ in $R[X]$. Let

$$d = \gcd(a_0, a_1, \ldots, a_n) \in R$$

If $d \notin R^\times$, then it has unique factorization into irreducibles in R (since R is a UFD) and necessarily $p(X) = d \cdot p'(X)$ where the gcd of the coefficients in $p'(X)$ is 1.
Now assume $\gcd(a_0, a_1, \ldots, a_n) = 1$; in particular, if $p(X) \notin R[X]^\times$ then $\deg p \geq 1$.
Consider $p(X) \in F[X]$ and note the $F[X]$ is a UFD (actually a Euclidean domain). This implies we can write

$$p(X) = A_1(X) \cdot A_2(X) \cdot \ldots \cdot A_k(X)$$

where $A_i(X) \in F[X]$ are irreducible. By Gauss's Lemma we can clear out the denominators and write

$$p(X) = a_1(X) \cdot a_2(X) \cdot \ldots \cdot a_k(X)$$

where $a_i(X) \in R[X]$. Then

$$\gcd(a_0, \ldots, a_n) = 1 \implies \gcd(\text{coeffs of } a_i(X)) = 1 \quad \forall i$$

By Corollary 13.2, since $a_i(X) \in R[X]$ is associate to $A_i(X)$ in $F[X]$, hence $a_i(X)$ is irreducible in $R[X]$. So we've shown there exists a factorization of $p(X)$ as a product

of irreducibles in $R[X]$.
The uniqueness follows directly from uniqueness in $F[X]$. ■

L14: Factorization Techniques

The goal of this lecture is to factor (or check for factors) of polynomials

Proposition 14.1: Linear factors are roots

Let F be a field and $p(X) \in F[X]$ a polynomial.
$p(X)$ has a factor of degree one in $F[X]$ *iff* $p(X)$ has a root in F, i.e $\exists \alpha \in F$, $p(\alpha) = 0$.

Proof.
$\implies$
If $p(X)$ has a factor of degree one in $F[X]$ i.e $p(X) = (\alpha X - \beta) \cdot q(X)$, $\alpha, \beta \in F$ with $\alpha \neq 0$. Then, since we are in a field, we have an inverse for α and so

$$p\left(\frac{\beta}{\alpha}\right) = \left(\alpha \cdot \left(\frac{\beta}{\alpha}\right) - \beta\right) \cdot q\left(\frac{\beta}{\alpha}\right) = 0 \cdot q\left(\frac{\beta}{\alpha}\right) = 0$$

$\impliedby$
Conversely, if $p(X)$ has a root $\alpha \in F$, then we can write (the division algorithm)

$$p(X) = q(X) \cdot (X - \alpha) + r(X)$$

where $r(X) = 0$ or $\deg r(X) < \deg(X - \alpha) = 1$ (i.e $r(X) \equiv r$ is a constant). Then, by substituting α we see

$$p(\alpha) = q(\alpha) \cdot (\alpha - \alpha) + r \implies 0 = 0 + r \implies r = 0$$

and therefore $p(X) = q(X) \cdot (X - \alpha)$ where $(X - \alpha)$ is degree one factor we are looking for. ■

Corollary 14.2: Multiple roots form product of linear factors as factor

If $p(X) \in F[X]$ has (not necessarily distinct) roots $\alpha_1, \alpha_2, \ldots, \alpha_k$, then $p(X)$ has

$$(X - \alpha_1) \cdot (X - \alpha_2) \cdot \ldots \cdot (X - \alpha_2)$$

as a factor.

Definition 14.3: Multiplicity

If $p(X) \in F[X]$ is divisible by $(X - \alpha)^k$, then we say that the root α has **multiplicity** k.

Corollary 14.4: $p(X)$ has at most n roots

If $\deg(p(X)) = n$, then it has at most n roots in F (even counting with multiplicity).

Corollary 14.5: Quadratics and cubics reducible *iff* they have roots in F

If $p(X) \in F[X]$ and $\deg p = 2$ or 3, then $p(X)$ is reducible *iff* $p(X)$ has a root in F.

Proposition 14.6: Rational Root Theorem

Let

$$p(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n \in \mathbb{Z}[X]$$

If $\frac{r}{s} \in \mathbb{Q}$ is in lowest terms (i.e $\gcd(r,s) = 1$) and $p\left(\frac{r}{s}\right) = 0$, then $r \mid a_0$ and $s \mid a_n$.
In particular, if $a_n = 1$ (i.e p is monic) and $p(d) \neq 0$ for all $d \in \mathbb{Z}$ such that $d \mid a_0$, then $p(X)$ has no roots in $\mathbb{Q}$.

Example 14.1. Let $p(X) = X^7 - 7X^2 - 2X + 1$. Then check if $X = \pm 1$ are roots of $p(X)$:

$$p(1) = 1^7 - 7 \cdot 1^2 - 2 \cdot 1 + 1 = -7 \neq 0$$
$$p(-1) = (-1)^7 - 7 \cdot (-1)^2 - 2 \cdot (-1) + 1 = -5 \neq 0$$

Since neither are equal to 0, then if $p(X)$ has any real roots, they are irrational.

Proof. Let $\alpha = \frac{r}{s}$ be a root of a polynomial $p(X) \in \mathbb{Z}[X]$. Then one writes

$$p\left(\frac{r}{s}\right) = a_0 + a_1 \cdot \left(\frac{r}{s}\right) + a_2 \cdot \left(\frac{r}{s}\right)^2 + \cdots + a_n \left(\frac{r}{s}\right)^n$$
$$\implies 0 = a_0 \cdot s^n + a_1 \cdot r \cdot s^{n-1} + a_2 \cdot r^2 \cdot s^{n-2} + \cdots + a_n \cdot r^n$$

First isolating r^n, we get that the terms on the right hand side all have a factor of s

$$\begin{aligned} a_n \cdot r^n &= -a_0 \cdot s^n - a_1 \cdot r \cdot s^{n-1} - \cdots - a_{n-1} \cdot r^{n-1} \cdot s \\ &= -s \cdot \left(a_0 \cdot s^{n-1} + a_1 \cdot r \cdot s^{n-2} + \cdots + a_{n-1} \cdot r^{n-1}\right) \end{aligned}$$

Since $\gcd(r,s) = 1$ then it can only be that $s \mid a_n$.
Similarly, isolating s^n, we get

$$\begin{aligned} a_0 \cdot s^n &= -a_1 \cdot r \cdot s^{n-1} - a_2 \cdot r^2 \cdot s^{n-2} - \cdots - a_n \cdot r^n \\ &= -r \cdot \left(a_1 \cdot s^{n-1} + a_2 \cdot r \cdot s^{n-2} + \cdots + a_n \cdot r^{n-1}\right) \end{aligned}$$

Since $\gcd(r,s) = 1$ then it can only be that $r \mid a_0$. ■

Example 14.2. Consider $p(X) = X^3 + 9X^2 - 2X + 1$ with possible roots $X = \pm 1$. We check

$$p(1) = 1^3 + 9 \cdot 1^2 - 2 \cdot 1 + 1 = 9 \neq 0$$
$$p(-1) = (-1)^3 + 9 \cdot (-1)^2 - 2 \cdot (-1) + 1 = 11 \neq 0$$

Hence, $p(X)$ has no roots in $\mathbb{Q}$ and by Corollary 14.5, is thus **irreducible** over $\mathbb{Q}$.

Claim: The polynomials $X^2 - p, X^3 - p \in \mathbb{Z}[X]$ where $p \in \mathbb{Z}$ is prime are irreducible over $\mathbb{Q}[X]$.

Proof. The only candidates for solutions are $X = \pm 1, \pm p$.
We check for $q(X) = X^2 - p$ (The proof for $X^3 - p$ is similar):

$$q(\pm 1) = (\pm 1)^2 - p = 1 - p \neq 0$$
$$q(\pm p) = (\pm p)^2 - p = p \cdot (p-1) \neq 0$$

A difference of squares/cubes involving a prime will factor into irrational roots. ■

Example 14.3. Consider $p(X) = X^2 + 1$. This is irreducible over $\mathbb{R}[X]$ as one can check

$$1^2 + 1 = 2 \neq 0$$
$$(-1)^2 + 1 = 2 \neq 0$$

On the other hand, it **is** reducible over $\mathbb{Z}/2\mathbb{Z}[X]$

$$1^2 + 1 \equiv 0 \pmod 2$$

Furthermore, $X^2 + X + 1$ is irreducible over $\mathbb{Z}/2\mathbb{Z}[X]$ as

$$0^2 + 0 + 1 = 1 \neq 0$$
$$1^2 + 1 + 1 = 1 \neq 0$$

It is important to see that reducibility largely depends on the coefficient ring.

Proposition 14.7: If irreducible in $(R/I)[X]$ then irreducible in $R[X]$

Let R be an integral domain and $I \subsetneq R$ a proper ideal. Let $p(X) \in R[X]$ be a non-constant, monic polynomial.
If $\overline{p(X)} \in (R/I)[X]$ is irreducible into polynomials of strictly lesser degree, then $p(X)$ is irreducible in $R[X]$.

Proof. Suppose $p(X)$, a non-constant monic polynomial, is reducible in $R[X]$, say

$$p(X) = a(X) \cdot b(X), \quad \deg a, \deg b < \deg p$$

In particular, because p is monic then can also choose a, b to be non-constant, monic polynomials, hence

$$\overline{p(X)} = \overline{a(X)} \cdot \overline{b(X)} \in (R/I)[X]$$

The reduction of p in $R[X]$ leads to a reduction of $\overline{p}$ in $(R/I)[X]$. Hence, the contrapositive, if $\overline{p}$ is irreducible in $(R/I)[X]$ then p is irreducible in $R[X]$, is also true. ■

Example 14.4.

