Math 28B: Introduction to Rings and Fields

Hussein Hijazi

Spring 2021

Lecture 1

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

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

Lecture 2

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 2.1: $\mathbb{Z}/n\mathbb{Z}$ 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 2.2: 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 2.3: 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 2.1: 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 2.2: 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 2.4: 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 2.2: 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 2.5: 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.

Lecture 3

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).

Definition 3.1: Polynomial 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: Set 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 3.1

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 3.3: 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 3.4

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

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

Proposition 3.2

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

$$\phi(p+q) = (p+q)(0) = p(0) + q(0) = \phi(p)\phi(q)$$
$$\phi(p \cdot q) = (p \cdot q)(0) = p(0) \cdot q(0) = \phi(p) \cdot \phi(q)$$

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

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

Lecture 4

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 4.1

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 4.1

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, $\operatorname{Ker} f = 2\mathbb{Z}$.
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 4.2

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

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

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 4.2: 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 4.1: 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.

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 4.2: 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

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

Lecture 5

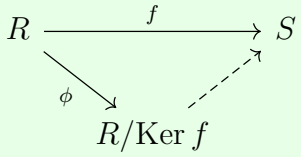
Isomorphism Theorems

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.



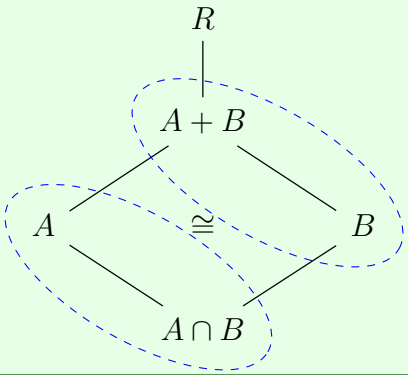
Theorem 5.2: The Second Isomorphism Theorem

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, $\operatorname{Ker} \phi = B$. ■

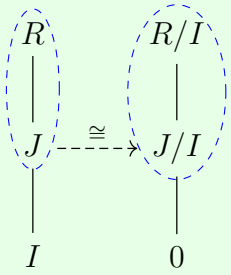
Theorem 5.3: The Third Isomorphism Theorem

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

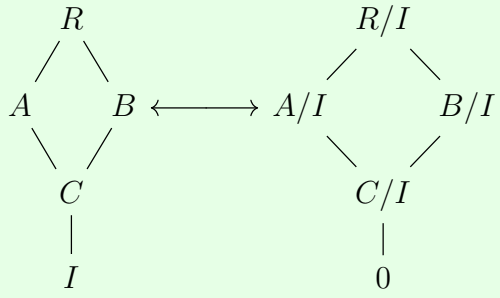
Let $I \subset R$ be an ideal.
Then the correspondence

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

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 5.1: 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: Insetead 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 5.1

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,

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

■

Lecture 6

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 6.1

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 $r_1, \ldots, r_n \in R$, $a_1, \ldots, a_n \in A$

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

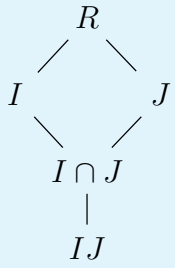
and since (A) is a left ideal, we have

$$RA = (A)$$

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

Proposition 6.2

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 $a \in R$.

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 6.2: 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 6.3

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

Theorem 6.1: 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

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

■

Lecture 7

Maximal Ideals

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

Proposition 7.1

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 7.1: 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 7.1: 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

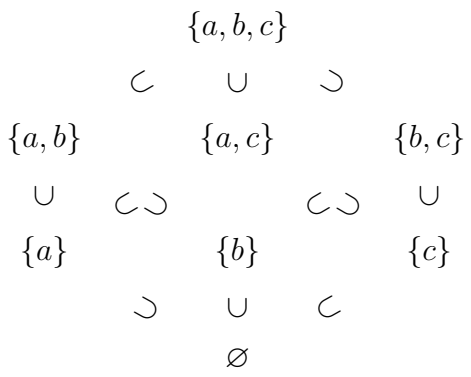
Definition 7.2: Partial Order

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 7.3: 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 7.1: Zorn's Lemma

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

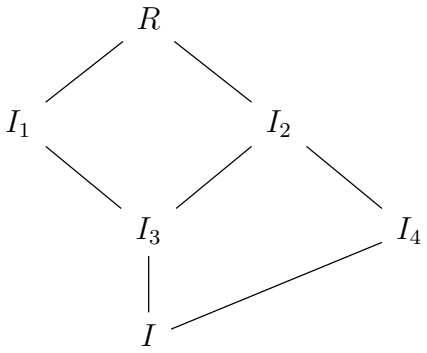
Proposition 7.2

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 7.1: 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 7.2: 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.

