MAT3004 Abstract Algebra I

Date: June 15, 2024

Steins;Gate

—El Psy Kongroo—

Contents

Chapter preliminary notes

Theorem 1.1 (Euclidean algorithm)

we can use Euclidean algorithm to find the greatest common divisor of 2 or more than 2 integers.

♡

Theorem 1.2 (bezout's theorem)

if $gcd(\alpha, \beta) = m$, then there are integers p,q s.t. $p\alpha + q\beta = m$

♡

Definition 1.1 (equivalence relation$\alpha \sim \beta$)

an equivalence relation on a set S is a set R of ordered pairs of elements of S s.t.

(a). $(a, a) \in R$ *for all* $a \in S$ *(reflexive property)*

(b). $(a, b) \in R$ *implies* $(b, a) \in R$ *(symmetric property)*

(c). $(a, b) \in R$ *and* $(b, c) \in R$ *imply* $(a, c) \in R$ *(transitive property)*

♣

Chapter Introduction

Definition 2.1

The systems $\mathbb{Z}, \mathbb{C}, \mathbb{R}, \mathbb{Q}$ are equipped with $(+)$ and $(\times)$: all elements in the system satisfy the following operations:

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

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

3. $a+b = b+a$

4. $ab = ba$

5. $a(b+c) = ab+bc$

♣

Definition 2.2 ($\mathbb{Z}_n$)

$\mathbb{Z}_n := \{0(modn), 1(modn), ..., (n-1)(modn)\}$, *which is the collection of remainders of integers upon division by n.*

♣

Remark $\mathbb{Z}_n$ is different from $\mathbb{Z}_n^*$!!! $\mathbb{Z}_n^* := \{[a] | 0 < a < n, gcd(a,n) = 1\}$. recall $[a]$:= a(modn)

Remark $\mathbb{Z}_n$ is equipped with + and $\times$.

✍ **Exercise 2.1** show that $\mathbb{Z}_n$ is equipped with + and $\times$.

Chapter Def of Group

Definition 3.1 (binary operation)

let S be a set. a binary operation $*$ on S is a function $*: S * S \longrightarrow S$

♣

Definition 3.2 (closeness)

let $(S, *)$ be a binary operation. for any subset $T \subset S$, we say T is closed under $*$ if $\forall t_1, t_2 \in T$ we have $t_1 * t_2 \in T$ and thus $(T, *)$ is also a binary operation.

♣

Example 3.1 any vector subspace $W \subset \mathbb{R}^2$ is closed under $+$, and the set $\{(x, y) : xy \geq 0, x, y \in \mathbb{R}\}$ is not closed under $+$.

Definition 3.3 (group)

a group $(G, *)$ is a set with a binary operation $*$ satisfying

1. *(associativity): $(a * b) * c = a * (b * c)$*
2. *(identity): there is an element $e \in G$ s.t. $e * a = a * e = a$ for all $a \in G$*
3. *(inverse): for all $b \in G$, there exists $b^{-1} \in G$ s.t. $b^{-1} * b = b * b^{-1} = e$*

♣

Example 3.2 $(\mathbb{Z}, +)$ is a group: check

1. $(a + b) + c = a + (b + c)$
2. take $e = 0$, we have $0 + a = a + 0 = a$
3. for any $b \in \mathbb{Z}$, take $b^{-1} = -b$: we have $(-b) + b = b + (-b) = 0$

Example 3.3

1. $(\mathbb{Z}, \times)$ is not a group since we cannot find the inverse for element other than 1 and -1
2. $(\mathbb{Q}, \times)$ is not a group since 0 has no inverse in $\mathbb{Q}$
3. $(\mathbb{Q}^*, \times)$ is a group, where $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$

Example 3.4 $(S, \circ)$ is a group, where $S = \{f : T \longrightarrow T \text{ is a bijection}\}$ and $\circ$ is the operation of composition of maps

Example 3.5

1. $(M_{2\times 2}(\mathbb{R}), +)$ is a group, $e = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$
2. $(M_{2\times 2}(\mathbb{R}), \times)$ is not a group, we can show that elements in $M2 \times 2$ are associative and the identity is $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ but we notice that $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ has no inverse.
3. $GL(2, \mathbb{R}) := \{A \in M_{2\times 2}(\mathbb{R}) | det(A) \neq 0\} = \{\text{all invertible matrices}\}$ then $(GL(2, \mathbb{R}), \times)$ is a group.
4. $(\mathbb{Z}_n, +)$ is a group: $e = [0]_n$, $[a]_n^{-1} = [-a]_n = [n - a]_n = [2n - a]_n = \ldots$
5. $(\mathbb{Z}_n, \times)$ is not a group: inverse of $0 \in \mathbb{Z}_n$ may not exist.

Remark we wonder given n, which $[a]_n$ has an inverse? the answer is that

$$[a]_n^{-1} \text{ exists} \Leftrightarrow gcd(a, n) = 1$$

Proof $(\longleftarrow)$: by bezout's theorem, $gcd(a, n) = 1 \longrightarrow \exists p, q$ s.t. $ap + bq = 1$ so we have $[ap + bq]_n = [1]_n = e$ we have $[p]_n[a]_n + [q \cdot n]_n = e \longrightarrow [p]_n[a]_n = e \longrightarrow [a]_n^{-1} = [p]_n$

Example 3.6 let $\mathbb{Z}_n^* = \{[a]_n | gcd(a, n) = 1\}$, then $(\mathbb{Z}_n^*, *)$ is a group. e.g. $\mathbb{Z}_8 = \{[1]_8, [3]_8, [5]_8, [7]_8\}$

Remark

1. we write ab or $a \cdot b$ instead of $a * b$ for short
2. we say the operation $*$ is abelian or commutative if $a * b = b * a$ for all $a, b \in G$. e.g. $(GL(2, \mathbb{R}), \times)$ is not abelian and $(\mathbb{Z}^*, *)$ is abelian.

Chapter Properties of Group

let $(G, *)$ be a group,

1. the identity element $e \in G$ is unique. i.e., if $e, e' \in G$ satisfy $ae = ea = a$ and $ae' = e'a = a$ for all $a \in G$, we have $e = e'$

   Proof put $a = e'$ first, we have $e' \cdot e = e \cdot e' = e'$ and put $a = e$ in the second equation, we have $ee' = e'e = e$ so we have $e' = ee' = e$
2. for each $g \in G$ $g^{-1} \in G$ is unique

   Proof if $gh = hg = e$ and $gh' = h'g = e$, we prove that $h' = h$: we have

   $$h = he = h(gh') = (hg)h' = eh' = h'$$

   we are done
3. for each $a \in G$, $\{ag|g \in G\}$ are distinct: i.e., if $g \neq h$, we have $ag \neq ah$

   Proof we use contrapositive statement: if $ag = ah$, we prove that $g = h$:

   $$ag = ah \to a^{-1}ag = a^{-1}ah \to (a^{-1}a)g = (a^{-1}a)h \to eg = eh \to g = h$$

Remark $\{ga|g \in G\}$ is also distinct: if $g \neq h$, then $ga \neq ha$

Definition 4.1 (cancellation)

for a group $(G, *)$, we say the operation $*$ is of cancellation if we have

$$c * a = c * b \to a = b \text{ for } \forall a, b, c \in G$$

♣

there is a proposition for finite group:

Proposition 4.1

for a finite set G, if we can define the operation $*$ on the set G, and the operation $*$ is of associativity, then we have

$$* \text{ has cancellation} \Leftrightarrow (G, *) \text{ is a group}$$

♠

Proof $(\to)$: we need to show $(G, *)$ has identity and inverse for all element in G.

1. (identity): note G is finite, consider $\forall a \in G$, $\langle a \rangle \subset G$, we have

   $$a^i = a^j \text{ for some } i > j$$

   and

   $$a^f := a^{i-j} \to \forall b \in G, a^f b = a^{i-j} b \to a^j a^f b = a^j a^{i-j} b = a^i b$$

   with cancellation, we have

   $$a^f b = b \to a^f \text{ is a left identity}$$

   similarly we can prove a^f is a right identity. we are done.
2. (inverse): $\forall a \in G$, $\langle a \rangle \subset G$, we have $a^f = e \to a^{f-1}a = a \cdot a^{f-1} = e$, we are done.

$(\leftarrow)$: for a group $(G, *)$, we want to prove $*$ is of cancellation. if $ac = bc$, consider the inverse c^{-1}, we have $acc^{-1} = bcc^{-1} \to ae = be \to a = b$ and $ca = cb$ is similar. we are done.

Chapter Cayley table

Definition 5.1 (order of group)

let $(G,*)$ be a group. the order of G, $ord(G)$ or $|G|$ is defined to be the number of elements in G

Definition 5.2 (cayley table)

let G be a finite group, i.e. $|G| < \infty$, then the cayley table of G is a table with rows and columns labelled by elements of G, for $a, b \in G$, the (a, b) entry of the table is equal to $a * b$

Example 5.1 let the group be $\mathbb{Z}_3, +$, the cayley table is

	$[0]_3$	$[1]_3$	$[2]_3$
$[0]_3$	$[0]_3$	$[1]_3$	$[2]_3$
$[1]_3$	$[1]_3$	$[2]_3$	$[0]_3$
$[2]_3$	$[2]_3$	$[0]_3$	$[1]_3$

Example 5.2 let the group be $\mathbb{Z}_8^*, \times$, the cayley table is

	$[1]_8$	$[3]_8$	$[5]_8$	$[7]_8$
$[1]_8$	$[1]_8$	$[3]_8$	$[5]_8$	$[7]_8$
$[3]_8$	$[3]_8$	$[1]_8$	$[7]_8$	$[5]_8$
$[5]_8$	$[5]_8$	$[7]_8$	$[1]_8$	$[3]_8$
$[7]_8$	$[7]_8$	$[5]_8$	$[3]_8$	$[1]_8$

Proposition 5.1

the rows and columns of any cayley table have distinct entries, so it contains all elements of G

Proof check the property 3. of a group and the remark

Example 5.3

Chapter Subgroup

Definition 6.1 (subgroup)

let $(G, \circ)$ be a group. a subset $H \in G$ is a subgroup of G if $(H, \circ_{|H \times H})$ forms a group. ♣

Proposition 6.1

a subset $H \in G$ is a subgroup $\Leftrightarrow$ the following holds:
1. $\forall h_1, h_2 \in H, h_1 \circ h_2 \in H$
2. $\forall a \in H, a^{-1} \in H$. ♠

Proof we need to prove that H is a group:

1. we show that $*|_{H\times H} : H \times H \longrightarrow H$ is a binary operation $(*)$ is closed in H
2. (associatity): $(a * b) * c = a * (b * c)$ holds for $\forall a, b, c \in H \subset G$
3. (identity): $e \in G$ is indeed an element in H
4. (inverse): by the condition, we know the inverse must exists.

Proposition 6.2

G is a group. a nonempty subset H of G is a subgroup if the following holds:

$$a, b \in H \Rightarrow ab^{-1} \in H$$

♠

Proof

Example 6.1

1. $G = (\mathbb{Z}, +), H = 2 * x|x \in \mathbb{Z}$, then $H \leqslant G$
2. $H = k\mathbb{Z}$, k is any positive integer, then $H \leqslant G$
3. $H =$ all odd integer, then $H \nleqslant G$
4. $G = (GL(n, \mathbb{R}), \times), H = SL(n, \mathbb{R}) := \{A \in GL(n, \mathbb{R})|det(A) = 1\}$, then $H \leqslant G$
5. $(\mathbb{Z}, +) \leqslant (\mathbb{Q}, +) \leqslant (\mathbb{R}, +) \leqslant (\mathbb{C}, +)$
6. $G = (\mathbb{Z}_8, +), H = \{[0], [3]\}$, then $H \nleqslant G$, $H' = \{[0], [4]\}, H \leqslant G$

Definition 6.2 (proper subgroup)

let $(G, *)$ be a group, a proper subgroup of G is $H \leqslant G$ with $H \neq G$ ♣

Definition 6.3 (trivial subgroup)

let (G,∘) be a group, a proper subgroup of G is $H = \{e\} \leqslant G$. ♣

Definition 6.4 (characteristic)

$\mathcal{F}$ is a field, then the characteristic of $\mathcal{F}$ is the smallest positive integer m s.t. $1_{\mathcal{F}} + \ldots + 1_{\mathcal{F}} = 0_{\mathcal{F}}$ and $char(\mathcal{F}) := m$; if no such m exists, we let $char(\mathcal{F}) = \infty$ ♣

Proposition 6.3

in a group G, let the order of the element a be n, we have:

1. $a^m = e \Leftrightarrow n|m$
2. $\forall k \in \mathbb{N}$, *the order* $|a^k| = \frac{n}{gcd(n,k)}$

♠

Chapter Cyclic Group

Definition 7.1 (cyclic subgroup)

let $(G, \circ)$ be a group, the cyclic subgroup generated by $g \in G$ is the subgroup $\langle g \rangle := \{g^m | m \in \mathbb{Z}\}$

♣

Definition 7.2 (cyclic group; generator)

let G be a group, we say G is a cyclic group if $\exists g \in G$ s.t. $G = \langle g \rangle$. we say that g is a generator of G.

♣

Remark G is called to be generated by a set X if G is the smallest group that contains all elements in $X := \{g^m | m \in \mathbb{Z}\}$, which means that every element of G can be obtained by multiplication or inverse operations on the set $X := \{g^m | m \in \mathbb{Z}\}$

Example 7.1 $(\mathbb{Z}_8, +)$ is cyclic

Proof because $\mathbb{Z}_8 = \langle [1] \rangle$

Example 7.2 $(GL(n, \mathbb{R}, \times)$ is not cyclic.