- $p(X) = X^2 + X + 1$ is irreducible in $(\mathbb{Z}/2\mathbb{Z})[X]$ then it is irreducible in $\mathbb{Z}[X]$
- $p(X) = X^2 + 1$ is irreducible in $\mathbb{Z}[X]$ but **is** reducible in $(\mathbb{Z}/2\mathbb{Z})[X]$.

The second example shows the proposition cannot be an "if and only if" statement (i.e its converse is not always true).

Warning: There exist polynomials which violate the converse of the proposition, e.g $X^4 + 1$, that are irreducible in $\mathbb{Z}[X]$ but are reducible in every $(\mathbb{Z}/p\mathbb{Z})[X]$ for $p \in \mathbb{Z}$ prime.

Example 14.5. Let $p(X, Y) = X^2 + XY + 1 \in \mathbb{Z}[X, Y] = (\mathbb{Z}[X])[Y]$, then if you mod out by all the terms including a factor of Y, you get polynomials of terms only in X, i.e

$$\mathbb{Z}[X, Y]/(y \cdot \mathbb{Z}[X, Y]) \cong \mathbb{Z}[X]$$

Specifically, $\overline{X^2 + XY + 1} \in \mathbb{Z}[X, Y]/(y \cdot \mathbb{Z}[X, Y])$. This is precisely $X^2 + 1$ and it is irreducible, hence by the proposition $X^2 + XY + 1$ is irreducible in $\mathbb{Z}[X, Y]$.

Theorem 14.8: Eisenstein's Criterion

Let R be an integral domain and $P \subset R$ a prime ideal. Let
$$q(X) = X^n + c_{n-1}X^{n-1} + \cdots + c_1 X + c_0 \in R[X]$$
Suppose $c_0, c_1, \ldots, c_{n-1} \in P$ and $c_0 \notin P^2$, then $q(X)$ is irreducible in $R[X]$.

This is stronger than the Rational Root Theorem which says how to find the rational roots, and hence you can find linear factors. But if it doesn't have rational roots, it might still be factorable into factors of degree greater than 1. Eisenstein's Criterion tells you in what situations this is possible (and more generally over arbitrary rings, not just $\mathbb{Z}$ and $\mathbb{Q}$).

Claim: $p(X) = X^4 + 3X^3 - 27X^2 + 9X + 6$ is irreduicble.

Proof. With Rational Root Theorem, you can check that $X = \pm 1, \pm 2, \pm 3, \pm 6$ are not roots and hence it has no linear factors. But with Eisenstein's Criterion, we can in fact show it is completely irreducible as $3, -27, 9, 6 \in 3\mathbb{Z}$ however $6 \notin 9\mathbb{Z}$. ■

Proof of Eisenstein's Criterion.
Suppose $q(X) = a(X) \cdot b(X)$ where $a, b \notin R[X]^\times$. Since q is monic, we may take a, b to be monic
$$\begin{aligned} a(X) =& X^k + a_{k-1}X^{k-1} + \cdots + a_1 X + a_0 \\ b(X) =& X^l + b_{l-1}X^{l-1} + \cdots + b_1 X + b_0 \end{aligned}$$
where $l, k > 0$ (since a, b are non-units).
We will follow in the same fashion as Prop 14.7 by looking at the quotient by the ideal P.
If $c_0, c_1, \ldots, c_{n-1} \in P$, then
$$\begin{aligned} \overline{q(X)} =& \overline{X^n + c_{n-1}X^{n-1} + \cdots + c_0} = \overline{X^n} \in (R/P)[X] \\ =& \overline{a(X)} \cdot \overline{b(X)} \end{aligned}$$
i.e $\overline{a(X)} \cdot \overline{b(X)} = \overline{X^n}$. Then, in particular, since there is no constant term in this product, we can say
$$\overline{a_0} \cdot \overline{b_0} = \overline{0} \implies a_0 \in P \text{ or } b_0 \in P$$
W.l.o.g let $a_0 \in P$, then $a(X) \cdot b(X)$ can be written
$$\begin{aligned} &(X^k + a_{k-1}X^{k-1} + \cdots + a_1 X + a_0) \cdot (X^l + b_{l-1}X^{l-1} + \cdots + b_1 X + b_0) \\ =& X^{k+l} + (a_{k-1} + b_{l-1})X^{k+l-1} + \cdots + (a_1 \cdot b_0 + a_0 \cdot b_1)X + a_0 \cdot b_0 \end{aligned}$$
Since P is a prime ideal, then $a_0 \cdot b_1 \in P$ and hence $a_1 \cdot b_0$ is in P because their sum needs to be the coefficient $c_1 \in P$ of the term X in $q(X)$. This implies $a_1 \in P$ or $b_0 \in P$.
If $a_1 \in P$ then
$$(a_2 \cdot b_0 + \underbrace{a_1 \cdot b_1}_{\in P} + \underbrace{a_0 \cdot b_2}_{\in P}) \implies a_2 \cdot b_0 \in P \implies a_2 \in P \text{ or } b_0 \in P$$

If you choose $b_0 \in P$ then you are done. If you choose $a_2 \in P$ and continue up the terms you will eventually be forced to choose $b_0 \in P$ anyways (check this yourself). Hence, $b_0 \in P$ and therefore $a_0 \cdot b_0 = c_0 \in P^2$ because both are in P.
Thus, we have shown the contrapositive, i.e q being irreducible implies $c_0 \in P^2$, which means the original statement (Eisenstein's Criterion), is also true. ■

Example 14.6. $X^n - p$ is irreducible if p is prime because $-p \in p\mathbb{Z}$ but $-p \notin p^2\mathbb{Z}$.

Corollary 14.9: nth roots of primes are irrational

$\sqrt[n]{p} \notin \mathbb{Q}$ for all $n \geq 2$ when p is prime.

Example 14.7. Let $p(X) = X^4 + 1$ and notice that $1 \notin P$ for any prime ideal (otherwise its the whole ring and not a prime ideal), therefore we can't apply Eisenstein's Criterion directly.
Consider

$$\begin{aligned} q(X) = p(X+1) &= (X+1)^4 + 1 \\ &= (X^4 + 4X^3 + 6X^2 + 4X + 1) + 1 \\ &= X^4 + 4X^3 + 6X^2 + 4X + 2 \end{aligned}$$

See that $2, 4, 6 \in 2\mathbb{Z}$ but $2 \notin 4\mathbb{Z}$, therefore we can apply Eisenstein's Criterion to $q(X)$ to conclude it is irreducible. Now, suppose $p(X)$ was reducible into $X^4 + 1 = a(X) \cdot b(X)$ then

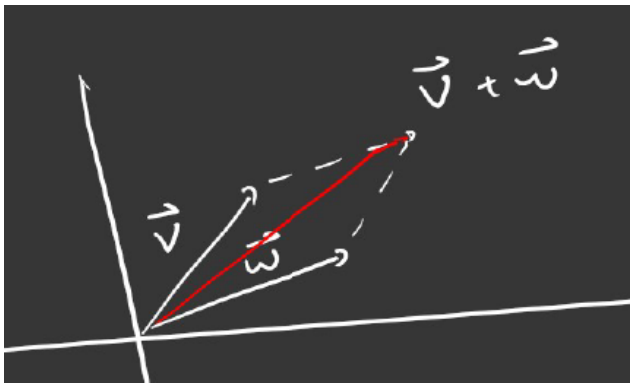
$$q(X) = (X+1)^4 + 1 = a(X+1) \cdot b(X+1)$$

i.e if $X^4 + 1$ is reducible then so is $q(X)$.
But by Eisenstein's Criterion $q(X)$ is irreducible, therefore $X^4 + 1$ is irreducible as well.

L15: Modules

Consider the vector space $\mathbb{R}^n := \{(a_1, \ldots, a_n) \mid a_i \in \mathbb{R},\ i = 1, 2, \ldots, n\}$. We know from our experiences in linear algebra that addition is defined as

$$\begin{matrix} \mathbf{v} = (v_1, \ldots, v_n) \\ \mathbf{w} = (w_1, \ldots, w_n) \end{matrix} \implies \mathbf{v} + \mathbf{w} := (v_1 + w_1, \ldots, v_n + w_n) \in \mathbb{R}^n$$



Note: $(\mathbb{R}^n, +)$ is an abelian (commutative) group with addition:

- (Additive identity) $\exists \mathbf{0} \in \mathbb{R}^n$ such that $\mathbf{0} + \mathbf{v} = \mathbf{v} + \mathbf{0} = \mathbf{v} \quad \forall \mathbf{v} \in \mathbb{R}^n$
- (Associative) $(\mathbf{v} + \mathbf{w}) + \mathbf{u} = \mathbf{v} + (\mathbf{w} + \mathbf{u}) \quad \forall \mathbf{v}, \mathbf{w}, \mathbf{u} \in \mathbb{R}^n$
- (Additive inverse) $\forall \mathbf{v} \in \mathbb{R}^n, \exists$ -$\mathbf{v} \in \mathbb{R}^n$ such that $\mathbf{v} + (-\mathbf{v}) = (-\mathbf{v}) + \mathbf{v} = \mathbf{0}$
- (Abelian) $\mathbf{v} + \mathbf{w} = \mathbf{w} + \mathbf{v} \quad \forall \mathbf{v}, \mathbf{w} \in \mathbb{R}^n$