Lecture 8

More on Maximal Ideals

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:

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

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 $M_a := \mathrm{Ker}(\mathrm{Ev}_a)$

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 $p(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$, 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

$$\mathbb{R}[x] = \{a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots + a_n x^n | a_k \in \mathbb{R},\ k = 0, 1, 2, \ldots n\}$$

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:

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

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

$$\mathbb{R}[x]/I \to \mathbb{C}$$
$$\overline{1} \mapsto 1$$
$$\overline{x} \mapsto i$$

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

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

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

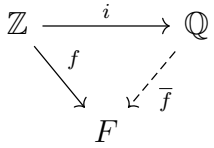
$$\mathbb{Z} \to \mathbb{Q}$$
$$n \mapsto \frac{n}{1}$$

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 8.1

$Q(R)$ 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

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

$$\begin{array}{ccc} R & \xrightarrow{\;i\;} & Q(R) \\ & \searrow^{f} \quad \swarrow_{\overline{f}} & \\ & F & \end{array}$$

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

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

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

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

Lecture 9

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

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

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 9.2: 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 9.1

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 9.2: 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 9.1

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 9.2

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. ■

Lecture 10

Euclidean Domains

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 10.1

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 10.1: 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 10.3: 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 10.4: 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 10.2

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

Theorem 10.1: 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 10.5: Principal Ideal Domain

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

Theorem 10.2

Every Euclidean domain is a PID, i.e

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

Theorem 10.3

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

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

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 10.4

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 10.5

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

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

■

Lecture 11

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 $a = u \cdot b$.

Proposition 11.1

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 then, $1 = r \cdot b$, so $b \in R^\times$. ■

Example 11.1 Irreducible but not prime.
Consider the ring

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

Then

- $N(a + b\sqrt{-5}) \coloneqq a^2 + 5b^2$
- $N(x \cdot y) = N(x) \cdot N(y)$
- $N(x) = \pm 1$ 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

$$b = 0 \implies N(a+b\sqrt{-5}) = N(a) = a^2 \implies N(a+b\sqrt{-5}) = 1 \implies a+b\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]^\times$$

■

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

Proof. We know

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

However, $3 \notin (2 + \sqrt{-5})$.
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 $3 \notin \pm(N(a + b\sqrt{-5}) \cdot N(2 + \sqrt{-5}))$ ■

Proposition 11.2

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

Proof. It suffices to show that irreducible $\implies$ 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

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

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

$$m \notin R^\times \implies s \in R^\times \implies (r) = (m)$$

■

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

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

Definition 11.2: 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) $r = p_1 \cdot p_2 \cdot \ldots \cdot p_k$ 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

Example 11.4 $\mathbb{Z}$ are a UFD

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

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

and $3, 2 \pm \sqrt{-5}$ are irreducibles.

Proposition 11.3

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

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

Hence

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

so by unique factorization, w.l.og

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

■

Proposition 11.4

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

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

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 $gcd(a, b)$.

Proof. Clearly $d \mid a$, $d \mid b$.
If $c \mid a$, $c \mid b$, then we want to see that $c \mid d$.
Unique factorization says for q_i irreducible, $q_i \neq q_j$ and $g_i > 0$, we have

$$c = q_1^{g_1} \bullet \ldots \bullet q_m^{g_m}$$

Since $c \mid a$, $c \mid b$, then after changing associates

$$\{q_1, \ldots, q_n\} \subset \{p_1, \ldots, p_n\},\ g_i \leq \min\{e_i, f_i\} \implies c \mid d$$

■

And so there exists a greatest common divisor of a, b in R. ■