Proof there are uncountably many elements in the set $GL(2, \mathbb{R})$, but clearly $\langle g \rangle$ is countable.

Example 7.3 $(\mathbb{Z}_8^*, \times)$ is not cyclic.

Proof just check every element in $\mathbb{Z}_8^*$ is not a generator of $\mathbb{Z}_8^*$.
(find out what is $\mathbb{Z}_8^*$ first!!!) ——$\mathbb{Z}_8^* = \{[1], [3], [5], [7]\}$
1.$\langle [1] \rangle = \{e\}$
2.$\langle [3] \rangle = \{[3], [1]\}$
3.$\langle [5] \rangle = \{[5], [1]\}$
4.$\langle [7] \rangle = \{[7], [1]\}$

✍ **Exercise 7.1from HW2** show that $(\mathbb{Z}_5^*, \times)$ is cyclic.

Proof we know that $\mathbb{Z}_5^* = \{[1], [2], [3], [4]\}$.
$\langle [1] \rangle = \{e\}$
$\langle [2] \rangle = \{[2], [4], [3], [1]\}$. so we find a generator.

Chapter Order

Definition 8.1 (order)

let G be a group. the order of an element $g \in G$ is equal to the order of the cyclic subgroup $\langle g \rangle$. in other words, the order of g is the smallest positive integer m s.t. $g^m = e$.

Remark recall that the order of a group G is the size of the set G.

Example 8.1

1. in $(\mathbb{Z}_8, +)$, $ord([4]) = 2, ord([6]) = 4, ord([1]) = 8.$ recall that $\mathbb{Z}_n := \{0(modn), 1(modn), ..., (n-1)(modn)\}$
2. $(GL(2,\mathbb{R}), \times) : \langle(\begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix})\rangle, \langle(\begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix})\rangle$ as $(\begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix})^{-1} = (\begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix})$ so the order is 2.
3. $\{\langle(\begin{matrix} 1 & 1 \\ 0 & 1 \end{matrix})\rangle = (\begin{matrix} 1 & 1 \\ 0 & 1 \end{matrix})^m | m \in \mathbb{Z}\} = \{(\begin{matrix} 1 & m \\ 0 & 1 \end{matrix}) | m \in \mathbb{Z}\}$, the order is ∞

Chapter Permutation Group

Definition 9.1 (permutation group S_n)
A permutation of X_n is a bijective map: $\sigma : X_n \longrightarrow X_n$. The permutation group is a collection of all permutation of X_n.

Remark note that X_n is a set!

Proposition 9.1
$(S_n, \circ)$ is a group.

Proof (closeness): $\circ : S_n \times S_n \longrightarrow S_n$ is closed since composition of 2 bijective maps is still bijective.
(associativity): $(\sigma_1 \circ \sigma_2) \circ \sigma_3 = \sigma_1 \circ (\sigma_2 \circ \sigma_3)$ holds since composition of maps is associative.
(identity): $e : 1 \longrightarrow 1, 2 \longrightarrow 2, \ldots, n \longrightarrow n : X_n \longrightarrow X_n$ satisfies:$\sigma \circ e = e \circ \sigma = \sigma, \forall \sigma \in S_n$.
(inverse): since $\sigma \in S_n$ is bijective, it must have $\sigma^{-1} \in S_n$ s.t. $\sigma^{-1} \cdot \sigma = \sigma \cdot \sigma^{-1} = e$

Remark Groups are used to study "symmetry". S_n is used to study the symmetry of n identical objects.

we want to study the calculation on S_n.

Definition 9.2 (cycle notation)
let $1 \leq i_1, i_2, \ldots \leq n$. a k-cycle: $(i_1, i_2, \ldots, i_k)$ is an element σ in S_n satisfying: $\sigma(i_{k-1}) = i_k$ and for $\forall j \notin i_1, i_2, \ldots, i_k, \sigma(j) = j$.

Example 9.1 $\tau := (1, 3, 2)$ in S_5

we have $\tau(1) = 3$, $\tau(3) = 2$, $\tau(2) = 1$, $\tau(4) = 4$, $\tau(5) = 5$.

Remark we can multiply (k-cycle) and (l-cycle) by composition of function.

Proposition 9.2
$(i_1, i_2, \ldots, i_k) = (i_2, i_3, \ldots, i_k, i_1) = \ldots$

Proposition 9.3
all $\sigma \in S_n$ can be written as product of disjoint cycles: $\sigma = \gamma_1\gamma_2 \ldots \gamma_n$, γ_i are cycles with no repeated entries among them.

Example 9.2 $(1)(2, 3)(4)$ are disjoint cycles.

Proposition 9.4
if γ_1 and γ_2 are two disjoint cycles, then $\gamma_1\gamma_2 = \gamma_1\gamma_2$

Proposition 9.5
let γ be a k-cycle in S_n, then $ord(\gamma) = k$. e.g. let $\gamma = (1342)$, we check $\gamma^2 = (14)(23)$, $\gamma^3 = (1243)$, $\gamma^4 = (1)(3)(4)(2) = e$, $ord(\gamma) = 4$

Proof

Example 9.3 $\gamma = (1, 3, 4, 2)$. then $\gamma^2 = (1, 3, 4, 2) \cdot (1, 3, 4, 2) = (1, 4)(3, 2)$, $\gamma^3 = (1, 4)(3, 2)(1, 3, 4, 2) = (1, 2, 4, 3) \neq e$, $\gamma^4 = (1, 3, 4, 2)(1, 2, 4, 3) = (1)(2)(3)(4) = e$. so we conclude that $\text{ord}(\gamma) = 4$.

Proposition 9.6

the inverse of a k-cycle $(i_1, i_2, \ldots, i_k)^{-1} = (i_1, i_k, i_{k-1}, \ldots, i_3, i_2)$

Proof ?need to check by oneself.

Chapter transposition

Definition 10.1 (transposition)

a 2-cycle $(i, j) \in S_n$ is called a transposition.

♣

Proposition 10.1

every $\sigma \in S_n$ can be written as a product of transpositions. (not necessary to be distinct)

♠

Proof if $\sigma = (a_1 a_2 ... a_k)$ is a k-cycle, we note that $\sigma = (a_1 a_k)...(a_1 a_3)(a_1 a_2)$ and in general all $\sigma \in S_n$ can be written as a product of disjoint cycles: $\sigma = (i_1...i_k)(j_1...j_l) = (i_1 i_k)(i_1 i_{k-1})...(i_1 i_2)(j_1 j_l)...(j_1 j_2)$

Remark the expression of $\sigma \in S_n$ into product of transportation is not unique. however, the number of transpositions in each expression must be odd or even.

Theorem 10.1

let $\sigma = \tau_1 \tau_2 ... \tau_k = \tau'_1 \tau'_2 ... \tau'_l$, where τ_i and τ'_l are transpositions, then $k = l mod(2)$.

♡

to prove the theorem, we need the following lemma:

Lemma 10.1

$e = \tau_1 \tau_2 ... \tau_k$, then k is even. $(*)$

♡

Proof we do induction on k:

1. if $k = 0$: $\sigma = e =$ product of 0 transportation
2. if k = 1: $\sigma = e \neq \tau_1$ for any transportation τ_1
3. by induction, suppose $(*)$ holds for $k \leqslant m \in \mathbb{Z}$. if $k = m + 1$, suppose $e = \tau_1 ... \tau_{m+1}$, $\tau_{m+1} = (a, b)$
   (a). if $\tau_m = (a, b)$, then $\tau_m \tau_{m+1} = e$

then we are ready to prove the theorem

Proof

Chapter Alternating Group

Definition 11.1 (even(odd))

an element $\sigma \in S_n$ is called even (or odd) if σ can be expressed into an even (or odd) number of transpositions. ♣

Remark any transposition is odd

a permutation $\sigma = \tau_1\tau_2...\tau_k$, where τ_i are transposition, then k and σ have the consistent parity.

Definition 11.2 (alternating group)

the alternating group A_n is a subgroup of S_n consisting of all even permutations σ. ♣

Proposition 11.1

$|A_n| = \frac{|S_n|}{2} = \frac{n!}{2}$ *for* $n \geqslant 1$. ♠

Proof

Example 11.1 A_4 is the "rotation" symmetries of a tetrahedron. (it does not include reflection symmetries.)

Chapter Dihedral Group

Definition 12.1

before giving the complete definition, we say that dihedral group describes the symmetries of a regular n-(poly)gons: n rotations and n reflections. ♣

Proposition 12.1

$|D_n| = 2n$ ♠

Definition 12.2 (principal s and principal r)

the principal reflection s of an n-gon is the reflection among the axis passing through "vertex 1" the principal rotation r is the rotation by $\frac{2\pi}{n}$ *radians.* ♣

Claim 12.0.1. $r^l \cdot s$ *is a reflection along the axis by rotating the principal axis of reflection by* $l \cdot \frac{\pi}{n}$

Proof

✍ **Exercise 12.1** show that in D_n, $r^l s = sr^{n-l}$.

Definition 12.3 (Dihedral group)

the dihedral group D_n *is* $\{e, r, r^2, ..., r^{n-1}, s, rs, r^2 s, ...r^{n-1} s\}$. *the multiplication of* D_n *satisfies:*$D_n\{rs|r^n = e, s^2 = e, r^l s = sr^{n-l}\}$ ♣

Proposition 12.2

every element in D_n *has order 2.* ♠

Proposition 12.3

we can reduce all elements of the form: $r^a s^b r^c s^d r^e s^f ... \in D_n$ *into one of the 2n elements in* D_n ♠

Example 12.1 in D_5, we can show that $r^6 s^{-5} r^3 s^4 = sr^2$

Definition 12.4 (product of groups)

let $G_1, ...G_k$ *be groups, we define the (exterior) product of* $G_1, ...G_k$ *as* $G_1 \times G_2 \times ... \times G_k := (g_1, ..., g_k)|g_1 \in G_1, ...g_k \in G_k$ ♣

Remark[multiplication of elements] $(g_1, ...g_k)(h_1, ...h_k) = (g_1 h_1, g_2 h_2, ...g_k h_k)$

Chapter Homomorphisms and isomorphisms

first give one example as motivation:

Example 13.1 consider two groups: $(\mathbb{Z}_2 \times \mathbb{Z}_2, *) \leftrightarrow (\mathbb{Z}_8^*, \star)$:
$(0,0) \leftrightarrow 1$
$(1,0) \leftrightarrow 3$
$(0,1) \leftrightarrow 5$
$(1,1) \leftrightarrow 7$
we find that $(1,0) * (1,1) = (2,1) = (0,1)$ and $3 \star 7 = 5(mod 8)$: we find this "identification between two groups respects multiplication"

Definition 13.1 (homomorphism and isomorphism)
let $(G, *)$ and $(H, \star)$ be groups, a homomorphism $\phi : G \longrightarrow H$ is a map that "respects" multiplications, i.e. $\phi(g_1 * g_2) = H_1 \star H_2$, if ϕ is a bijective homomorphism, ϕ is called an isomorphism $(\cong)$ ♣

Example 13.2 examine that $\phi : D_4 \longrightarrow S_4$ is a homomorphism

Example 13.3 show that $\phi : D_n \longrightarrow S_n$ is an injective homomorphism. e.g. $\phi(r) = (12...n)$ and $\phi(s) = (2n)(3, n-1)$, s is the reflection with the axis passing vertex 1.

Remark we say a map is injective, then the map is of course not surjective.

Example 13.4 $\phi : A_3 \longrightarrow \mathbb{Z}_3$

Example 13.5 any linear transformation: $T : (\mathbb{R}^n, +) \longrightarrow (\mathbb{R}^m, +)$ is a homomorphism

Example 13.6 $(\mathbb{Z}, +) \longrightarrow (\mathbb{Z}_n, '+')$: define the map: $\pi(a) = [a]_n$. check that $\pi(a+b) = \pi(a) + \pi(b)$

Remark the addition defined on $\mathbb{Z}_n$ is different from the addition defined on $\mathbb{Z}$.

Proposition 13.1 (composition)
1. $\phi : G \longrightarrow H$ and $\psi : H \longrightarrow K$ are homomorphism, then $\psi \circ \phi$ is also a homomorphism.
2. if $\phi : G \longrightarrow H$ is a homomorphism, then $\phi(e_G) = e_H$.
3. if $\phi : G \longrightarrow H$ is an isomorphism, then its inverse $\phi^{-1} : H \longrightarrow G$ is a homomorphism ♠

Proof

Definition 13.2 (kernel and image)
let $\phi : G \longrightarrow H$ be a homomorphism, kernel $ker(\phi) := \{g \in G : \phi(g) = e_H\}$
image $im(\phi) := \{\phi(g) : g \in G\}$ ♣

Remark $ker(\phi) \leqslant G, im(\phi) \leqslant H$

Example 13.7 $\phi : S_n \longrightarrow (\pm 1, \times), ker(\phi) = \sigma \in S_n : \phi(\sigma) = 1$

Example 13.8 the determinant: $(GL(n, \mathbb{R}), \times) \longrightarrow (\mathbb{R}^*, \times)$ is a homomorphism: recall that $det(AB) = det(A)det(B)$
the kernel $ker(det) = A \in GL(n, \mathbb{R}) : det(A) = 1 := SL(n, \mathbb{R})$
$im(det) = \mathbb{R}^*$ (recall the definition of $GL(n, \mathbb{R})$)

✍ **Exercise 13.1** $\psi := S_n \longrightarrow GL(n, \mathbb{R})$ is a homomorphism if

$$\sigma \longrightarrow A_\sigma := \begin{cases} 1, & \text{on the } (\sigma(i), i) \text{ entries} \\ 0, & \text{elsewhere} \end{cases}$$

Example 13.9 n = 3, we have $(132) \longrightarrow A_{(132)} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$

Proposition 13.2

$\phi : G \longrightarrow H$ is a homomorphism, then we have:
1. ϕ is an injective iff $ker(\phi) = \{e_G\}$
2. ϕ is surjective iff $im(\phi) = H$
3. if G is cyclic/abelian, then $\phi(G)$ is also cyclic/ abelian.

