1. Rings

Recap of Abelian Group

Definition Abelian Groups

An Abelian (commutative) group R is a set with a binary operation

$$+ : R \times R \to R$$
$$(a,b) \mapsto a+b$$

such that

(0) $a+b = b+a \quad \forall a,b \in R$

(1) $a+(b+c) = (a+b)+c$

(2) $\exists\, 0 \in R$ s.t $0+a = a+0 \quad \forall a \in R$

(3) $\forall a \in R, \exists\, (-a) \in R$ s.t $a+(-a) = (-a)+a = 0$

Notation: We write $a+(-b) = a-b$

Definition of a ring

Definition Ring

A ring R is a set with 2 binary operations

addition	multiplication
$R \times R \to R;$	$R \times R \to R;$
$(a,b) \mapsto a+b$	$(a,b) \mapsto a \times b$

satisfying following axioms

i) $(R,+)$ is an Abelian group

ii) $(a \times b) \times c = a \times (b \times c) \quad \forall a,b,c \in R$

iii) $a \times (b+c) = a \times b + a \times c \quad \forall a,b,c \in R$

$(a+b) \times c = a \times c + b \times c \quad \forall a,b,c \in R$

Notation: $a \times b$ is represented by ab

Basic Example of a Ring

1) Proposition. $\mathbb{Z}$ is a ring

Proof:

- $\mathbb{Z}$ is closed under binary operations $+$ (addition) and $\times$ (multiplication)

i) $(\mathbb{Z},+)$ is an Abelian Group

ii) $\forall\, a,b,c \in \mathbb{Z}$,

$$(a\times b)\times c = (ab)\times c = abc$$
$$= a\times(bc) = a\times(b\times c)$$

iii) $\forall\, a,b,c \in \mathbb{Z}$

$$a(b+c) = ab + ac$$
$$(a+b)c = ac + bc$$

Remark:

i) In the definition of a ring, we do not assume existence of a multiplicative inverse a^{-1}

ii) We do not assume existence of multiplicative identity

Ex: $2 \in \mathbb{Z}$, $2^{-1} \notin \mathbb{Z}$ eventhough $2^{-1}2 = 1 = e$

In $\mathbb{Z}$, $1 \in \mathbb{Z}$, contains multiplicative identity

$0 \in \mathbb{Z}$, $\cancel{0^{-1}}$

Remark: $(R,+)$ is Abelian group $\Longrightarrow 0 \in R$

Remark: In general, multiplication is not commutative

Commutative Ring

Definition. Commutative Ring

A ring is commutative if $\forall\, a,b \in R$,

$$a\times b = b\times a$$

i.e. multiplication is commutative

More Examples of Rings

1) $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all commutative rings with identity under usual + and x

2) $\mathbb{N}$ and $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$ with usual + and x are not rings as $(\mathbb{N}, +)$ and $(\mathbb{N}_0, +)$ are not groups

3) $R = 2\mathbb{Z} = \{2z : z \in \mathbb{Z}\}$ with usual operations + and x is a commutative ring

For identity, $\forall z \in \mathbb{Z}$, $ze = z \implies e = 1 \notin 2\mathbb{Z}$

$\implies 2\mathbb{Z}$ does not contain multiplicative identity

4) Consider $M_n(\mathbb{R})$: nxn matrices with real entries

Matrix addition is commutative

$A + B$: Matrix Addition

$A \times B$: Matrix Multiplication

$R = M_n(\mathbb{R})$ is a non-commutative ring, identity I_n. So are $M_n(\mathbb{C})$, $M_n(\mathbb{Q})$ and $M_n(\mathbb{Z})$

5) For a ring and any $n \in \mathbb{N}$, $M_n(R)$ is the set of all nxn matrices with entries in R.

For any ring, $M_n(R)$ is a ring

6) **Proposition**

$(\mathbb{Z}_n, \oplus, \otimes)$ is a commutative ring with identity 1. Denote this ring by

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

Proof:

(i) Already seen that $(\mathbb{Z}/n\mathbb{Z}, \oplus)$ is an abelian group

(ii) $\forall [a], [b], [c] \in \mathbb{Z}_n$,

$$[a] \otimes ([b] \otimes [c]) = [a] \otimes [bc] = [a(bc)]$$

$$= [(ab)c] = [ab] \otimes [c] = ([a] \otimes [b]) \otimes [c]$$

(iii) Let $[a], [b], [c] \in \mathbb{Z}/n\mathbb{Z}$. Then

$$[a]([b] \oplus [c]) = [a][b+c] = [a(b+c)]$$

$$= [ab + ac] = [ab] \oplus [ac]$$

$$= [a][c] \oplus [a][c]$$

Similarly $([a] \oplus [b])[c] = [a][c] \oplus [b][c]$.

7) **Proposition**

Let X be a set, $X \neq \phi$, $R = 2^X$ powerset.

Define binary operations; $\forall A, B \in R$,

$$A + B = A \Delta B = (A \setminus B) \cup (B \setminus A) \quad \text{(symmetric difference)}$$

$$A \times B = A \cap B$$

Then $(R, +, \times)$ is a ring with 0 element ϕ, identity X

Proof:

i) (0) $A \Delta B = (A \setminus B) \cup (B \setminus A) = (B \setminus A) \cup (A \setminus B) = B \Delta A$

(1) $A \Delta (B \Delta C) = (A \Delta B) \Delta C$

(2) $A \Delta \phi = A$

(3) $A \Delta A = \phi \Longrightarrow$ A is its own inverse

Therefore (R, Δ) is an Abelian group

ii) Observe that for any subsets $A, B, C \subseteq X$

$$(A \cap B) \cap C = A \cap (B \cap C)$$

which is basic set theory

iii) Enough to check for all subsets $A, B, C \subseteq X$, the equality

$$A \cap (B \Delta C) = (A \cap B) \Delta (B \cap C)$$

Since $\cap$ is commutative

It holds true because both sides are the collection of elements of X that belong to A and to precisely one of two subsets B and C.

And $X \neq \phi$ and $A \cap X = A$ for any $A \subseteq X$. So X is the identity of our ring

■

Remarks:

If there exists an element $1 \in R$ such that $1 \neq 0$ and

$$1a = a1 = a \qquad \forall a \in R$$

then R is a ring with identity

The identity element $1 \in R$, if it exists is unique

2. Elementary property of rings

Remark. Any ring R is an Abelian Group relative to addition $+$, so

i) $0 \in R$ identity is unique

ii) $\forall a \in R, \exists -a \in R$ s.t $a + (-a) = 0$, $-a$ is unique

Lemma

i) $\forall a \in R, \; a0 = 0 = 0a$

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

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

Proof:

i) $a \times 0 = a0 = a \times (0 + 0)$

$= a \times 0 + a \times 0$

Adding $-a0$ to both sides,

$$0 = a0 - a0 = a0 + (a0 - a0) = a0$$

$\Longrightarrow \; 0 = a0 + 0$

$\Longrightarrow \; 0 = a0$

ii) $a(-b) + ab = a((-b) + b)$

$= a0 = 0$

$\Longrightarrow \; a(-b) + ab = 0$

$\Longrightarrow \; a(-b) = -(ab)$

Dual for showing $(-a)b = -(ab)$

iii) $(-a)(-b) = -((-a)b)) = -(-(ab)) = ab$ by ii

$\blacksquare$

In particular, if R has an identity 1, then $\forall a, b \in R$,

- $(-1)b = -(1b) = -b$
- $(-1)(-1) = 1 \times 1 = 1$

Subrings

Definition Subring

Let R be any ring $(+,\times)$, let $S \subseteq R$ be any subset

We say S is called a **subring** of R if:

(a) $0 \in S$ (identity)

(b) $a,b \in S \implies -a \in S,\ a+b \in S,\ a \times b \in S$ (closure)

Remark: If $S \subseteq R$ is a ring under the same operations $+$ and $\times$ as $R \implies S$ is a subring of R

Proposition

If $S \subseteq R$ is a subring, then S is a ring relative to the same operations $+, \times$ as on R

Proof:

(i) From defn of subring

$$\left.\begin{array}{l} \underline{\text{Closure}}:\ a+b \in S \\ \underline{\text{Identity}}:\ 0 \in S \\ \underline{\text{Inverse}}:\ \forall a \in S,\ -a \in S \end{array}\right\} \begin{array}{l} \implies S \leq (R,+) \\ \implies (S,+) \text{ is an Abelian Group} \end{array}$$

(ii) $\forall a,b,c \in S \implies a,b,c \in R$ and since $S \subseteq R$ is closed under $\times$

$$a(bc) = (ab)c$$

(iii) $$a(b+c) = ab+ac$$

$$(a+b)c = ac+bc$$

Hence by defn of a ring, S is a ring. ■

Examples of Subrings

1) $\overbrace{\mathbb{C} \supseteq \mathbb{R} \supseteq \mathbb{Q}}^{\text{fields}} \supseteq \mathbb{Z}$ not a field

$\mathbb{C}$ $(+,\times)$ a ring; $\mathbb{R}$ subring $\Downarrow$ ring; $\mathbb{Q}$ subring $\Downarrow$ ring

2) $\mathbb{N} \subseteq \mathbb{Z}$ NOT a subring

$0 \notin \mathbb{N},\ \forall n \in \mathbb{N},\ -n \notin \mathbb{N}$

3) $\mathbb{Z} \supseteq 2\mathbb{Z}$ is a $\underset{\text{ring}}{\underset{\Downarrow}{\text{subring}}}$ without an identity

$0 \in 2\mathbb{Z} \subseteq \mathbb{Z}$

$\mathbb{Z}$ is a ring with multiplicative identity $1 \in \mathbb{Z} : \forall z \in \mathbb{Z},\ 1 \cdot z = z$

$1 \notin 2\mathbb{Z} \implies 2\mathbb{Z}$ is a ring without an identity

4) $\forall n > 1$

$M_n(\mathbb{C}) \supseteq M_n(\mathbb{R}) \supseteq M_n(\mathbb{Q}) \supseteq M_n(\mathbb{Z})$ subrings

Definition Square free

Fix any $d \in \mathbb{Z}$, $d \neq 0$, $d \neq 1$.

d is square free $\iff p^2 \nmid d \quad \forall p$, prime

i.e. d is not divisible by p^2 $\forall$ primes p

$d \in \{\ldots, -6, -5, -3, -2, -1, 2, 3, 5, 6, \ldots\}$

(5) $R = \mathbb{C}$ is a ring. Define $S \subseteq R$

$S = \{a + b\sqrt{d} : a, b \in \mathbb{Z},\ d$ prime free$\} = \mathbb{Z}[d]$ with $+, \times$

Claim: $S = \mathbb{Z}[d]$ is a subring of $\mathbb{C} = R$

(a) $0 = 0 + 0\sqrt{d}$ identity

(b) $a + b\sqrt{d},\ a' + b'\sqrt{d} \in S$

- $-a - b\sqrt{d} \in S$
- $(a + a') + (b + b')\sqrt{d} \in S$
- $(a + b\sqrt{d})(a' + b'\sqrt{d}) = \underset{\mathbb{Z}}{\underset{\cap}{(aa' + bb'd)}} + \underset{\mathbb{Z}}{\underset{\cap}{(ab' + db')}}\sqrt{d} \in S$

Hence S is a subring $\implies S$ a ring ∎

if $d > 0 \implies S \subseteq \mathbb{R}$ subring

Definition

$d = -1 \implies \mathbb{Z}[i] = \{a + ib : a, b \in \mathbb{Z}\}$ are called Gaussian integers

(6) **Proposition**

Let R be any ring. Let X be any non-empty set. Consider

$$F_R^X = \{f \mid f : X \longrightarrow R\}$$

Define the binary operations + and × on F_R^X, $\forall x \in X$ by

$$(f+g)(x) = f(x) + g(x)$$

$$(f \times g)(x) = (fg)(x) = f(x)g(x)$$

F_R^X is a ring

Proof:

i) (0) $\forall x \in X$, $(f+g)(x) = f(x) + g(x)$

$= g(x) + f(x)$ since $f(x), g(x) \in R$, $(R,+)$ Abelian

$= (g+f)(x)$

(1) $(f+(g+h))(x) = f(x) + (g+h)(x)$

$= f(x) + (g(x) + h(x))$

$= (f(x) + g(x)) + h(x)$ since $f(x), g(x), h(x) \in R$, $(R,+)$ group

$= (f+g)(x) + h(x)$

$= ((f+g)+h)(x)$ $\quad \forall x \in X$

(2) 0 function: $0 : X \rightarrow R;\ x \mapsto 0$

$(f+0)(x) = f(x) + 0(x) = f(x) + 0$

$= f(x)$

$= 0 + f(x)$

$= (0+f)(x)$

(3) Inverse function $(-f)(x) = -f(x)$

$(f+(-f))(x) = f(x) + (-f(x))$

$= f(x) - f(x)$

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

Hence $(F_R^X, +)$ is an Abelian group

3. Homomorphisms and Isomorphisms

Definition Ring Homomorphism

Let R, S be any 2 rings. A function

$$\alpha : R \to S$$

is a ring homomorphism if $\forall a, b \in R$

i) $\alpha(a \underset{R}{+} b) = \alpha(a) \underset{S}{+} \alpha(b)$

ii) $\alpha(a \underset{R}{\times} b) = \alpha(a) \underset{S}{\times} \alpha(b)$

If R and S are rings with identity 1 and

$$\alpha(1) = 1$$

then α is a unital ring homomorphism

Remark: By Group Theory, if $\alpha : R \to S$ is a ring homomorphism, then α is a group homomorphism

$$\alpha : (R,+) \longrightarrow (S,+)$$

i) $\alpha(0_R) = 0_S$

ii) $\alpha(-a) = -\alpha(a)$

Definition

If $\alpha : R \to S$ is a ring homomorphism and α is bijective, then α is a ring isomorphism

If $\exists$ an isomorphism $\alpha : R \longrightarrow S$, then R is isomorphic to S denoted by

$$R \cong S$$

Properties of Homomorphisms

Lemma

(a) The identity map

$$i: R \to R \,;\; i(a) = a$$

is a ring isomorphism ; $R \cong R$

(b) If $\alpha : R \to S$ is a ring isomorphism, then

$$\alpha^{-1} : S \to R$$

is a ring isomorphism ; $R \cong S \implies S \cong R$

(c) If $\alpha : R \to S$ and $\beta : S \to T$ are ring homomorphism (isomorphism) then

$$\beta\alpha : R \to T$$

is a ring homomorphism (isomorphism) ; $R \cong S$ and $S \cong T \implies R \cong T$

(d) Suppose $R \cong S$.

$$R \text{ is commutative} \iff S \text{ is commutative}$$

Proof :

(a) $\forall\, a, b \in R$

$$i(a+b) = a+b = i(a) + i(b)$$

$$i(ab) = ab = i(a)\, i(b)$$

and identity maps are bijections

(b) Let $x, y \in S$. From Group Theory

$$\alpha^{-1}(-x) = -\alpha^{-1}(x)$$

$$\alpha^{-1}(x+y) = \alpha^{-1}(x) + \alpha^{-1}(y)$$

Put $a = \alpha^{-1}(x)$ and $b = \alpha^{-1}(y)$. Then $\alpha(a) = x$ and $\alpha(b) = y$

As α is a homomorphism,

$$\alpha(ab) = \alpha(a)\alpha(b) = xy$$

$$\implies \alpha^{-1}(x)\alpha^{-1}(y) = ab = \alpha^{-1}(xy)$$

Further α is a bijection $\implies \alpha^{-1}$ is a bijection.

(c) By Group Theory, $\beta\alpha$ preserves $+$ operation

$\forall\ a, b \in R$

$$(\beta\alpha) = \beta(\alpha(ab)) = \beta(\alpha(a)\alpha(b)) = \beta(\alpha(a))\beta(\alpha(a)) = (\beta\alpha)(a)\ (\beta\alpha)(b)$$

$\Longrightarrow$ $\beta\alpha$ is a homomorphism

α and β are bijection $\Longrightarrow$ $\beta\alpha$ are bijection

(d) Suppose R is commutative. $\forall\ a, b \in R$

$$\alpha(a)\alpha(b) = \alpha(ab) = \alpha(ba) = \alpha(b)\alpha(a)$$

Suppose S is commutative. $\forall\ a, b \in S$

$$\alpha^{-1}(a)\alpha^{-1}(b) = \alpha^{-1}(ab) = \alpha^{-1}(ba) = \alpha^{-1}(b)\alpha^{-1}(a)$$

■

Examples

1) Let

$$S = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a, b \in \mathbb{R} \right\} \subseteq M_2(\mathbb{R})$$

S is a subring of $M_2(\mathbb{R})$.

Indeed $0_{2\times 2} \in S$ and $\forall\ X, Y \in S$, $-X, X+Y \in S$

Checking XY

$$XY = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{pmatrix} \in S$$

Now define function

$$\alpha(a+ib) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

α is a bijection (group theory)

Moreover

$$\alpha((a+ib) + (c+id)) = \alpha((a+c) + i(b+d)) = \begin{pmatrix} a+c & b+d \\ -(b+d) & a+c \end{pmatrix}$$

$$= \begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \alpha(a+ib) + \alpha(c+id)$$

$$\alpha((a+ib)(c+id)) = \alpha(ac-bd+i(ad+bc))$$

$$= \begin{pmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{pmatrix} = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} c & d \\ -d & c \end{pmatrix}$$

$$= \alpha(a+ib)\alpha(c+id)$$

Thus α is a ring homomorphism $\Longrightarrow$ α is a ring isomorphism

$$\mathbb{C} \cong S$$

2) Let $m,n \in \mathbb{N}$ and $m|n$. Define

$$\alpha : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z};$$
$$\alpha([z]_n) = [z]_m$$

For any $z \in \mathbb{Z}$, for any $w \in \mathbb{Z}$, we have

$$[z]_n = [w]_n \iff n|(z-w)$$
$$\iff m|(z-w) \quad \text{since } m|n$$
$$\iff [z]_m = [w]_m$$

therefore α is well-defined. We have equalities

$$\alpha([z]_n \oplus [w]_n) = \alpha([z+w]_n)$$
$$= [z+w]_m = [z]_m \oplus [w]_m$$
$$= \alpha([z]_n) \oplus \alpha([w]_n)$$

and similarly for $\alpha([z]_n[w]_n) = \alpha([z]_n)\alpha([w]_n)$

$\Longrightarrow$ α is a ring homomorphism.

