Group Theory

· Set

A set is a collection of elements

$X = \{x_1, x_2, \cdots x_n\} = \{x_i\}$

$= \{x \mid x \text{ satisfies property } P\}$.

· Map

A map f from x to y is a rule which assigns a unique element of y to an element of x.

① surjective: iff $\{f(x) \mid x \in X\} = f(X) = Y$

② injective: iff $x_1 \neq x_2$, then $f(x_1) \neq f(x_2)$
or if $f(x_1) = f(x_2)$, then $x_1 = x_2$

③ bijective: both ① and ②

· Product

A product of X and Y is a set

$X \times Y = \{(x, y) \mid x \in X, y \in Y\}$.

· Equivalence Relations

An equivalence relation R or $(\sim)$ is a subset $R \subseteq X \times X$, such that:

① reflexivity: $\forall x \in X.\ (x, x) \in R$

② symmetry: if $(x, y) \in R$, then $(y, x) \in R$

③ transtivity: if $(x, y), (y, z) \in R$, then $(x, z) \in R$

· Equivalence Class

An equivalence class of $x \in X$ is

$[x] = \{y \in X \mid (x, y) \in R\} = \{y \in x \mid x \sim y\}$

· Quotient

A quotient of X by R is $X/_R$ = all R-equivalence classes.

· $\mathbb{Z}/n\mathbb{Z}$

$\forall a, b \in \mathbb{Z}$, $a \sim b$ iff $n \mid a - b$

· Group

A group $(G, *)$ is a set G and a binary operation $* : G \times G \to G$. s.t.

$\forall (g_1, g_2),\ * (g_1, g_2) = g_1 * g_2$

① associativity: $(a * b) * c = a * (b * c)$

② identity: $\exists e = e_G \in G.\ \forall a \in G$:

$a * e = e * a = a$

③ inverse: $\forall a \in G.\ \exists a^{-1} \in G$:

$a * a^{-1} = a^{-1} * a = e$

· Homomorphism

A homomorphism from $(G, *)$ to $(H, \odot)$ is a map (of sets): $f: G \to H$. s.t.

$\forall x, y \in G\ \ f(x * y) = f(x) \odot f(y)$

Group Theory

· Symmetric Groups

Let X be a set, we define $Sym(X) = S_X = S_{|X|}$ is a group of all bijective maps $f: X \to X$

· Subgroup

$G = (G, *)$ is a group. Subgroup H of G is a group H with the group operation restricted from G.

1) identity: $e_G \in H$

2) closure: $\forall h_1, h_2 \in G,\ h_1 \cdot h_2 \in H$

3) inverses: $\forall h \in H,\ h^{-1} \in H$

· Proper Subgroup

Proper subgroup of G is a subgroup which is not trivial or G itself.

· Cyclic Subgroup

$\langle a \rangle$ = cyclic subgroup of G generated by a as a set $\{a^k \mid k \in \mathbb{Z}\}$ and operation $* = *_G$.

· Isomorphism

Isomorphism is bijective homomorphism.

$f: (G, *) \to (K, \circ)$. $f(g * h) = f(g) \circ f(h)$

(which is bijective. injective and surjective)

· Kernel

kernel of ϕ. kernel is the preimage of identity

$\phi: G \to H$. $\ker(\phi) = g \in G : \phi(g) = e_G$.

· Coset

$H \leq G$. $\forall g \in G$, $gH = g * H = \{g * h \mid h \in H\}$ is the coset of g.

· Direct Product

G, H are groups. direct product of G & H is a set $G \times H = \{(g, h) \mid g \in G, h \in H\}$ with the following operation:

$(g_1, h_1) \cdot (g_2, h_2) = (g_1 g_2, h_1 h_2)$

· Normal

$H \leq G$. H is normal iff $\forall g \in G$, $gH = Hg$

or iff $\forall g \in G$. $gHg^{-1} = H$

· Inner Direct Product

G is a group. $H, K \leq G$. G is the internal direct product of H and K iff

① $G = H \cdot K = \{hk \mid h \in H, k \in K\}$

(warning: $H \cdot K \neq H \times K$)

② $H \cap K = e_G$ (i.e. as small as possible)

③ $hk = kh$ for any $h \in H, k \in K$ (warning: G is not abelian)

Group Theory

· Permutation Group

permutation group G (on set X) is a subgroup of $Sym(X)$

· Stabilizer

$G \leq Sym(X)$. For each $x \in X$.

$G_x = Stab_G(x) = \{\sigma \in G \mid \sigma(x) = x\}$.

· Orbit

$x \in X$. orbit of x under G is the full set $Orb_G(x) = \{g(x) \mid g \in G\} = O_x = O(x)$

· Group Action ($G \times X \to X$) "G acts on X"

"G acts on X" is the following map:

$\Phi: G \times X \to X$. $(g, x) \mapsto g \circ x = g(x)$

s.t. 1) $\forall x \in X.\ e_G(x) = x$

2) $\forall g_1, g_2 \in G.\ \forall x \in X.$

$(g_1 * g_2)(x) = g_1(g_2(x))$

· Left Regular Action on G itself

$G = (G, *)$. $X = G$ as a set

$\Phi: G \times G \to G$. $(g, h) \mapsto \lambda_g(h) = g * h$

· abelian

A group G is abelian or commutative iff $g_1 \cdot g_2 = g_2 \cdot g_1$ for each $g_1, g_2 \in G$.