Proof 1. $(\longrightarrow)$ we prove that $ker(\phi) = e_G$ using the definition of injective and the property of homomorphsim that $\phi(e_G) = e_H$
$(\longleftarrow)$ we prove that ϕ is an injective using a property of homomorphism: $\phi(x^{-1}) = \phi^{-1}(x)$ (proof: $\phi(x^{-1}) \times \phi(x) = \phi(x^{-1} \times x) = \phi(e_G) = e_H \longrightarrow \phi(x^{-1}) = \phi^{-1}(x)$)

Proof 2. $(\longrightarrow)$ we prove that $im(\phi) = H$, the definition of surjective map says that $\forall h \in H, \exists g \in G s.t. \phi(g) = h$ i.e. $im(\phi) \geqslant H$, recall that $im(\phi) \leqslant H \longrightarrow im(\phi) = H$
$(leftarrow)$ I think this is proved by the definition of surjective map.

Remark if $\phi : G \longrightarrow H$ is isomorphism, then "many" properties of G remains true for H, such as G is cyclic/ abelian $\Leftrightarrow$ H is also cyclic/abelian.

Exercise 13.2 a. do we have $\phi :(\mathbb{Z}_6, +) \longrightarrow S_3$ is an isomorphism?
b. do we have $\phi : \mathbb{Z}_4 \longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_2$ is an isomorphism?

Theorem 13.1

let G = $\langle g \rangle$ be a cyclic group, then if $|G| = \infty$, then $G \cong (\mathbb{Z}, +)$; if $|G| = n$, then $G \cong (\mathbb{Z}_n, +)$

Proof

Chapter lagrange's theorem

Definition 14.1 (equivalence relation)

S is a set, an equivalence relation $\sim$ on S satisfies for all a,b,c $\in$ S, 1. $a \sim a$;
2. $a \sim b, b \sim c \rightarrow a \sim c$;
3. $a \sim b \leftrightarrow b \sim a$

♣

Definition 14.2 (equivalence class)

an equivalence class of S with representative $a \in S$ is the set $C_a := \{b \in S : b \sim a\}$

♣

Remark if $a \sim c$, then $C_a = C_c$

Example 14.1 in $GL(n, \mathbb{R})$, $C_{\begin{pmatrix} y & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix}} = \{B | det(B) = det(\begin{pmatrix} y & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix})\} = \{B | det(B) = y\}$

Remark M is a matrix $C_M := C_{\begin{pmatrix} det(M) & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix}}$, if $det(M) \neq det(M') \rightarrow C_M \bigcap C_{M'} = \phi$

for a set S, we can partition S into disjoint union of equivalence class $S = C_\alpha \sqcup C_\beta \sqcup ...$, where $\sqcup$ means disjoint union. for the above example, we have $(GL(n, \mathbb{R}), \sim) = \bigsqcup_{y \in \mathbb{R}^*} C_{\begin{pmatrix} y & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix}}$

Definition 14.3 (left coset)

let $H \leqslant G$, the left coset of H with representative $a \in G$ is the equivalence class: $aH = C_a = \{b \in G | a \sim b\} = \{b \in G | a^{-1}b \in H\} = \{b \in G | a^{-1}b = h, h \in H\} = \{ah | h \in G\}$

♣

Remark relation between left coset and equivalent class: we can write $G = \bigsqcup_{\alpha \in A} \alpha H$ for some indexed set A

Definition 14.4

let $H \leqslant G$, the index $[G : H]$ is equal to the number of the left coset in $G = \bigsqcup_{\alpha \in A} \alpha H$ for some indexed set A

♣

Example 14.2 a. $3\mathbb{Z} \leqslant \mathbb{Z}, \mathbb{Z} = (0 + \mathbb{Z}) \sqcup (1 + \mathbb{Z}) \sqcup (2 + \mathbb{Z}), [\mathbb{Z} : 3\mathbb{Z}] = 3$
b. $[GL(n, \mathbb{R}) : SL(n, \mathbb{R})] = \infty$
c. $G = S_3, |S_3| = 6$, $H = \{e, (12)\}$, $eH = \{ee, e(12)\}$, $(23)H = \{(23), (132)\}$, $(13)H = \{(13), (123)\}$, $[S_3 : H] = 3$

Theorem 14.1 (lagrange)

let $|G| < \infty$ and $H \leqslant G$, then $[G : H] \cdot [H] = [G]$

♡

Proof

Corollary 14.1

let $|G| < \infty$, *and* $g \in G$, *then* $ord(g) \mid |G|$

Corollary 14.2 (Fermat's little theorem)

let $a \in \mathbb{Z}$, *and* a *is not a multiple of* p, *then* $p|(a^{p-1} - 1)$, *i.e.* $a^{p-1} \equiv 1(mod p)$

Chapter normal subgroup

Definition 15.1 (right coset)

define $a \sim_R b \Leftrightarrow ab^{-1} \in H$. we can check that this is also an equivalence relation with equivalence class: $R_a := \{b|b \sim_R a\} = Ha = \{ha|h \in H\}$

♣

it is easy to notice that not all groups have subset H s.t. left coset equals to right coset.

Example 15.1 a. $G = S_3, H = A_3$, check that $gA_3 = A_3g, \forall g \in G$
b. $G = D_n, H = \langle s\rangle = \{e, s\}, rH = \{r, rs\}, Hr = \{r, sr\}$, recall that $rs = sr^{n-1}$, for $n > 2$, we have $rs \neq sr, \rightarrow rH \neq Hr$.

Definition 15.2 (normal group)

let $H \leqslant G$, we say H is a normal subgroup of G, ($H \lhd G$) if $gH = Hg, \forall g \in G$

♣

Example 15.2 a. $A_n \lhd S_n$
b. $SL(n, \mathbb{R}) \lhd GL(n, \mathbb{R})$ c. $\langle s\rangle \ntriangleleft D_n$ for $n \geqslant 2$

Theorem 15.1

let $H \leqslant G$, the following are equivalent:
a. $H \lhd G$: $gH = Hg, \forall G$
b. $\forall h \in H, g \in G, ghg^{-1} \in H$
c. $gHg^{-1} = H, \forall g \in G$

♡

Proof

Corollary 15.1

let $\phi : G \longrightarrow H$ be a homomorphism of groups, then $ker(\phi) \lhd G$

♡

Proof using the equivalent definition of normal group in the above theorem b.
take any $k \in ker(\phi)$, i.e. $\phi(k) = e_H$, we want to prove that $gkg^{-1} \in ker(\phi)$. consider $\phi(gkg^{-1} = \phi(g)\phi(k)\phi(g^{-1}) = \phi(g)e_H\phi(g^{-1}) = \phi(g)\phi(g^{-1}) = \phi(g)\phi(g)^{-1} = e_H$, so we have $gkg^{-1} \in ker(\phi)$, which proves that $ker(\phi) \lhd G$, we are done.
note $\phi(g)\phi(g^{-1}) = \phi(gg^{-1}) = \phi(e_G) = e_H$ and thus $\phi(g^{-1}) = \phi(g)^{-1}$

Example 15.3 $SL(n, \mathbb{R}) \lhd GL(n, \mathbb{R})$

Chapter quotient group

Definition 16.1 (quotient group)

let $H \lhd G$, the quotient group is defined as

$$G \setminus H := \{\text{all H-left coset of } G = \{aH | a \in G\}$$

the multiplication rule is defined to be

$$(aH) * (bH) := (abH)$$

Remark a. $|G/H|$ = the number of H-left coset of G = $[G : H]$, if $|G| < \infty$, then by lagrange theorem, we have $[G : H] = |G|/|H|$

b. the multiplication rule of $(G/H, *)$ gives a group: $[(aH) * (bH)] * (cH) = (aH) * [(bH) * (cH)] = (abc)H$ and the identity of the group is $e_{G/H} = eH$, and the inverse of the group: $(bH)^{-1} = b^{-1}H$ since $b^{-1}H * bH = (b^{-1}b)H = eH$

Remark given $a_1 \neq a_2$ and $b_1 \neq b_2$ we can still have $a_1H = a_2H$ and $b_1H = b_2H$. it is also true that: $(a_1H)(b_1H) = (a_2H)(b_2H)$, i.e. $(a_1b_1)H = (a_2b_2)H$

Example 16.1 we can show that $\mathbb{Z}/n\mathbb{Z} \cong Z_n$

Theorem 16.1 (first isomorphism theorem)

let $\phi : G \longrightarrow H$ be a homomorphism, then $ker(\phi) \lhd G$, and $G/ker(\phi) \cong im(\phi)$

Proof

Definition 16.2 (simple group)

we say a group G is simple if there is no proper, nontrivial, normal subroups of G, i.e. $k \lhd G \Leftrightarrow k = \{e\}$ or G

Example 16.2 1. $GL(n, \mathbb{R})$ is not a simple since $SL(n, \mathbb{R}) \lhd GL(n, \mathbb{R})$

2. $A_n \lhd S_n$

3. A_n is simple for $n \geqslant 5$, $k = \{e, (13)(24), (12)(34), (14)(23)\} \lhd A_4$

Remark for $|G| < \infty$, we have $|G| = |G/k| \times |k|$, but it does not implies that $G \cong G/k \times k$. for example: $G = S_3, H = A_3$, $G/H = \mathbb{Z}_2$, but $S_3 \ncong A_3 \times \mathbb{Z}_2$, notice that S_3 is not abelian but $A_3, \mathbb{Z}_2$ are abelian and thus $A_3 \times \mathbb{Z}_2$ is abelian.

Chapter classification of all finite abelian subgroup

what we are going to do is try to classify all finite abelian subgroup. we first recall examples of finite abelian group: $(\mathbb{Z}_n, +)$, $(\mathbb{Z}_n^*, \times)$, $(\mathbb{Z}_m \times \mathbb{Z}_n, +)$

Exercise 17.1 whether do we have: $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$? the exercise is natural since both two groups are abelian and have order mn.

the answer is true for the case that $gcd(m,n) = 1$: there is a counterexample: $\mathbb{Z}_4 \ncong \mathbb{Z}_2 \times \mathbb{Z}_2$ since $\mathbb{Z}_4$ is cyclic and $\mathbb{Z}_2 \times \mathbb{Z}_2$ is not cyclic.

Proof we want to show that there is an isomorphism $\phi : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ with $gcd(m,n) = 1$:
1. show that ϕ is a homomorphism
2. show that ϕ is surjective and injective

Theorem 17.1

all finite abelian group G are isomorphic to a product of cyclic groups: $G \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \ldots \times \mathbb{Z}_{n_k}$ *and the expression may not be unique. (what is the requirement for n_i?)*

Proof 1. we first show that if $|G| = p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r}$, then $G \cong H_{p^{a_1}} \times H_{p^{a_2}} \times \ldots \times H_{p^{a_r}}$
2. we show that all abelian groups H_{p^a} of order p^a is isomorphic to $\mathbb{Z}_{p^{k_1}} \times \mathbb{Z}_{p^{k_2}} \times \ldots \times \mathbb{Z}_{p^{k_r}}$ with $a = k_1 + k_2 + \ldots + k_r$ and $k_1 \leqslant k_2 \leqslant \ldots \leqslant k_r$
(this does not mean that $\mathbb{Z}_8 \cong \mathbb{Z}_4 \times \mathbb{Z}_2 \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$)
$1. + 2. \to G \cong (\mathbb{Z}_{p_1^{k_1}} \times \mathbb{Z}_{p_1^{k_2}} \times \ldots \times \mathbb{Z}_{p_1^{k_x}}) \times (\mathbb{Z}_{p_2^{k_1}} \times \mathbb{Z}_{p_2^{k_2}} \times \ldots \times \mathbb{Z}_{p_2^{k_y}}) \times \ldots \times (\mathbb{Z}_{p_r^{k_1}} \times \mathbb{Z}_{p_r^{k_2}} \times \ldots \times \mathbb{Z}_{p_r^{k_z}})$

Exercise 17.2 show that $\mathbb{Z}_8 \ncong \mathbb{Z}_4 \times \mathbb{Z}_2 \ncong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

Corollary 17.1

if $\phi : G \to H$ is an isomorphism and $ord(g) = l$ for $g \in G$, then $ord(\phi(g)) = l$

Proof

Example 17.1 we wonder the abelian group G of order 360 may be isomorphic to ...?

Proof note that $360 = 2^3 3^2 5^1$. we claim that there are 6 choices of abelian groups for group G of order 360 to be isomorphic to. these 6 groups are not isomorphic
this result gives a full description (of the structure) of abelian groups of order 360: we can check: $\mathbb{Z}_{360} \cong \mathbb{Z}_8 \times \mathbb{Z}_9 \times \mathbb{Z}_5$ why? and $\mathbb{Z}_{180} \times \mathbb{Z}_2 \cong$

Theorem 17.2

if G is abelian and $|G| = mn$ with $gcd(m,n) = 1$, then $G \cong H_m \times H_n$ where H_m, H_m are abelian groups of order m, n respectively.