$\mathbb{R}^n$ also has **scalar multiplication**: If $a \in \mathbb{R}$ and $\mathbf{v} \in \mathbb{R}^n$ then

$$a \cdot \mathbf{v} = (av_1, av_2, \ldots, av_n) \in \mathbb{R}^n$$

We can think of scalar multiplication as a map

$$\begin{aligned} \mathbb{R} \times \mathbb{R}^n &\to \mathbb{R}^n \\ (a, \mathbf{v}) &\mapsto a \cdot \mathbf{v} \end{aligned}$$

Suppose $a, b \in \mathbb{R}$ and $\mathbf{v}, \mathbf{w} \in \mathbb{R}^n$, then scalar multiplication has the following properties

(1) $(a + b) \cdot \mathbf{v} = a \cdot \mathbf{v} + b \cdot \mathbf{v}$

(2) $(ab) \cdot \mathbf{v} = a \cdot (b \cdot \mathbf{v})$

(3) $a \cdot (\mathbf{v} + \mathbf{w}) = a \cdot \mathbf{v} + a \cdot \mathbf{w}$

(4) $1 \cdot \mathbf{v} = \mathbf{v}$

Definition 15.1: R-module

Let R be a ring.
A **(left) module over** R or (R-**module**) is a set M with
(1) a binary operation $+$ such that $(M, +)$ is an Abelian group,
(2) an action of R on M i.e a map

$$R \times M \to M$$
$$(r, m) \mapsto r \cdot m$$

such that for $r, s \in R$ and $m, n \in M$
(i) $(r + s) \cdot m = r \cdot m + s \cdot m$
(ii) $(rs) \cdot m = r \cdot (s \cdot m)$
(iii) $r \cdot (m + n) = r \cdot m + r \cdot n$
(iv) If $1 \in R$ then $1 \cdot m = m$ and the module is called **Unital**.

Note: We can define a **right** R-module by $m \cdot r$ with scalar multiplication on the right.The only difference is associativity being $m \cdot (rs) = (m \cdot r) \cdot s$. Contrast this to property (ii) which says the action of rs on m is the action of s first and then acting by r , whereas now, it is the action of r first then acting by s and these two notions coincide only when R is commutative.
We will always be talking about left R-modules unless explicitly stated
Note: If R is a commutative ring then any left R-module has a natural right R-module structure as well: $(rs) \cdot m = (sr) \cdot m \longleftrightarrow m \cdot (sr) = m \cdot (rs) = (m \cdot r) \cdot s$

Definition 15.2: F-vector space

If F is a field, then we refer to F-modules as F-**vector spaces**. In this sense $\mathbb{R}^n$ is an $\mathbb{R}$-vector space.

Observe If $R \subset S$ is as subring and M is an S-module then M is also a R-module by restricting scalar multiplication to R. For example, $\mathbb{C}^2$ is a $\mathbb{C}$-vector space but it is also an $\mathbb{R}$-vector space.
If $a \in \mathbb{R}$, $\mathbf{v} = (v_1, v_2) \in \mathbb{C}^2$ then $a \cdot \mathbf{v} = (av_1, av_2) \in \mathbb{C}^2$ still makes sense.

Example 15.1. For any ring R, consider

$$R^n := \{(a_1, \ldots, a_n) \mid a_i \in R,\ i = 1, 2, \ldots, n\}$$

with component-wise addition

$$(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) := (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n)$$

Exercise: $(R^n, +)$ is an abelian group. Scalar multiplication is also component-wise, for $a \in R$ and $(a_1, \ldots, a_n) \in R^n$, defined as

$$a \cdot (a_1, \ldots, a_n) := (a \cdot a_1, \ldots, a \cdot a_n)$$

Exercise: $(R^n, +)$ is an R-module with this scalar multiplication.
This is called the **free R-Module of rank** n.

Example 15.2. The **trivial module** $0 \coloneqq \{\mathbf{0}\}$ which has $\forall r \in R$, $r \cdot \mathbf{0} \coloneqq \mathbf{0}$.

Example 15.3. Any ideal of a ring $I \subset R$ is an R-module with scalar multiplication as ring multiplication:

$$\begin{aligned} R \times I &\to I \\ (r, a) &\mapsto ra \end{aligned}$$

Example 15.4. Quotient rings of R are R-modules with scalar multiplication as ring multiplication:

$$\begin{aligned} R \times R/I &\to R/I \\ (r, \bar{a}) &\mapsto \overline{r \cdot a} \end{aligned}$$

Exercise: Module property (ii) $(rs) \cdot \bar{a} = r \cdot (s \cdot \bar{a})$ holds.

Recall a vector subspace $W \subset \mathbb{R}^n$ is a subset such that

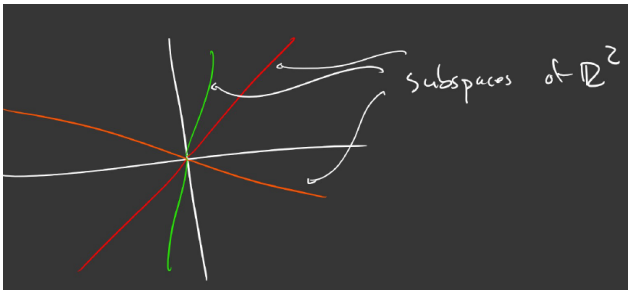
(i) $\mathbf{w}_1 + \mathbf{w}_2 \in W, \quad \forall \mathbf{w}_1, \mathbf{w}_2 \in W$

(ii) $\mathbf{0} \in W$

(iii) $a \cdot \mathbf{w} \in W, \quad \forall a \in \mathbb{R}, \mathbf{w} \in W$

(iv) $-\mathbf{w} \in W, \quad \forall \mathbf{w} \in W$

Example 15.5. $\mathbb{R}^2$ has subspaces $\mathbf{0}, \mathbb{R}^2, \text{Span}\left\{ \begin{pmatrix} a \\ b \end{pmatrix} \mid a, b \in \mathbb{R} \right\}$



Definition 15.3: Submodule, Subspace

A **submodule** of an R-module M is a subgroup $N \subset M$ such that it is closed under scalar multiplication, i.e for all $r \in R, n \in N, r \cdot n \in N$.
If F is a field, we call F-submodules **F-subspaces**

Example 15.6. Every module is a submodule of itself.

Example 15.7. Every module has the 0-module.

Example 15.8. If we think about a ring R as a module over itself, then the submodules of R are the ideals of R.

Note: The only subspaces of $\mathbb{R}$ are 0 or $\mathbb{R}$ (since the only ideals in a field are 0 and the field itself).

Example 15.9. $\mathbb{Z}$**-modules**.
Let M be any abelian group. Define for all $n \in \mathbb{Z}$ and $a \in M$,

$$n \cdot a := \begin{cases} \underbrace{a + a + a + \cdots + a}_{n\text{-times}} & n > 0 \\ 0 & n = 0 \\ \underbrace{(-a) + (-a) + (-a) + \cdots + (-a)}_{(-n)\text{-times}} & n < 0 \end{cases}$$

Exercise: $(n+m) \cdot a = n \cdot a + m \cdot a$ and $(nm) \cdot a = n \cdot (m \cdot a)$
This is a common sense way to come up with a $\mathbb{Z}$-module structure on any abelian group and so $\{\mathbb{Z}\text{-modules}\} = \{\text{Abelian groups}\}$ For example $\mathbb{Z}/4\mathbb{Z}$ is a $\mathbb{Z}$-module as

$$n \cdot \overline{0} = \overline{0}, \quad n \cdot \overline{1} = \overline{n}, \quad n \cdot \overline{2} = \overline{2n}, \quad n \cdot \overline{3} = \overline{3n}$$

We can then immediately think of a large list of $\mathbb{Z}$-modules: $\mathbb{Z}^n$ for $n \geq 1$ and $\mathbb{Z}/n\mathbb{Z}$ for $n \geq 2$.

Example 15.10. $(\mathbb{Z}/n\mathbb{Z})$**-module**
Let M be a $(\mathbb{Z}/n\mathbb{Z})$-module.
Then

$$\begin{aligned} &\underbrace{(1 + 1 + 1 + \cdots + 1)}_{n\text{-times}} \cdot a = 0 \cdot a = 0 \quad \forall a \in M \\ =&\underbrace{1 \cdot a + 1 \cdot a + 1 \cdot a + \cdots + 1 \cdot a}_{n\text{-times}} \\ =&\underbrace{a + a + a + \cdots + a}_{n\text{-times}} \end{aligned}$$

So in a $\mathbb{Z}/n\mathbb{Z}$-module, the sum of any element with itself n times is going to be equal to 0.
For example $\mathbb{Z}/2\mathbb{Z}$ is a $(\mathbb{Z}/4\mathbb{Z})$-module because 1 added to itself four times is 0 as seen

$$\underbrace{(1 \bmod 2) + (1 \bmod 2)}_{0 \bmod 2} + \underbrace{(1 \bmod 2) + (1 \bmod 2)}_{0 \bmod 2} = 0 \bmod 2$$

A **linear transformation** $T\colon \mathbb{R}^n \to \mathbb{R}^m$ is a map between two vector spaces such that

$$T(\mathbf{v} + \mathbf{w}) = T\mathbf{v} + T\mathbf{w}$$
$$T(a\mathbf{v}) = a \cdot T\mathbf{v}$$

As an example,

$$\begin{aligned} T\colon \mathbb{R}^3 &\to \mathbb{R}^2 \\ (x, y, z) &\mapsto (2x + y - z, x + 2y) \end{aligned}$$

which, recall, we can represent as a matrix

$$\begin{pmatrix} 2 & 1 & -1 \\ 1 & 2 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 2x + y - z \\ x + 2y \end{pmatrix}$$

Definition 15.4: R-module homomorphism, F-linear transformation

Let R be a ring and M, N be R-modules.
An **R-module homomorphism** from M to N is a map $f: M \to N$ such that
(1) $f(m+n) = f(m) + f(n) \quad \forall m, n \in M$
(2) $f(a \cdot m) = a \cdot f(m) \quad \forall a \in R, m \in M$
If F is a field, we call F-module homomorphisms **F-linear transformations**.