Note: $|\mathbb{Z}/n\mathbb{Z}| = n$, $|\mathbb{Z}/m\mathbb{Z}| = m$

Hence α is a ring isomorphism only if $m=n$

Important!

Let R and S are rings with multiplicative identity $1_R \in R$ and $1_S \in S$

If $\alpha : R \longrightarrow S$ is an onto homomorphism (or isomorphism) then

$$\alpha(1_R) = 1_S$$

4. Units and Fields

Definition Unit

Take any $a \in R$. If $\exists\, b \in R$ s.t

$$ab = ba = 1$$

then 'a' is called a unit of our ring

Remark: Let R be any ring with the identity $1 \in R$

1) Assume $R \neq \{0\}$, then $1 \neq 0$

Indeed $\forall a \in R$, if $1 = 0$, then $\forall a \in R$

$$a = a.1 = a.0 = 0 \Longrightarrow R = \{0\} \;※$$

2) If a is a unit $\Longrightarrow$ $ab = ba = 1$

$\Longrightarrow b = a^{-1}$, a is invertible

Notation: Set of all units

$$U(R) = \{a \in R : a \text{ is a unit}\}$$

Remark:

(a) Consider $1 \in R$. Then $1 \times 1 = 1 \times 1 = 1 \Longrightarrow 1 \in U(R)$

$\Longrightarrow 1^{-1} = 1$

The identity $1 \in R$ is unique, while there may be other units

(b) Note that $0 \cdot b = 0 \neq 1 \;\; \forall b \in R \Longrightarrow U(R) \not\ni 0$

(c) If $a \in U(R)$, then the element b such that

$$ba = 1 = ab$$

is unique

If $a \in U(R)$ is a unit $\Longrightarrow b = a^{-1}$ is unique

Lemma

Suppose for some $a \in R$, $\exists\, b, c \in R$ such that

$$ab = ca = 1 \implies b = c \text{ and so } a \in U(R)$$

proof: $b = 1b = (ca)b = c(ab) = c1 = c \implies b = c$ ■

Corollary

Suppose that $ab' = b'a$ and $ab = ba = 1$. Then

$$ab = 1 = \underset{\substack{\shortparallel \\ c}}{b'}a \implies b' = b$$

Proposition

Let $(R, +, \times)$ be any ring with an identity such that $R \neq \{0\}$

Then $(U(R), \times)$ is a group

Proof:

Identity: We know that 1 is a unit of R, that is $1 \in U(R)$.

$\forall\, a \in U(R)$, $a \times 1 = a = a \times 1$

Associative: We know that $\times$ is associative on $R \implies$ associative on $U(R)$

Inverse: If $u, v \in U(R)$, $\exists\, u^{-1}, v^{-1} \in R$ such that

$$uu^{-1} = 1 = u^{-1}u \quad \text{and} \quad vv^{-1} = 1 = v^{-1}v$$

Note that u is the inverse of u^{-1}; $u = (u^{-1})^{-1} \implies u^{-1} \in U(R)$

Closure: Further

$$(uv)(v^{-1}u^{-1}) = (u)(vv^{-1})u^{-1} = u1u^{-1} = uu^{-1} = 1$$

$$\implies (uv)^{-1} = v^{-1}u^{-1}$$

and similarly

$$(v^{-1}u^{-1})(uv) = 1$$

Hence $uv \in U(R)$ by definition ■

Examples of Units

1) $R = \mathbb{Z} \ni 0, 1$. Hence

$U(R) = U(\mathbb{Z}) = \{1, -1\}$: - NOT closed under +

- closed under x

2) $U(M_n(\mathbb{R})) = \{\text{invertible matrices}\}$

$= \{A \in M_n(R) : \det A \neq 0\} = GL(n, \mathbb{R})$

$\Longrightarrow U(M_n(\mathbb{R})) = GL(n, \mathbb{R})$: General Linear Group

3) $U(\mathbb{R}) = \mathbb{R} \setminus \{0\}$

$U(\mathbb{Q}) = \mathbb{Q} \setminus \{0\}$

$U(\mathbb{C}) = \mathbb{C} \setminus \{0\}$

4) **Proposition**

$U(\mathbb{Z}/n\mathbb{Z}) = \{[a] : a \in \mathbb{Z} \text{ and } \gcd(a, n) = 1\}$

Proof:

If $[a] \in U(\mathbb{Z}/n\mathbb{Z}) \Longrightarrow [a][b] = [1]$ for some $[b] \in U(\mathbb{Z}/n\mathbb{Z})$

$\Longrightarrow [ab] = [1]$

$\Rightarrow n \mid (ab - 1)$

$\Longrightarrow ab - 1 = nq$ for some $q \in \mathbb{Z}$

$\Longrightarrow ab - nq = 1$

$\Longrightarrow \gcd(a, n) = 1$ Bezout's Theorem

Conversely if $\gcd(a, n) = 1 \Rightarrow \exists\, s, t \in \mathbb{Z}$ such that $1 = as + nt$

$\Rightarrow [1] = [as + nt]$

$\Rightarrow [1] = [as]$

$\Rightarrow [1] = [a][s]$

5) **Proposition**

For p prime, $U(\mathbb{Z}/p\mathbb{Z}) = (\mathbb{Z}/p\mathbb{Z}) \setminus \{[0]\}$

Proof: If $[a] \neq [0] \Rightarrow p \nmid a \Rightarrow \gcd(a, p) = 1$ and $[a]$ is a unit by previous

Fields

Definition Field

A field is a commutative ring $\mathbb{F}$ with an identity 1 such that

$$U(\mathbb{F}) = \mathbb{F} \setminus \{0\}$$

Example: $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/p\mathbb{Z}$; p prime are all fields.

5. Zero Divisors and Integral Domains

Zero Divisors

Definition Zero Divisors

Let R be a ring and $R \neq \{0\}$

An element $a \in R$ is a zero divisor if for some $b \in R \setminus \{0\}$, $b \neq 0$

$$ab = 0 \quad \text{or} \quad ba = 0$$

Set of zero divisors

$$ZD = \{\text{zero divisors of } R\}$$

Remark: 0 is a 0 divisor $\Longrightarrow 0 \in ZD(R)$

Examples:

1) $R = \mathbb{Z} \Longrightarrow ZD(\mathbb{Z}) = \{0\}$

2) Consider $R = M_2(\mathbb{C})$. Take

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

$$AB = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \Longrightarrow A, B \in ZD(R)$$

Non-Zero Divisors

Definition Non-Zero Divisors

$a \in R$ is a non-zero divisor if $\forall b \in R \setminus \{0\}$, we have

$$ab \neq 0 \quad \text{and} \quad ba \neq 0$$

Set of non-zero divisors

$$NZD = \{\text{non-zero divisors of } R\}$$

So if $a \in NZD(R)$ then

$$ab = 0 \Longrightarrow b = 0 \quad \forall a \in R \quad ; \quad ba = 0 \Longrightarrow b = 0 \quad \forall a \in R$$

Integral Domains

Definition Integral Domains

An integral domain is a commutative ring with identity $1 \in R$ s.t

$$ZD = \{0\}$$

that is has NO non-trivial non-zero. Equivalently

$$NZD(R) = R \setminus \{0\}$$

Example

$R = \mathbb{Z}$, $ZD(R) = \{0\} \Longrightarrow$ Integral Domain

Remark: For any ring R, the condition $ZD(R) = \{0\}$ is equivalent to either of

i) $\forall a, b \in R \setminus \{0\}$, we have $ab \neq 0$

ii) $\forall a, b \in R$, the equality $ab = 0 \Longrightarrow a = 0$ or $b = 0$

Observe and compare

R is a field if $R \neq \{0\}$		R is an ID if
1) R is a commutative ring		1) R is a commutative ring
2) R has identity 1		2) R has identity 1
3) $U(R) = R \setminus \{0\}$	$\Longrightarrow$	3) $ZD(R) = \{0\}$

Lemma

(a) If R is a ring with an identity 1, then $U(R) \subseteq NZD(R)$

(b) Any field is an integral domain

Proof:

(a) Take any $a \in U(R)$. Suppose that

$ab = 0$ for some $b \in R$. $\quad a \in U(R) \Longrightarrow a \neq 0$

Then $b = 1b = (a^{-1}a)b = a^{-1}(ab) = a^{-1}0 \Longrightarrow b = 0$

Similarly $ba = 0 \Longrightarrow b = 0$

$$\Longrightarrow a \notin ZD(R) \Longrightarrow a \in NZD(R)$$

(b) Let R be a field. Then, properties 1,2 for a field $\Longrightarrow$ 1,2 for an ID

R a field $\Longrightarrow$ R is a commutative ring with an identity

By part (a), $U(R) \subseteq NZD(R)$

Now $$R\setminus\{0\} \underset{\substack{\uparrow \\ \text{by defn of field}}}{=} U(R) \subseteq NZD(R) \subseteq R\setminus\{0\} \; ;$$

Observe ▶ $0 \in ZD(R) \Longrightarrow 0 \notin ZD(R)$

▶ $a \in R\setminus\{0\} \Longrightarrow a \in U(R)$ field

$\Longrightarrow a \in NZD(R)$

Therefore $NZD(R) = R\setminus\{0\} \Longrightarrow R$ is an integrable domain. ■

Example of Integral Domains

1) For $R = \mathbb{Z}$; $U(\mathbb{Z}) = \{1, -1\}$

$NZD(\mathbb{Z}) = \mathbb{Z}\setminus\{0\}$

Hence $U(\mathbb{Z}) \subseteq NZD(\mathbb{Z})$, but $U(\mathbb{Z}) \neq NZD(R) = \mathbb{Z}\setminus\{0\}$

Thus $\mathbb{Z}$ is an ID

$\mathbb{Z}$ is not a field

2) In $M_2(\mathbb{R})$, the matrix $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ is a 0 divisor because

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

3) In $\mathbb{Z}/n\mathbb{Z}$, we have $ZD(\mathbb{Z}/n\mathbb{Z}) = \{0\} \cup \{[a] : a \in \mathbb{Z},\ a \neq 0,\ \gcd(a,n) > 1\}$

Indeed if $\gcd(a,n) = d > 1$, then

$$\left[\frac{n}{d}\right] \neq [0]$$

$$[a]\left[\frac{n}{d}\right] = \left[a\,\frac{n}{d}\right] = \left[\frac{a}{d}\right][n] = [0]$$

Conversely if $\gcd(a,n) = 1 \Rightarrow [a]$ is a unit

$\Longrightarrow [a]$ is not a zero divisor as

$U(R) \subseteq NZD(R)$

Cancellation Property

Theorem Cancellation Property

Let R be any ring, let $a \in R$ be a non-zero divisor, i.e. $a \in N2D(R)$.

Then $\forall\, b, c \in R$, we have

$$\text{i) } ab = ac \implies b = c$$

$$\text{ii) } ba = ca \implies b = c$$

Proof:

i) $ab = ac \implies a(b-c) = 0$

$\implies b - c = 0$ since $a \in N2D(R)$, $a \neq 0$

$\implies b = c$

ii) Dual Argument

■

Proposition

Let R be a finite ring with an identity 1. Then

$$U(R) = N2D(R)$$

Proof: Due to previous Lemma, $U(R) \subseteq N2D(R)$. Lets prove the opposite inclusion

Let $R \setminus \{0\} = \{a_1, a_2, \dots, a_n\}$ for some $n \in \mathbb{N}$ and $1 \in R \setminus \{0\}$

Fix $a_i \in N2D(R)$. Then $a_i a_j \neq 0$ for $j = 1, \dots, n$. So

$$\{a_i a_j : j = 1, \dots, n\} \subseteq R \setminus \{0\}$$

If $a_i a_j = a_i a_k \implies a_j = a_k$ by cancellation property.

$\implies j = k$

Thus

$$|\{a_i a_j : j = 1, \dots, n\}| = n \text{ and } |R \setminus \{0\}| = n$$

Therefore

$$\{a_i a_j : j = 1, \dots, n\} = R \setminus \{0\}$$

But $1 \in R \setminus \{0\} = \{a_i a_j : j = 1, \dots, n\} \implies \exists\, a_\ell$ s.t $a_i a_\ell = 1$

Similarly considering opposite order

Similarly for fixed a_i, consider $\{a_k a_i : 1, \cdots, n\}$ and a particular k s.t $a_k a_i = 1$

Now

$$a_\ell = 1a_\ell = (a_k a_i)a_\ell = a_k(a_i a_\ell) = a_k 1 = a_k$$

Hence $a_i \in U(R)$ ■

Corollary

Let R be a finite integral domain. Then, R is a field.

Proof:

The ring is an integral domain $\Longrightarrow$ R is commutative

Also $1 \in R$ and $ZD(R) = \{0\}$. By the above proposition

$$U(R) = NZD(R) = R \setminus \{0\}$$

$\Longrightarrow$ R is a field ■

Wedderburn Theorem

Theorem Wedderburn Theorem

Let R be a finite ring with an identity 1 such that

$$ZD(R) = \{0\}.$$

Then R is a field

Jacobson Theorem

Theorem Jacobson Theorem

Let R be a ring such that $\forall a \in R$, $\exists\, n = n(a) > 1$ such that

$$a^n = a.$$

Then R is commutative

Example: Suppose that

$$a^2 = a \quad \forall a \in R$$

Then R is commutative.

Indeed $\forall a, b \in R$; $(a+b) = (a+b)^2 = (a+b)(a+b) = a^2 + ab + ba + b^2 = a+b$

$$\Longrightarrow ab + ba = 0$$

Also $(-a) = (-a)^2 = (-a)(-a) = a^2 = a \Longrightarrow (-a) = a \ \forall a \in R$

Hence $ab + ba = 0 \Longrightarrow ab - ba = 0$

$$\Longrightarrow ab = ba$$

Finite Rings with $ZD = \{0\}$

Theorem

Let R be any ring with $|R| > 1$.

Suppose that $ZD(R) = \{0\}$. Prove that R is a ring with identity

Proof:

Suppose R is a ring with $ZD = \{0\}$.

Let $R \setminus \{0\} = \{a_1, \cdots, a_n\}$ for some $n \in \mathbb{N}$,

$\Longrightarrow a_i \in NZD(R)$

$\Longrightarrow a_i a_l \neq 0$ for $l = 1, \cdots, n$

$\{a_i a_l : l = 1, \cdots, n\} = R \setminus \{0\}$

$\Longrightarrow a_i a_j = a_i$ for some j

$\Longrightarrow \cancel{a_i} a_j a_k = \cancel{a_i} a_k$ since $a_i \in NZD$, cancellation property

$\Longrightarrow a_j a_k = a_k$ for any k

Similarly for $k = j$

$a_j a_j = a_j \Longrightarrow a_k a_j \cancel{a_j} = a_k \cancel{a_j}$

$\Longrightarrow a_k a_j = a_k$

$\Longrightarrow a_j$ identity

■

Units are NOT zero divisors

Theorem

Let R be any ring, then,

$$U(R) \cap ZD(R) = \phi$$

Proof: (by contradiction):

Suppose $\exists\, a \in R$ s.t $a \in U(R)$ and $a \in ZD(R)$

If $a \in ZD(R) \Longrightarrow \exists\, b \in R \setminus \{0\}$ s.t

$$ab = 0 \quad \text{or} \quad ba = 0$$

1) $ab = 0 \Longrightarrow b = (a^{-1}a)\, b = a^{-1}(ab) = a^{-1} 0 = 0$

$\Longrightarrow b = 0$ $\not\#$

2) Similar

Hence empty intersection $\blacksquare$

6. Ideals of a Ring

Definition of Ideals

Definition Ideals of a ring

Let R be any ring and $I \subseteq R$ be any subset

The subset I is an **ideal** if

i) $0 \in I$

ii) $a \in I \implies -a \in I$

iii) $a, b \in I \implies a+b \in I$

iv) $a \in I,\ r \in R \implies ar,\ ra \in I$

Note:

- ▶ $\forall$ rings R, ideal $\implies$ subrings
- ▶ Converse **NOT** always true. In general

  subring $\not\Longrightarrow$ ideal

Examples of ideals

(1) $R = \mathbb{Z}$, take any $n \in \mathbb{N} \subseteq \mathbb{Z}$, put

$I = n\mathbb{Z} = \{nz \mid z \in \mathbb{Z}\}$. This is an ideal

proof:

i) $0 \in I$ by $z=0$

ii) take any $\underset{a}{\underset{\shortparallel}{nz}} \in I \implies n(-z) = \underset{-a}{\underset{\shortparallel}{-nz}} \in I$

iii) take $a = nz$, $b = nw$ for $z, w \in \mathbb{Z}$

$a+b = nz + nw = n(z+w) \in I$

iv) $\left.\begin{matrix} a = nz \\ r = w \end{matrix}\right\} \implies ar = (nz)w = n(zw) \in I$

and $ar = ra \in I$

■

(2) Take any $R=\mathbb{Q} \supset S = \mathbb{Z}$ is a subring

We know that $\mathbb{Z}$ is a ring itself

$\Longrightarrow$ S is a subring

But S is not an ideal of $\mathbb{Q}$

proof: counterexample:

Property (iv) does not hold

$a=2,\ r=\frac{2}{3} \in \mathbb{Q} \Longrightarrow ar = \frac{4}{3} \notin \mathbb{Z}$ $\blacksquare$

(3) General example: Trivial Ideals

$\forall R$ a ring

- $I=\{0\}$ is an ideal as

  i) $0+0=0$,

  ii) $-0=0\in\{0\}$

  iv) $0\times r = 0 \in \{0\}$ $\forall r\in R$

- $I=R$ is also an ideal

Theorem

(a) Suppose $R\neq\{0\}$ has an identity $1\neq 0$.

If $I\subseteq R$ is an ideal and $1\in I$, then

$$I=R$$

(b) Suppose that R has identity 1. Also suppose that $\forall a\in R\setminus\{0\}, \exists b\in R$ s.t either

$$ab=1 \quad \text{or} \quad ab=1$$

Then $\{0\}$ and R are the only ideals of R

(c) If R is a field, then $\{0\}\subseteq R$ and R are the only ideals of R

Proof:

(a) Suppose $1\in I$ and $I\subseteq R$ be an ideal. By defn of ideal

$\forall a\in R,\ \forall a\in I$, we have $ra\in I$.