Corollary 17.2

by the above theorem, we have: every abelian group G with $|G| = p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r}$ is isomorphic to $H_1 \times H_2 \times \ldots \times H_r$ where $|H_1| = p_1^{a_1}, \ldots, |H_r| = p_r^{a_r}$

Theorem 17.3

every abelian group of order p^a is isomorphic to $\mathbb{Z}_{p^{k_1}} \times \mathbb{Z}_{p^{k_2}} \times \ldots \times \mathbb{Z}_{p^{k_r}}$ with $k_1 \leqslant k_2 \leqslant \ldots \leqslant k_r$ and $a = k_1 + k_2 + \ldots + k_r$

Proof (guideline)

Chapter Rings: basic knowledge

Introduction

- *definition of ring*
- *how to check a subring*
- *subring*
- *product ring*
- *commutative, unital*
- *field*

Definition 18.1 (ring)

a ring is a set equipped with two binary operations: $+ : R \times R \to R$ *and* $\cdot : R \times R \to R$ *s.t.*
a. $(R, +)$ *is an abelian group with additive identity* 0_R*, and* $(R, \times)$ *is not necessary to be a group.*
b. $(R, \cdot)$ *is associative*
c. $(R, +, \cdot)$ *is distributive:* $a \cdot (b + c) = a \cdot b + a \cdot c$ *and* $(b + c) \cdot a = b \cdot a + c \cdot a$

Example 18.1 a. $\mathbb{Z}[i] := \{a + bi|a, b \in \mathbb{R}\}$ is a ring
b. $n\mathbb{Z} = \{nk|k \in \mathbb{Z}\}$ is a ring
c. $M_{n\times n}(\mathbb{R})$ forms a ring

Definition 18.2 (unital)

let $(R, +, \cdot)$ *be a ring, we say* R *is unital if there is a multiplicative identity* 1_R *i.e.* $r \cdot 1_R = 1_R \cdot r = r$ *for all* $r \in R$*.*

in $M_{n\times n}(R)$, $I_R = I_{n\times n}$; in Z_n, $1_R = [1]$; but $n\mathbb{Z}$ has no 1_R for $n > 1$, so $n\mathbb{Z}$ is not a unital ring.

Definition 18.3 (commutative)

$(R, +, \cdot)$ *is a ring, we say* $(R, +, \cdot)$ *is commutative if* $ab = ba, \forall a, b \in \mathbb{R}$*.*
notice $M_{n\times n}(R)$ *is not commutative.*

Definition 18.4 (unit)

if R *is unital, the unit of* R *is defined as* $U(R) := \{r \in R|\exists r^{-1} \in R \text{ s.t. } rr^{-1} = r^{-1}r = 1_R\}$
e.g. $U(\mathbb{Z}) = \{1, -1\}$, $U(\mathbb{Q}) = Q^* = Q \setminus \{0\}$ *since* $(\frac{a}{b})^{-1} = (\frac{b}{a})$, $U(\mathbb{Z}[i]) - \{1, -1, i, -i\}$, $U(M_{n\times n}(R)) = GL(n, \mathbb{R})$

Remark

1. the additive identity 0_R is unique in R. if R is unital, then the multiplicative unit 1_R is also unique.
2. write $-r \in R$ as the additive inverse of $r \in R$, $r + (-r) = 0_R$
3. similarly for $s \in U(R)$, we write s^{-1} as the multiplicative inverse of s, i.e. $s \cdot s^{-1} = s^{-1}s = 1_R$
4. for $n \in \mathbb{N}$, write $n \cdot r := \overbrace{r + r + \ldots + r}^{\text{n copies}}$
5. if R is commutative, then for $a, b \in R$, we write $a|b$ as a divides b, and a is a factor of b if $\exists c \in R$ s.t. $b = ac$

Proposition 18.1

a. $0_R \cdot r = r \cdot 0_R, \forall r \in R$
b. $(-1_R) \cdot r = -r = r(-1_R)$
c. $(-1_R) \cdot r = r = (-r)(-1_R)$

Proof

Remark if $m \in \mathbb{Z}$, and $m < 0$, $m \cdot r := (-r) + (-r) + \ldots + (-r) = ((-1_R) + (-1_R) + \ldots + (-1_R)) \cdot r$

Definition 18.5 (product ring)

$(R,+,\cdot)$ and $(S,+,\cdot)$ are rings, the product ring $(R\times S,+,\cdot)$ is defined by a. $(r,s)+(r',s'):=(r+r',s+s')$ and b. $(r,s)\cdot(r',s')=(r\cdot_R r',s\cdot_S s')$ where $\cdot_R$ is the multiplication on R and $\cdot_S$ is the multiplication on S. ♣

Definition 18.6 (subring)

let $R'\subset R$ be a subset, then R' is a subring of R if $+_R|_{R'\times R'}: R'\times R'\to R'$; $\cdot_R|_{R'\times R'}: R'\times R'\to R'$ gives a ring structure of R'. ♣

Theorem 18.1 (equivalent definition of subring)

let $(R,+,\cdot)$ be a ring, a subset $R'\subset R$ is a subring iff $\forall a,b\in R'$, we have:

a. $a+b\in R'$

b. $-a\in R'$

c. $a\cdot b\in R'$ ♡

Definition 18.7 (field)

a field $\mathcal{F}$ is a unital, commutative ring s.t. $U(\mathcal{F})=\mathcal{F}\setminus\{0_{\mathcal{F}\}}$ ♣

Example 18.2 $\mathbb{Z}$ is not a field since $U(\mathbb{Z})=\{1,-1\}$.
$\mathbb{Q},\mathbb{R},\mathbb{C}$ are fields.

Remark $R[X]:=\{a_nx^n+\ldots+a_0|a_i\in R\}$ is a ring if R is a ring. if R is commutative/unital, then $R[x]$ is also commutative/unital.

Chapter ring homomorphism

Introduction

- ring homomorphism
- unital homomorphism
- properties of ring homomorphism
- kernel and image

Definition 19.1 (ring homomorphism)

let R, S be rings, then a map $\phi : R \longrightarrow S$ is a ring homomorphism if ϕ satisfies:

a. $\phi(r + r') = \phi(r) + \phi(r')$

b. $\phi(r \cdot r') = \phi(r)\phi(r')$

Definition 19.2 (unital)

if R,S are unital, a homomorphism ϕ is called unital if $\phi(1_R) = 1_S$

Remark a. if $\phi : R \longrightarrow S$ is bijective, then we say $R \longrightarrow S$ is an isomorphism

b. for groups, $(G, \cdot)$ and $(H, \cdot)$: any homomorphism $\phi : G \longrightarrow H$ i.e. $\phi(g_1 \cdot g_2) = \phi(g_1)\phi(g_2)$ satisfies $\phi(e_G) = e_H$. however, for ring homomorphism since G,H are not groups, so we have $\phi(e_G) = e_H$ automatically.

Example 19.1 a. $\phi : \mathbb{Z} \longrightarrow \mathbb{Z}$: $\phi(n) = 2n$ is a group homomorphism but ϕ is not a ring homomorphism: $\phi(a \cdot b) = 2(ab) \neq \phi(a)\phi(b) = 4(ab)$

b. $\phi : \mathbb{Z}_{10} \longrightarrow \mathbb{Z}_{10} : \phi([a]_{10}) = [2a]_{10}$ is not a ring homomorphism but $\psi : \mathbb{Z}_{10} \longrightarrow \mathbb{Z}_{10} : \psi([a]_{10}) = [5a]_{10}$ is a ring homomorphism and ψ is not unital since $\psi([1]_{10}) = [5 \cdot 1]_{10} \neq [1]_{10}$

c.

d.

e.

Remark $\phi : \mathbb{Z}_8 \longrightarrow \mathbb{Z}_4 \times \mathbb{Z}_2$ is not isomorphic since $\phi([4]) = ([0], [0])$, so $ker(\phi) \neq \{0\}$. however, if $gcd(m, n) = 1$, then $\phi : \mathbb{Z}_{mn} \longrightarrow \mathbb{Z}_m \times \mathbb{Z}_n$ is an isomorphism.

Proposition 19.1

let $\phi : R \longrightarrow S$ be any ring homomorphism, we have

a. $\phi(0_R) = 0_S$

b. $\phi(-a) = -\phi(a)$

c. if R, S are unital and ϕ is unital homomorphism, then $\phi(a^{-1}) = (\phi(a))^{-1}$

d. if ϕ is an isomorphism, then $\phi^{-1} : S \longrightarrow R$ is also a ring homomorphism

Proof

Proposition 19.2

let $\phi : R \longrightarrow S$ be a ring homomorphism, then we have:

a. $ker(\phi) = \{r \in R : \phi(r) = 0_S\} \leqslant R$

b. $im(\phi) = \{\phi(r) : r \in R\} \leqslant S$

c. ϕ is an isomorphism $\Leftrightarrow ker(\phi) = \{0_R\}$ and $im(\phi) = S$

Proof

Chapter integral domain

Introduction

- *zerodivisor, integral domain*
- *cancellation property*
- *field $\subset$ ID*

recall in groups we have $ker(\phi) \ntriangleleft G$ is a normal group, the analog for rings is called ideals.

Definition 20.1 (zerodivisor; integral domain)

let R be a ring. an element $a \in R \setminus \{0\}$ is a zerodivisor if $\exists r \in R \setminus \{0\}$ s.t. $a \cdot r = 0_R$ or $r \cdot a = 0_R$. recall if $a = 0_R$, $a \cdot r = r \cdot a = 0_R$. a ring R is called an integral domain(ID) if R is commutative and R has no zerodivisor.

Example 20.1 $\mathbb{Z}_6$ is not an integral domain since $[2][3] = [6] = [0] \Rightarrow 2$ and 3 are zerodivisor of $\mathbb{Z}_6$

Proposition 20.1 (cancellation property)

let R be a commutative ring. then R is ID iff whenever $c \neq 0$, $c \cdot a = c \cdot b$ in R, we have $a = b$.

Proof $(\Rightarrow)$: given $ca = cb$, we have $ca + (-(cb)) = 0_R$, $ca + c(-b) = c(a + (-b)) = 0$, therefore if R is an ID, we have: c and $(a + (-b))$ nonzero otherwise we have zerodivisors, and we have already know that $c \neq 0$, we have $a + (-b) = 0 \Rightarrow a = b$ $(\Leftarrow)$: suppose R is not an ID, given $c \neq 0$, if we have $ca = cb \Rightarrow c(a - b) = 0$, which does not imply that $a = b$ and it contradicts with the assumption that $a = b$, so R is an ID.

Proposition 20.2

a field is always an ID

Proof field F is commutative so we use the last proposition to prove the F is an ID: suppose $ca = cb, c \neq 0, c(a-b) = 0$. since F is a field, $c \neq 0 \Rightarrow c^{-1}$ exists $\Rightarrow c^{-1}c(a - b) = c^{-1} \cdot 0 = 0 \Rightarrow I \cdot (a - b) = 0 \Rightarrow a = b$, we are done.

Chapter ideals

Introduction

- ideal
- ideals generated by Γ
- principal ideal
- ideal of intersection and addition
- kernel and ideal

Definition 21.1 (ideal)

let R be a ring, a subset $I \subset R$ is an ideal $I \lhd R$ if:
a. $(I, +)$ forms a subgroup of $(R, +)$
b. $\forall i \in I, x \in R$, we have $ix \in I$ and $xi \in I$.

Remark if $I \lhd R$, then $I \leqslant R$ since b. in the definition implies that $i \cdot i' \in I$ and $i' \cdot i \in I$.

Example 21.1

1. $\forall a, b \in \mathbb{Z}$, we have $a \cdot b \in \mathbb{Z}$. we have $\mathbb{Z} \leqslant \mathbb{Q}$, but $\mathbb{Z} \ntriangleleft \mathbb{Q}$: we take $2 \in \mathbb{Z}$, $\frac{1}{3} \in \mathbb{Q}$, but $2 \cdot \frac{1}{3} = \frac{2}{3} \in \mathbb{Z}$, so $\mathbb{Z}$ is not an ideal of $\mathbb{Q}$.
2. $n\mathbb{Z} \lhd \mathbb{Z}$
3. $R = \mathbb{Z}[x]$, $I = \{p(x) \in R | p(0) = 0\}$: polynomials with zero coefficient at constant term. then $I \lhd R$: we check:
   (a). $p(x) = a_1 x + \ldots + a_n x^n$, $q(x) = b_1 x + \ldots + b_m x^m \in I$, we have $p + q \in I, -q \in I$
   (b). for any $r(x) = c_0 + c_1 x + \ldots + c_l x^l$, $r(x) \cdot p(x) = p(x) \cdot r(x) = (c_0 \cdot a_1)x + (c_1 \cdot a_1 + c_0 + c_0 a_2)x^2 + \ldots \in I$
4. $R = \mathbb{Z}[x]$, $I = \{\text{polynomials with even constant term}\}$, then $I \lhd R$ why?

we want to know how to construct ideals?

Definition 21.2 (ideals generated by Γ)

let R be a ring, $\Gamma \subset R$ is a subset, then the ideals generated by Γ is $\langle \Gamma \rangle :=$ the smallest ideal containing all $r \in \Gamma$.