L16: R-module homomorphisms

Definition 16.1: $\mathrm{Hom}_R(M,N)$, Kernel, Image, Isomorphism

The **set of R-module homomorphisms from M to N** is denoted $\mathrm{Hom}_R(M,N)$.
The **kernel** of an R-module homomorphism $f \in \mathrm{Hom}_R(M,N)$ is

$$\mathrm{Ker}\, f \coloneqq \{m \in M \mid f(m) = 0\}$$

The **image** of $f \in \mathrm{Hom}_R(M,N)$ is

$$\mathrm{Im}\, f \coloneqq \{n \in N \mid \exists m \in M,\ f(m) = n\}$$

If $f \in \mathrm{Hom}_R(M,N)$ is bijective then we say f is an **isomorphism of R-modules**. We say M, N are **isomorphic** if there is an isomorphism $f\colon M \to N$ and we write $M \cong N$.

Example 16.1. $R = \mathbb{Z}, M = \mathbb{Z}$ is a $\mathbb{Z}$-module.
Note: A subtle distinction between this and the ring of integers $\mathbb{Z}$ is that you don't have multiplication between the elements of the module but rather it has an action of the integers by multiplication.
What do the $\mathbb{Z}$-module homomorphisms from $\mathbb{Z}$ to $\mathbb{Z}$ look like? Consider

$$\begin{aligned} f\colon \mathbb{Z} &\to \mathbb{Z} \\ 1 &\mapsto a \\ n &\mapsto \underbrace{a + a + a + \cdots + a}_{n\text{-times}} \end{aligned}$$

Then we see that, in this case, f is specified by where it sends one, i.e $f(1) = a$.

Note: There are functions f which are R-module homomorphisms from $\mathbb{Z}$ to $\mathbb{Z}$ which are not ring homomorphisms from $\mathbb{Z}$ to $\mathbb{Z}$. Consider the doubling function

$$\begin{aligned} f_2\colon \mathbb{Z} &\to \mathbb{Z} \\ 1 &\mapsto 2 \end{aligned}$$

is a $\mathbb{Z}$-module homomorphism as

$$\begin{aligned} f_2(m+n) &= 2 \cdot (m+n) = 2 \cdot m + 2 \cdot n = f_2(m) + f_2(n) \\ f_2(a \cdot m) &= 2 \cdot (a \cdot m) = a \cdot 2 \cdot m = a \cdot f_2(m) \end{aligned}$$

However it is **not** a ring homomorphism as

$$f_2(2 \cdot 3) = 2 \cdot 2 \cdot 3 = 12 \neq 24 = 4 \cdot 6 = (2 \cdot 2) \cdot (3 \cdot 2) = f_2(2) \cdot f_2(3)$$

Proposition 16.2: Kernel and Image are submodules

Suppose $f \in \mathrm{Hom}_R(M,N)$. Then the kernel, $\mathrm{Ker}\, f \subset M$, and the image, $\mathrm{Im}\, f \subset N$, are R-submodules.

Proof. First we prove the claim for the kernel. If $a, b \in \operatorname{Ker} f$ and $r \in R$ then

- $f(0) = 0 \implies 0 \in \operatorname{Ker} f$
- $f(a+b) = f(a) + f(b) = 0 + 0 = 0 \implies a + b \in \operatorname{Ker} f$
- $f(r \cdot a) = r \cdot f(a) = r \cdot 0 = 0 \implies r \cdot a \in \operatorname{Ker} f$
- $0 = f(0) = f(a + (-a)) = f(a) + f(-a) = 0 + f(-a) = f(-a) \implies -a \in \operatorname{Ker} f$

hence, $\operatorname{Ker} f \subset M$ is a submodule.
If $a, b \in \operatorname{Im} f, r \in R$ such that $a = f(a'), b = f(b')$ for $a', b' \in M$, then

- $f(0) = 0 \implies 0 \in \operatorname{Im} f$
- $a + b = f(a') + f(b') = f(a' + b') \implies a + b \in \operatorname{Im} f$
- $r \cdot a = r \cdot f(a') = f(r \cdot a') \implies r \cdot a \in \operatorname{Im} f$
- $-a = -f(a') = f(-a') \implies -a \in \operatorname{Im} f$

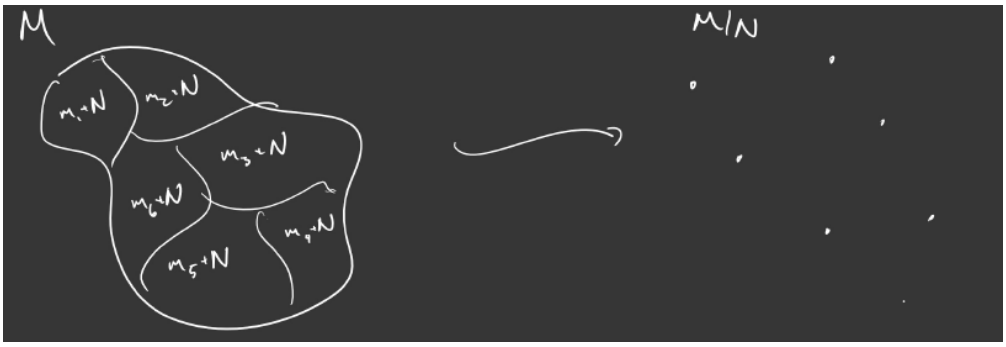
Hence, $\operatorname{Im} f$ is a submodule. ■

Definition 16.3: Coset

If $N \subset M$ is an R-submodule and $m \in M$, then the N **coset** of m is

$$m + N \coloneqq \{m + n \mid n \in N\}$$

Exercise: We can define an equivalence relation on M by $m \sim m'$ if and only if $m + N = m' + N$ as sets.



Definition 16.4: Quotient Module

The **quotient module** of M by N is

$$M/N \coloneqq \{m + N \mid m \in M\}$$

Proposition 16.5: Quotient Module is R-module

Quotient modules are R-modules.

Proof. Define addition of cosets as

$$(m + N) + (m' + N) \coloneqq (m + m') + N$$

Just as for rings, we will write $\overline{m}$ for $m \in M$ if N is understood.
It is simple enough to check that the addition is well defined:

$$m + N = m_1 + N \implies m - m_1 = n \in N$$
$$m' + N = m_1' + N \implies m' - m_1' = n' \in N$$

Then by direct calculation

$$\begin{aligned}(m_1 + N) + (m_1' + N) = (m + m_1') + N &= (m + n + m' + n') + N \\ &= (m + m') + \underbrace{(n + n')}_{\in N} + N = (m + m') + N\end{aligned}$$

If $r \in R$ and $m + N \in M/N$. The R-action is then defined

$$r \cdot (m + N) \coloneqq (r \cdot m) + N$$

Exercise: Check that the R-action is well defined. ■

Proposition 16.6: Canonical quotient map is surjective

The natural quotient map

$$\begin{aligned}p \colon M &\to M/N \\ m &\mapsto M + N\end{aligned}$$

is a surjective R-module homomorphism such that $\operatorname{Ker} p = N$.

Proof. Properties of an R-module homomorphism:

$$p(a + b) = (a + b) + N = (a + N) + (b + N) = p(a) + p(b)$$
$$p(r \cdot a) = (r \cdot a) + N = r \cdot (a + N) = r \cdot p(a)$$

Surjectivity is clear as before (think of the representative of the coset).
Suppose $a \in \operatorname{Ker} p$, then $f(a) = a + N = 0 + N$ i.e. there exists $n \in N$ such that $a - 0 = n \in N$ and hence $a = n \in N$ so that $a \in N$. Hence, $\operatorname{Ker} p \subset N$. Suppose $n \in N$. Then

$$f(n) = n + N \implies n - 0 \in N \implies n + N = 0 + N \implies f(n) = 0 + N \implies n \in \operatorname{Ker} p$$

and therefore $N \subset \operatorname{Ker} p$. ■

Theorem 16.7: The First Isomorphism Theorem

Let M, N be R-modules and $f \in \operatorname{Hom}_R(M, N)$. Then $\operatorname{Ker} f \subset M$ is a submodule and

$$M/\operatorname{Ker} f \cong \operatorname{Im} f$$

Theorem 16.8: The Second Isomorphism Theorem

Let $A, B \subset M$ be submodules, then

$$(A + B)/B \cong A/A \cap B$$

Theorem 16.9: The Third Isomorphism Theorem

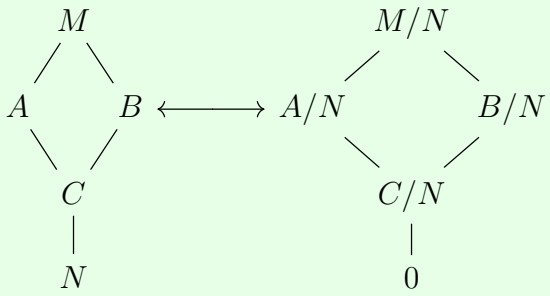
Let $A \subset B \subset M$ be submodules, then

$$(M/A)/(B/A) \cong M/B$$

Theorem 16.10: The Fourth Isomorphism Theorem

There is a bijection of sets

$$\{\text{submodules of } M \text{ containing } N\} \longleftrightarrow \{\text{submodules of } M/N\}$$