In particular this holds for $a=1 \Longrightarrow ra=r$

$$\Rightarrow r \in I \quad \forall r \in R$$

$$\Rightarrow R \leq I$$

$$\Rightarrow R = I$$

(b) Take any ideal $I \leq R$. If $I = \{0\}$, nothing to prove.

Suppose $I \neq \{0\}$ and $0 \in I \Rightarrow \exists\, a \in R \setminus \{0\}$ such that $a \in I$

By hypothesis, $\exists\, b \in R$ such that

$$ba = 1 \text{ or } ba = 1 \Rightarrow 1 \in I \quad \text{by defn of ideal}$$

$$\Rightarrow I = R \quad \text{by (a)}$$

(c) In a field R, $\forall a \in R \setminus \{0\}$, $\exists\, a^{-1}$ so (b) $\Rightarrow$ (c)

■

Kernels and Images

Definition Kernel / Image

Let $\alpha : R \longrightarrow S$ be any ring homomorphism $\forall R, S$ rings

The kernel of R: $\ker \alpha = \{ r \in R \mid \alpha(r) = 0 \}$

The image of R: $\operatorname{Im} \alpha = \{ s \in S \mid s = \alpha(r) \text{ for some } r \in R \}$

Another way of writing image is

$$\operatorname{Im} \alpha = \{ \alpha(r) \in S \mid r \in R \}$$

Lemma

Let $\alpha : R \longrightarrow S$ be any ring homomorphism. Then

(a) $\operatorname{Im} \alpha \leq S$ is a subring (not always an ideal)

(b) $\ker \alpha \trianglelefteq R$ is an ideal

Proof:

(a) $\alpha : R \longrightarrow S$ is a ring homomorphism

In particular, this is a group homomorphism w.r.t '+' operation

$$\alpha : (R, +) \longrightarrow (S, +)$$

So $\operatorname{Im} \alpha \leq S$ is an additive subgroup

Hence by properties of homomorphisms from group theory

i) $\alpha(0) = 0 \Longrightarrow 0 \in \operatorname{Im}\alpha$

ii) If $a, b \in \operatorname{Im}\alpha$, then $\exists\, x, y \in R$ such that

$$a = \alpha(x) \quad b = \alpha(y)$$

By group theory

$$-a = -\alpha(x) = \alpha(-x) \in \operatorname{Im}\alpha$$

Finally

$$a+b = \alpha(x) + \alpha(y) = \alpha(x+y) \quad \text{and} \quad ab = \alpha(x)\alpha(y) = \alpha(xy)$$

Hence $-a, a+b, ab \in \operatorname{Im}\alpha$

Therefore $\operatorname{Im}\alpha$ is a subring.

(b) Need to show that $\ker\alpha \subseteq R$ is an ideal.

i) $0 \in R$, $\alpha(0_R) = 0_S$ by Group Theory $\Longrightarrow 0 \in \ker\alpha$

ii) $\forall\, a \in \ker\alpha$

$$\alpha(-a) = -\alpha(a) = -0 = 0 \Longrightarrow -a \in \ker\alpha$$

iii) $a, b \in \ker\alpha \Longrightarrow \alpha(a) = \alpha(b) = 0$

$$\alpha(a+b) = \alpha(a) + \alpha(b) = 0 + 0 = 0 \Longrightarrow a+b \in \ker\alpha$$

iv) $\forall\, \alpha \in \ker\alpha$, $\forall\, r \in R$

$$\alpha(ar) = \alpha(a)\alpha(r) = 0\alpha(r) = 0 \Longrightarrow ar \in \ker\alpha$$

$$\alpha(ra) = \alpha(r)\alpha(a) = \alpha(r)0 = 0 \Longrightarrow ra \in \ker\alpha$$

Hence $-a, a+b, ra, ar \in \ker\alpha \Longrightarrow \ker\alpha$ is an ideal $\blacksquare$

Proposition

Let $\alpha : R \longrightarrow S$ be any ring homomorphism.

Then α is one-to-one $\iff$ $\ker\alpha = \{0\}$

Proof:

$(\Longrightarrow)$: Suppose α is one-to-one.

$\alpha(0_R) = 0_S \implies 0 \in \ker\alpha$

If $r \in \ker\alpha \implies \alpha(r) = 0 = \alpha(0)$

$\implies r = 0 \quad \forall r \in R$ since α is 1-1

Hence $\ker\alpha = \{0\}$

$(\Longleftarrow)$: Suppose that $\ker\alpha = \{0\}$. Then $\forall u, v \in R$

$$\alpha(u) = \alpha(v) \iff \alpha(u-v) = 0$$
$$\iff u-v \in \ker\alpha$$
$$\iff u = v \qquad \blacksquare$$

Corollary

Let R be a field, S be any ring and $\alpha : R \longrightarrow S$ be any ring homomorphism. Then either

$\mathrm{Im}\,\alpha = \{0\}$ or α is one-to-one

More generally, the same property of α holds if we replace the hypothesis that R is a field by a weaker property that

$1 \in R$ and $\forall a \in R \setminus \{0\}$, $\exists\, b \in R$ such that $ab = ba = 1$

Proof:

By part (b) of the Lemma on pg 26, $\ker\alpha$ is an ideal.

By part (b) of the Theorem on pg 25, $\ker\alpha = \{0\}$ or $\ker\alpha = R$

Case 1: $\ker\alpha = \{0\} \implies \alpha$ is one-to-one

Case 2: $\ker\alpha = R \implies \alpha$ maps all elements of R to 0

$\implies \forall r \in R, \alpha(r) = 0$

$\implies \mathrm{Im}\,\alpha = \{0\} \qquad \blacksquare$

7. Examples of Ideals

(1) For any ring R, the identity

$$i : R \longrightarrow R$$

is a ring isomorphism (seen above)

Proposition

Zero function $\omega : R \rightarrow R$;

$$a \mapsto 0$$

is a ring homomorphism

proof:

$$\alpha(ab) = 0 = 0 \times 0 = \alpha(a) \times \alpha(b)$$

$$\alpha(a+b) = 0 = 0 + 0 = \alpha(a) + \alpha(b) \qquad \blacksquare$$

Hence

$$\ker i = \{a \in R : i(a) = 0\} = \{a \in R : a = 0\} = \{0\}$$

$$\ker \omega = \{a \in R : \omega(a) = 0\} = R$$

are ideals of R

(2) Let

$$T_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, b, c \in \mathbb{R} \right\}$$

$T_2(\mathbb{R}) \leq M_2(\mathbb{R})$ is a subring

Define $\alpha : T_2(\mathbb{R}) \longrightarrow \mathbb{R}$

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

This is a ring homomorphism since

$$\alpha\left(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} + \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix} \right) = \alpha \begin{pmatrix} a+a' & b+b' \\ 0 & c+c' \end{pmatrix} = a + a' = \alpha \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} + \alpha \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix}$$

$$\alpha\left(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix} \right) = \alpha \begin{pmatrix} aa' & ab' + bc' \\ 0 & cc' \end{pmatrix} = aa' = \alpha \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \alpha \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix}$$

Here

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in \ker\alpha \iff \alpha\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = 0$$

$$\iff a = 0$$

Therefore

$$\ker\alpha = \left\{ \begin{pmatrix} 0 & b \\ 0 & c \end{pmatrix} : b, c \in \mathbb{R} \right\}$$

and $\ker\alpha$ is an ideal

Proposition

Let R be any ring, $I, J \leq R$ be any ideal

$I \cap J$ is an ideal of R

Proof:

i) $0 \in I$ and $0 \in J \implies 0 \in I \cap J$

ii) $a \in I \cap J \implies a \in I$ and $a \in J$

$\implies -a \in I$ and $-a \in J$

$\implies -a \in I \cap J$

iii) $a, b \in I \cap J \implies a, b \in I$ and $a, b \in J$

$\implies a+b \in I$ and $a+b \in J$

$\implies a+b \in I \cap J$

iv) $r \in R$, $a \in I \cap J \implies r \in R$, $a \in I$ and $a \in J$

$\implies ra, ar \in I$ and $ar, ra \in J$

$\implies ra, ar \in I \cap J$

■

Sum of Ideals

Let R be any ring and $I, J \leq R$ be any 2 ideals.

Define

$$\boxed{I + J = \{a + b : a \in I, b \in J\}}$$ Sum of ideals

Lemma

(a) $I+J$ is an ideal of R

(b) The union $I \cup J \subseteq I+J$

(c) The sum $I+J$ is the smallest ideal of R containing $I \cup J$

Proof:

(a) i) $0 = \underset{\underset{I}{\cap}}{0} + \underset{\underset{J}{\cap}}{0} \in I+J$

ii) $\forall a \in I$ and $s \in J$

$$-(a+s) = \underset{\underset{I}{\cap}}{(-a)} + \underset{\underset{J}{\cap}}{(-s)} \in I+J$$

iii) $\underset{\underset{I+J}{\cap}}{(a+b)} + \underset{\underset{I+J}{\cap}}{(c+d)} = \underset{\underset{I}{\cap}}{(a+c)} + \underset{\underset{J}{\cap}}{(b+d)} \in I+J$ + is Abelian

iv) $\underset{\underset{I}{\cap}}{(a+b)}\underset{\underset{J}{\cap}}{(c+d)} = (ac+bc)+(ad+bd) \in I+J$

Observe that $a \in I$ and $c \in I \Longrightarrow ac \in I$
$c \in I$ and $b \in R \Longrightarrow bc \in I$ $\Bigg\} \Longrightarrow ac+bc \in I$

Similarly $b \in J$ and $d \in J \Longrightarrow bd \in J$
$d \in I$ and $a \in R \Longrightarrow ad \in J$ $\Bigg\} \Longrightarrow ad+bc \in J$

Hence $(ac+bc)+(ad+bd) \in I+J \Longrightarrow I+J$ is a subring

More generally for $a \in I$, $b \in J$, $r \in R$

$$(a+b) \times r = \underset{\underset{I}{\cap}}{ar} + \underset{\underset{J}{\cap}}{br} \in I+J$$

$$r \times (a+b) = \underset{\underset{I}{\cap}}{ra} + \underset{\underset{J}{\cap}}{rb} \in I+J$$

$\Longrightarrow I+J$ is an ideal of R.

(b) Suppose $a \in I \implies a = a + 0 \in I + J$

$\implies I \subseteq I + J$ (*)

Suppose $b \in I \implies b = 0 + b \in I + J$

$\implies J \subseteq I + J$ (*)

From (*) $I \cup J \subseteq I + J$

(c) We need to show if $K \leq R$ is any ideal of R containing $I \cup J$, then K also contains $I+J$

Take any ideal $K \leq R$ such that $I \cup J \subseteq K$.

Need to show that $I + J \subseteq K$

$I, J \subseteq K \implies \forall a \in A,\ b \in J,\ a, b \in K$

$\implies a + b \in K$

Hence $I + J \subseteq K$ ■

Example of a sum

$R = \mathbb{Z}$, then $I = 4\mathbb{Z}$, $J = 10\mathbb{Z}$. Then

$I + J \leq \mathbb{Z}$ is an ideal

Claim: $4\mathbb{Z} + 10\mathbb{Z} = 2\mathbb{Z}$

proof:

$(\subseteq)$: Suppose $x \in 4\mathbb{Z} + 10\mathbb{Z} \implies x = 4z + 10w = 2(2u + 5v)$

$\implies x \in 2\mathbb{Z}$

$(\supseteq)$: Suppose $y \in 2\mathbb{Z}$

$\forall y \in 2\mathbb{Z}$, $y = 2z$ for some $z \in \mathbb{Z}$. Observe $2 = -8 + 10$

$$y = 2z = (-8+10)z = (-8)z + 10z$$

$$= (4(-2)) + 10z \in 4\mathbb{Z} + 10\mathbb{Z}$$ ■

More generally for any $m, n \in \mathbb{N}$

$$m\mathbb{Z} + n\mathbb{Z} = \gcd(m,n)\mathbb{Z}$$

proof:

$(\subseteq)$: Suppose $z \in m\mathbb{Z} + n\mathbb{Z} \implies z = am + nb$, $a, b \in \mathbb{Z}$

Let $d=\gcd(m,n)$

$d|m$ and $d|n \Rightarrow m=d\ell$ and $n=dk$ for some $k,\ell\in\mathbb{Z}$

$\Rightarrow z=a(d\ell)+b(dk)$

$\Rightarrow z=d(a\ell+bK)$

$\Rightarrow d|z$

$\Rightarrow z\in d\mathbb{Z}$

$(\supseteq)$: Suppose $z=d\mathbb{Z} \Rightarrow d|z$

$\Rightarrow z=dk$ for some $k\in\mathbb{Z}$

$\gcd(m,n)=d \Rightarrow \exists\, s,t\in\mathbb{Z}$ s.t

$d=ms+nt$

$z=(ms+nt)k = m(ks)+n(tk)\in m\mathbb{Z}+n\mathbb{Z}$

$\Rightarrow a\mathbb{Z}+b\mathbb{Z}=d\mathbb{Z}$

$\blacksquare$

More generally, for any $m,n\in\mathbb{Z}$,

$$m\mathbb{Z}\cap n\mathbb{Z}=\mathrm{lcm}(m,n)\mathbb{Z}$$

proof:

$z\in m\mathbb{Z}\cap n\mathbb{Z} \Leftrightarrow z\in m\mathbb{Z}$ and $z\in n\mathbb{Z}$

$\Leftrightarrow m|z$ and $n|z$

$\Leftrightarrow \mathrm{lcm}(m,n)|z$

$\Leftrightarrow z\in \mathrm{lcm}(m,n)\mathbb{Z}$

$\blacksquare$

8. Factor Rings

Reminder of Cosets

Let $(G,+)$ be any Abelian group, $H \leq G$ subgroup.

Definition Coset

$(G,+)$ be any Abelian group, $H \leq G$ subgroup. Then

$$\forall a \in G, \quad a+H = \{a+x \mid x \in H\} \leq G$$

is a coset of a relative to H.

In

$$\underset{\substack{\uparrow \\ \text{representative}}}{a}+H$$

Properties of Cosets

Lemma

(i) $a+H = b+H \iff a-b \in H$

(ii) $a+H = b+H \iff (a+H) \cap (b+H) \neq \emptyset$

(iii) $a+H = H = 0+H \iff a \in H$

Proposition

$H \leq G$ and $(G,+)$ Abelian $\implies H \trianglelefteq G$ normal

Proof:

$$\forall h \in H, \quad h = hgg^{-1} = ghg^{-1} \quad \forall g \in G$$

■

Factor Group

Definition Factor Group

Let $(G,+)$ be any Abelian group, $H \leq G$ subgroup.

$$G/_H = \{a+H : a \in G\} = \{\text{set of all cosets in } G \text{ relative to } H\}$$

Factor/Quotient group

Factor Rings

Now let R be any ring $\Longrightarrow$ $(R,+)$ is an Abelian group.

Let $I \subseteq R$ be any ideal of R. Then

$I \subseteq R$ is a subgroup relative to $+$ $\Longrightarrow$ we have R/I

Consider factor set R/I with binary operation

- Addition: $(a+I)+(b+I) = (a+b)+I$
- Multiplication: $(a+I)\times(b+I) = (a\times b)+I$

Proposition

The binary operations $+, \times$

$+: (a+I)+(b+I) = (a+b)+I$

$\times: (a+I)\times(b+I) = (a\times b)+I$

are well-defined

Proof:

By Group Theory, the set R/I is an Abelian group under $+$

In particular, $+_{R/I}$ is well-defined

Showing via explicit calculation:

Suppose $a+I = a'+I$ and $b+I = b'+I$ for some $a, a', b, b' \in R$

$\Longrightarrow$ $a-a' \in I$ and $b'-b \in I$

Hence

$(a-a') + (b-b') \in I$ and $ab - a'b' = (a-a')b + a'(b-b') \in I$

$\Longrightarrow$ $(a+b)-(a'+b') \in I$ and $ab-a'b' \in I$

$\Longrightarrow$ $(a+b)+I = (a'+b')+I$ and $(ab)+I = (a'b')+I$

Therefore

$$\begin{aligned} \underline{+}: (a+I)+(b+I) &= (a+b)+I \\ &= (a'+b')+I \\ &= (a'+I)+(b'+I) \end{aligned}$$

$$\begin{aligned}\underline{\times}:\ (a+I)\times(b+I) &= (ab)+I \\ &= (a'b')+I \\ &= (a'+I)\times(b'+I)\end{aligned}$$

■

Proposition

$(R/I, +, \times)$ is a ring with $+, \times$ defined above

Proof: By Group Theory, the set R/I is an Abelian group.

Associativity: For any 3 cosets $a+I$, $b+I$, $c+I \in R/I$

$$\begin{aligned}((a+I)\times(b+I))\times(c+I) &= (ab+I)\times(c\times I) \\ &= (ab)c+I \\ &= a(bc)+I \\ &= (a+I)\times(bc\times I) \\ &= (a+I)\times((b+I)\times(c+I))\end{aligned}$$

Distributivity:

i) $$\begin{aligned}(a+I)\times((b+I)+(c+I)) &= (a+I)\times((b+c)\times I) \\ &= a(b+c)\times I \\ &= (ab+ac)\times I \\ &= (ab+I)+(ac+I) \\ &= (a+I)\times(b+I)+(a+I)\times(c\times I)\end{aligned}$$

ii) Similar

By Group Theory, $(R/I, +)$ is an Abelian group.