Remark if R is unital and commutative, and $\Gamma = \{\gamma_1, \gamma_2, \ldots, \gamma_k\}$ is a finite set, then $\langle \Gamma \rangle = \langle \gamma_1, \gamma_2, \ldots, \gamma_k \rangle = \{a_1\gamma_1 + a_2\gamma_2 + \ldots + a_k\gamma_k | a_i \in \mathbb{R}\}$

Example 21.2

1. recall we have $n\mathbb{Z} \lhd \mathbb{Z}$, let $\Gamma = \{n\}$,$\langle n \rangle = \{an | a \in \mathbb{Z}\} = n\mathbb{Z}$
2. $R = \mathbb{Z}[x]$, $\Gamma = \{x\}$, then $\langle x \rangle = \{xp(x) | p(x) \in R\} = \{p(x) \in R | p(0) = 0\}$
3. $R = \mathbb{Z}[x]$, $\Gamma = \{2, x\}$, $\langle 2, x \rangle := \{2p(x) + xq(x) | p(x), q(x) \in R\} = \{\text{all polynomials with even constant coefficients}\}$

Proposition 21.1

let R be unital commutative ring, then $\langle \gamma_1, \gamma_2, \ldots, \gamma_k \rangle = \{a_1\gamma_1 + \ldots + a_k\gamma_k\}$ is an ideal of R.

Proof we need to show 3 things:

1. show that $\{a_1\gamma_1 + \ldots + a_k\gamma_k | a_i \in R\} \lhd R$
2. show that $\gamma_1, \ldots, \gamma_k \in \{a_1\gamma_1 + \ldots + a_k\gamma_k\}$
3. show that if any $I \lhd R$ s.t. $\gamma_1, \ldots, \gamma_k \in I$, then $\{a_1\gamma_1 + \ldots + a_k\gamma_k\} \subset I$, which means that $\{a_1\gamma_1 + \ldots + a_k\gamma_k\}$ is the smallest ideal containing $\gamma_1, \ldots, \gamma_k$, by the definition of ideal, we are done.

Definition 21.3 (principal ideal)

let R be unital commutative, $I \lhd R$ is a principal ideal if $I = \langle r \rangle$ for some $r \in R$, e.g. $\{0\} = \langle 0 \rangle$, and $R = \langle 1 \rangle$

Definition 21.4 (ideal of intersection and addition)

let $I_1, I_2, ..., I_k \triangleleft R$, we define $I_1 + ... + I_k = \{i_1 + ...i_k | i_j \in I_j\}$, and define $\bigcap_{l=1}^{k} = \{i \in R | i \in I_l, \forall l = 1, 2, ..., k\}$, then they are also ideals in R.

Example 21.3 let $R = \mathbb{Z}$, $I_l = \langle m_l \rangle = m_l\mathbb{Z} \to I_1 + ... + I_k = \langle gcd(m_1, ..., m_k) \rangle$ e.g. $\langle 2 \rangle + \langle 3 \rangle = \langle 1 \rangle$, $I_1 \cap I_2 \cap ... \cap I_k = \langle lcd(m_1, ..., m_k) \rangle$ e.g. $\langle 2 \rangle \cap \langle 3 \rangle = \langle 6 \rangle$

Proposition 21.2

let $\phi : R \to S$ be a ring homomorphism, then $\ker(\phi) \triangleleft R$

Proof we have proved that $ker(\phi) \leqslant R$ (check the chapter: ring homomorphism), which guarantees that $\ker(\phi)$ is a additive subgroup of R. we only need to prove that $\forall i \in ker(\phi), x \in R$, we have $ix \in ker(\phi)$ and $xi \in ker(\phi)$: since $\phi(ix) = \phi(i)\phi(x) = 0 \cdot \phi(x) = 0 \in S$ and $\phi(xi) = \phi(x)\phi(i) = \phi(x) \cdot 0 = 0 \in S$, we conclude that xi and $ix \in ker(\phi)$, we are done.

Chapter quotient ring

Introduction

- *quotient ring*
- *first isomorphism theorem for rings*

Definition 22.1 (quotient ring)

let R be a ring, $I \triangleleft R$ is an ideal, then the quotient ring $(R \setminus I, +, \cdot)$ is defined by $R \setminus I := \{r + I | r \in R\}$, and the addition in $(r + I)$ is defined by $(r + I) + (r' + I) := (r + r') + I$. the multiplication is defined by: $(r + I) \cdot (r' + I) := r \cdot r' + I$ ♣

Remark we need to check the operations are well-defined. for example, suppose $(r + I) = (s + I)$ and $(r' + I) = (s' + I)$, we must check that $rr' + I = ss' + I$, how?

Example 22.1 let $R = \mathbb{R}[x]$, $I = \langle x^2 + 1 \rangle$, the elements of R/I are of the form $\{p(x) + I | p(x) \in R\}$, i.e. $x^2 + \langle x^2 + 1 \rangle = (-1 + (x^2 + 1)) + \langle x^2 + 1 \rangle = -1 + \langle x^2 + 1 \rangle$. more generally, by division algorithm, $p(x) = q(x)(x^2 + 1) + r_0 + r_1 x$, we have $p(x) + I = (r_0 + r_1 x) + I$, $R/I := \{(a_0 + a_1 x) + I | a_0, a_1 \in \mathbb{R}\}$

Example 22.2 some arithmetic in $R \setminus I, I = \langle x^2 + 1 \rangle$:
a. $(2 + I)((x + 3) + I) = (2x + 6) + I$
b. $0_{R \setminus I} = 0 + I$
c. $1_{R \setminus I} = 1 + I$
d. $(x + I)(x + I) = x^2 + I = -1 + I = -1_{R \setminus I}$
e. $R = \mathbb{Z}[x]$, $I_3 = \langle 2, x \rangle$, $R \setminus I_3 = \{(a_0 + a_1 x + \ldots + a_n x^n) + \langle 2, x \rangle\}$, we have $R \setminus I_3 = \{a_0 + (a_1 + \ldots + a_n x^n - 1)x + \langle 2, x \rangle\} = \{a_0 + \langle 2, x \rangle\} = \{0 + \langle 2, x \rangle, 1 + \langle 2, x \rangle\}$, so we have $R \setminus I_3 \cong \mathbb{Z}_2$

Theorem 22.1 (first isomorphism theorem for rings)

let $\Phi : R \longrightarrow S$ be ring homomorphism, then we have an isomorphism of rings $\phi : R \setminus ker(\Phi) \cong im(\Phi)$. (so ϕ is a bijection) ♡

Proof

Example 22.3

Example 22.4

Chapter Chinese remainder theorem

Introduction

- rings' coprime
- CRT

Definition 23.1 (coprime)
let R be commutative ring. two ideals $I_1, I_2 \triangleleft R$ are coprime if $I_1 + I_2 = R$
♣

in number theory, we have the CRT:

Theorem 23.1 (Chinese remainder theorem)
let $m_1, m_2, ..., m_r$ be pairwise coprime positive integers, and let $a_1, a_2, ..., a_r$ be integers. then the system:

$$\begin{cases} x \equiv a_1 (mod m_1) \\ x \equiv a_2 (mod m_2) \\ \quad \cdots \\ x \equiv a_r (mod m_r) \end{cases}$$

has a solution. moreover, if x_0 is a solution, then the complete solution of the system is given by $x = x_0 + km$, where k is any integer and $m = m_1 m_2 ... m_r$
♡

in abstract algebra, the CRT is:

Theorem 23.2 (Chinese remainder theorem)
let R be commutative. unital rings $I_1, I_2, ..., I_k \triangleleft R$ and $\forall I_i$ and I_j are coprime, then we have

$$R/(I_1 \cap I_2 \cap ... \cap I_k) \cong R/I_1 \times R/I_2 \times ... \times R/I_k$$
♡

we want to explain the relation between two versions:
let $m_1, m_2, ..., m_r$ be pairwise coprime integers, we have

$$m_1\mathbb{Z} \cap m_2\mathbb{Z} \cap ... m_r\mathbb{Z} = lcd(m_1, m_2, ..., m_r)\mathbb{Z} = m_1 m_2 ... m_r \mathbb{Z}$$

the first equality is due to the definition of intersection of ideals (check the chapter ideals), and the second equality is due to the condition that $m_1, m_2, ..., m_r$ are coprime. so we apply the CRT version 2 and get

$$\mathbb{Z}/(m_1 m_2 ... m_r \mathbb{Z}) \cong (\mathbb{Z}/m_1\mathbb{Z}) \times (\mathbb{Z}/m_2\mathbb{Z}) \times ... \times (\mathbb{Z}/m_r\mathbb{Z})$$

for $x \in \mathbb{Z}/(m_1 m_2 ... m_r \mathbb{Z})$, we have $(a_1, a_2, ..., a_r) \in (\mathbb{Z}/m_1\mathbb{Z}) \times (\mathbb{Z}/m_2\mathbb{Z}) \times ... \times (\mathbb{Z}/m_r\mathbb{Z})$

Example 23.1 $R = \mathbb{Z}$, $I_1 = \langle m \rangle$, $I_2 = \langle n \rangle$, $I_1 + I_2 = \langle gcd(m, n) \rangle$ (why?), so we have I_1, I_2 are coprime $\Leftrightarrow I_1 + I_2 = \langle 1 \rangle = \mathbb{Z} \Leftrightarrow gcd(m, n) = 1$, i.e. m, n are coprime.

Example 23.2 m, n are coprime, $R = \mathbb{Z}$, $I_1 = \langle m \rangle$, $I_2 = \langle n \rangle$, $gcd(m, n) = 1$, then by CRT we have: $\mathbb{Z} \setminus \langle m \rangle \cap \langle n \rangle \cong \mathbb{Z} \setminus I_1 \times \mathbb{Z} \setminus I_2$. $\mathbb{Z} \setminus \langle lcm(m, n) \rangle = \mathbb{Z} \setminus mn\mathbb{Z} \cong \mathbb{Z} \setminus n\mathbb{Z} \times \mathbb{Z} \setminus m\mathbb{Z} \Rightarrow \mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$

Corollary 23.1
$\mathbb{Z} \setminus p_1^{\alpha_1} p_2^{\alpha_2} ... p_k{}_{\mathbb{Z}}^{\alpha_k} \cong \mathbb{Z} \setminus p_1^{\alpha_1}{}_{\mathbb{Z}} \times \mathbb{Z} \setminus p_2^{\alpha_2}{}_{\mathbb{Z}} \times ... \times \mathbb{Z} \setminus p_k^{\alpha_k}{}_{\mathbb{Z}}$
♡

Proof consider $\Phi : R \to R \setminus I_1 \times R \setminus I_2 \times ... \times R \setminus I_k$, $\Phi(r) := (r + I_1, r + I_2, ..., r + I_k)$. we can prove that Φ is a unital ring homomorphism. then we use the first homomorphism theorem to prove it. we check 2 things: (a) $im(\Phi) = R \setminus I_1 \times ... \times R \setminus I_k$ and (b) $ker(\Phi) = I_1 \cap I_2 \cap ... \cap I_k$

Chapter prime and maximal ideal

Introduction

- prime ideal and maximal ideal
- prime ideal and prime number
- prime ideal and ID
- maximal ideal and field
- maximal ideal $\subset$ prime ideal if R is unital and commutative
- r, s associates $\Leftrightarrow \langle r\rangle = \langle s\rangle \Leftrightarrow r \sim s$

Definition 24.1 (prime ideal and maximal ideal)

a. I is a prime ideal if $\forall a, b \in R$ satisfying $ab \in I$ then either $a \in I$ or $b \in I$

b. I is a maximal ideal if for any $J \triangleleft R$ s.t. $I \subset J \subset R$, then $J = I$ or $J = R$.

Remark all ideals $I \triangleleft \mathbb{Z}$ are of the form $I = \langle n\rangle, n \in N$, namely $I \triangleleft \mathbb{Z} \to (I, +) \leqslant (\mathbb{Z}, +)$ as subgroups $\to I = n\mathbb{Z}$ for some n.(check the definition of $\langle\Gamma\rangle$)
consider prime ideal in $R = \mathbb{Z}$, we have the following claim:
$I = \langle n\rangle \triangleleft \mathbb{Z}$ is prime $\Leftrightarrow$ n is prime number or 0.

Proof [proof of the claim] ($\rightarrow$): suppose $n = xy$ is not a prime number, $x, y \in \mathbb{N}$ not equal 1, then we want to show: $\langle n\rangle$ is not a prime ideal: $\forall x, y \in \mathbb{Z}, xy = n \in \langle n\rangle$ but $x, y \notin \langle n\rangle$, so $\langle n\rangle$ is not a prime ideal.
($\leftarrow$): suppose $n = p$ is a prime number, we want to show that $\langle n\rangle$ is a prime ideal:
since for all $a, b \in \mathbb{Z}$ s.t. $ab \in \langle p\rangle \to ab = kp$ for $k \in \mathbb{Z}$which is equivalent to $p|ab$ and $\Leftrightarrow p|a$ or $p|b \Leftrightarrow a = mp$ or $b = m'p \Leftrightarrow a \in \langle p\rangle$ or $b \in \langle p\rangle$. check the definition of prime ideal, we conclude that $\langle n\rangle$ is a prime ideal.

the remark says that there is a $1-1$ map between prime numbers in $\mathbb{Z}$ and prime ideals. in general R we do not have prime numbers but we still have prime ideals in R. then these prime ideals in R plays the same roles as prime integers in $\mathbb{Z}$. and the philosophy is to rather study elements $r \in R$, we study ideals $\langle r\rangle \in R$.