Proposition 16.11: $\mathrm{Hom}_R(M,N)$ is an R-module

Suppose M, N are R-modules, then $\mathrm{Hom}_R(M,N)$ is itself an R-module

Proof. Define addition for $f, g \in \mathrm{Hom}_R(M,N)$ as

$$(f+g)(m) \coloneqq f(m) + g(m)$$

Exercise: Check that

$$\begin{aligned} 0 \colon M &\to N \\ m &\mapsto 0 \end{aligned}$$

is the additive identity and

$$\begin{aligned} -f \colon M &\to N \\ m &\mapsto -f(m) \end{aligned}$$

is the additive inverse. Thus it is shown that $\mathrm{Hom}_R(M,N)$ is an abelian group with the binary operation $+$.
Then the R-action for $r \in R$ and $f \in \mathrm{Hom}_R(M,N)$ is

$$\begin{aligned} (r \cdot f) \colon M &\to N \\ m &\mapsto r \cdot f(m) \end{aligned}$$

Exercise: Check that $\mathrm{Hom}_R(M,N)$ satisfies all the R-module action properties. ■

Note: These operations are the same operations one learns for functions in middle school (even linear transformations in Linear Algebra):

$$f: \mathbb{R}^n \to \mathbb{R}^m$$

This can be seen by the following

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} a+e & b+f \\ c+g & d+h \end{pmatrix}$$
$$\alpha \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \alpha a & \alpha b \\ \alpha c & \alpha d \end{pmatrix}$$

But there is one additional operation that you can preform with homomorphisms which can not be performed by elements of the module, and that is function composition.

Proposition 16.12

If $f \in \mathrm{Hom}_R(M,N), g \in \mathrm{Hom}_R(N,L)$ then $g \circ f: M \to L$ and $g \circ f \in \mathrm{Hom}_R(M,L)$

Proof. Shown by direct check of homomorphism properties
$g \circ f(x+y) = g(f(x+y)) = g(f(x)+f(y)) = g(f(x)) + g(f(y)) = g \circ f(x) + g \circ f(y)$
$g \circ f(a \cdot x) = g(f(a \cdot x)) = g(a \cdot f(x)) = a \cdot g(f(x)) = a \cdot g \circ f(x)$ ■

In particular, if $M = N = L$, then $f, g \in \mathrm{Hom}_R(M,M)$ and $g \circ f \in \mathrm{Hom}_R(M,M)$, i.e. you stay in the same set by composition if the domain and range are the same set. This leads naturally to the following observation

Corollary 16.13: $\mathrm{Hom}_R(M,M)$ is a ring

$\mathrm{Hom}_R(M,M)$ is a ring with 1. In this ring, addition are $f+g$ and multiplication as composition $f \circ g$.

Proof. We know $(\mathrm{Hom}_R(M,M), +)$ is an abelian group.
It remains to check that composition is/has
(**Associativity**)

$$[(f \circ g) \circ h](x) = (f \circ g)[h(x)] = f[g(h(x))] = f[(g \circ h)(x)] = [f \circ (g \circ h)](x)$$

(**Distributivity over** $+$)
$[f \circ (g+h)](x) = f[(g+h)(x)] = f[g(x)+h(x)] = f(g(x))+f(h(x)) = (f \circ g)(x)+(f \circ h)(x)$
(**Identity**) The identity map is simply given by

$$\mathrm{Id}: M \to M$$
$$m \mapsto m$$

Exercise: Check that this is truly the identity for composition. ■

Definition 16.14: Endomorphisms and Endomorphism Ring

The ring $\mathrm{Hom}_R(M, M)$ is called the **endomorphism ring** of M. We sometimes denote it by $\mathrm{End}_R(M)$.
The elements of $\mathrm{End}_R(M)$ are **endomorphisms**.

Example 16.2. If M is any R-module and $a \in R$ where R is commutative, then we can define

$$\begin{aligned} a \cdot \mathrm{Id} \colon M &\to M \\ m &\mapsto a \cdot m \end{aligned}$$

is an endomorphism.

Proof. Simply check homomorphism properties

$$(a \cdot \mathrm{Id})(m+n) \coloneqq a \cdot (m+n) = a \cdot m + a \cdot n = (a \cdot \mathrm{Id})(m) + (a \cdot \mathrm{Id})(n)$$
$$(a \cdot \mathrm{Id})(r \cdot m) \coloneqq a \cdot (r \cdot m) = (ar) \cdot m = (ra) \cdot m = r \cdot (a \cdot m) = r \cdot (a \cdot \mathrm{Id})(m)$$ ■

This leads naturally the the following map from the ring R to the endomorphisms:

$$\begin{aligned} f \colon R &\to \mathrm{End}_R(M) \\ r &\mapsto r \cdot \mathrm{Id} \end{aligned}$$

Claim: This map is a ring homomorphism.

Proof. We check ring homomorphism properties for $r, s \in R$

$$f(r+s) \coloneqq (r+s) \cdot \mathrm{Id} = r \cdot \mathrm{Id} + s \cdot \mathrm{Id} = f(r) + f(s)$$
$$f(rs) = (rs) \cdot \mathrm{Id} = (r \cdot \mathrm{Id}) \circ (s \cdot \mathrm{Id}) = f(r) \cdot f(s)$$ ■

The equality in blue can be seen by evaluating at $m \in M$,

$$[(rs) \cdot \mathrm{Id}](m) = (rs) \cdot m = r \cdot (s \cdot m) = r \cdot (s \cdot \mathrm{Id})(m) = (r \cdot \mathrm{Id}) \circ (s \cdot \mathrm{Id})(m)$$

Warning: This map is not always injective as seen by the following example:

Example 16.3. $\mathbb{Z}/4\mathbb{Z}$ is a $\mathbb{Z}$-module and so consider the map

$$\begin{aligned} f \colon \mathbb{Z} &\to \mathrm{End}(\mathbb{Z}/4\mathbb{Z}) \\ 4 &\mapsto 4 \cdot \mathrm{Id} \end{aligned}$$

However we can see that $\mathrm{Ker}\, f$ does not contain only 0,

$$4 \cdot \mathrm{Id}(\overline{a}) = 4 \cdot \overline{a} = \overline{4a} = \overline{0} \implies 4 \in \mathrm{Ker}\, f$$

Hence, f is not injective.

L17: Spanning sets and free modules

Definition 17.1

Let M be an R-module.
An R-**linear combination** of elements $m_1, \dots, m_n \in M$ is an element of the form

$$a_1 \cdot m_1 + a_2 \cdot m_2 + \cdots + a_n \cdot m_n \quad a_i \in R$$

We say a subset $A \subset M$ **spans** or **generates** the module if every element of M is an R-linear combination of elements in A.
More generally, if $B \subset M$, the **submodule spanned/generated by** B is

$$RB \coloneqq \{a_1 \cdot m_1 + a_2 \cdot m_2 + \cdots + a_n \cdot m_n \mid n \in \mathbb{Z}^+,\ a_i \in R,\ m_i \in B\}$$

Exercise: Show that RB is an R-module

Example 17.1. For any ring R with $1 \neq 0$ every element is a "linear combination" of $\{1\}$ i.e. if $r \in R$, then $r = r \cdot 1$.
So $R = R\{1\}$ is spanned by a single element as an R-module

Example 17.2. The polynomial ring $R[X]$ has a natural R-module structure:
If $a \in R, p(X) = a_0 + a_1 X + \cdots + a_n X^n \in R[X]$ then

$$a \cdot (a_0 + a_1 X + \cdots + a_n X^n) \coloneqq (a \cdot a_0) + (a \cdot a_1) \cdot X + \cdots + (a \cdot a_m) X^n$$

$R[X]$ is spanned by $\{1, X, X^2, X^3, X^4, \dots\}$

Observe $R[X]$ has **no** finite spanning set! To see this, suppose $R[X]$ is spanned by

$$p_1(X), p_2(X), \dots, p_n(X) \in R[X]$$

Let $d = \max\{\deg p_1(X), \dots, \deg p_n(X)\}$ Then $d < \infty \implies \forall a_1, \dots, a_n \in R$
$\deg[a_1 \cdot p_1(X) + a_2 \cdot p_2(X) + \cdots + a_n \cdot p_n(X)] \leq d \implies X^{d+1} \notin \text{Span}\{p_1(X), \dots, p_n(X)\}$

Definition 17.2

We say an R-module M is **finitely generated** if it is has a finite spanning set. We say M is **cyclic** if it is spanned by a single element.

Example 17.3. If R is a ring, $A \subset R$. Then $RA = (A)$ (the module generated by A is the ideal generated by A). A cyclic submodule of R is just a principal ideal.