Has identity $I = 0+I$

inverse: $-(a+I) = (-a+I)$

Abelian as

$$(a+I)+(b+I) = (a+b)+I = (b+a)+I = (b+a)+(a+I)$$

■

Examples

1) Let $R=\mathbb{Z}$ and $\forall n\in\mathbb{N}$, we have ideal

$$I=n\mathbb{Z}\leq\mathbb{Z}.$$

For any $a,b\in\mathbb{Z}$, we have

$$a+I=b+I \iff a-b\in n\mathbb{Z} \iff n\mid(a-b) \iff a\equiv b \bmod n$$

Hence in quotient ring $\mathbb{Z}/I$, we have

$$a+I=[a]$$

and

$$R/_{I}=\mathbb{Z}/_{n\mathbb{Z}}=\{[0],[1],\dots,[n-1]\}=\mathbb{Z}_n$$

$+$ and $\times$ are usual modulo n rules

Fundamental Theorem of Homomorphisms for Rings

Theorem

Let R,S be any rings and $\alpha:R\longrightarrow S$ be a homomorphism

Then $\ker\alpha\leq R$ an ideal of R and $\mathrm{Im}\,\alpha\leq S$ is a subring of S and

$$R/_{\ker\alpha}\cong\mathrm{Im}\,\alpha$$

<u>Proof:</u> Let $I=\ker\alpha$

Define

$$\bar{\alpha}:R/_{\ker\alpha}\longrightarrow\mathrm{Im}\,\alpha \quad \text{by}$$

$$\bar{\alpha}(a+I)=\alpha(a) \qquad \forall a\in R$$

show that $\bar{\alpha}$ is bijective and a ring homomorphism

<u>Well-defined</u>: Take $a,b\in I$ such that

$$\begin{aligned} a+I=b+I &\iff a-b\in I=\ker\alpha \\ &\iff \alpha(a-b)=0 \\ &\iff \alpha(a)-\alpha(b)=0 \\ &\iff \alpha(a)=\alpha(b) \end{aligned}$$

$$\iff \bar{\alpha}(a+I) = \bar{\alpha}(b+I)$$

onto: $\forall\, u \in \mathrm{Im}\,\alpha$, take any $u = \alpha(a)$ for some $a \in R$ and

$$\alpha(a+I) = \alpha(a) = u$$

1-1:
$$\begin{aligned} \bar{\alpha}(a+I) = \bar{\alpha}(b+I) &\implies \alpha(a) = \alpha(b) \\ &\implies \alpha(a) - \alpha(b) = 0 \\ &\implies \alpha(a-b) = 0 \\ &\implies a-b \in I = \ker\alpha \\ &\implies a+I = b+I \end{aligned}$$

homomorphism: let $a+I,\ b+I \in R/_I$. Then

$$\begin{aligned} \bar{\alpha}((a+I)+(b+I)) &= \bar{\alpha}((a+b)+I) \\ &= \alpha(a+b) \\ &= \alpha(a) + \alpha(b) \\ &= \bar{\alpha}(a+I) + \bar{\alpha}(b+I) \end{aligned}$$

$$\begin{aligned} \bar{\alpha}((a+I)\times(b+I)) &= \bar{\alpha}((a\times b)+I) \\ &= \alpha(a\times b) \\ &= \alpha(a)\times\alpha(b) \\ &= \bar{\alpha}(a+I)\times\bar{\alpha}(b+I) \end{aligned}$$

$\blacksquare$

9. Examples of Factor Rings

(1) Canonical Homomorphism

Let I be an ideal of R

$$\pi : R \longrightarrow R/I ;$$
$$a \longmapsto a+I$$

Lemma

π is an onto homomorphism with $\operatorname{Ker}\pi = I$

Proof:

homomorphism: $\forall\, a, b \in R$

$$\pi(a+b) = (a+b)+I = (a+I)+(b+I) = \pi(a) + \pi(b)$$
$$\pi(a\times b) = (a\times b)+I = (a+I)\times(b+I) = \pi(a) \times \pi(b)$$

onto: $\forall\, a+I \in R/I,\ \exists\, a \in R$ s.t $\pi(a) = a+I$ ■

Note: 0 element of R/I is $0+I = I$

$$a \in \operatorname{Ker}\pi \iff \pi(a) = I \iff a+I = I$$
$$\iff a \in I$$

Therefore $\operatorname{Ker}\pi = I$

(2) Direct Product Ring

Definition Cartesian Product

Let R, S be rings. Define

$$R\times S = \{(r,s) : r\in R,\ s\in S\}$$

Define addition and multiplication

addition: $(r,s) + (r', s') = (r+r', s+s') \in R\times S$

multiplication: $(r,s) \times (r',s') = (rr', ss')$

Proposition

Let R and S be rings. Then

$(R \times S, +, \times)$ is a ring with addition and multiplication defined above

Claim: $I \subseteq R \times S$; $I = \{(0,s)$ is an ideal$\}$

i) $(0,0) \in I$

ii) $(0,s) + (0,s') = (0, s+s') \in I$

iii) $(0,s) \times (a,b) = (0, sb) \in I$

Claim: $R \times S/_{I} \cong R$

Define map

$$\alpha : R \times S \longrightarrow R$$
$$(r,s) \longmapsto r$$

homomorphism: $\alpha((r,s)(r',s')) = \alpha((rr', ss'))$

$$= rr'$$
$$= \alpha((r,s))\alpha((r',s'))$$

onto: $\forall r \in R, \exists\, (r,0) \in R \times S$ s.t

$$\alpha((r,0)) = r$$

$$(r,s) \in \operatorname{Ker}\alpha \iff \alpha((r,s)) = 0$$
$$\iff r = 0$$
$$\iff (r,s) = (0,s)$$

Caution: Let R be any ring and $I \leq R$, be any ideal.

In general, it is not true then

$$\left(R/_{I}\right) \times I \not\cong R$$

Example: $R = \mathbb{Z}$, $I = 2\mathbb{Z}$

$$R/I = \mathbb{Z}/2\mathbb{Z} = \mathbb{Z}_2 = \{[0],[1]\}$$

Then $(\mathbb{Z}_2 \times \mathbb{Z}) \not\cong \mathbb{Z}$

Suppose $a \in (\mathbb{Z}_2 \times 2\mathbb{Z})$, $a \neq 0$

Observe

$$([1],0) \in \mathbb{Z}_2 \times 2\mathbb{Z} \Longrightarrow ([1],0) + ([1],0) = ([0],0)$$

Therefore $a + a = 0$

if $\exists$ an isomorphism, $\alpha : \mathbb{Z}_2 \times 2\mathbb{Z} \longrightarrow \mathbb{Z}$

$$\alpha(a) \in \mathbb{Z} , \alpha(a) \neq 0$$

$$\alpha(a+a) = \alpha(a) + \alpha(a) = 0 \quad ※$$

(3) Let

$$T_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a,b,c \in \mathbb{R} \right\}$$

10. Binomial Theorem

Let R be any ring. Then in general $\mathbb{Z} \subseteq R$

In particular for $z \in \mathbb{Z}$ and $r \in R$, we do not know (yet) what is $z \cdot r$

$r \in R$, $2r = r + r$

We can still define $z \cdot r$ $\forall z \in \mathbb{Z}$ $\forall r \in R$ "by hand"

Case 1: $\forall r \in R$, if $z = 0$, $0 \cdot r = 0 \in R$

Case 2: $z \in \mathbb{Z}_{>0}$, $zr = r + r + \cdots + r := zr$

Case 3: $z \in \mathbb{Z}_{<0}$, $(-z) > 0 \underset{\text{case 2}}{\Longrightarrow} (-z)r \in R$

$$-z(r) = z(-a) = (-a) + \cdots + (-a) = -(za)$$

$$zr = -(-zr)$$

Example: $-2r = -r - r = (-2)r = (-2r)$

Proposition

For any $z, w \in \mathbb{Z}$ and $a, b \in R$

i) $(z+w)a = za + wa$

ii) $(zw)a = z(wa)$

iii) $z(a+b) = za + zb$

iv) $(za)(wb) = (zw)(ab)$

Proof:

By direct verification using new multiplication rule

$$\times : \mathbb{Z} \times R \longrightarrow R$$

$$\times : (z, a) \longmapsto za$$

iii) 1) $z = 0$, $0(a+b) = 0 = 0a + 0b = 0 + 0 = 0 \in R$

2) $z \in \mathbb{Z}_{>0}$ $z(a+b) = (a+b) + \cdots + (a+b)$

$$= \underbrace{a + \cdots + a}_{z} + \underbrace{b + \cdots + b}_{z} \qquad \text{Abelian}$$

$$= za + zb$$

3) $z \in \mathbb{Z}_{<0}$: By the fact that $-(u+v) = (-u)+(-v)$ in an Abelian group

$$z(a+b) = -((-z)(a+b)) = -(-(za)+(-(zb))) = za+zb$$

$$z(a+b) = -(\underbrace{(a+b)+\cdots+(a+b)}_{-z \text{ times}})$$

$$= -\underbrace{(a+b)-\cdots\cdots-(a+b)}_{z}$$

$$\underbrace{-a-\cdots-a}_{-z} + (\underbrace{-b-\cdots\cdots-b}_{-z})$$

$$\underbrace{-(a+b)-\cdots\cdots-(a+b)}_{z}$$

$\blacksquare$

Proposition

$\forall$ ring homomorphism; $\alpha : R \longrightarrow S$

$$\alpha(za) = z\alpha(a) \qquad \forall z \in \mathbb{Z} \quad \forall a \in R$$

Proof: Proof is a consequence of Group Theory

Binomial Theorem

For any $n \in \mathbb{N}$

$$\binom{n}{k} = \frac{n!}{(n-k)!k!} \quad , \quad k = 0,1,\dots,n$$

Theorem Binomial Theorem

Let R be any commutative ring.

Let $a,b \in R$ and $n \in \mathbb{N}$. Put $a^n b^0 = a^n$ and $a^0 b^n = b^n$. Then

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$$

Proof: (By induction):

Base case: $n = 1$

$$(a+b)^1 = a+b = a^1b^0 + a^0b^1 = \binom{1}{0}a^1b^0 + \binom{1}{1}a^0b^1 = a+b$$

Inductive hypothesis: Suppose property true for $n \in \mathbb{N}$

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^{k}$$

Inductive step: Showing that $\forall n \in \mathbb{N}$, $P(n) \Longrightarrow P(n+1)$

$$(a+b)^{n+1} = (a+b)(a+b)^n = (a+b) \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^{k}$$

$$= \sum_{k=0}^{n} \binom{n}{k} a^{n+1-k} b^{k} + \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^{k+1}$$

we used equality $ab = ba$.

$$= \binom{n}{0} a^{n+1} b^{0} + \sum_{k=1}^{n} \binom{n}{k} a^{n+1-k} b^{k} + \sum_{k=0}^{n-1} \binom{n}{k} a^{n-k} b^{k+1}$$

$$+ \binom{n}{n} a^{0} b^{n+1}$$

shifting index

$$= \binom{n}{0} a^{n+1} b^{0} + \sum_{k=1}^{n} \binom{n}{k} a^{n+1-k} b^{k} + \sum_{k=1}^{n} \binom{n}{k-1} a^{n+1-k} b^{k} \quad (k+1 = k')$$

$$+ \binom{n}{n} a^{0} b^{n+1}$$

$$= \binom{n}{0} a^{n+1} b^{0} + \sum_{k=1}^{n} \left[\binom{n}{k} + \binom{n}{k-1} \right] a^{n+1-k} b^{k} + \binom{n}{n} a^{0} b^{n+1}$$

Observe $\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}$

$$\binom{n}{n} = \binom{n}{0} = \binom{n+1}{0} = \binom{n+1}{n+1} = 1$$

Hence we get

$$(a+b)^{n+1} = \binom{n+1}{0} a^{n+1} b^{0} + \sum_{k=1}^{n} \binom{n+1}{k} a^{n+1-k} b^{k} + \binom{n+1}{n+1} a^{0} b^{n+1}$$

$$\Longrightarrow (a+b)^{n+1} = \sum_{k=0}^{n+1} \binom{n+1}{k} a^{n+1-k} b^{k} \qquad \blacksquare$$

11. Characteristics of Rings and Fields

Let R be any ring with identity $1 \in R$. Then consider the subset

$$C = \{z1 : z \in \mathbb{Z}\} = \{\ldots\ldots, -(2\cdot1), -1, 0, 1, 2\cdot1, 3\cdot1, \cdots\}$$

List might have repeats. For example $R = \mathbb{Z}_2$

$$C = \{[0], [1]\}$$

If $R = \mathbb{R}$ or $\mathbb{C}$ $\implies C = \mathbb{Z}$

Proposition

Let R be any ring with identity $1 \in R$

$C \subseteq R$ is a subring

Proof:

i) $0 \in C$

$\forall\, z\cdot1, w\cdot1$ where $z, w \in \mathbb{Z}$

ii) $-(z1) = (-z)1 \in C$

iii) $z\cdot1 + w\cdot1 = (z+w)1 \in C$

iv) $(z1)(w1) = (zw)(1\cdot1) = (zw)(1) \in C$ ■

Characteristics

Definition

Let R be an integral domain. The **characteristic** of R is

$$\operatorname{char} R = \begin{cases} \operatorname{ord} 1 \text{ in } C & \text{if this order is finite} \\ 0 & \text{if } \operatorname{ord} 1 = \infty \end{cases}$$

Meaning ord 1 in C as an additive group

Examples of Characteristics

1) $R = \mathbb{Z}$; $C = \mathbb{Z}$

$$\underset{C}{\operatorname{ord}}\ 1 = \underset{R}{\operatorname{ord}}\ 1 = \infty \implies \operatorname{char} \mathbb{Z} = 0$$

Similarly $\text{char}\,\mathbb{R}=0$; $\text{char}\,\mathbb{C}=0$, $\text{char}\,\mathbb{Q}=0$

2) $R=\mathbb{Z}_2$; $\underset{[1]}{\underset{\shortparallel}{-[1]}},[0],[1],\underset{[0]}{\underset{\shortparallel}{[2]}} \implies \operatorname{ord}_{C}[1] = \operatorname{ord}_{C}[1] = \operatorname{ord}_{\mathbb{Z}_2}[1] = 2$

$\text{char}\,\mathbb{Z}_2 = 2$

Theorem

Let R be an integral domain $(1\in R)$. Then

$\text{char}\,R=0$ or $\text{char}\,R=p$, p is prime

Proof: (contradiction)

Consider $C=\{z1 : z\in\mathbb{Z}\}$ an additive group

$$\operatorname{ord}_C 1 = \begin{cases} \infty \implies \text{char } R = 0 \\ \text{some natural number} \end{cases}$$

Suppose $\operatorname{ord}_C 1 = mn$ where $m,n\in\mathbb{N}$ (not prime).

We will get a contradiction. By defn of order

$0=(mn)1=(m1)(n1) \implies m1=0$ or $n1=0$ as R is an integral domain

Case 1: $m1=0 \implies \underbrace{1\cdots\cdots1}_{m\text{ times}}=0$

By definition of order, the minimum number of times $k=mn$

$$\underbrace{1+1+\cdots\cdots+1}_{k\text{ times}}=0$$

is mn. But $\operatorname{ord}_C(1)=mn$ and $m\le n$ ⨳

But $\operatorname{ord}_C 1 = mn$ and $m\le mn \implies m=mn$

$\implies n=1$

Similarly we get $n1=0 \implies n=mn$

$\implies m=1$

This means $\operatorname{ord}_c 1$ cannot be factorized as mn unless $m=1$ or $n=1$

$\implies \operatorname{ord}_c 1$ is prime ■

Now let $z \in \mathbb{Z}$ and $b \in R$. By using $(za)(wb) = (zw)(ab)$ with $a = 1 \in R$, $w = 1 \in \mathbb{Z}$

$$(z1)b = (z1)(1b) = z(1b) = zb$$

Let $b \neq 0$, $\operatorname{char} R = 0$, then

$$zb = 0 \iff (z1)b = 0 \iff z1 = 0 \iff z = 0$$

If $\operatorname{char} R = p$, then

$$zb = 0 \iff (z1)b = 0 \iff z1 = 0 \iff p \mid z$$

Important Technique

In some mathematical proofs have this mathematical structure

We need to show $q = 0$

Typically we prove that $kq = 0$ for some $k \in \mathbb{Z}$ and $k \neq 0$

Suppose that $k = p$

$$q \in \underset{\substack{\uparrow \\ \text{field}}}{F}, \quad \operatorname{char} F = p$$

We get

$$pq = 0 \iff (p \cdot 1)q = 0$$

Personal Explanation

R be any integral domain, $1 \in R$

$(R, +)$ is an Abelian group

$$\operatorname{char} R = \begin{cases} \operatorname{ord}(1) & \\ \infty & \text{if } \operatorname{ord}(1) = \infty \end{cases}$$

$\operatorname{ord}(1)$ is the order of element $1 \in R$ as an additive group

$\operatorname{ord}(1) = n$ is the least $n \in \mathbb{N}$ s.t $n \cdot 1 = 0$

identity of group $(R, +)$
similar to $a^n = e$ $(G, *)$

$\operatorname{ord}(1) = \infty$ if $n \cdot 1 \neq 0$ $\forall n \in \mathbb{N}$

12. Rings of Polynomials

Let R be any commutative ring with identity $1 \in R, 1 \neq 0$

Let x be a formal symbol $(x \notin R)$

A polynomial in x over R is a formal expression

$$f = a_0 + a_1 x + \cdots + a_n x^n$$

where $n \in \mathbb{N}^0 = \mathbb{N} \cup \{0\}$ and $a_0, \ldots, a_n \in R$.

a_i is the co-efficient of x^i

Conventions

(a) $x^0 = 1$ and $x^1 = x$

(b) We can miss terms $a_i x^i$ with $a_i = 0$ (0 coefficient)

<u>For example</u>: $1 + \cancel{0x^1} + 2x^2 = 1 + 2x$

(c) We abbreviate $1x^i = x^i$

(d) A polynomial of form $ax^0 = a1 = a$ is called a constant polynomial

(e) Consider 2 polynomials

$$f = a_0 + a_1 x + \cdots + a_n x^n$$

$$g = b_0 + b_1 x + \cdots + b_m x^m$$

When $m = n$: $f = g \iff a_0 = b_0, \ a_1 = b_1, \ \ldots, \ a_n = b_n$

When $n > m$, apply convention (b)

$$g = b_0 + b_1 x + b_2 x^2 + \cdots + b_m x^m + 0x^{m+1} + \cdots + 0x^n$$

$$\Longrightarrow b_{m+1} = 0, \ \ldots, \ b_n = 0$$

Similar for $n > m$. Then for equality, we have

if $m \geq n$ $\quad f = g \iff a_0 = b_0, \ a_1 = b_1, \cdots a_n = b_n, \ b_{n+1} = \cdots = b_m = 0$

if $m \leq n$ $\quad f = g \iff a_0 = b_0, \ a_1 = b_1, \cdots a_n = b_n, \ a_{m+1} = \cdots = a_n = 0$

Ring of Polynomials

Definition

Let R be any commutative ring with identity $1 \in R, 1 \neq 0$

Denote the set of all polynomials over R by

$$R[x]$$

Define addition and multiplication

Addition: $(+)$

$\forall f, g \in R[x]$

$$f = a_0 + a_1 x + \cdots + a_n x^n$$
$$g = b_0 + b_1 x + \cdots + b_m x^m \qquad m, n \in \mathbb{N}^0$$

$$\boxed{\begin{gathered} f + g = c_0 + c_1 x + \cdots + c_\ell x^\ell \quad , \quad \ell = \max\{n, m\} \\ c_i = \begin{cases} a_i + b_i & \text{if } i \leq \min\{m, n\} \\ a_i & \text{if } m < i \leq n \\ b_i & \text{if } n < i \leq m \end{cases} \qquad (c_0 = a_0 + b_0) \end{gathered}}$$

By convention (e), assume $n = m$. If $m \neq n$, then append 0 terms to the "shorter polynomial

$$f + g = (a_0 + b_0)x^0 + (a_1 + b_1)x^1 + \cdots + (a_n + b_n)x^n$$

Multiplication: $(\times)$

$$f \times g = (a_0 + a_1 x + \cdots + a_n x^n) \times (b_0 + b_1 x^1 + \cdots + b_m x^m) = d_0 + d_1 x + \cdots + d_{n+m} x^{n+m}$$

where for $0 \leq k \leq m + n$

$$d_k = \sum_{\substack{i,j \\ i+j=k}} a_i b_j$$

Note that

$$f \times g = (a_0 x^0 + a_1 x^1 + \cdots + a_n x^n)(b_0 x^0 + b_1 x^1 + \cdots + b_m x^m)$$
$$= a_0 b_0 x^0 + (a_0 b_1 + a_1 b_0) x^1 + \cdots\cdots + a_n b_m x^{n+m}$$

Proposition Ring of Polynomials

Let R be any commutative ring with identity $1 \in R, 1 \neq 0$

Then

$$(R[x], +, \times)$$

is a commutative ring with an identity.