Example 24.1 for $R = \mathbb{Z}$, $\langle n\rangle \triangleleft \mathbb{Z}$ is maximal ideal $\Leftrightarrow$ n is prime $\Leftrightarrow \langle n\rangle$ is prime ideal

Example 24.2 a. $R = \mathbb{Z}_{12} \cong \mathbb{Z}/12\mathbb{Z}$ we have $I \triangleleft R = \langle 0\rangle$ or $\langle 1\rangle$ or $\langle 2\rangle$ or $\langle 3\rangle$ or $\langle 4\rangle$ or $\langle 6\rangle$: $\langle 1\rangle$ is not prime nor maximal; $\langle 2\rangle, \langle 3\rangle$ are prime ideals (also maximal ideals), $\langle 0\rangle, \langle 4\rangle, \langle 6\rangle$ are not prime ideals since we have $[3][4] \in \langle 0\rangle$ but $[3] \notin \langle 0\rangle$ nor $[4] \notin \langle 0\rangle$. and $\langle 4\rangle$ is not maximal since $\langle 4\rangle \subset \langle 2\rangle \subset R$
b. $R = \mathbb{Z}[x]$, $I = \langle x\rangle$, then $I \triangleleft R$ is prime but I is not maximal ideal (why???)

Proposition 24.1

let R be unital commutative and $I \triangleleft R$, then we have:

a. I is prime $\Leftrightarrow R/I$ is ID

b. I is maximal $\Leftrightarrow R/I$ is a field.

Proof we first prove a:
let $(a+I), (b+I) \in R/I$, then $(a+I)\cdot(b+I) = 0_{R/I} \leftrightarrow ab + I = 0 + I \Leftrightarrow ab \in I$. therefore if I is a prime ideal, then $a \in I$ or $b \in I \Leftrightarrow a + I = 0 + I$ or $b + I = 0 + I \Leftrightarrow a + I$ or $b + I = 0_{R/I} \Leftrightarrow R/I$ is an ID.
we prove b:
we have two asides in the proof.
aside1: let F be a field, then all ideals $I \triangleleft F$ must be $\{0\}$ or F and thus we have $\forall$ ideal $J/I \triangleleft R/I$ we have: $J/I = \{0_{R/I}\}$ or $J/I = R/I \Leftrightarrow J = I$ or $J = R$ here for the last equivalence we use the correspondence theorem (see HW9)
aside2: let R be unital commutative, then R is a field $\Leftrightarrow$ the ideal of R are $\{0\}$ or R.
with aside2, we only need to prove that: the ideal of R/I are $\{0\}$ or R/I $\Leftrightarrow$ I is a maximal ideal, and we again use correspondence theorem.(?)

the proof of aside1 is in HW8

Proof [proof for aside2] ($\Rightarrow$): is proved by aside1
($\leftarrow$): suppose we have I s.t. $\{0\} \subsetneqq I \subsetneqq R$, then $1I$, otherwise $r \cdot 1 = r \in I, \forall r \in R$ and thus $I = R$. take any nonzero $x \in I$. then $\forall r \in R, x \cdot r \in I$ by the definition of $I \triangleleft R$ and thus $x \cdot r \neq 1, \forall r \in R$ since $1 \notin I$, so x has no multiplicative inverse $x^{-1} \in R$ and thus R is a field.

Example 24.3 R = $\mathbb{Z}[x]$, $I = \langle x \rangle$, then $R/I = \{a(x) + \langle x \rangle\} \cong \{a_0 + \langle x \rangle | a_0 \in \mathbb{Z}\} \cong \mathbb{Z}$, so we have $\mathbb{Z}$ is ID $\longrightarrow R/I$ is prime and $\mathbb{Z}$ is not a field $\longrightarrow$ I is not a maximal ideal.

Corollary 24.1

let R be unital and commutative, then all maximal ideals $I \triangleleft R$ are prime. ♡

Proof using the last proposition, we know that I is a maximal ideal implies that R/I is a field. recall we know that field must be ID, and we use the proposition again to conclude that I is a prime ideal.

Definition 24.2 (ideal interpretation)

let R be commutative and unital.
a. we say $r|s$ (r divides s) if $\langle s \rangle \subset \langle r \rangle$ as ideals
b. an element $r \in R$ is called prime if $\langle r \rangle \triangleleft R$ is a prime ideal. (r is called prime if $r|xy \longrightarrow r|x$ or $r|y$)
c. we say r,s are associates if $\langle r \rangle = \langle s \rangle$ as ideals. (r,s are called to be associates if $r|s$ and $s|r$)
d. we say a is irreducible if $\langle a \rangle \subset \langle b \rangle \subset R$, then we have $\langle b \rangle = \langle a \rangle$ or $\langle b \rangle = R$. (a is called to be irreducible if $a = xy \longrightarrow$ either x is a unit or y is a unit.) ♣

Chapter principal ideal domains (PID)

Introduction

- *PID*
- *prime ideals* $\Leftrightarrow$ *maximal ideals if R is a PID*
- *fields* $\subset$ *PID*
- $\mathbb{Z}$ *is a PID but* $\mathbb{Z}[x]$ *is not a PID.*

Definition 25.1 (principal ideal domain)

let R be an integral domain, we say R is PID if all ideals $I \triangleleft R$ are principal, i.e. $I = \langle a \rangle$ for some $a \in R$

Example 25.1

1. all fields F are PIDs, since the only ideal $I \triangleleft F$ are $I = \langle 0 \rangle$ or $I = F = \langle e \rangle$
2. $\mathbb{Z}$ is a PID since all $(I, +) \triangleleft (\mathbb{Z}, +)$ must be the form $I = \langle a \rangle = a\mathbb{Z}$ for some $a \in \mathbb{Z}$ (prove it)
3. (refer to HW9Q5) $\mathbb{Z}[x]$ is not a PID:

   Proof we note that $I = \langle 2, x \rangle$ is not principal: suppose on contrary, $I = \langle 2, x \rangle = \langle p(x) \rangle$ for some $p(x) \in \mathbb{Z}[x]$. we first show that $1 \notin \langle 2, x \rangle = \{2a(x)+b(x)x | a(x), b(x) \in \mathbb{Z}[x]\}$, $deg(1) = 0$ and $deg(2a(x)+b(x)x) \geq deg(b(x)x) \geq 1$, so we have $1 \notin \langle 2, x \rangle$.

   by our assumption, we have $\langle 2, x \rangle = \langle p(x) \rangle$, since $2 \in \langle p(x) \rangle$, $\exists q(x) \in \mathbb{Z}[x]$ s.t. $2 = p(x)q(x)$, $deg(2) = deg(p(x)q(x)) \Rightarrow 0 = deg(p(x)q(x)) = deg(p(x)) + deg(q(x)) \geq 0 \Rightarrow deg(p(x)) = deg(q(x)) = 0$, we have:
   $$\begin{cases} p(x) = \pm 2 \\ q(x) = \pm 1 \end{cases} \text{or} \begin{cases} p(x) = \pm 1 \\ q(x) = \pm 2 \end{cases}$$
   if $p(x) = \pm 1$, $1 = p(x)^2 \in \langle p(x) \rangle$, which violates the fact we have proved that $1 \in \langle 2, x \rangle$.

   if $p(x) = \pm 2$, $x \in \langle p(x) \rangle = \pm 2 \cdot p(x), p(x) \in \mathbb{Z}[x]$, which is impossible since the coefficient of $xin \pm 2p(x)$ must be even and the coefficient of x is 1, we conclude that $\langle 2, x \rangle$ is not a principal ideal and thus $\mathbb{Z}[x]$ is not a PID.
4. if F is a field $(\mathbb{Q}, \mathbb{R}, \mathbb{C})$, then $F[x]$ is a PID. (prove it)

Proposition 25.1

let R be PID, then all prime ideals are maximal ideals. therefore I is prime ideal $\Leftrightarrow$ I is maximal ideal for PIDs.

Proof let $I \triangleleft R$ be prime ideal, since R is a PID, we know that $I = \langle a \rangle$ for some $a \in R$, suppose $I \subset J \subset R$, we want to prove that $J = I$ or $J = R$: since R is a PID, $J = \langle b \rangle$ for some $b \in R$, we have $\langle a \rangle \subset \langle b \rangle \subset R$, which implies that $b|a$, since I is a prime ideal, we know that a is a prime, $b|a \Rightarrow b = 1$ or $a \Rightarrow J = \langle b \rangle = \langle a \rangle = I$ or $J = \langle 1 \rangle = R$, we are done.

Chapter irreducible elements

Introduction

- irreducible element
- $a \sim b \Leftrightarrow a = ub$, R is an ID and $u \in U(R)$
- R is ID, prime element r is irreducible
- R is PID, prime element $\Leftrightarrow$ irreducible element

Definition 26.1 (irreducible element)

let R be commutative and unital, an element $a \in R$ is called irreducible if for all principal ideals $\langle b \rangle$ satisfying $\langle a \rangle \subset \langle b \rangle \subset R$, then $\langle b \rangle = \langle a \rangle$ or $\langle b \rangle = R$. in other words, $\langle a \rangle$ is maximal among all principal ideals.

Remark it is important to compare $\langle a \rangle$ being a maximal ideal and being an irreducible ideal.

Lemma 26.1

let R be a ID, then $a \in R$ is irreducible $\Leftrightarrow$ whatever $a = xy, \forall x, y \in R$, we have $a \sim x$ or $a \sim y$ review the definition of $a \sim b$ (a and b are associates: $\langle a \rangle = \langle b \rangle$)

Proof $(\Rightarrow)$: suppose $a = xy$, we have $x|a$ or $y|a \Rightarrow \langle a \rangle \subset \langle x \rangle$ or $\langle a \rangle \subset \langle y \rangle$, since we assume that a is irreducible, $\langle a \rangle \subset \langle x \rangle$ implies that $\langle a \rangle = \langle x \rangle$ or $\langle x \rangle = R$, which means that $a \sim x$ or $x \sim 1$. notice that $x \sim 1 \Leftrightarrow x \cdot x' = 1$ for $\forall x' \in R$, which implies that x is a unit of R. since $a = xy$, we have $a \sim y$
$(\Leftarrow)$: suppose RHS holds, we want to show that if $\langle a \rangle \subset \langle x \rangle \subset R$ for some $x \in R$, then $\langle x \rangle = \langle a \rangle$ or $\langle x \rangle = R$, by definition we know that a is irreducible. since $\langle a \rangle \subset \langle x \rangle$, we have $x|a$. RHS $\Rightarrow a \sim x$ or $a \sim y$, if $a \sim x$, by the definition of $\sim$, we know that $\langle a \rangle = \langle x \rangle$, else if $a \sim y$, which is equivalent as $a = uy$ for some $u \in U(R) \Rightarrow a = uy = xy \Rightarrow x = u \in U(R)$, so we have x is a unit of R. we conclude that $\langle x \rangle = \langle a \rangle$ or $\langle x \rangle = R$. we are done.

Remark by the above lemma, we have: a is irreducible indicates that if $a = xy$, then either x is a unit or y is a unit.
the whole point is that irreducibility is essential in factorization of elements in R: take any nonzero $r \in R$, if r is not irreducible then by the lemma, there are b and c non-units s.t. r = bc. we continue to check if b and c are irreducible. suppose b is not irreducible, then $b = b_1 b_2$ are not units. $r = bc = b_1 b_2 c = \ldots$ we can factorize r into a product of irreducibles and a (product of) units

Exercise 26.1 why we study irreducible or prime ID?
the answer is we want to factorize elements in R into a product of irreducibles or primes, just like what we do in $\mathbb{Z}$ or $\mathbb{R}[x]$

Lemma 26.2

if R is ID, $a \sim b \Leftrightarrow a = ub$ for some unit $u \in U(R)$

Proof

in general we want to study factorization of any $r \in R$ into $r = x_1 x_2 \ldots x_k$ for $x_1, x_2, \ldots, x_k$ prime or irreducible.

Exercise 26.2 if there is such factorization, is it unique?

the exercise is not true in general: let $R = \mathbb{Z}[\sqrt{-5}]$, we have 2 factorizations of 6 into irreducibles:

$$6 = (1 + \sqrt{-5})(1 - \sqrt{-5}) = (2 + 0 \cdot \sqrt{-5})(3 + 0 \cdot \sqrt{-5})$$

but in PID, we find the factorization is unique.

Proposition 26.1

let R be ID, if $0 \neq r, r \in R$ is a prime element (check definition 24.2), then r is irreducible

Proof if $r = xy$ then we have $1 \cdot r = xy$, $r|xy \Rightarrow r|x$ or $r|y \Rightarrow \langle x \rangle \subset \langle r \rangle$ or $\langle y \rangle \subset \langle r \rangle$. WLOG we assume $\langle x \rangle \subset \langle r \rangle$, since $r = xy$, we have $x|r \Rightarrow \langle r\rangle \subset \langle x\rangle$ and similarly we have $\langle r\rangle \subset \langle y\rangle$. combine the two inequalities we have $\langle r\rangle = \langle x\rangle$ or $\langle r\rangle = \langle y\rangle$, by the definition of irreducible elements, we know that r is irreducible.

Proposition 26.2

let R be a PID and $0 \neq r \in R$, then r is irreducible $\Leftrightarrow$ r is prime.

Proof $(\Rightarrow)$: suppose r is irreducible, we prove that $\langle r\rangle$ is maximal ideal, and then by a corollary in the chapter prime and maximal ideal we know that $\langle r\rangle$ is a prime ideal and thus r is a prime. suppose $\langle r\rangle \subset I \subset R$, then since R is PID, $I = \langle b\rangle$ for some $b \in R$, then by the definition of $r \in R$ to be irreducible, we have $\langle b\rangle = \langle r\rangle$ or $\langle b\rangle = R$. by the definition of maximal ideal, we are done. $(\Leftarrow)$: we know that PID must be an ID, and by the last proposition we are done.