Example 17.4. R a ring, $F = R^n$ is the free R-module of rank n. F has a natural spanning set:

$$E_n \coloneqq \left\{ \begin{array}{c} e_1 = (1, 0, 0, \dots, 0) \\ e_2 = (0, 1, 0, \dots, 0) \\ e_3 = (0, 0, 1, \dots, 0) \\ \cdots \\ e_n = (0, 0, 0, \dots, 0, 1) \end{array} \right\}$$

Any element $(a_1, a_2, \ldots, a_n) \in R^n$ can be written as

$$\begin{aligned}(a_1, a_2, \ldots, a_n) =& a_1 \cdot (1, 0, 0, \ldots, 0) + a_2 \cdot (0, 1, 0, \ldots, 0) + \cdots + a_n \cdot (0, 0, 0, \ldots, 1) \\ =& a_1 \cdot e_1 + a_2 \cdot e_2 + \cdots + a_n \cdot e_n\end{aligned}$$

Recontextualizing the free R-module of rank n:

Consider the set $\{1, 2, 3, \ldots, n\}$ A function

$$\begin{aligned}a\colon \{1, 2, 3, \ldots, n\} &\to R \\ 1 &\mapsto a(1) = a_1 \\ 2 &\mapsto a(2) = a_2 \\ &\cdots \\ n &\mapsto a(n) = a_n\end{aligned}$$

we can think of an ordered n-tuple of elements in R as a function

$$a\colon \{1, 2, \ldots, n\} \to R$$

i.e. we can think of R^n as

$$R^n = \{a\colon \{1, 2, \ldots, n\} \to R$$

The obvious addition is

$$\begin{aligned}a + b\colon \{1, 2, \ldots, n\} &\to R \\ 1 &\mapsto a(1) + b(1) \\ 2 &\mapsto a(2) + b(2) \\ &\cdots \\ n &\mapsto a(n) + b(n)\end{aligned}$$

The obvious scalar multiplication is

$$\begin{aligned}r \cdot a\colon \{1, 2, \ldots, n\} &\to R \\ 1 &\mapsto r \cdot a(1) \\ 2 &\mapsto r \cdot a(2) \\ &\cdots \\ n &\mapsto r \cdot a(n)\end{aligned}$$

Definition 17.3

Fix a ring R. An R-module F is **free** on a set A if $\forall m \in F$ there are **unique** elements

$$m_1, m_2, \ldots, m_n \in A$$
$$a_1, a_2, \ldots, a_n \in R$$

s.t. $m = a_1 \cdot m_1 + a_2 \cdot m_2 + \cdots + a_n \cdot m_n$.
We call A set of **free generators** of F or a **basis** of F.
Note: Usually, we ask that the basis is **ordered** in some way.

Example 17.5. The set $E_n = \{e_1, e_2, \ldots, e_n\}$ is a basis for the free module of rank n.

Example 17.6. $\mathbb{Z}/2\mathbb{Z}$ is a non-free Z-module.

$$\begin{aligned} \overline{1} &= 1 \cdot \overline{1} \\ &= 3 \cdot \overline{1} \end{aligned}$$

Example 17.7. Is every submodule of a free module free?
$\mathbb{Z}/4\mathbb{Z}$ is a free module over $\mathbb{Z}/4\mathbb{Z}$
Exercise: Check that $\mathbb{Z}/4\mathbb{Z} = \mathbb{Z}/4\mathbb{Z}\{\overline{1}\}$ is free.
$2\mathbb{Z}/4\mathbb{Z} = \{\overline{0}, \overline{2}\} \subset \mathbb{Z}/4\mathbb{Z}$ is a submodule.
BUT:

$$\begin{aligned} \overline{2} \cdot \overline{2} &= \overline{0} \\ \overline{0} \cdot \overline{2} &= \overline{0} \end{aligned}$$

There is no unique way of writing $\overline{0}$ as a $(\mathbb{Z}/4\mathbb{Z})$-linear combination of $\{\overline{2}\}$. This implies $2 \cdot \mathbb{Z}/4\mathbb{Z} = (\overline{2})$ is **not** free

Example 17.8. Fix a ring R. Let A be **any** set

$$F_R(A) \coloneqq \{\phi \colon A \to R \mid \phi(a) = 0 \text{ for all but finitely many } a \in A\}$$

Proposition 17.4

$F_R(A)$ is a free module over R on the set A.

Proof. Let $\phi, \psi \colon A \to R$ then addition

$$\begin{aligned} \phi + \psi \colon A &\to R \\ a &\mapsto \phi(a) + \psi(a) \end{aligned} \qquad \begin{aligned} r \cdot \phi \colon A &\to R \\ a &\mapsto r \cdot \phi(a) \end{aligned}$$

Consider the inclusion map

$$\begin{aligned} \iota: A &\to F_R(A) \\ a &\mapsto \phi_a: A \to R \\ x &\mapsto \begin{cases} 1 & x = a \\ 0 & x \neq a \end{cases} \end{aligned}$$

Obviously this map is injective. If $\phi_a = \phi_b$ then $\phi_a(a) = 1 = \phi_b(a) \implies a = b$.
We call $\iota(A) = E_A$ and we see that
(1) E_A spans $F_R(A)$

Proof. $(\phi: A \to R) \in F_R(A)$
Let $\{a_1, \dots, a_n\} \subset A$ such that $\phi(a_i) \neq 0$. Then

$$\begin{aligned} &\phi(a_i) = \phi(a_i) \cdot 1 = \phi(a_i) \cdot \phi_{a_i}(a_i) \\ \implies &\phi \equiv \underbrace{\phi(a_1)}_{\in R} \cdot \phi_{a_1} + \underbrace{\phi(a_2)}_{\in R} \cdot \phi_{a_2} + \cdots + \underbrace{\phi(a_n)}_{\in R} \cdot \phi_{a_n} \\ \implies &\phi \in \operatorname{Span} E_a \end{aligned}$$

■

(2) $F_R(A)$ is free on E_A

Proof. Suppose

$$\begin{aligned} \phi =& r_1 \cdot \phi_{a_1} + r_2 \cdot \phi_{a_2} + \cdots + r_n \cdot \phi_{a_n} \\ =& s_1 \cdot \phi_{a_1} + s_2 \cdot \phi_{a_2} + \cdots + s_n \cdot \phi_{a_n} \end{aligned}$$

Then

$$\begin{aligned} &(r_1 - s_1) \cdot \phi_{a_1} + (r_2 - s_2) \cdot \phi_{a_2} + \cdots + (r_n - s_n) \cdot \phi_{a_n} = 0 \\ \implies &(r_1 - s_1) \cdot \underbrace{\phi_{a_1}(a_1)}_{=1} + (r_2 - s_2) \cdot \cancelto{0}{\phi_{a_2}(a_1)} + \cdots + (r_n - s_n) \cdot \cancelto{0}{\phi_{a_n}(a_1)} = 0 \\ \implies &(r_1 - s_1) \cdot 1 = (r_1 - s_1) = 0 \implies r_1 = s_1 \end{aligned}$$

Similarly $r_i = s_i \, \forall i$

■

■

Theorem 17.5

Let R be a ring, A is any set, M is an R-module such that there exists $f: A \to M$. There is a unique R-module homomorphism

$$\Phi_A: F(A) \to A$$

such that

TIKZ

Proof.

$$\Phi_A \colon F(A) \to M$$
$$(\phi \colon A \to R) \mapsto \sum_{a \in A} \underbrace{\phi(a)}_{\in R} \cdot \underbrace{f(a)}_{\in M}$$

■

Corollary 17.6

If R is a ring and F is any free module on a set A, then $F \cong F(A)$

Proof. $A \subset F$ that generates F freely over R, $j \colon A \to F$

$$\begin{array}{ccc} A & \xrightarrow{\iota} & F(A) \\ & \searrow^{j} & \downarrow{\scriptstyle \Phi_A} \\ & & F \end{array}$$

There is an obvious map

$$\Psi_A \colon F \to F(A)$$
$$r_1 a_1 + \cdots + r_n a_n \mapsto r_1 \phi_{a_1} + r_2 \phi_{a_2} + \cdots + r_n \phi_{a_n}$$

Clearly this map

$$\begin{array}{ccc} A & \xrightarrow{\iota} & F(A) \\ & \overset{j}{\searrow} & \downarrow{\scriptstyle \Phi_A} \quad \curvearrowright \mathrm{Id}_{F(A)} \\ & \underset{\iota}{\searrow} & F \\ & & \downarrow{\scriptstyle \Psi_A} \\ & & F(A) \end{array}$$

By uniqueness $\Psi_A \circ \Phi_A = \mathrm{Id}_{F(A)}$ and hence $\Phi_A \colon F(A) \to F$ is an R-module isomorphism

■

L18: Abstract linear algebra

Definition 18.1

A subset A of an R-module M is said to be **linearly independent** if for $a_1, \dots, a_n \in R$ and $m_1, \dots, m_n \in A$ such that

$$a_1 \cdot m_1 + \cdots + a_n \cdot m_n = 0$$

Then $a_1 = a_2 = \cdots = a_n = 0$.
If A is *not* linearly independent then we say it is **linearly dependent**

Example 18.1. A basis B for a free R-module is linarly independent i.e

$$B = \{1, X, X^2, X^3, \dots\}$$

is linearly independent in $\mathbb{R}[X]$(when viewed as an R-module).