Proof: Fill later

Corollary

The zero and identity of $R[x]$ is

i) Zero: 0 polynomial $f = 0 = 0x^0 = 0 \cdot 1$

ii) Identity: Constant polynomial $f = 1 = 1 \cdot x^0$

Proof:

i) Consider $f = 0 \cdot x^0 = 0 \cdot 1 = 0$

This is the zero element of $R[x]$

For any $g \in R[x]$

$$0 \cdot g = d_0 x^0 + \cdots d_m x^m$$

$$d_k = \sum_{\substack{i,j \\ i+j=k}} a_i b_j = 0 b_k \quad i=0 \text{ as } f=0 \text{ polynomial, 1 term}$$

$$= 0 \quad 0 \in R$$

$$\Longrightarrow 0 \cdot g = 0x^0 + \cdots + 0x^m = 0x^0$$

ii) Similarly $f = 1 \cdot x^0 = 1 = 1 \cdot 1$ is the identity element of $R[x]$

For any $g \in R[x]$,

$$1 \cdot g = d_0 x^0 + \cdots d_m x^m$$

$$d_k = \sum_{\substack{i,j \\ i+j=k}} a_i b_j = 1 b_k \quad i=0 \text{ as } f=1 \text{ polynomial, 1 term}$$

$$= b_k \quad 0 \in R$$

$$1 \cdot g = b_0 x + \cdots + b_m x^m = g$$

■

Degree of a polynomial

Let $f \neq 0$, $f \in R[x]$ a non-zero polynomial. Then for some $n \geq 0$,

$$f = a_0 + a_1 x + \cdots + a_n x^n$$

where atleast one of the coefficients is 0

By convention (b) $a_n \neq 0$.

Definition Degree of Polynomial

Let $f \neq 0$, $f \in R[x]$ a non-zero polynomial.

$$f = a_0 + a_1 x + \cdots + a_n x^n$$

with $a_n \neq 0$. Then degree of polynomial is

$$\deg(f) = n$$

Theorem

Let R be an integral domain

Then $R[x]$ is an integral domain, i.e. $\forall f, g \in R[x] \setminus \{0\}$

$$fg \neq 0 \quad \text{and} \quad \deg(fg) = \deg(f) + \deg(g)$$

Proof:

By definition, R is a commutative ring with identity such that $ZDR = \{0\}$.

By above proposition, $R[x]$ is a commutative ring with identity 1

Let $f, g \in R[x] \setminus \{0\}$. Then

$$f = a_0 + \cdots + a_n x^n \quad \text{and} \quad g = b_0 + \cdots + b_m x^m$$

where $a_n \neq 0$ and $b_m \neq 0$. Here

$$n = \deg f \quad \text{and} \quad m = \deg g$$

By definition

$$fg = a_0 b_0 + \cdots + a_n b_m x^{n+m}$$

$a_n \neq 0$ and $b_m \neq 0 \implies a_n b_m \neq 0$ since R is an ID, $ZD(R) = \{0\}$

If $a_n b_m = 0 \implies a_n = 0$ or $b_m = 0_{\#} \implies a_n b_m \neq 0$

Therefore $f \times g \neq 0$ and $\deg(fg) = n + m = \deg(f) + \deg(g)$

It also follows that $ZD(R[x]) = \{0\} \implies R[x]$ is an integral domain. ∎

Non-Example

Theorem fails if R is NOT an integral domain.

Consider $R = \mathbb{Z}/4\mathbb{Z}$, $[2] \in R$ and $[2] \times [2] = [4] = 0$

$$f = [1] + [2]x \quad \deg f = 1$$

$$f^2 = ([1]+[2]x)([1]+[2]x) = 1 + [4]x + [4]x^2 = [1]$$

$$\deg f^2 = 0 \neq 2 = \deg f + \deg f$$

Moreover

$$f \in U(R[x]). \text{ But } f \notin R \implies f \notin U(R)$$

Corollary

Suppose R is an integral domain

Then units are

$$U(R[x]) = U(R)$$

Proof:

($\supseteq$): Take any $a \in U(R)$. Then a has an inverse, say b such that

$$ab = ba = 1$$

But both a and b are constant polynomials. So

$$U(R) \subseteq U(R[x])$$

($\subseteq$): To prove $U(R[x]) \subseteq U(R)$, take any $f \in U([R])$.

Hence $\exists g \in R[x]$ s.t $f \cdot g = 1 \neq 0 \implies f \neq 0, g \neq 0$ $\quad$ $R[x]$ is an ideal

$$0 = \deg fg = \deg f + \deg g$$

$\implies \deg f = \deg g = 0$

$\implies f$ is constant polynomial

$\implies f \in R \subseteq R[x]$ and $\exists g \in R$ s.t $fg = 1$

$\implies f \in U(R)$

∎

13. Division Algorithm for Polynomials

Let F be any field. So F is a commutative ring with identity 1, $U(F) = F \setminus \{0\}$

Theorem

Let $R = F$ be any field. Let $f, g \in F[x]$ where $g \neq 0$

Then $\exists$ unique $q, r \in F[x]$ such that $r = 0$ or $r \neq 0$

$$f = gq + r \qquad \deg(r) < \deg g$$

<u>Proof</u>:

1) <u>Proof of existence</u>:

a) If $\deg g = 0$, then g is a constant polynomial $g \neq 0$

We know that $U(F) = F \setminus \{0\} \implies \exists\, g^{-1}$ another constant polynomial and

$$f = (g^{-1}g)f = g(\underset{\substack{\uparrow \\ F[x]}}{g^{-1}f}) = gq + 0$$

b) Suppose $\deg g = m > 0$. Let $L := \{f - gq : q \in F[x]\}$

i) Suppose $0 \in L$. Then $\exists\, q \in F[x]$ s.t $f - gq = 0 \iff f = gq + 0$

ii) Suppose $0 \notin L$. Then $\min\{\deg s \mid \underset{\substack{\neq \\ 0}}{s} \in L\} := k$

Pick any $s = r \in L$ such that $\deg r = k$

Then $r = f - gq$ for some $q \in F[x] \implies f = gq + r$

$L \ni r \neq 0$. Need to show that $\deg r < \deg g$

Write $g = b_0 + b_1x + \cdots + b_m x^m$ for some $m \in \mathbb{Z}_{\geq 0}$, assume $b_m \neq 0$

$r = c_0 + c_1 x + \cdots + c_k x^k$ where $c_k \neq 0$

Suppose $k \geq m$ and get a contradiction. Consider

$c_k b_m^{-1} x^{k-m} \in F[x]$

$$\text{Consider } s = r - c_k b_m^{-1} x^{k-m} g = \overbrace{\boxed{(c_0 + c_1x + \cdots + c_k x^k)}}^{\text{degrees} \leq k} - \overbrace{c_k b_m^{-1} x^{k-m} \overbrace{(b_0 + b_1 x + \cdots\cdots + b_m x^m)}^{\deg \leq m}}^{\deg \leq m + k - m}$$

cancel

Then either $s = 0$ or $s \neq 0$. But

$\deg s < k$ ※

A contradiction: $0 \notin L$

$$r \in L \Rightarrow r = f - gq \text{ for some } q \in F[x]$$

$$L \ni s = r - c_k b_m^{-1} x^{k-m} g = f - gq - c_k b_m^{-1} x^{k-m} g$$

$$= f - (g + c_k b_m^{-1} x^{k-m}) g \in L$$

But $0 \notin L$ so $s \neq 0$, remains $\deg s < k$ and $s \in L$, but k is minimal $\lightning$ contradicts defn of L

This means that $k \geq m$ not possible $\Rightarrow \underset{\deg r}{\underset{\parallel}{k}} < \underset{\deg g}{\underset{\shortparallel}{m}}$

2) <u>Uniqueness</u>

Suppose $f = gq + r$ where $r = 0$ or ($r \neq 0$ and $\deg r < \deg g$)

$f = gq' + r'$ where $r' = 0$ or ($r' \neq 0$ and $\deg r' < \deg g'$)

Let us show that then $r = r'$ and $q = q'$

$$0 = gq + r - gq' - r' \Leftrightarrow r - r' = g(q - q')$$

Suppose that $r' - r \neq 0$. Then $\deg(r - r') < \deg g$

i) $r = 0,\ r' \neq 0$ $\quad \deg(r' - r) = \deg(-r) < \deg g$

ii) $r = 0,\ r' \neq 0$ $\quad \deg(r' - r) = \deg(r') < \deg g$

iii) $r \neq 0,\ r' \neq 0$ $\quad \deg(r' - r) \leq \max\{\deg r, \deg r'\} < \deg g$

$$\deg g > \deg(r' - r) = \deg(g(q - q')) = \deg g + \underset{\substack{\vee\!| \\ 0}}{\deg(q - q')} \quad ✗$$

So $r' - r = 0 \Leftrightarrow r' = r$

Then $g(q - q') = 0$. But F is a field $\Rightarrow$ F is an integral domain

Then $F[x]$ has property $ZD(F[x]) = \{0\}$

So $\underset{\neq 0}{g}(q - q') = 0 \Rightarrow q - q' = 0 \Leftrightarrow q = q'$ ■

Example of a field F

$F = \mathbb{Z}/p\mathbb{Z}$ where p is a prime number $(p \in \mathbb{Z})$

Claim: F is a field, $F = \{[0], [1], \dots, [p-1]\}$

- F is commutative
- $F \ni 1$ identity
- F is finite, commutative ring

$$U(F) = F \setminus \{0\} \iff ZD(F) = \{0\}$$

Take any class $[k]$ which is a zero-divisor in $\mathbb{Z}/p\mathbb{Z}$

$$k = 0, 1, \dots, p-1 \quad ; \quad \ell = 0, 1, \dots, p-1$$

$$[k][\ell] = [0] \iff k\ell = pm \quad \text{for some } m = 0, 1, 2, \dots$$

$$k\ell = 0, p, 2p, \dots \; ; \; k, \ell < p \qquad X$$

$$k\ell = 0 \text{ in } \mathbb{Z}$$

So k is a zero divisor iff $k = 0$

Example of Division Algorithm

$F = \mathbb{Z}/5\mathbb{Z}$

$f = [1]x^5 + [3]x^4 + [2]x^2 + [4]$

$g = [2]x^2 + [1]$

Solve $f = gq + r$, where either $r = 0$, $r \neq 0$ $\deg(r) < \deg g = 2$

Step 1: $5 = \deg f = \deg(gq + r) \Rightarrow \deg(gq) = 5$

$$\Rightarrow \deg(q) + \deg(g) = 5$$

$$\Rightarrow \deg(q) = 3$$

$$\left(\begin{array}{ll} q = ax^3 + bx^2 + cx + d & \text{where } a, b, c, d \in \mathbb{Z}/5\mathbb{Z} \\ r = ux + v & \text{where } u, v \in \mathbb{Z}/5\mathbb{Z} \end{array} \right)$$

Step 2: $[1]x^5+[3]x^4+[2]x^2+[4]=([2]x^2+[1])(ax^3+bx^2+cx+d)+ux+v$

$$=[2]ax^5+[2]bx^4+(a+[2]c)x^3+(b+[2]d)x^2+(c+u)x+(d+v)x^0$$

Step 3: Equating co-efficients

$$\begin{array}{l|l|l}
\left.\begin{array}{ll} \text{i)} & [1]=[2]a \\ \text{ii)} & [3]=[2]b \\ \text{iii)} & [0]=a+[2]c \\ \text{iv)} & [2]=b+[2]d \end{array}\right\}\times[3] & \begin{array}{l}[3]=a\\ [4]=b\\ [0]=[3]a+c\\ [1]=[3]b+d\end{array} & \begin{array}{l}a=[3]\\ b=[b]\\ c=[1]\\ d=[4]\end{array} \\
\begin{array}{ll} \text{v)} & [0]=c+u \\ \text{vi)} & [4]=d+v\end{array} & \begin{array}{l}[0]=c+u\\ [4]=d+v\end{array} & \begin{array}{l} u=[4]\\ [v]=[0]\end{array}
\end{array}$$

Observe

$$[2][3]=[1]\implies[2]^{-1}=[3]$$

14. Polynomial Functions

Let R be any commutative ring with identity $1 \in R$.

Let $r \in R$ range over R and $f \in R[x]$. Then

$$f = a_0 x^0 + a_1 x^1 + \cdots + a_n x^n, \quad \text{where } n \in \mathbb{N} \cup \{0\}$$

$a_0, a_1, \cdots, a_n \in R$ are coefficients and x only a formal symbol.

Define polynomial function $f(r)$ with values in R by

$$f(r) = \underset{\overset{\shortparallel}{a_0}}{a_0 1} + \underbrace{a_1 r}_{\in R} + \underbrace{a_2 r^2}_{= a_2 r r \in R} + \cdots + a_n r^n \qquad \forall r \in R$$

Then we have a correspondence

$$\begin{aligned} R[x] &\to \{\text{polynomial functions}\} \\ f &\mapsto f(r) \end{aligned}$$

Remark: if $R = \mathbb{R}, \mathbb{C}$, this correspondence is 1-1

$$f(r) = g(r) \Longrightarrow f = g \quad \text{equality of polynomials}$$

$$\Longrightarrow f \mapsto f(r) \quad 1\text{-}1$$

NOT true for an arbitrary ring or a field

Non-Example:

$$R = \mathbb{Z}/2\mathbb{Z} = \{\underset{\shortparallel}{[0]}, \underset{\shortparallel}{[1]}\}$$

$$0 \neq 1$$

Take
$$\left.\begin{aligned} f &= [1] + x \\ g &= [1] + x + x^2 + [0]x^3 + x^4 \end{aligned}\right\} f \neq g \text{ as elements of } R[x]$$

$$f \mapsto f(r): \quad f([0]) = [1], \quad f([1]) = [0]$$

$$g \mapsto g(r) \quad g([0]) = [1], \quad g([1]) = [0]$$

$$\Longrightarrow f(r) = g(r) \quad \forall r \in R$$

15. Principal Ideal Domain

Let R be any commutative ring with an identity 1.

Lemma

Let R be any commutative ring with $1 \in R$

i) For any given $a \in R$, consider the set

$$aR = \{ar \mid r \in R\}$$

Then aR is an ideal containing aR

ii) aR is the smallest ideal containing a

Proof:

i) a) $0 = a0 \in R$

b) $ar + as = a(r+s) \in aR$

c) $-ar = a(-r) \in aR$

d) $ar.s = a(\underbrace{rs}_{\overset{\cap}{R}}) \in aR$

$a = a1 \in aR$

ii) Take any ideal $I \subseteq R$ containing the given $a \in R$

We need to show $aR \subseteq I$

We know $\forall a \in I, \forall r \in R, ar \in I \implies aR \subseteq I$ ■

Definition Principal ideal

The ideal

$$aR = \{ar : r \in R\}$$

is called **principal ideal** (generated element $a \in R$)

Examples of Principal ideals

1) $\{0\}$ is a principal ideal of any ring R

$$\{0\} = \{0r \mid r \in R\} \quad ; \quad 0 \in R$$

2) For $R=\mathbb{Z}$, $n\mathbb{Z}$ is a principal ideal for any $n\in\mathbb{N}$ generated by $a=n$

Principal Ideal Domain

Definition Principal Ideal Domain

A principal ideal domain (PID) is an integral domain (ID) where every ideal is principal

Proposition

The ring $\mathbb{Z}$ is a principal ideal domain

Proof:

We know that $\mathbb{Z}$ is an ID. We need to show that every ideal of $\mathbb{Z}$ is principal

(1) $\{0\}\subseteq\mathbb{Z}$ is principal as in example (1) above

(2) Let $S\neq\{0\}$ be any non-zero ideal of $\mathbb{Z}$. We find $n\in\mathbb{N}$ such that

$$S=n\mathbb{Z}$$

Take any $a\neq 0$, $a\in S \implies -a\in S$, hence $S\cap\mathbb{N}\neq\emptyset$.