Chapter factorization domains

Introduction

- *factorization domain*
- *ACCP*
- *PID satisfies ACCP*
- *satisfying ACCP $\Rightarrow$ being factorization domain*
- *unique factorization into nonunit irreducibles in ID*
- *generalized fundamental theorem of arithmetic*
- *UFD, PID $\subset$ UFD*

Definition 27.1 (factorization domain)

let R be ID, we say R is a factorization domain if for all $r \neq 0 \in R$, r can be factorized into a finite number of irreducibles up to units, i.e. $r = x_1 \ldots x_k$, x_i are irreducible. ♣

Example 27.1 $R = \mathbb{Z}$ is a factorization domain since by fundamental theorem of algebra, we know that every element in R can be factorized into a product of prime numbers up to units 1 or -1.

Remark by convention, $1 \in R$ can be factorized into a product of zero irreducible elements (1 is treated as not irreducible)

Definition 27.2 (ascending chain condition of principal ideal (ACCP))

let R be ID, we say R has the ascending chain condition of principal ideal if for all $I_1, I_2, \ldots$ principal ideals s.t. $I_1 \subset I_2 \subset \ldots$ then there must be a place s.t. $I_n = I_{n+1}$ ♣

Lemma 27.1

if R is PID, then R satisfies ACCP ♡

Proof suppose we have a sequence of principal ideals, $I_1 = \langle a_1 \rangle \subset I_2 = \langle a_2 \rangle \subset I_3 \subset \ldots$ then we claim that $\bigcup_{i=1}^{\infty} I_i = \langle r \rangle$ is an ideal (proof in HW10). then $r \in \bigcup_{i=1}^{\infty} I_i \Rightarrow r \in I_m$ for some m and thus $r \in I_{m+1}, I_{m+2}, \ldots \Rightarrow \bigcup_{i=1}^{\infty} = \langle r \rangle \subset I_{m+1}, I_{m+1}, \ldots \Rightarrow \langle r \rangle = \bigcup_{i=1}^{\infty} I_i = I_{m+1} = I_{m+2} = \ldots$

Lemma 27.2

if R satisfies ACCP, then R is a factorization domain. ♡

Proof

Remark if R is PID, then we can factorize any $r \neq 0$ into a finite product of irreducibles/primes $r = x_1 x_2 \ldots x_k$

✍ **Exercise 27.1** is this factorization unique? i.e. suppose $x_1 x_2 \ldots x_k = y_1 y_2 \ldots y_l$ be two factorizations of irreducibles/primes, is it true that $k = l$ and there is a permutation $\sigma \in S$ s.t. ???

Theorem 27.1

if R is PID, then R is a factorization domain. ♡

Proof check the above two lemmas, we have: R is PID $\Rightarrow$ R satisfies ACCP $\Rightarrow$ R is a factorization domain.

Example 27.2

Remark

1. in factorization of $r \in R$, we only use nonunit irreducible element
2. ordering of those nonunit irreducible factors do not matter
3. the nonunit irreducible factors of $r \in R$ can differ by 1 or -1 or generally they can differ by a unit.

Theorem 27.2

let R be an ID, suppose we have two factorizations of $0 + r \in R$: $r \sim x_1 x_2 \ldots x_k \sim y_1 y_2 \ldots \sim y_l$ where x_i, y_j are nonunit primes, then we must have: $k = l$ and there exists a permutation $\sigma \in S_k$ s.t. $x_i \sim y_{\sigma(i)}$ for $i = 1, 2, \ldots, k$. in other words, the factorization of any $r \in R$ is unique.

Proof we will prove a stronger version: $x_1 x_2 \ldots x_k \sim y_1 y_2 \ldots y_l$ and x_i, y_j are nonunit irreducibles.

Example 27.3 let $R = \mathbb{Z}$, we factorize $r = 60$ into nonunit irreducibles: $60 \sim 2 \cdot 2 \cdot 3 \cdot 5 \sim (-3)(-2)5 \cdot 2$, then we can check the theorem: $k = l = 4$ and we define a permutation such that $x_1 = 2 \sim y_1 = -2$, $x_2 = 2 \sim y_4 = 2$, $x_3 = 3 \sim y_1 = (-3)$, $x_4 = 5 \sim y_3 = 5$

Corollary 27.1

let R be a PID, then every $0 \neq r \in R$ can be uniquely factorized into a product of finite number of primes.

Proof by the first remark of this chapter, we have a factorization of r into irreducibles, by the fact that $r \in R$ (R is PID) is irreducible is equivalent as r is a prime, and by the last theorem we know that: for PID, the factorization of primes is unique.

Remark this corollary generalizes the fundamental theorem of arithmetic from $R = \mathbb{Z}$ to PID.

Definition 27.3 (unique factorization domain (UFD))

let R be ID, then R is called unique factorization domain if every $0 \neq r \in R$ can be factorized uniquely into a finite number of irreducibles.

Example 27.4 all PIDs are UFDs; $\mathbb{Z}[x]$ is a UFD (proved later) but not a PID. so we have

$$PID \subset UFD$$

Chapter Euclidean domain

Introduction

- Euclidean domain
- ED ⊂ PID
- dedekind-harsse function
- for R being an ID, having dedekind-harsse function ⇔ PID
- field ⊂ ED

Definition 28.1 (Euclidean domain)

let R be an integral domain, then we say R is an Euclidean domain if there is a norm function $N : R \setminus \{0\} \rightarrow \mathbb{N} \setminus \{0\}$ satisfying that: $\forall a, b \neq 0 \in R$, we either have $b|a$ or $\exists q, r \neq 0 \in R$ s.t. $a = qb + r$, with $N(r) < N(b)$. we say N is multiplicative if it satisfies $N(rs) = N(r)N(s), \forall r, s \in R \setminus \{0\}$

Example 28.1

1. $R = \mathbb{Z}$ is an ED: $N(a) := |a|$
2. $R = \mathcal{F}[x]$ is an ED, $\mathcal{F}$ is a field: $N(p(x)) := deg(p(x)) =$ the leading power of $p(x)$
3. $R = \mathbb{Z}[i]$ is an ED: $N(a + bi) := a^2 + b^2$

Theorem 28.1

if R is a field, then R is an ED

Proof let $N : R \setminus \{0\} \longrightarrow \mathbb{N} \setminus \{0\}$ be defined as $N(x) = 1, \forall x$, then $\forall a \in R$ and $b \neq 0 \in R$, we prove that either $b|a$ or $\exists q, r \in R$ s.t. $a = bq + r$ with $N(r) < N(b)$: in a field, we can always find $b^{-1}a$ in the field s.t. $b(b^{-1}a) = a$ and thus $b|a$. we are done.

Theorem 28.2

if R is ED, then R is also PID.

Proof using the proposition below.

Definition 28.2 (dedekind-harsse function)

let R be an ID, a dedekind-harsse function in R is a map $N : R \setminus \{0\} \longrightarrow \mathbb{N} \setminus \{0\}$ s.t. $\forall a, b \in R \setminus \{0\}$, either: we have $b|a$ or $\exists p, q \in R, r \in R \setminus \{0\}$ s.t. $pa = qb + r$ with $N(r) < N(b)$

Example 28.2 if R is ED with $N : R \setminus \{0\} \longrightarrow \mathbb{N} \setminus \{0\}$, then N is automatically a dedekind-harsse function (let $p = 1$)

Proposition 28.1

let R be ID, then R is PID ⇔ R has dedekind-harsse function (and consequently all EDs are PIDs).

Proof (⇒): if R is PID, we know that R is UFD. for all $x \neq 0 \in R$, we can define $N : R \setminus \{0\} \longrightarrow \mathbb{N} \setminus \{0\}$ to be $2^{\#}$, # is the number of irreducible nonunit number in the factorization of x, e.g. $N(81) = 2^4$ since $81 = 3 \cdot 3 \cdot 3 \cdot 3$ and $N(15) = 2^2$ since $15 = 3 \cdot 5$. we claim that N is a dedekind-harsse function.
suppose $a, b \in R \setminus \{0\}$ with $b \nmid a$, we prove that there exists $p, q \in R$ and $r \in R \setminus \{0\}$ s.t. $pa = qb + r$ with $N(r) < N(b)$. we have $\langle r \rangle = \langle a, b \rangle \supsetneq \langle b \rangle$, since R is PID, $\langle a, b \rangle = \langle r \rangle$ for some r, then r satisfies $r \in \langle r \rangle = \langle a, b \rangle \rightarrow r = pa - qb$ for some p, q, so we have $\langle r \rangle \supsetneq \langle b \rangle \Rightarrow r|b$, we have: r is strictly smaller than b ⇒r$\cdot z = b$, z is a nonunit. let $x_1x_2...x_m$ be the irreducible nonunit factorization of r and $y_1y_2...y_n$ be the irreducible nonunit factorization of z, then $N(r) = 2^m < 2^{m+n} = N(b)$, N is a dedekind-harsse function.
(⇐)suppose R has a dedekind-harsse function $N : R \setminus \{0\} \rightarrow \mathbb{N} \setminus \{0\}$, let $I \triangleleft R$ be any ideal. pick $b \in I \setminus \{0\}$ be s.t. $N(b)$ is minimal among all elements in I. we claim that $I = \langle b \rangle$: obviously $\langle b \rangle \subset I$, for all $a \in I \setminus \{0\}$, we have $a \in \langle b \rangle$

or $a\langle b\rangle \Leftrightarrow r = pa - qb$. since $b \in I, a \in I, r = pa - qb \in I$and $N(r) < N(b)$, which violates with $N(b)$ is minimal among all elements in I, so only the possibility $a \in \langle b\rangle$ holds, so we have $\forall a \in I \setminus \{0\}, a \in \langle b\rangle$, i.e. $I = \langle b\rangle$, R is a PID by definition.

Chapter gaussian integers

Definition 29.1 (integer prime; gaussian prime)

we call $p \in \mathbb{Z}$ is an integer prime if it is prime in $\mathbb{Z}$; we call $p + 0i \in \mathbb{Z}[i]$ is a gaussian prime if it is prime in $\mathbb{Z}[i]$

Remark observe that:

a. $n = ab \in \mathbb{Z}$ is not an integer prime, then $n + 0i \in \mathbb{Z}[i]$ is not a gaussian prime.

b. $U(\mathbb{Z}[i]) = \{\pm 1, \pm i\}$, therefore $z \in U(\mathbb{Z}[i]) \leftrightarrow N(z) = 1$

c. if $N(z) = p$, p is an integer prime, e.g. $N(2+i) = 5$ then $z = 2 + i$ is a gaussian prime.

Proof suppose contrary z is not a gaussian prime, then z is not gaussian irreducible, $z = xy$ and x, y are nonunits$\rightarrow$ $N(z) = N(xy) = N(x)N(y)$ (x, y are nonunits $\rightarrow N(x) \neq 1$ and $N(y) \neq 1$) so p is not a integer prime. we reach a contradiction.

Lemma 29.1 (classification of gaussian prime of form $a + bi, a, b \neq 0$)

let $a + bi \in \mathbb{Z}[i]$ with $b \neq 0$. then $(a + bi)$ is gaussian prime $\longleftrightarrow N(a + bi) = a^2 + b^2 = p$ is integer prime

Proof ($\leftarrow$): proved above

($\rightarrow$): suppose $(a + bi)$ is a gaussian prime, then $\overline{a + bi} = a - bi$ is also a gaussian prime. consider $(a + bi)(a - bi) = a^2 + b^2 = p_1 p_2 ... p_r$, p_i are prime integers in $\mathbb{Z}$. then we have $r \leqslant 2$, otherwise suppose $(a + bi)(a - bi) = p_1 p_2 p_3$, there are 2 gaussian prime factors on LHS while there are (more than) 3 gaussian prime factors on RHS. this contradicts the fact that the $\mathbb{Z}[i]$ is $ED \rightarrow PID \rightarrow UFD$. so we have $r \leqslant 2$, suppose $r = 2$: $(a + bi)(a - bi) = pq$, p, q are integer primes. by $\mathbb{Z}[i]$ being UFD, this implies that $p, q \in \mathbb{Z}[i]$ are also gaussian primes. otherwise we will have more than 2 factors on RHS again. by unique factorization, we have $\begin{cases} p \sim a + bi \\ q \sim a - bi \end{cases}$ or $\begin{cases} p \sim a - bi \\ q \sim a + bi \end{cases}$ and they are both impossible. suppose $p \sim a + bi$, we have $p = u(a + bi)$, $u \in U(\mathbb{Z}[i]) = \{\pm 1, \pm i\} \rightarrow p = a + bi$ or $-a - bi$ or $ai - b$ or $-ai + b$, which is impossible by the definition of integer prime that $p \in \mathbb{Z}$.

Remark we wonder when is $a, ai \in \mathbb{Z}[i]$ a gaussian integer? (we only need to study $a + 0i \in \mathbb{Z}[i]$ since $a \sim ai$)

Theorem 29.1

all gaussian primes of the form $a + 0i$ is a gaussian prime, then $a = p$ must be an integer prime.

Proof by definition, we know that if $a + 0i$ is a gaussian prime, then $a = p$ must be an integer prime.