Definition 18.2

A **basis** of a free R-module is a linearly independent spanning set

Example 18.2. $\{0\} \subset M$ is not linearly independent (assumign $R \neq 0$) e.g $1 \cdot 0 = 0 = 0 \cdot 0$

Example 18.3. $\mathbb{Z}/2\mathbb{Z}$ as a $(\mathbb{Z}/4\mathbb{Z})$-module.
The only possible linearly independent subset is $\{\overline{1}\}$

$$\overline{2} \in \mathbb{Z}/4\mathbb{Z} \implies \overline{2}_r \cdot \overline{1}_2 = \overline{0}_2 \in \mathbb{Z}/2\mathbb{Z}$$

Theorem 18.3

If V is a finitely generated vector space over a field F, then V is a free F-vector space

Proof. Let $A = \{v_1, \dots, v_n\}$ be a finite spanning set of V.
We may suppose no proper subset of A is spanning. We show that A is linearly independent:
Suppose otherwise, then let $\alpha_1, \dots, \alpha_n \in F$ such that

$$\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n = 0$$

such that $\alpha_1, \dots, \alpha_n$ not all zero.
After possibly rearraning, we may assume $\alpha_1 \neq 0$. Since F is a field, $\frac{1}{\alpha_1} \in F$ which implies

$$\begin{aligned} v_1 =& \frac{1}{\alpha_1} \cdot (-\alpha_2 v_2 - \alpha_3 v_3 - \cdots - \alpha_n v_n) \\ =& \left(\frac{-\alpha_2}{\alpha_1}\right) \cdot v_2 + \left(\frac{-\alpha_3}{\alpha_1}\right) \cdot v_2 + \cdots + \left(\frac{-\alpha_n}{\alpha_1}\right) \cdot v_2 \end{aligned}$$

and hence $v_1 \in \text{Span}\{v_2, \dots, v_n\}$. But if any vector can be written by this span, then

we have

$$\text{Span}\{v_2, \dots, v_n\} = V$$

contradicting the fact that A is minimal. Hence A is linearly independent.
It remains to show that V is a free F-vector space. Suppose $v \in V$ and $a_i, b_i \in F$ with

$$\begin{aligned} v =& a_1 \cdot v_2 + a_2 \cdot v_2 + \cdots + a_n \cdot v_n \\ =& b_1 \cdot v_1 + b_2 \cdot v_2 + \cdots + b_n \cdot v_n \end{aligned}$$

Then we have

$$(a_1 - b_1) \cdot v_1 + (a_2 - b_2) \cdot v_2 + \cdots + (a_n - b_n) \cdot v_n = 0$$

Since A is linearly independent then for all i

$$a_i - b_i = 0 \implies a_i = b_i$$

Therefore, V is free on A. ■

Corollary 18.4

If V is a finitely generated F-vector space and A is a minimal spannig set, then V is a free F-vector space on A and A is a basis for V.

Corollary 18.5

If V is an F-vector space with finite spanning set A, then A contains a basis B for V.

Proof. Take a minimal spanning subset of A. ■

Theorem 18.6

Suppose V is an F-vector space with basis $A = \{a_1, \dots, a_n\}$ and $B = \{b_1, \dots, b_m\}$ is a linearly independent set.
After possibly rearranging A, the sets

$$C_k \coloneqq \{b_1, \dots, b_k, a_{k+1}, \dots, a_n\} \quad \forall 0 \leq k \leq m$$

are bases for V. In particular $n \geq m$.

Proof. Prove this by induction:
When $k = 0$, $C_0 = A = \{a_1, \dots, a_n\}$ this is already true.
Now suppose C_k is a basis for V, we will show C_{k+1} is a basis for V.

$$\begin{aligned} & C_k = \{b_1, \dots, b_k, a_{k+1}, \dots, a_n\} \text{ spans } V \\ \implies & b_{k+1} = \alpha_1 \cdot b_1 + \alpha_2 \cdot b_2 + \cdots + \alpha_k \cdot b_k + \alpha_{k+1} \cdot a_{k+1} + \cdots + \alpha_n \cdot a_n \end{aligned}$$

Now B is linearly independent and so there exists $a_{k+i} \neq 0$ for some $i \geq 1$.

After rearranging, we may assume $\alpha_{k+1} \neq 0$, and so

$$\begin{aligned} a_{k+1} =& \frac{1}{\alpha_{k+1}} \cdot (b_{k+1} - \alpha_1 \cdot b_1 - \cdots - \alpha_k \cdot b_k - \alpha_{k+2} \cdot a_{k+2} - \cdots - \alpha_n \cdot a_n) \\ =& \left(\frac{1}{\alpha_{k+1}}\right) \cdot b_{k+1} + \left(\frac{-\alpha_1}{\alpha_{k+1}}\right) \cdot b_1 + \cdots + \left(\frac{-\alpha_k}{\alpha_{k+1}}\right) \cdot b_k + \left(\frac{-\alpha_{k+2}}{\alpha_{k+1}}\right) \cdot a_{k+2} + \cdots + \left(\frac{-\alpha_n}{\alpha_{k+1}}\right) \cdot b_n \end{aligned}$$

This implies

$$\begin{aligned} & a_{k+1} \in \operatorname{Span}\{b_1, \ldots, b_{k+1}, a_{k+2}, \ldots, a_n\} = \operatorname{Span} C_{k+1} \\ \implies & \operatorname{Span} C_{k+1} \supset \operatorname{Span}\{b_1, \ldots, b_k, a_{k+1}, \ldots, a_n\} = \operatorname{Span} C_k = v \\ \implies & \operatorname{Span} C_{k+1} = V \end{aligned}$$

It remains to show C_{k+1} is linearly independent.

Suppose

$$\begin{aligned} & \beta_1 \cdot b_1 + \cdots + \beta_k \cdot b_k + \beta_{k+1} \cdot b_{k+1} + \gamma_{k+2} \cdot a_2 + \cdots + \gamma_n a_n = 0 \\ =& \left(\sum_{i=1}^{k} \beta_i \cdot b_i\right) + \beta_{k+1} \cdot \left(\sum_{i=1}^{k} \alpha_i \cdot b_i + \sum_{j=k+1}^{n} \alpha_j \cdot a_j\right) + \left(\sum_{j=k+2}^{n} \gamma_j \cdot \alpha_j\right) \\ =& \left[\sum_{i=1}^{k} (\beta_i + \beta_{k+1}\alpha_i) \cdot b_i\right] + (\beta_{k+1}\alpha_{k+1}) \cdot a_{k+1} + \left[\sum_{j=k+2}^{n} (\beta_{k+1}\alpha_j + \gamma_j) \cdot a_j\right] \end{aligned}$$

Because C_k is linearly independent then

$$\beta_i + \beta_{k+1}\alpha_i = 0, \quad \beta_{k+1}\alpha_{k+1} = 0, \quad \beta_{k+1}\alpha_j + \gamma_j = 0$$

By assumption $a_{k+1} \neq 0$ and so since F is a field then $B_{k+1} = 0$ and hence $\beta_i = \gamma_j = 0$.

Therefore, C_{k+1} is linearly independent. ■

Corollary 18.7

If V is an F-vector space with basis $B = \{b_1, \ldots, b_n\}$, then any linearly independent set A has at most n elements and any spanning set C has at least n elements.

Corollary 18.8

Any two bases B, B' of a finitely generated F-vector space have the same cardinality.

Definition 18.9

If V is a finitely generated F-vector space, then the **dimension** of V is

$$\dim_F V \coloneqq \dim V \coloneqq \text{ cardinality of any basis of } V$$

We say V is finite dimensional

If V is not finitely generated, then we say it is **infinite dimensional** ($\dim V = \infty$)

Example 18.4.

- $\dim \mathbb{R}^2 = 2$
- $\dim\{\text{real polynomials of degree at most } 3\} = 4$
- $\dim \mathbb{R}[X] = \infty$

Corollary 18.10

If V is a finite dimensional F -vector space with $B = \{b_1, \ldots, b_n\}$, then B defines an F-vector space isomorphism

$$\Phi_B : V \xrightarrow{\cong} F^n$$

Proof. First

$$\begin{aligned} \Phi_B : V &\to F^n \\ b_1 &\mapsto e_1(1, 0, 0, \ldots, 0) \\ b_2 &\mapsto e_2(0, 1, 0, \ldots, 0) \\ &\cdots \\ b_n &\mapsto e_n(0, 0, \ldots, 0, 1) \end{aligned}$$

extend this linearly i.e

$$\begin{aligned} \Phi_B(\alpha_1 \cdot b_1 + \alpha_2 \cdot b_2 + \cdots + \alpha_n b_n) =& \alpha_1 \cdot \Phi_B(b_1) + \alpha_\bullet \Phi_B(b_2) + \cdots + \alpha_\bullet \Phi_B(b_n) \\ =& \alpha_1 \cdot e_1 + \alpha_2 \cdot e_2 + \cdots + \alpha_n \cdot e_n \end{aligned}$$

Check injectivity

$$\operatorname{Ker} \Phi_B = \{\alpha_1 \cdot b_1 + \cdots + \alpha_n \cdot b_n \mid \alpha_1 \cdot e_1 + \alpha_2 \cdot e_2 + \cdots + \alpha_n \cdot e_n = 0\} = \{0\}$$

Check surjectivity, we have

$$v = \alpha_1 \cdot e_1 + \cdots + \alpha_n \cdot e_n \in F^n$$

then

$$\Phi_B(\alpha_1 \cdot b_1 + \cdots + \alpha_n \cdot b_n) = v$$

■

L19: Rank-nullity and spaces

Recall: If $A = \{v_1, \dots, v_n\}$ is linearly independent in a finite dimensional vector space V and $B = \{b_1, \dots, b_n\}$ is a basis.
Then after possibly reordering

$$C_i = \{v_1, \dots, v_i, b_{i+1}, \dots, b_n\}$$

is a basis for all $0 \leq i \leq k$ and in particular, $k \leq n$.