Let n be the minimal natural number in S $(n>0)$

$$n=\min\{s\in S \mid s>0\}\in S$$

$(\subseteq)$: Showing $n\mathbb{Z}\subseteq S$

Observe by property of ideals

$$nz\in S \quad \forall z\in\mathbb{Z} \implies n\mathbb{Z}\subseteq S$$

$(\supseteq)$: Remain to prove $n\mathbb{Z}\supseteq S$. Take any $u\in S\subseteq\mathbb{Z}$. Then

$$u=nq+r \text{ where } 0\leq r<n$$

$\implies r=u-nq$, where $u\in S$ and $nq\in S$ property of ideals

if $r>0$ and $r=u-nq<n\in S$, we contradict minimality of n

$\implies r=0$

$\implies u\in n\mathbb{Z}$ ■

Theorem

Let F be any field. Then the ring

$$F[x]$$

is a principal ideal domain

Proof:

We already know that $F[x]$ is an integral domain. Need to show every ideal of $F[x]$ is principal.

(1) $\{0\} \subseteq F[x]$ is principal

(2) Suppose $I \neq \{0\}$ is any non-zero ideal of $F[x]$.

Let $g \in I$ be such that $g \neq 0$ and $\deg g$ is minimal for all elements of I.

We will show

$$I = gF[x]$$

($\supseteq$): By definition of ideal,

$$gF[x] \subseteq I \quad (gf \in I \ \ \forall f \in F[x])$$

($\subseteq$): Suppose $f \in I$. By division algorithm for $F[x]$

$$f = gq + r \qquad q, r \in F[x] \qquad r = 0 \text{ or } r \neq 0$$

$$\deg(r) < \deg(g)$$

$\Longrightarrow$ $r = f - gq$, $f, gq \in I$

$\Longrightarrow$ $r \in I$ closure of ideal under $+$

$\deg(r) < \deg(g) \in I$ contradicts minimality of $\deg(g)$

$\Longrightarrow$ $r = 0$

$\Longrightarrow$ $f \in gF[x]$

$\Longrightarrow$ $I \subseteq gF[x]$

Generators

$aD = \{ad : d \in D\}$

To generate aD

$a = awd$ for some $w \in D \implies wd = 1$

$\implies w$ is a unit

16. Divisibility of Integral Domains

Let D denote integral domain

i) D is commutative

ii) $1 \in D$

iii) $ZD(D) = \{0\}$

For example, $D = \mathbb{Z}, \mathbb{Z}[\underset{\substack{\uparrow \\ \text{square-free}}}{\sqrt{d}}]$, $F, F[x]$, F a field.

Divisibility

Definition

We say that $b \in D$ divides $a \in D$ if

$$a = bc \quad \text{for some } c \in D$$

denoted $b | a$

For example if $b=0$, then $a = 0c = 0 \Longrightarrow b=0$ divides only $a=0$

Remark: Let $b \in U(D)$. Then $\forall a \in D$, we have

$$a = a \cdot 1 = a(b^{-1}b) = \underbrace{(ab^{-1})}_{c} b$$

In particular, if $D=F$ is a field and $b \neq 0$, then $b \in U(F)$

$\Longrightarrow$ so all non-zero elements of a field divide every element

Irreducibility and Prime

Definition

i) An element $a \in D$ is irreducible if $a \neq 0$, $a \notin U(D)$ and if for any $b, c \in D$,

$$a = bc \Longrightarrow b \in U(D) \quad \text{or} \quad c \in U(D)$$

ii) An element $p \in D$ is prime if $p \neq 0$, $p \notin U(D)$ and if for some $a, b \in D$

$$p | ab \Longrightarrow p | a \text{ or } p | b$$

iii) Elements $a, b \in D$ are associates if $a = bu = ub$ for some $u \in U(D)$

We write $a \sim b$

Example

$D=\mathbb{Z}$, Recall $U(\mathbb{Z})=\{+1,-1\}$

iii) $a\sim b$ in $\mathbb{Z} \iff |a|=|b|$

ii) An element $p\in\mathbb{Z}$ is prime $\iff p\neq 0,\ p\neq 1,-1$ and

$$p|ab \implies p|a \text{ or } p|b$$

But $p|ab \iff |p|\,\big|\,|a||b|$

Then $p|a$ or $p|b \implies |p|\,\big|\,|a|$ or $|p|\,\big|\,|b|$

So $|p|$ is a prime number

$p\in\mathbb{Z}$ is "prime" element $\iff |p|$ is a prime number

i) By defn, $a\in\mathbb{Z}$ is irreducible if $a\neq 0$; $a\neq 1,-1$ and if

$$a=bc \text{ for some } b,c\in\mathbb{Z}$$

$$\implies b=\pm1 \text{ or } c=\pm1$$

$a=bc \implies |a|=|bc|=|b||c| \implies |a|$ is a prime number again

For $D=\mathbb{Z}$, $\{$irreducible elements$\}$ = $\{$prime elements$\}$

(The equality does not hold in general)

Non-Example

$D=\mathbb{Z}[\sqrt{-3}]$: $d=-3$

$a=2$ irreducible, not prime

Proposition

Let D be any integral domain.

If $p\in D$ is prime $\implies p$ is irreducible

Proof:

Let $p\in D$ be prime. So $p\neq 0$, $p\notin U(D)$ by definition

Suppose $p=bc$. Then $p=1\cdot bc \implies p|bc$

$$\implies p|b \text{ or } p|c$$

__Case 1:__ $p \mid b \implies b = pd$ for some $d \in D$

$p \neq 0$, D is an ID, $p \notin ZD(D)$

$$\implies \cancel{p} = bc = (pd)c = \cancel{p}(dc) \quad \text{Cancellation property}$$

$$\implies 1 = dc \implies c \in U(D)$$

__Case 2:__ $p \mid c \implies b \in U(D)$

So p is irreducible ■

Remarks/ Important facts

(1) If $a \in D$ is irreducible and $a = bc$, then $a \sim b$ or $a \sim c$

(2) If $p \in D$ is prime and

$$p \mid a_1 \cdots a_n$$

for $a_1, \dots, a_n \in D$, then

$$p \mid a_i \qquad \text{for some index } 1 \leq i \leq n$$

In particular $\forall a \in D$

$$p \mid a^n \implies p \mid a$$

(3) If $b \mid a$ and $a \in U(D)$ then $a = bc$ so that $1 = b(ca^{-1}) \implies b \in U(D)$

Lemma

i) The relation $\sim$ is an equivalence relation on D

So D splits into a disjoint union of equivalence classes relative to $\sim$

ii) Equivalence classes of 0 and 1 in D are respectively $\{0\}$ and $U(D)$

__Proof:__

i) __Reflexive:__ $\forall a \in D$, $a = a \cdot 1 \implies a \sim a$

__Symmetry:__ $\forall a, b \in D$, $a \sim b \implies a = bu$, $u \in U(D)$

$$\implies b = au^{-1}, \; u^{-1} \in U(D)$$

$$\implies b \sim a$$

__Transitive:__ $\forall a, b, c \in D$, $a \sim b$ and $b \sim c \implies a = bu$, $b = cv$, $u, v \in U(D)$

$$\implies a = c(vu), \; uv \in U(D)$$

$\implies a \sim c$

ii) $0 \sim 0$ (reflexive) $\implies 0 \in [0]$

$a \sim 0 \implies a = 0u$, $u \in U(D)$

$\implies a = 0$

$\implies [0] = \{0\}$

$a \sim 1 \implies a = 1u = u$, $u \in U(D)$

$\implies a \in U(D)$

$\implies [1] \subseteq U(D)$

$v \in U(D) \implies v = 1v \implies v \sim 1 \implies U(D) \subseteq [1]$

$$\left.\begin{array}{l} [1] \subseteq U(D) \\ U(D) \subseteq [1] \end{array}\right\} \implies [1] = U(D)$$

■

Example

$D = \mathbb{Z}$, then $\mathbb{Z} = \{0\} \sqcup \{-1,+1\} \sqcup \underset{\substack{\cup \\ \text{equivalence classes in } \mathbb{Z}}}{\{2,-2\}} \sqcup \{3,-3\} \sqcup \cdots$

Remarks/ Important facts: continued

(4) If $b|a$ and $a|b \implies a \sim b$

<u>proof</u>:

$a|b \implies a = bc$ for some $c \in D$

$b|a \implies b = ad$ for some $b \in D$

Then

$$a1 = a = bc = adc$$

If $a = 0 \implies b = 0 \implies a \sim b$

If $a \neq 0 \implies a \in NZD(D)$ (since D is an integral domain)

$\implies dc = 1$ cancellation property

$\implies c, d \in U(D)$

$\implies a \sim b$

■

(5) If $p, q \in D$ are primes and $p | q \Longrightarrow p \sim q$

<u>proof</u>:

$p | q \Longrightarrow q = q1 = pr$ for some $r \in D$

$\Longrightarrow q | pr$

$\Longrightarrow q | p$ or $q | r$ since q prime

$q | r \Longrightarrow r = qs$ for some $s \in D$

$q = pr = pqs = qps \Longrightarrow 1 = ps$ by cancellation property

$\Longrightarrow p \in U(D) \divideontimes$

Hence $q | p$ and $p \sim q$ by (4) above ■

(6) D is an integral domain, $a, a', b, b' \in D$, $a \sim a'$, $b \sim b'$

$$a | b \Longleftrightarrow a' | b'$$

(7) $p \in D$ prime and $p \sim q \Longrightarrow q$ is prime

<u>proof</u>:

$p \in D$ is prime $\Longrightarrow p \neq 0$ and $p \notin U(D)$

$p \sim q \Longrightarrow q \neq 0, q \notin U(D)$ by Lemma page 59(ii)

Suppose $q | ab \Longrightarrow p | ab$ by (6)

$\Longrightarrow p | a$ or $p | b$

$\Longrightarrow q | a$ or $q | b$ ■

(8) $a \in D$ irreducible. $a \sim b \in D \Longrightarrow b$ is irreducible

<u>proof</u>: $a \in D$ irreducible $\Longrightarrow a \neq 0, a \in U(D)$

$a \sim b \Longrightarrow b \neq 0, b \notin U(D)$ by defn.

$a = bu$ for some $u \in U(D)$

Suppose $b = cd$ for some $c, d \in D$

$$a = bu = (cd)u = c(du)$$

a irreducible $\Longrightarrow c \in U(D)$ or $du \in U(D)$

Case 1: $du \in U(D)$ here

$$d = (du)u^{-1} \in U(D) \implies d \in U(D)$$

Hence $c \in U(D)$ or $d \in U(D) \implies b$ irreducible $\blacksquare$

Proposition

Let D be a principal ideal domain

$$p \in D \text{ is irreducible} \iff p \text{ is prime}$$

Proof:

We have already proven for any ID, p prime $\implies p$ irreducible

Now let $p \in D$ be irreducible. Then p is prime.

We already have $p \neq 0$, $p \notin U(D)$. Suppose $p \mid bc$ for some $b, c \in D$

(need to show $p \mid a$ or $p \mid b$)

Now $bc = pa$ for some $a \in D$

Consider principal ideals $pD, bD \subseteq D$. Then consider ideal

$$pD + bD = \{sp + tb : s, t \in D\}$$

Sum of ideals are ideals. D is a PID $\implies pD + bD$ is principal

$$pD + bD = dD \quad \text{for some } d \in D$$

Then $p = p1 + b0 \in dD$

$b = p0 + b1 \in dD$

In particular $d \mid p \implies p = dq$ for some $q \in D$

p is prime $\implies p$ is irreducible

$\implies c \in U(D)$ or $q \in U(D)$

Case 1: q is a unit $\implies p \sim d$ and $d \mid b$

$\implies p \mid b$ by remark (6)

Case 2: d is a unit.

$d \in pD + bD \implies d = sp + tb$ for some $s, t \in D$

$$c = 1c = dd^{-1}c = (sp+tb)d^{-1}c = spd^{-1}c + tbcd^{-1} = spd^{-1}c + tpad^{-1}$$
$$= p(sd^{-1}c + tad^{-1})$$

$$\Longrightarrow \quad p \mid c$$

■

Unique Factorization Theorem

Now lets have some $a \in D$ and try to factorize

$$a = p_1 \cdots p_m \text{ where each } p_i \in D, \text{ prime}$$

Theorem Unique Factorization Theorem

Let D be any integral domain

Let $a \in D$,

$$a = p_1 \cdots p_m = q_1 \cdots q_n \quad m, n \in \mathbb{N}, \quad p_i, q_j \in D \text{ prime}$$

Then $m = n$ and one can rearrange $q_1, \cdots q_m$ so that

$$p_i \sim q_i \qquad \forall i = 1, \dots, m$$

Hence a decomposition of $a \in D$ as a product of primes is essentially unique

Proof: (by induction on m):

Base case: $m = 1$

Suppose then $a = p_1 = q_1 \cdots q_n$

p_1 prime $\Longrightarrow$ p_1 irreducible

$$\Longrightarrow a = q_1 \cdots q_n \text{ irreducible} = (\overset{b}{\overset{\shortparallel}{q_1 \cdots q_{n-1}}})\overset{c}{\overset{\shortparallel}{q_n}}$$

Suppose $n > 1$. Here

$$q_n \text{ prime} \Longrightarrow q \notin U(D)$$

Then $q_1 \cdots q_{n-1} \in D$ is a unit. And so $\exists r \in D$ s.t

$$q_1 \cdots q_{n-1} r = 1 \Longrightarrow q_1^{-1} = q_2 \cdots q_{n-1} r, \; \cdots, \; q_{n-1}^{-1} = q_1 \cdots q_{n-2} v$$

$$\Longrightarrow q_1, \cdots, q_{n-1} \in U(D) \quad \text{closure, group theory}$$

$$\Longrightarrow q_1, \cdots, q_{n-1} \text{ is prime and units} \; \text{※}$$

Hence $n = 1$, $a_1 = p_1 = q_1$

Inductive step: Suppose $m > 1$ and $P(m)$ holds for $m-1$ instead of m.

Let $a = (p_1)(\cdots p_m) = q_1 \cdots q_n$ where each factor p_i, q_j is prime

$\Longrightarrow p_1 | q_1 \cdots q_n$ and p_1 prime

By remark (2), p_1 divides atleast one of the factors

$q_1 \cdots q_n$, i.e.

$p_1 | q_j$ for some index j

By rearranging $q_1 \cdots q_n$, assume

$p_1 | q_1$

By remark (5) then $p_1 \sim q_1 \Longleftrightarrow p_1 = q_1 u$ for some $u \in U(D)$

$$p_1 p_2 \cdots p_m = p_1 u q_2 \cdots q_n .$$

So $p_1 \neq 0 \Rightarrow p_1 \notin ZD(D) = \{0\}$. By cancellation property

$$\Longrightarrow \underbrace{p_2 \cdots p_m}_{\text{prime}} = \underbrace{(uq_2)}_{\text{prime}} \underbrace{q_3 \cdots q_n}_{\text{prime}}$$

uq_2 prime by remark (7).

By induction assumption, $m-1 = n-1 \Longrightarrow m = n$

By rearranging $uq_2, q_3, \cdots, q_m$ we can make them associated to $p_2 \cdots p_m$ respectively

$q_2 \sim uq_2 \sim p_2$

$q_3 \sim p_3$

$\vdots$

$q_n \sim p_n$

$p_1 \sim q_1 u \sim q_1$

■

Remark: Let D be any integral domain and $a \in D$ be irreducible, not prime

Then a does NOT decompose into prime factors

Proof: (contradiction):

Suppose $a = pq$, $p, q \in D$, prime

p prime $\Longrightarrow p \notin U(D) \Longrightarrow q \in U(D)$ primes irreducible

$\Longrightarrow a \sim p \Longrightarrow a$ is prime (Remark) ⚡

$\blacksquare$

More Examples

1)

17. Examples of irreducible elements

Let $d \in \mathbb{Z} \setminus \{1\}$ be square free

$d \neq 0$

$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$$

is a subring of $\mathbb{C}$ with the identity

$$1 + 0\sqrt{d}$$

Usual + and x operations on $\mathbb{Z}[\sqrt{d}]$

$$(a+b\sqrt{d}) + (c+e\sqrt{d}) = (a+c) + (b+e)\sqrt{d}$$

$$(a+b\sqrt{d}) \times (c+e\sqrt{d}) = (ac+bed) + (ae+bc)\sqrt{d}$$

Proposition

$\mathbb{Z}[\sqrt{d}]$ is an integral domain

Proof: $D = \mathbb{Z}[\sqrt{d}]$

1) D is commutative

2) $D \ni 1 = 1 + 0i = 1 + 0\sqrt{d}$

3) $$\underset{\{0\}}{\overset{}{\underset{\shortparallel}{ZD(D)}}} \subseteq ZD(\mathbb{C}) = \{0\}$$

■

Norm

Definition

The norm on $D = \mathbb{Z}[\sqrt{d}]$ is the function

$$N: \mathbb{Z}[\sqrt{d}] \longrightarrow \mathbb{N}^0 = \mathbb{N} \cup \{0\}$$

$$N(a+b\sqrt{d}) = |a^2 - db^2| \geq 0$$

Remarks

(a) $N(a+b\sqrt{d}) = |(a+b\sqrt{d})(a-b\sqrt{d})|$

(b) If $d<0$, then $N(a+b\sqrt{d}) = a^2 \underbrace{-d}_{\overset{\vee}{0}} b^2 \geq 0$

Proposition

(i) Any $z \in \mathbb{Z}[\sqrt{d}]$ has a unique presentation

$$z = a + b\sqrt{d} \quad \text{for some } a, b \in \mathbb{Z}[\sqrt{d}]$$

so our definition of N is correct (well-defined)

(ii) $N(z) = 0 \iff z = 0$

(iii) $N(zw) = N(z)N(w) \quad \forall z, w \in \mathbb{Z}[\sqrt{d}]$

(iv) $z \in U(\mathbb{Z}[\sqrt{d}]) \iff N(z) = 1$

Proof:

i) Let $a + b\sqrt{d} = c + e\sqrt{d}$ for $a, b, c, e \in \mathbb{Z}$

Then $(a-c) = (e-b)\sqrt{d} \implies \underset{\overset{\vee}{0}}{(a-c)^2} = \underset{\overset{\vee}{0}}{(e-b)^2}\, d \neq 0$ (*)