1. $p = 2$: 2 is not a gaussian prime since $2 = (1 + i)(1 - i)$ can be factorized into 2 nonunits.
2. $p \equiv 3(mod4)$: we claim that $p + 0i$ is always a gaussian prime, then suppose contrary $p = (x + yi)(x - yi)$ for some nonunits $x + \pm yi \in \mathbb{Z}[i]$, then $p = x^2 + y^2$, $x, y \in \mathbb{Z}$. but note that $x^2 \equiv 0, 1(mod4)$, $y^2 \equiv 0, 1(mod4)$, we have $x^2 + y^2 \equiv 0, 1, 2(mod4)$. this contradicts $p \equiv 3(mod4)$, so we proved that $p + 0i$ is a gaussian prime.
3. $p \equiv 1(mod4)$: we claim that p is not a gaussian prime: suppose on contrary p is a gaussian prime, then we can prove that $p | m^2 + 1$ for some $m \in \mathbb{Z}$ (HW10). we have $p | (m + i)(m - i) \rightarrow p | (m + i)$ or $p | (m - i)$, suppose $p | (m + i)$, then $\exists z \in \mathbb{Z}[i]$ s.t. $p \cdot z = m + i \in \mathbb{Z}[i]$, we have $p \cdot z = m + i \in \mathbb{C} \rightarrow Z = \frac{m}{p} + \frac{1}{p} i \in \mathbb{C}$ which means $z \in \mathbb{Z}[i]$ since $\frac{1}{p} \notin \mathbb{Z}[i]$, so we reach a contradiction since we assume $z \in \mathbb{Z}[i]$.

Corollary 29.1 (fermat)

let $p \in \mathbb{Z}$ be integer prime satisfying $p \equiv 1(mod4)$, then $\exists x, y \in \mathbb{Z}$ s.t. $p = x^2 + y^2$

Proof by the above theorem, we know that p is not a gaussian prime, we have $\exists x + yi \in \mathbb{Z}[i]$ s.t. $(x + yi) | p \rightarrow (x - yi) | p$. suppose $(x + yi)z = p$, $x + yi$ and z are nonunit. we have $N(x + iy)N(z) = N(p) = p^2$ and $N(x + yi) \neq 1, p^2$, so we have

$N(x+iy) = N(z) = p \to p = (x+iy)(x-iy) \to p = x^2 + y^2$

the answer to the above exercise that when $a \in \mathbb{Z}$ is a gaussian prime is: all gaussian primes are of the form:
1. $a + bi(a^2 + b^2 = p,$ p is a prime)
2. q, $q \equiv 3(mod 4)$ is prime

Example 29.1

Example 29.2

Remark similarly by studying ED in $\mathbb{Z}[\sqrt{-2}]$, we can solve the diophantine equation $x^2 + y^2 = z^2$ for integers $x, y, z \in \mathbb{Z}$

Chapter polynomial rings

let R be an ID, our goal is to understand when $p(x) \in R[x]$ is irreducible in $R[x]$. **Remark** a. if R is ID, then $R[x]$ is ID
b. by (a), we have: $p(x) \in R[x]$ is irreducible $\Leftrightarrow$ whatever $p(x) = q(x)h(x)$ is factorized into 2 polynomials, $h(x)$ or $q(x)$ is a unit in $R[x]$.
c. the units in $R[x]$ are of the form $r + 0x + 0x^2 + ... \in R[x]$ where $r \in R$ is a unit in R. e.g. $u(x) = 1, -1$ in $\mathbb{Z}[x]$ and in $\mathbb{Q}[x]$, $u(x) = a \neq 0$, a is a constant polynomial.

Example 30.1 a. all units in $R = \mathbb{C}[x]$ are of the form $u(x) = (x - \alpha), \alpha \in \mathbb{C}$
b. let R = $\mathbb{R}$, all irreducible polynomials in $\mathbb{R}[x]$ are of the form of a unit multiple of: $(x - \beta)$ for $\beta \in \mathbb{R}$ or $(x^2 + \gamma x + \delta)$ for $\gamma, \delta \in \mathbb{R}$ with $\gamma^2 - 4\delta < 0$ so there is no real roots.
c. what about $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$? we will give some sufficient conditions on when $p(x) \in \mathbb{Z}[x]$ or $\mathbb{Q}[x]$ to be irreducible below:

Remark why do we study irreducible polynomials? let $\mathcal{F}$ be a field (like $\mathbb{Q}$), recall $\mathcal{F}[x]$ is a ED with norm function $N(p(x)) = deg(p(x))$. so we have $\mathcal{F}[x]$ is a PID and hence $p(x)$ is irreducible iff $p(x)$ is prime $\Leftrightarrow \langle p(x)\rangle \triangleleft \mathcal{F}[x]$ is prime $\Leftrightarrow \langle p(x)\rangle \triangleleft \mathcal{F}[x]$ is maximal $\leftrightarrow \mathcal{F}[x]/\langle p(x)\rangle$ is a field. and then we construct a new field from an old field $\mathcal{F}$.

Example 30.2 let $\mathcal{F} = \mathbb{Q}$, $p(x) = x^4 + x^3 + x^2 + x + 1 \in \mathbb{Q}[x]$ is irreducible.
consider $\mathbb{S} := \mathbb{Q}[x]/\langle p(x)\rangle = \{f(x)+\langle p(x)\rangle : f(x) \in \mathbb{Q}[x]\} = \{a_4x^4+a_3x^3+a_2x^2+a_1x+a_0+\langle p(x)\rangle : a_0, a_1, a_2, a_3, a_4 \in \mathbb{Q}\}$. our observations are:
a. we have an injective ring homomorphism $i : \mathbb{Q} \to \mathbb{S} : \alpha \to \alpha + \langle p(x)\rangle : \overline{\alpha}$
b. we can see $p(x) = 1x^4+1x^3+1x^2+1x+1$ as a polynomial $p(x) = \overline{1}x^4+\overline{1}x^3+\overline{1}x^2+\overline{1}x+\overline{1} \in \mathbb{S}[x]$. take $\Theta := x+\langle p(x)\rangle \in \mathbb{S}$ then substitute $\Theta \in \mathbb{S}$, $p(x) \in \mathbb{S}[x] : p(\Theta) = (1x^4 + 1x^3 + 1x^2 + 1x + 1) + \langle p(x)\rangle \in \mathbb{S}$. so we have $p(\Theta) = 0 \in \mathbb{S}$ i.e. Θ is a root of $p(x) \in \mathbb{S}[x]$

Example 30.3 $f(x) = x^2 + 1 \in \mathbb{R}[x]$ is irreducible, then $\mathbb{S} := \mathbb{R}[x] \setminus \langle x^2 + 1\rangle$ and we have $\mathbb{R} \hookrightarrow \mathbb{S}$. all elements in $\mathbb{S}$ are of the form $(ax+b)+\langle x^2+1\rangle, a, b \in \mathbb{R}$. in particular, let $\alpha = x+\langle x^2+1\rangle$, then $f(\alpha) = \alpha^2+1_{\mathbb{S}} = (x+\langle x^2+1\rangle)^2+(1+\langle x^2+1\rangle) = x^2 + \langle x^2 + 1\rangle + 1 + \langle x^2 + 1\rangle = 0_{\mathbb{S}}$. we have: all elements in $\mathbb{S}$ are of the form $a\alpha + b$ with α satisfying $\alpha^2 + 1 = 0$. we have $S \cong \mathbb{C}$ by $a\alpha + b \to ai + b$

Definition 30.1 ($\tilde{\phi}$)

let R, S be integral domains and $\phi : R \to S$ be a unital ring homomorphism, (e.g. $\phi : \mathbb{Z} \to \mathbb{Q}$; $\phi : \mathbb{Z} \to \mathbb{Z}_p$: $a \to [a]_p$), then we define $\tilde{\phi} : R[x] \to S[x]$ by $\tilde{\phi}(a_nx^n+...+a_1x+a_0) := \phi(a_n)x^n+\phi(a_{n-1})x^{n-1}+...+\phi(a_0) \in \mathbb{S}[x]$ ♣

Example 30.4

Theorem 30.1 (reduction test)

let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial. suppose $\exists$ a prime number p s.t. under $\tilde{\phi} : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$, $\tilde{\phi}(f(x)) \in \mathbb{Z}_p[x]$ is irreducible in $\mathbb{Z}_p[x]$, then $f(x) \in \mathbb{Z}[x]$ is irreducible. ♡

Proof suppose $f(x) = x^n + a_{n-1}x^{n-1} + ... + a_0 = g(x) \cdot h(x) \in \mathbb{Z}[x]$. we prove that $g(x)$ or $h(x)$ is a unit in $\mathbb{Z}[x]$, i.e. $g(x) = \pm 1$ or $h(x) = \pm 1$, then $\tilde{\phi}(f) = \tilde{\phi}(g) \cdot \tilde{\phi}(h)$, we have

$$deg(\tilde{\phi}(g)) + deg(\tilde{\phi}(h)) = deg(\tilde{\phi}(f)) = deg(f) = deg(g(x)) + deg(h(x))$$

note that $deg(\tilde{\phi}(g)) \leqslant deg(g)$ and $deg(\phi(\tilde{h})) \leqslant deg(h)$, we have $deg(\tilde{\phi}(g)) = deg(g)$ and $deg(\tilde{\phi}(h)) = deg(h)$, recall that we have the condition that $\tilde{\phi}(f(x))$ is irreducible in $\mathbb{Z}_p[x] \Rightarrow deg(\tilde{\phi}(g)) = 0$ or $deg(\tilde{\phi}(h)) = 0 \Rightarrow deg(g) = 0$ or $deg(h) = 0$

Example 30.5

Theorem 30.2 (eisenstein's theorem)

let $f(x) = a_n x^n + ... + a_1 x + a_0 \in \mathbb{Z}[x]$ be a primitive polynomial, i.e. $gcd(a_n, a_{n-1}, ..., a_0) = 1$, suppose $\exists$ prime number p s.t.
a. $p|a_i, \forall 0 \leqslant i < n$
b. $p \nmid a_n$
c. $p^2 \nmid a_0$, then $f(x) \in \mathbb{Z}[x]$ is irreducible.

Proof let $f(x) = g(x) \cdot h(x) \in \mathbb{Z}[x]$. let $\tilde{\phi} : \mathbb{Z}[x] \Rightarrow \mathbb{Z}_p[x]$, by a., b., $\tilde{\phi}(f) = \tilde{\phi}(g) \cdot \tilde{\phi}(h) = [a_n]_p x^n + 0 + ... + 0 \Rightarrow \tilde{\phi}(g) \cdot \tilde{\phi}(h) \sim x^n \Rightarrow$, so we have $\tilde{\phi}(g) \sim x^i, \tilde{\phi}(h) \sim x^{n-i}$ for some $0 \leq i \leq n$. suppose $0 < i < n$, then $\tilde{\phi}(g)\alpha x^i, \tilde{\phi}(h) = \beta x^{n-i}$ in $\mathbb{Z}_p[x] \Rightarrow g(x) = c_i x^i + ... + c_0$, $h(x) d_i x^{n-i} + ... + d_0$ where c_0 and d_0 are multiples of $p \Rightarrow f(x) = g(x)h(x) = ... + c_0 d_0$, note $c_0 d_0$ is a multiple of p^2, which violate c. so we have $\tilde{\phi}(g) \sim x^i, \tilde{\phi}(h) \sim x^{n-i}$ for $i = 0$ or $n \Rightarrow deg(g) = 0$ or $deg(h) = 0$, since $f = gh$ is primitive, we have $g = \pm 1$ or $h = \pm 1$. we are done.

Example 30.6 a. $x^3 + 2x + 6$ is irreducible in $\mathbb{Z}[x]$: let $p = 2$ and we can use the last theorem. however we cannot use the reduction test: let $p = 3$, $\tilde{\phi}(x^3 + 2x + 6) = x^3 + 2x$ is reducible in $\mathbb{Z}_3[x]$

Theorem 30.3 (gauss' lemma)

let $f(x) \in \mathbb{Z}[x]$ be a nonconstant polynomial, thus $f(x) \in \mathbb{Z}[x]$ is irreducible $\Leftrightarrow f(x) \in \mathbb{Q}[x]$ is irreducible and $f(x)$ is primitive.

Corollary 30.1

$\mathbb{Z}[x]$ is a UFD.

Chapter field

one reason to study fields is to study roots of polynomials $p(x) \in \mathcal{F}[x]$ where $\mathcal{F}$ is a field. to do so, one has to extend our base field $\mathcal{F}$ to a larger field K. e.g. $x^2 + 1 \in \mathbb{R}[x]$ has roots in $K = \mathbb{C}$.
there are two fields we are interested in:

1. number field: a subfield of $\mathbb{C}$ like $\mathbb{R}, \mathbb{Q}, \mathbb{Q}[i] = \{a + bi | a, b \in \mathbb{Q}\}$, $Q[\sqrt{2}] = \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}$
2. finite field: $|\mathcal{F}| < \infty$, e.g. $\mathbb{Z}_2, \mathbb{Z}_3, \ldots$

Definition 31.1 (characteristic)

$\mathcal{F}$ is a field, then the characteristic of $\mathcal{F}$ is the smallest positive integer m s.t. $1_{\mathcal{F}} + \ldots + 1_{\mathcal{F}} = 0_{\mathcal{F}}$ and $char(\mathcal{F}) := m$; if no such m exists, we let $char(\mathcal{F}) = \infty$

♣

Theorem 31.1

all fields with $|\mathcal{F}| < \infty$ must have $|\mathcal{F}| = p^m$ for some p prime and m positive integer. moreover if $|\mathcal{F}_1| = |\mathcal{F}_2| = p^m$, then $\mathcal{F}_1 \cong \mathcal{F}_2$ as rings.

♡