Corollary 19.1

If $A = \{a_1, \dots, a_n\}$ is a linearly independent set in a finite dimensional F-vector space V, then there is a basis $B \supset A$.

Proof. Take any basis D for V and apply replacement to A and D. ■

Theorem 19.2

Let V be an F-vector space, $W \subset V$ a subspace. Then, in particular, V/W is an F-vector space and

$$\dim V/W + \dim W = \dim V$$

(if either side is infinite, then both are)

Proof. Suppose V is finite dimensional and $\dim V = n$ and $\dim W = m$.
Let $B = \{v_1, \dots, v_m\} \subset W$ be a basis for W. Then $B \subset V$ is linearly independent and by the building up lemma there exists

$$B' = \{v_1, \dots, v_m, v_{m+1}, \dots, v_n\}$$

which is a basis for V.
Consider the quotient map

$$\phi \colon V \to V/W$$

■

Definition 19.3

If $\varphi \colon V \to W$ is an F-linear transformation, we sometimes refer to the kernel of φ as the **null space** of φ.
The **nullity** of φ is the $\dim \operatorname{Ker} \varphi$.
The **rank** of φ is the $\dim \operatorname{Im} \varphi$.
If $\operatorname{Ker} \varphi = 0$, then we say φ is **non-singular**, otherwise we say φ is **singular**.
The **cokernel** of φ is

$$\operatorname{Coker} \varphi := W/\operatorname{Im} \varphi$$

Corollary 19.4

If $\varphi: V \to W$ is an F linear transformation, then:
(1) $\operatorname{Ker}\varphi \subset V$ and $\operatorname{Im}\varphi \subset W$ are subspaces.
(2) (Rank-nullity) $\dim V = \dim \operatorname{Ker}\varphi + \dim \operatorname{Im}\varphi$.

Proof. First isomorphism theorem implies $\operatorname{Im}\varphi \cong V/\operatorname{Ker}\varphi$ and hence

$$\dim V = \dim \operatorname{Ker}\varphi + \dim \operatorname{Im}\varphi$$

■

Corollary 19.5

If $\varphi: V \to W$ is an F-linear transformation and $\dim V = \dim W$, then the following are equivalent:
(1) φ is an isomorphism
(2) $\operatorname{Ker}\phi = 0$ (i.e. φ is injective)
(3) $\operatorname{Im}\varphi = W$ (i.e. φ is surjective)
(4) If $B \subset V$ is a basis, then

$$\phi(B) \coloneqq \{\phi(v_1), \dots, \phi(v_n) \mid v_1, \dots, v_n \in B\}$$

is a basis for W.

The dual of a vector space

Definition 19.6

Let V be an F-vector space. The **dual space** is

$$V^* \coloneqq \operatorname{Hom}_F(V, F)$$

Elements of V^* are called **linear functionals**

Example 19.1. Let V be the vector space of continuous functions $f: [0,1] \to \mathbb{R}$, then the integral operator is a linear functional on V

$$\int : V \to \mathbb{R}$$
$$f \mapsto \int_0^1 f \,\mathrm{d}x$$

Lemma 19.7

If $B = \{v_1, \dots, v_n\}$ is a basis for V, then any linear functional $f \in V^*$ is determined by its values on B.

Proof. If $v \in V$, then

$$\begin{aligned} & v = a_1 v_1 + a_2 v_2 + \cdots + a_n v_n \\ \implies & f(a_1 + \cdots + a_n v_n) = a_1 f(v_1) + \cdots + a_n f(v_n) \\ \implies & a_1 \alpha_1 + \cdots + a_n \alpha_n \end{aligned}$$

given $\alpha_1 = f(v_1), \ldots, \alpha_n = f(v_n)$. ■

Definition 19.8

Let $B = \{v_1, \ldots, v_n\}$ be a basis for V. Denote by $v_i^* \in V^*$ the linear functional

$$v_i^*(v_j) \coloneqq \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases}$$

Theorem 19.9

$B^* = \{v_1^*, \ldots, v_n^*\}$ is a basis for V^*. In particular, if $\dim V = n$, then $\dim V^* = n$.

Proof. Let $f \in V^*$, $v \in V$ with $v = a_1 v_1 + \cdots + a_n v_n$.
Then

$$f(v) = f(a_1 v_1 + \cdots + a_n v_n) = a_1 f(v_1) + \cdots + a_n f(v_n)$$

On the other hand,

$$v_1^*(v) = v_1^*(a_1 v_1 + \cdots + a_n v_n) = a_1 \underbrace{v_1^*(v_1)}_{=1} + \cancelto{0}{a_2 v_1^*(v_2)} + \cdots + \cancelto{0}{a_n v_1^*(v_n)} = a_1$$

Through this same logic it shown

$$v_i^*(v) = a_i \quad i = \{1, \ldots, n\}$$

Returning to the first equation

$$\begin{aligned} f(v) &= a_1 f(v_1) + \cdots + a_n f(v_n) \\ &= v_1^*(v) f(v_1) + \cdots + v_n^*(v) f(v_n) \\ &= (f(v_1) v_1^* + \cdots + f(v_n) v_n^*)(v) \end{aligned}$$

Hence $f = \sum_{i=1}^n f(v_i) v_i^*$ and B^* is spanning.
On the other hand, if $\alpha_1, \ldots, \alpha_n \in F$ such that

$$\alpha_1 v_1^* + \cdots + \alpha_n v_n^*$$

Then

$$(\alpha_1 v_1^* + \cdots + \alpha_n v_n^*)(v_i) = \alpha_i = 0 \, \forall i$$

Therefore, B^* is also linearly independent and we conclude B^* is a basis for V^*. ■

Note: If $\varphi: V \to W$ is a linear transformation, then there is an induced map

$$\varphi^*: W^* \to V^*$$
$$(f: W \to F) \mapsto (f \circ \varphi: V \to W \to F)$$

Theorem 19.10

If $\varphi: V \to W$ is a linear transformation of finite dimensional vector spaces inducing $\varphi^*: W^* \to V^*$. Then,

$$\operatorname{Ker} \varphi^* \cong \operatorname{Coker} \varphi$$
$$\operatorname{Coker} \varphi^* \cong \operatorname{Ker} \varphi$$

as F-vector spaces.

Proof. Let $B = \{v_1, \ldots, v_n\}$ a basis for $\operatorname{Ker} \varphi$, $B' = \{v_1, \ldots, v_n, v_{n+1}, \ldots, v_m\}$ a basis for V and $\varphi(B') = \{\varphi(v_{n+1}), \ldots, \varphi(v_m)\}$ a basis for $\operatorname{Im} \varphi$.
Since $\operatorname{Im} \varphi \subset W$ is a subspace then

$$C = \{\varphi(v_{n+1}), \ldots, \varphi(v_m), w_1, \ldots, w_k\}$$

is a basis for W.
Dualizing, we get the dual basis

$$C^* = \{\varphi(v_{n+1})^*, \ldots, \varphi(v_m)^*, w_1^*, \ldots, w_k^*\}$$

a basis for W^*.
Let $v \in V$ and consider

$$\varphi^*: W^* \to V^*$$
$$\varphi^*[\varphi(v_{n+i})^*](v) = \varphi(v_{n+i})^*(\varphi(v))$$

Since we can write $v = \sum_{j=1}^m a_j v_j$ then

$$\varphi^*[\varphi(v_{n+i})^*](v) = \varphi(v_{n+i})^* \left(\sum_{j=n+1}^m a_j \varphi(v_j) \right) = a_{n+i}$$

and hence

$$\varphi^*(w_j^*)(v) = w_j^*(\varphi(v)) = w_j^* \left(\sum_{j=n+1}^m a_j \varphi(v_j) \right) = 0$$

implying

$$\operatorname{Ker} \varphi^* = \operatorname{Span}\{w_1^*, \ldots, w_k^*\}$$
$$\operatorname{Im} \varphi^* = \operatorname{Span}\{v_{n+1}^*, \ldots, v_m^*\}$$

Therefore

$$\operatorname{Coker} \varphi = W/\operatorname{Im} \varphi = \frac{\operatorname{Span}\{\varphi(v_{n+1}), \ldots, \varphi(v_m), w_1, \ldots, w_k\}}{\operatorname{Span}\{\varphi(v_{n+1}), \ldots, \varphi(v_m)\}} = \operatorname{Span}\{\overline{w}_1, \overline{w}_2, \ldots, \overline{w}_k\}$$

and $\operatorname{Ker}\varphi = \operatorname{Span}\{v_1, \ldots, v_n\}$ to give

$$\operatorname{Coker}\varphi^* = V^*/\operatorname{Im}\varphi^* = \frac{\operatorname{Span}\{v_1, \ldots, v_n, v_{n+1}, \ldots, v_m\}}{\operatorname{Span}\{v_{n+1}^*, \ldots, v_m^*\}} = \operatorname{Span}\{\overline{v}_1, \overline{v}_2, \ldots, \overline{v}_n\}$$

■

FOUR SUBSPACES GRAPHIC

L20: The Matrix of a linear transformation