Suppose $e \neq b$, we know that $d \neq 0$, $d > 0$ to avoid contradiction

$$\begin{aligned} d > 0 \text{ and } d \neq 1 &\implies d > 1 \in \mathbb{Z} \\ &\implies d \text{ has a prime factor in } \mathbb{Z}_{>0} \\ &\implies p \mid (a-c)^2 \\ &\implies p \mid (a-c) \end{aligned}$$

So p occurs at LHS (*) even number of times and odd number of times in RHS ⨳

Therefore $e = b \implies a = c$

ii) Let $z = a + b\sqrt{d}$. By using Remark (a) and (i) of our proposition, we have

$$\begin{aligned} N(z) = 0 &\iff |a^2 - db^2| = 0 \iff |(a + b\sqrt{d})(a - b\sqrt{d})| = 0 \\ &\iff (a + b\sqrt{d})(a - b\sqrt{d}) = 0 \iff a + b\sqrt{d} = 0 \text{ or } a - b\sqrt{d} = 0 \\ &\iff a = b = 0 \iff z = 0 \end{aligned}$$

iii) $z = a + b\sqrt{d}$, $w = c + e\sqrt{d}$, $a, b, c, e \in \mathbb{Z}$

$$\begin{aligned} N(zw) &= N((a + b\sqrt{d})(c + e\sqrt{d})) \\ &= N((ac + bed) + (bc + ae)\sqrt{d}) \\ &= |(ac + bed)^2 - d(bc + ae)^2| \end{aligned}$$

$$= |a^2c^2 + 2acbed + b^2e^2d^2 + db^2c^2 - 2bcaed - da^2e^2|$$

$$= |a^2c^2 + b^2e^2d^2 - db^2c^2 - da^2e^2|$$

$$= |(a^2 - db^2)(c^2 - de^2)|$$

$$= |a^2 - db^2| \times |c^2 - de^2|$$

$$= N(z)\,N(w)$$

iv) $z \in U(\mathbb{Z}[\sqrt{d}])$, then $zw = 1$ for some $w \in \mathbb{Z}[\sqrt{d}]$. Then by (iii)

$$1 = N(1) = N(zw) = N(z)N(w)$$

$\Longrightarrow N(z) = 1$ and $N(w) = 1$. Conversely, let $z = a + b\sqrt{d}$ with $a, b \in \mathbb{Z}$

$$N(z) = 1 \Longrightarrow |a^2 - db^2| = 1 \Longrightarrow |(a+b\sqrt{d})(a-b\sqrt{d})| = 1$$

$$\Longrightarrow (a+b\sqrt{d})(\pm(a-b\sqrt{d})) = 1$$

$$\Longrightarrow z \in U(\mathbb{Z}[\sqrt{-d}])$$

■

Theorem

Let $d \in \mathbb{Z} \setminus \{0, 1\}$ be square free (can have $d = -1$, $i = \sqrt{-1}$)

The units of $\mathbb{Z}[\sqrt{d}]$ are:

i) $1, -1, i, -i$ if $d = 1$

ii) $1, -1$ if $d < -1$

iii) $1, -1$ and infinitely many others if $d > 1$

Proof:

i) Let $d = -1$. Then $z = a + bi$, $a, b \in \mathbb{Z}$

By (iv) above, $z \in U(\mathbb{Z}[i]) \Longleftrightarrow N(z) = 1$

$$\Longleftrightarrow a^2 + b^2 = 1$$

$$\Longleftrightarrow (a, b) = (1, 0), (-1, 0), (0, 1), (0, -1)$$

$\Longleftrightarrow$ units are ± 1 and $\pm i$

ii) $d < -1$:

Then $z = a + b\sqrt{d} \in \mathbb{C}$, but $a, b \in \mathbb{Z}$

By (iv) above, $z \in U(\mathbb{Z}[\sqrt{d}]) \iff N(z)=1 \iff 1=a^2-db^2 \geq 0$

$$1=a^2-\underset{\underset{1}{\vee}}{\underbrace{d}}\,\underset{\underset{\mathbb{Z}}{\rotatebox{90}{$\in$}}}{\underbrace{b^2}} \implies b=0,\ a^2=1 \iff z=1,-1$$

iii) $d>1$.

Then $1,-1 \in U(\mathbb{Z}[\sqrt{d}])$. Further $z=a+b\sqrt{d}$, $a,b\in\mathbb{Z}$

$$z\in U(\mathbb{Z}[\sqrt{d}]) \iff |a^2-db^2|=1$$

$\iff$ has solutions $(a,b)\neq(\pm1,0)$ by Number Theory

$\iff$ $z=a+b\sqrt{d}$ also has $z^2, z^3, \dots$ are distinct units ■

Constructing our Example

Consider ring $\mathbb{Z}[\sqrt{-3}]$, $d=-3$. If $z=a+b\sqrt{-3}\in\mathbb{Z}[\sqrt{-3}]$

$$z=a+b\sqrt{-3} \implies N(z)=a^2+3b^2\neq 2$$

Now suppose

$$w\in\mathbb{Z}[\sqrt{-3}] \text{ such that } N(w)=4$$

Proposition

w is irreducible

Proof:

Indeed $N(w)\neq 0,1 \implies w\neq 0,\ w\notin U(\mathbb{Z}[\sqrt{-3}])$

Now suppose $w=xy$ for some $x,y\in\mathbb{Z}[\sqrt{-3}]$

By (iii) of our proposition,

$$w=xy \implies 4=N(w)=N(xy)$$

$$\implies 4=\underset{\underset{\mathbb{Z}_{\geq 0}}{\rotatebox{90}{$\in$}}}{N(x)}\,\underset{\underset{\mathbb{Z}_{\geq 0}}{\rotatebox{90}{$\in$}}}{N(y)}$$

$$\implies 4=4\cdot1=1\cdot4=\cancel{2\cdot2}$$

$$\implies N(x)=1,\ N(y)=4 \quad\text{or}\quad N(x)=4,\ N(y)=1$$

$$\implies x\in U(\mathbb{Z}[\sqrt{-3}]) \quad\text{or}\quad y\in U(\mathbb{Z}[\sqrt{-3}])$$

x is a unit or y is a unit

So w is irreducible by definition

$$N(w) = 4 \iff w \text{ is irreducible}$$ ■

Now consider

$$w = 1+\sqrt{-3} \qquad N(1+\sqrt{-3}) = 4$$

$$w = 1-\sqrt{-3} \qquad N(1-\sqrt{-3}) = 4$$

$$\underbrace{w = 2+0\sqrt{3} = 2}_{\text{all irreducible}} \qquad N(2) = 4$$

Now, $4 \in \mathbb{Z}[\sqrt{-3}]$

$$4 = 2 \times 2 = (1-\sqrt{-3})(1+\sqrt{-3})$$

Units of $\mathbb{Z}[\sqrt{-3}]$ are

$$U(\mathbb{Z}[-1]) = \{-1, 1\}$$

Thus

$$2 \nmid 1+\sqrt{-3} \quad \text{and} \quad 2 \nmid 1+\sqrt{-3}$$

Does NOT contradict factorization theorem since $1+\sqrt{-3}$, $1-\sqrt{-3}$, 2 are NOT prime

proof: (by contradiction)

Suppose $(1+\sqrt{-3})$ is prime.

$$(1+\sqrt{-3}) \mid 4 = 2 \times 2 \implies (1+\sqrt{-3}) \mid 2 \qquad \text{defn of prime}$$

$$\implies 2 = (1+\sqrt{-3})z \quad \text{for some } z \in \mathbb{Z}[\sqrt{-3}]$$

$$\implies 4 = N(2) = N(1+\sqrt{-3})\,N(z)$$

$$\implies 4 = 4N(z)$$

$$\implies N(z) = 1$$

$$\implies z \in U(\sqrt{-3}) = \{1, -1\} \implies z = 1, -1$$

$$\implies z \text{ a unit } \#$$

Similar for other elements ■

18. Unique Factorisation Domains

Definition

Let D be any integral domain

D is called a unique factorization domain UFD if

i) $\forall a \in D\setminus\{0\}$ with $a \notin U(D)$, then

$$a = p_1 p_2 \cdots p_m \quad , m \in \mathbb{N} \text{ and } p_i \text{ irreducible } \forall i = 1, \dots, m \text{ in } D$$

ii) Such a decomposition of a is essentially unique, that is if

$$a = p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n$$

where all p_i, $i = 1, \dots, m$ and all q_j with $j = 1, \dots, n$ are irreducible in D, then $m = n$.

We can then relabel the q_j so that

$$p_i \sim q_i \quad \text{for each } i = 1, \dots, m$$

Remark: If all irreducibles in D are prime, then (ii) holds by unique factorization theorem

Example

(1) Ring $\mathbb{Z}$ is a UFD. Indeed $\mathbb{Z}$ is an integral domain with

$$U(\mathbb{Z}) = \{1, -1\}$$

Irreducibles in $\mathbb{Z}$ are prime numbers in the sense of Number Theory and also their negatives.

Every $z \in \mathbb{Z}\setminus\{0, 1, -1\}$ can be written as product of these $\Longrightarrow$ (i) holds

All irreducibles in $\mathbb{Z}$ are prime by ring theory $\Longrightarrow$ (ii) holds

(2) Ring $\mathbb{Z}[\sqrt{-3}]$ is NOT a UFD because (ii) fails

$$4 = 2 \times \underset{\uparrow}{2} = \underset{\uparrow}{(1+\sqrt{-3})}\,\underset{\uparrow}{(1-\sqrt{-3})}$$

irreducible, not associated

Proposition

Let D be a UFD and $p \in D$

$$p \text{ irreducible} \iff p \text{ is prime}$$

Proof:

We know if D is any integral domain, then

$$p \text{ prime} \implies p \text{ irreducible}$$

We let D be a UFD and $p \in D$ be any irreducible elements.

We let D be a UFD and $p \in D$ be any irreducible elements.

Need to prove p is prime

p irreducible $\implies p \neq 0,\ p \notin U(D)$ and

$$p = ab \implies a \in U(D) \text{ or } b \in U(D)$$

Need to prove if $p | ab \implies p | a$ or $p | b$

Suppose $p | ab$

$$p | ab \implies pc = ab \text{ for some } c \in D$$

if $a = 0 \implies p | a$
if $b = 0 \implies p | a$

Suppose $a, b \neq 0$. Then $ab \neq 0$ (if $ab = 0$, $a \in ZD\{D\} = \{0\}$ ※ $a \neq 0$)

Hence $c \neq 0$.

If $a \in U(D) \implies p | b$ by remark (6)

If $b \in U(D) \implies p | a$ by remark (6)

Let $a, b \notin U(D)$.

Claim: $a, b \notin U(D) \implies c \notin U(D)$

proof:

if $c \in U(D)$. Then $p \sim ab$, where $a, b \notin U(D)$, $a, b \neq 0$

By remark 8; ab is irreducible as an associate of p ※ ■

Now let us apply UFD conditions to a and b

$$a = p_1 \cdots p_m \quad \text{and} \quad b = q_1 \cdots q_n$$

where all p_i with $i = 1, \dots, m$ and q_j with $j = 1 \cdots n$ are irreducible in D. Then

$$pc = ab = p_1 p_2 \cdots p_m q_1 \cdots q_n$$

is a factorization of pc as a factorization of $m+n$ irreducible elements.

But also c factorizes into a product of irreducible elements. Due to (ii), c must have exactly $m+n-1$ irreducible factors while

$$\begin{array}{ccc} p \sim p_i \text{ for some } i \in \{1, \dots, m\} & \text{or} & p \sim q_j \text{ for some } j \in \{1, \dots, n\} \\ \Downarrow & & \Downarrow \\ p \mid a & \text{or} & p \mid b \end{array}$$

$\Longrightarrow$ p prime by definition ■

Theorem

Let D be a principal ideal domain.

D is a PID $\Longrightarrow$ D is a unique factorization domain

Proof:

We know D is a PID. Then

$$p \text{ prime} \iff p \text{ irreducible}.$$

By unique factorization theorem, any decomposition into a product of primes is essentially unique.

So part (ii) of defn of UFD is okay

i) proof by contradiction

Suppose a is not a product of irreducibles

In particular a is not a product of irreducibles. So

$$a = a_1 b_1 \qquad a \in D \setminus \{0\}, \ a, b \notin U(D)$$

a_1 and b_1 cannot be as a product of irreducibles

Suppose a_1 is not a product of irreducibles (w.l.o.g)

$$a_1 = \underset{\substack{\uparrow \ \uparrow \\ \text{not product of irreducibles}}}{a_2 b_2} \qquad a_2, b_2 \neq 0, \ a_2, b_2 \notin U(D)$$

Continuing, we get $a_1, b_1, \cdots, a_i = a_{i+1} b_{i+1}$, each a_i is not a product of irreducibles

Consider $I_i = a_i D$.

Since $a_i = a_{i+1} b_{i+1} \implies a_i \in a_{i+1} D$. Hence we have

$$a_1 D \subseteq a_2 D \subseteq \cdots$$

Let

$$I = \bigcup_{i \in \mathbb{N}} a_i D$$

I a PID. In particular, we have

$$c \in cD = I = \bigcup_{i \in \mathbb{N}} a_i D$$

$c \in cD \implies \exists\, n \in \{1, \cdots, \}$ s.t $c \in a_n D$. Then

$$I_n = a_n D \subseteq I = cD \subseteq a_n D$$

$$\implies I = a_n D$$

$a_{n+1} \in I \implies a_{n+1} \in a_n D \implies a_{n+1} = a_n b$ for some $b \in D$. Hence

$$\cancel{a}_n = a_{n+1} b_{n+1} = \cancel{a}_n b b_{n+1}, \quad a_n \neq 0 \in NZD$$

$$\implies 1 = b b_{n+1}$$

$$\implies b_{n+1} \in U(D) \text{ a unit } \divideontimes$$

A contradiction. Hence a is a product of irreducibles.

$\blacksquare$

19. Prime Ideals

Definition Proper Ideals

Let R be any ring

An ideal of R is proper if $I \neq R$

Prime Ideals

Definition Prime Ideals

Let R be any ring

An ideal P of a ring is prime if

i) P is proper

ii) $\forall a,b \in R$

$$ab \in P \implies a \in P \text{ or } b \in P$$

Examples of prime ideals

(1) If $R \neq \{0\}$ but $ZD(R) = \{0\}$, then $\{0\}$ is prime

(i) ✓

(ii) $ab = 0 \implies a = 0$ or $b = 0$

(2) $R = \mathbb{Z}$ and I be a non-zero ideal of $\mathbb{Z}$

Any ideal of $\mathbb{Z}$ has form $I = n\mathbb{Z}$ for some $n \in \mathbb{N}^0 = \mathbb{N} \cup \{0\}$

I is prime $\iff$ n is prime

proof:

- $n = 0 \implies I = 0\mathbb{Z} = \{0\}$ and we know $ZD(\mathbb{Z}) = \{0\}$. So

  $n = 0 \implies I$ is prime

- $n \in \mathbb{N}$, $n \geq 1$, n not prime. Then

  $$n = ab \qquad 1 < a, b < n$$

  Then $n = n \cdot 1 \in n\mathbb{Z} \implies n \nmid a$, $n \nmid b \implies a \notin I = n\mathbb{Z}$ and $b \notin I = n\mathbb{Z}$

- $n \in \mathbb{N}$ be prime, $n = p > 1$

Consider $I = p\mathbb{Z}$, p prime. pick any $c \in p\mathbb{Z}$. Now

$$c = pz \quad \text{for some} \quad z \in \mathbb{Z}$$

For any $a, b \in \mathbb{Z}$

$$ab \in I \implies p \mid ab \implies p \mid a \text{ or } p \mid b$$
$$\implies a \in I \text{ or } b \in I.$$

Properties of Prime Ideals

(P1) **Theorem**

Let P be any proper ideal of R

$$P \text{ is prime} \iff ZD\left(R/_P\right) = \{0\}$$

Proof:

($\implies$): Suppose P is prime.

Suppose $(a+P)(b+P) = 0+P \implies ab+P = 0+P$
$$\implies ab \in P$$
$$\implies a \in P \text{ or } b \in P \qquad P \text{ prime}$$
$$\implies a+P = 0+P \text{ or } b+P = 0+P$$

($\impliedby$): Suppose $ZD\left(R/_P\right) = \{0\}$. Suppose $ab \in P$

$$(a+P)(b+P) = (ab+P) = 0+P \implies \left\{\begin{matrix} a+P = 0+P \implies a \in P \\ b+P = 0+P \implies b \in P \end{matrix}\right\} \implies \text{prime ideal}$$

(P2) **Corollary**

Let R be any commutative ring with $1 \in R$

ideal P of R is prime $\iff$ $R/_P$ is an ID

Proof:

1) R commutative $\iff a \times b = b \times a$
$$\iff (ab+P) = (ba+P)$$

$\iff R/P$ commutative

2) $ZD\left(R/_P\right) = \{0\}$ by above

3) Showing that $1+P$ is the identity

$(1+P)(a+P) = 1a + P = a+P$

If $1+I = 0+I \implies 1 \in I$

$\implies P = R$ ※ (P is proper)

(P3) Proposition

Let D be an ID. Then $\forall a \in D$

(i) $aD = \{0\} \iff a = 0$

(ii) $aD = D \iff a \in U(D)$

(iii) aD is a non-zero prime ideals of $D \iff a$ is prime

Proof:

i) $(\Leftarrow)$: $a = 0 \implies aD = \{0\}$

$(\Rightarrow)$: Contrapositive:

$a \neq 0 \implies a = a \cdot 1 \in aD$ since $1 \in D$

$\implies aD \neq \{0\}$

ii) $(\Rightarrow)$: Suppose $aD = D \implies x = ad$ for $x \in D = aD$

In particular $1 = ad$ for some $d \implies a$ is a unit

$\implies a \in U(D)$

$(\Leftarrow)$: Suppose $a \in U(D)$

$(\subseteq)$: $x \in aD \implies x = ad$ for some $d \in D$

$\implies x \in D$ by closure on ideals

$(\supseteq)$: Suppose $d' \in D$

$$d' = 1 \cdot d' = a(\underset{\underset{D}{\cap}}{a^{-1}d'}) \in aD$$

iii) By (i), $a \neq 0$, by ii) $a \notin U(D) \Longleftrightarrow aD \neq D$ (proper)

$$\begin{aligned} aD \text{ is prime} &\Longleftrightarrow bc \in aD \Longrightarrow b \in aD \text{ or } c \in aD \\ &\Longleftrightarrow bc = ad \Longrightarrow b = ap \text{ or } c = aq \\ &\Longleftrightarrow a \mid bc \Longrightarrow a \mid b \text{ or } a \mid c \\ &\Longleftrightarrow a \text{ prime} \end{aligned}$$

■

20. Maximal Ideals

Let R be any ring

Maximal Ideals

Definition Maximal Ideals

An ideal M of R is **maximal** if

(i) M is proper, $M \neq R$

(ii) For any ideal $I \subseteq R$

$$M \subseteq I \subseteq R \implies I = M \text{ or } I = R$$

Properties of Maximal Ideals

(M1) **Theorem**

Let R be any commutative ring with $1 \in R$. Let M be any ideal of R. Then

$$M \text{ maximal} \iff R/M \text{ is a field}$$

(M2) **Corollary**

Let D be a PID and $I \neq \{0\}$ be a non-zero ideal. Then

$$I \text{ is maximal} \iff I \text{ is prime}$$

(M3) **Proposition**

Let D be any ID. Then $\forall a \in D \setminus \{0\}$

i) If the ideal aD of D is maximal, then a is irreducible

ii) If D is a PID and a irreducible, then $aD \subseteq D$ is maximal

(M4) **Corollary**

Let R be any commutative ring with an identity 1 and P be any ideal of R

$$P \text{ maximal} \implies P \text{ is prime}$$

Example

Consider $\mathbb{Z}[x]$ Then

i) $\mathbb{Z}[x]$ is a UFD

ii) $\mathbb{Z}[x]$ is not a PID

<u>proof</u>:

(ii) Let $I = 2\mathbb{Z}[x]$

$J = x\mathbb{Z}[x]$

$I+J \subseteq \mathbb{Z}[x]$ is an ideal

<u>Claim</u>: $I+J$ is not principal, i.e.

$I+J \neq f\mathbb{Z}[x] \quad \forall$ fixed polynomials $\mathbb{Z}[x]$

Suppose $I+J = f\mathbb{Z}[x]$

$I \ni 2\cdot 1 \implies 2\cdot 1 = 2 = 2\cdot 1 + x\cdot 0 \in I+J = f\mathbb{Z}$

$0 \neq 2 = fg$ for some $g \in \mathbb{Z}[x]$

$$\deg(2) = 0 = \underset{\substack{\text{\rotatebox{90}{$\leq$}} \\ 0}}{\deg(f)} + \underset{\substack{\text{\rotatebox{90}{$\leq$}} \\ 0}}{\deg(g)} \implies f \text{ is constant}, f \neq 0$$

$x = x\cdot 1 \in J \subseteq I+J = f\mathbb{Z}[x] \implies 1x = fh$ for some $h \in \mathbb{Z}[x]$

$\implies f = \pm 1$ since f is constant

$$\implies 1 = \underset{\substack{\shortparallel \\ f}}{(\pm 1)}(\pm 1) \in f\mathbb{Z}[x]$$

$\implies I+J = \mathbb{Z}[x] \ni 1$

$$\implies 1 = \underset{\substack{\uparrow \\ \text{odd}}}{\,}\,2\underset{\substack{\uparrow \\ \text{has even constant term}}}{u} + xv \quad \text{※}$$

Hence $I+J$ not principal ■

Claim: $I + J$ is maximal.

Take any polynomial $f \in 2R + xR \implies f = 2a_0 + a_1 x + \cdots$

$\implies$ f is polynomials of even constant terms

If $I + J \leq K$ is any bigger ideal, it contains odd constant term polynomial, say

$2k-1 + a_1 x + \cdots\cdots$

By closure of ideals

$$(\underset{\overset{\uparrow}{I+J}}{2k + a_1 x + \cdots\cdots}) - (2k-1 + a_1 x + \cdots) = 1 \in K \implies K = \mathbb{Z}[x]$$

21. Irreducible Polynomials

Let F be any field such as

Eg: $F = \mathbb{R}, \mathbb{C}$, $F = \mathbb{Z}/p\mathbb{Z}$ p prime

We know $R = F[x]$ is a PID $\Longrightarrow$ R is an integral domain

Every ideal I of R has form $I = fR$, $f \in R = F[x]$

Corollary

For any polynomials $f \in F[x]$

f is prime $\Longleftrightarrow$ f is irreducible

i.e.

$\{\text{all primes in } F[x]\} = \{\text{irreducible in } F[x]\}$

Note:

$$\begin{tikzcd} f \text{ is constant} \arrow[r, Leftrightarrow] & f = 0 \arrow[d, Rightarrow] & \text{or} & f \in U(F[x]) \arrow[d, Rightarrow] \\ & \text{no degree} & & \deg(f) = 0 \end{tikzcd}$$

Irreducible Polynomials

Definition

Take $f \in F[x]$ which is irreducible when

i) $f \neq 0$

ii) $f \notin U(F[x]) \Longleftrightarrow f \neq a \in F$ constant polynomial $\Big\}$ $f \neq$ constant

iii) $f = gh$ for some $f = gh$ for $g, h \in F[x]$, then one of the factors are constant

i.e. $f = gh \Longrightarrow f$ or g is a non-zero constant

(f does not factorise into non-constant terms)

Lemma

Let $f \in F[x]$ and $\deg f = 1$. Then

f is irreducible

Proof:

Take $f \in F[x]$ of $\deg f = 1$. Then

$$f = ax + b,\ a \neq 0,\ b \in F \implies f \neq \text{constant}$$

Suppose $f = ax + b = gh \implies \deg(gh) = \deg(g)\deg(h) = 1$

Either $\deg(g) = 1,\ \deg(h) = 0 \rightarrow h$ non-zero const

$\deg(g) = 0,\ \deg(h) = 1$

g non-zero const

$\implies f$ is irreducible ∎

Lemma

Let $f \in F[x]$ such that $\deg f = 2$ or 3

Then f is irreducible $\iff$ f has no root in F

$(f(a) \neq 0 \quad \forall a \in F)$

Proof: both ways contrapositive

$(\implies)$: Suppose f has a root. We will show f is not irreducible.

$\exists\, a \in F$ s t $f(a) = 0$. Let us divide by $(x-a)$ with a remainder

$$f = (x-a)q + r \quad \text{where} \quad \underbrace{\underbrace{r = 0}_{\text{zero const}} \quad \text{or} \quad \underbrace{r \neq 0 \text{ but } \deg(r) < 1}_{\text{non-zero const}}}_{r \text{ is a const}}$$

$$0 = f(a) = 0q + r \implies r = 0$$

$$2,3 = \deg f = \underbrace{\deg(x-a)}_{1} + \deg q = 1,2 \ \Big| \implies f \text{ is not irreducible}$$

$(\impliedby)$: Suppose f is not irreducible. Need to prove f has a root

So $f = uv$, u, v are non-constant polynomials

$$2,3 = \deg(f) = \underset{\substack{\rotatebox{90}{$\leq$} \\ 1}}{\deg(u)} + \underset{\substack{\rotatebox{90}{$\leq$} \\ 1}}{\deg(v)} \implies \deg(u) = 1 \text{ or } \deg(v) = 1$$

Suppose $\deg u = 1 \implies u = cx + d$, where $c \neq 0 \implies c^{-1} \in F$

$$f = (cx+d)v = c(x + c^{-1}d) \implies x = c^{-1}d, \text{ then } x \text{ is a root}$$

Similar for $\deg v = 1$

∎

① Consider the principal ideal $I = fF[x]$

Then by (M1)

I is prime $\iff$ maximal by (M1)

② Now consider quotient ring:

$$F[x]/I \quad \text{where} \quad I = fF[x]$$

By (M3) $F[x]/I$ is a field

Classification Theorem

Theorem

Let G be any finite field.

(i) The multiplicative group $U(G) = G \setminus \{0\}$ is cyclic

(ii) All finite fields G with the same number of elements $|G|$ are isomorphic as rings

(iii) The number $|G| = p^n$ for some prime p, $n \in \mathbb{N}$

(iv) For any prime p, there exists an irreducible polynomial $f \in \mathbb{Z}/p\mathbb{Z}[x]$ of degree n such that the field

$$(\mathbb{Z}/p\mathbb{Z})[x]/I \text{ has size } p^n \text{ and } I = f(\mathbb{Z}/p\mathbb{Z})[x]$$

Proposition

Let $f \in F[x]$ be irreducible. Put $I = fF[x]$. Then

$$F[x]/I \text{ is a field.}$$

Moreover, the map

$$\theta : F \longrightarrow F[x]/I$$

$$a \longmapsto a + I$$

is a one-to-one homomorphism, $F = \mathrm{Im}\,\theta \leq D/I$

Proof:

By the proposition (M3), $I = fF[x]$ of $F[x]$ is maximal. Then by theorem (M1),

$$F[x]/_{I} \text{ is a field}$$

homomorphism: Proved in Factor Rings chapter

one-to-one: Take any $a, b \in F$ such that $\theta(a) = \theta(b)$

$$\theta(a) = \theta(b) \iff a + I = b + I$$

$$\iff a - b \in I = fF[x]$$

$$\iff a - b = fg$$

If $a - b \neq 0$

$$0 = \deg(a-b) = \deg(fg) = \deg f + \deg g > 0 \quad ⨳ \quad \text{since } f \text{ not constant}$$

$$\iff a = b$$

∎

In particular, $\theta : \mathbb{Z}/p\mathbb{Z} \to (\mathbb{Z}/p\mathbb{Z})[x]/_{f(\mathbb{Z}/p\mathbb{Z})(x)}$

$$D/_{I} \supseteq \operatorname{Im}\theta \cong \mathbb{Z}/p\mathbb{Z}$$

Example

Suppose that $f = cx + d$ where $c, d \in F$ and $c \neq 0$.

Then f is irreducible by Lemma pg 80 and by proposition pg 81, the factor ring

$$F[x]/_{fF[x]} \text{ is a field.}$$

Claim: $F[x]/_{fF[x]} \cong F$

Already shown for $I = fF[x]$, the map

$$\theta : F \to F[x]/_{I} : a \mapsto a + I$$

is one-to-one homomorphism.

Onto: By division algorithm for $F[x]$, $u \in F[x]$ can be written as

$$u = (cx + d)q + r$$

where the remainder $r \in F$ is constant

$$(cx+d)q \in I \implies u+I = r+I$$

Theorem

Let $n \in \mathbb{N}$ and F be any field

Let $f \in F[x]$ be an irreducible polynomial of degree n, $\deg(f)=n$. Put $I = fF[x]$

i) Then the ring

$$F[x]/fF[x] \text{ is a vector space}$$

over the field F of dimension n under the operation

$$(u+I)+(v+I)=(u+v)+I$$

$$a \times (u+I) = au + I$$

$\forall\, u,v \in F[x]$ and $a \in F$

ii) The vector space $F[x]/I$ has a basis

$$1+I,\ x+I,\ \cdots,\ x^{n-1}+I \qquad (*)$$

Proof $(D = F[x],\ I = fF[x])$

(i) Let us make our set D/I a vector space over F

Vector space structure

$$\forall a \in F,\ \forall u,v \in D \quad (u+I)+(v+I)=(u+v)+I$$

$$a(u+I) = au+I$$

Rings axioms $\implies$ vector space axioms

(ii) Take any $u \in F[x]$ and divide f with a remainder r

$u = fq + r$ where $q \in F[x]$ and either $r=0$ or $r=0$ or $r \neq 0$

$\deg(r) < \deg f = n$

$D/I \ni u+I = \underset{\uparrow \atop I=fD}{\boxed{fq}} + r + I = r+I$, here r is a linear combination (with coefficients from F) of $1, x, x^2, \cdots, x^{n-1}$

$\Longrightarrow$ (*) a spanning set D/I

$$r = a_0 + a_1x + \cdots + a_{n-1}x^{n-1}, \quad a_0, a_1, a_2, \cdots, a_{n-1} \in F$$

Since $u + I = r + I$,

$$F[x]/I = \{(a_0 + a_1x + \cdots + a_{n-1}x^{n-1}) + I : a_i \in F\}$$

$$= \{a_0(1+I) + a_1(x+I) + \cdots + a_{n-1}(x^{n-1}+I) : a_i \in F\}$$

$\Longrightarrow$ $1+I,\ x+I,\ \cdots,\ x^{n-1}+I$ span $F[x]/I$.

Finally need to prove that (*) is linearly independent in D/I

Suppose

$$a_0(1+I) + a_1(x+I) + \cdots + a_{n-1}(x^{n-1}+I) = 0+I$$

$$\Longleftrightarrow (a_01+I) + (a_1x+I) + \cdots + (a_{n-1}x^{n-1}+I) = 0+I$$

$$\Longleftrightarrow (a_0 + a_1x + \cdots + a_{n-1}x^{n-1}) + I = I$$

$$\Longleftrightarrow (a_0 + a_1x + \cdots + a_{n-1}x^{n-1}) \in I = fF[x]$$

Hence

$$\underbrace{a_0 + a_1x + \cdots + a_{n-1}x^{n-1}}_{\text{suppose this is } \neq 0} = fg \text{ for some } g \in F[x]$$

$$n > \deg(a_0 + \cdots + a_{n-1}x^{n-1}) = \underset{\overset{\|}{n}}{\deg f} + \underset{\overset{\vee\!|}{0}}{\deg g} \geq n \ \text{⨳}$$

$$\Longrightarrow a_0 + a_1x + \cdots + a_{n-1}x^{n-1} = 0$$

$$\Longrightarrow a_0 = a_1 = a_2 = \cdots = a_{n-1} = 0$$

$\Longrightarrow$ (*) is linearly independent ■

22. Examples of Irreducible Polynomials

Let F be a field and $f \in F[x]$ be irreducible. Consider the field

$$F[x]/I \ , \quad I = f F[x]$$

Let $\boxed{X = x + I}$. Then for any $g = b_0 + b_1 x + \cdots b_m x^m \in F[x]$, its coset in $F[x]/I$ equals

$$g(X) = b_0 + b_1(x+I) + \cdots + b_m(x+I)^m$$

Examples

(1) $F = \mathbb{R}$ and $f \in \mathbb{R}[x]$

$f = x^2 + 1$ irreducible $\iff$ $f(a) \neq 0 \quad \forall a \in R$

(Lemma 2)

New field $\mathbb{R}[x] / (x^2+1)\mathbb{R}[x]$

$$1 + I \ , \quad x + I = X \quad \text{is a basis}$$

Any element of our new field is

$$a(1+I) + b(x+I) = a(1+I) + bX$$

New field contains $\mathbb{R}$ as a subring

$$\{ a(1+I) = a \in I \mid a \in \mathbb{R} \}$$

Further

$$X^2 = (x+I)^2 = x^2 + I = (x^2+1) - 1 + I = -1 + I$$

$$\Rightarrow X^2 = -1 \quad \text{in new field}$$

We can define a ring isomorphism

$$\text{"new field"} \longrightarrow \mathbb{C}$$

$$a(1+I) + bX \longmapsto a + bi$$

(2) $F = \mathbb{Q}$; $f = x^3 - 2$ irreducibles $f(a) \neq 0 \quad \forall a \in \mathbb{Q}$

Consider $a^3 - 2 = 0 \iff a = \sqrt[3]{2} \notin \mathbb{Q}$. So irreducible in $\mathbb{Q}[x]$

New field $\mathbb{Q}[x]/f\mathbb{Q}[x]$ has basis over $\mathbb{Q}$ of $1+I$, $\underset{X}{\underset{\shortparallel}{x+I}}$, $\underset{X^2}{\underset{\shortparallel}{x^2+I}}$

Suppose $X, Y \in \mathbb{Q}[x]/f\mathbb{Q}[x]$, $a, b \in \mathbb{Q}$

Our addition and multiplication are $\mathbb{Q}$-linear

$(aY+bZ)+(a'Y'+b'Z') = aY + a'Y' + bZ + b'Z'$ $\forall Y, Z \in$ new field Y', Z'

$(aY+bZ)(a'Y'+b'Z') = aa'YY' + ab'YZ' + ba'ZY' + ab'Y'Z'$

Therefore enough to compute addition and multiplication for basis cosets

$+$ $Y \backslash Z$	1	X	X^2
1	2	$X+1$	$1+X$
X	$X+1$	$2X$	$X+X^2$
X^2	X^2+1	X^2+X	$2X^2$

$\times$ $Y \backslash Z$	1	X	X^2
1	1	X	X^2
X	X	X^2	2
X^2	X^2	2	$2X$

$X \times X^2 = X^3 = (x+I)^3 = x^3 + I = (x^3-2) + 2 + I = 2 + I$

$X^2 \times X^2 = X^4 = X^3 \times X = 2X$

(2) $F = \mathbb{Z}/2\mathbb{Z} = \{[0], [1]\}$

Calculating irreducible polynomials in $F[x]$

Take any $f \in F[x]$ of degree 2

$$f = [1]x^2 + ax + b1$$

f is irreducible $\implies b \neq [0] \implies b = [1]$ $(b = [0] \implies f(0) = [0])$

Hence

$f = [1]x^2 + ax + [1] \implies$ 1) $f = [1]x^2 + [1]$

2) $f = [1]x^2 + [1]x + [1]$

1) $f([1]) = [1] + [1] = [0]$

2) $\left.\begin{array}{l} f([0]) \neq 0 \\ f([1]) \neq 0 \end{array}\right\} \implies$ irreducible by Lemma 2

The field $F[x]/_I$ has $2^2 = 4$ elements. They are

$$[0]+I, \; [1]+I, \; x+I, \; ([1]+x)+I$$

New notation:

$$[0]+I = [0]$$

$$[1]+I = 1$$

$$x+I = X$$

All elements take form,

$$aX + b$$

Drawing tables

+	0	1	X	X+1
0	0	1	X	X+1
1	1	0	X+1	X
X	X	X+1	0	1
X+1	X+1	X	1	0

x	0	1	X	X+1
0	0	0	0	0
1	0	1	X	X+1
X	0	X	X+1	1
X+1	0	X+1	1	X

$$X^2 = x^2 + I = x^2 + x + [1] - (x - [1]) + I = -x - [1] + I = x + [1] + I$$