· Order

$a \in G$. order of a is minimal $n \in \mathbb{N}$.

s.t. $a^n = e_G$

· Quotient Group

Fix a normal subgroup H of a group G. Then the set of cosets G/H forms a group with the operation

$g_1H \cdot g_2H := (g_1 \cdot g_2)H$

· image

$\varphi: G \to H$. $im(\varphi) = \{\varphi(g) : g \in G\}$.

($im(\varphi)$ is a subgroup of H)

Ring Theory

- Ring

Ring is a set with 2 operations $(R, *, \circ)$ with

→ $(R, +)$ is an abelian (①) group (②~④) ✓

→ $(R, \times)$ is associative (⑤)

→ $(R, +, \times)$ distributivity: (⑥)

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

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

→ identity for "+": 0

units for "×": 1 (⑦)

- Commutative ring with 1_R

→ "×" is commutative (⑧)

- Field

1~8 + $R^\times = R \setminus \{0\}$. i.e. $a \in R$. and $a \neq 0$ then $\exists b \in R.\ ab = 1$

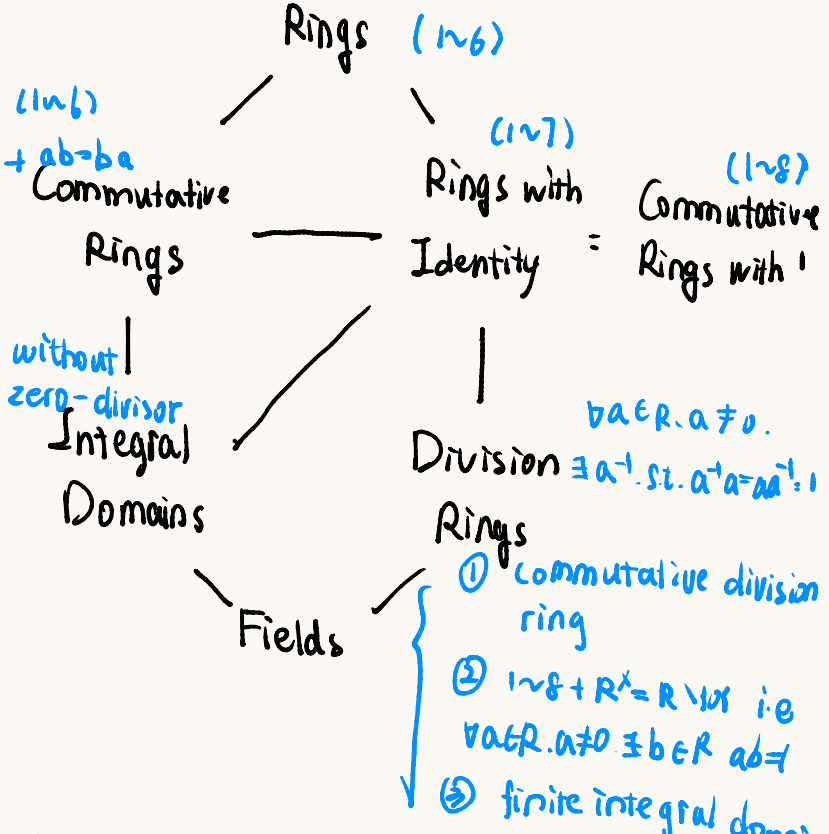
- Integral Domain

A non-trivial commutative ring with identity is called integral domain if $\forall a, b \in R$ s.t. $ab = 0 \rightarrow a = 0$ or $b = 0$ (without zero-divisor)

- Division Ring

A ring R with an identity in which every non-zero element in R is a unit ($\forall a \in R.\ a \neq 0.\ \exists a^{-1}.$ s.t $a^{-1}a = aa^{-1} = 1$)

RING



- Units

A unit $a \in R$ is an element s.t. $\exists b \in R.\ ab = 1_R$

Ring Theory

- **Zero Divisors**

A zero-divisor is an element a s.t. $\exists c \neq 0.\ a \cdot c = 0_R$

- **Division Algorithm**

$\forall (a,b).\ a,b \in \mathbb{Z}$. there exists a pair $(q,r).\ q,r \in \mathbb{Z}.\ a = bq + r$. where $0 \leq |r| < b$.

- **Division Algorithm for $\mathbb{Q}[T]$.**

$\forall\ (f(T), g(T)).\ f, g \in \mathbb{Q}[T]$. there exists $(q,r).\ q,r \in \mathbb{Q}[T]$. $f = gq + r$ where $0 \leq \deg(r) < \deg(g)$

- **Division Algorithm for $\mathbb{Z}[i]$**

for $\mathbb{Z}[i] = \{a + bi \mid a,b \in \mathbb{Z}\}$.
$\forall x, y \in \mathbb{Z}[i]$. there exists $q,r \in \mathbb{Z}[i]$. $x = y \cdot q + r$. where $N(r) < N(y)$

- **Ring Homomorphism**

1) $\phi(r+t) = \phi(r) + \phi(t)$
2) $\phi(r \times_R t) = \phi(r) \times_S \phi(t)$
3) $\phi(1_r) = 1_t$

- **Ring Isomorphism**

$\phi: R \to S$ is bijective homomorphism of rings

- **Ideal**

m in R is ideal if:
1) additive subgroup ($\forall a,b \in I.\ a+b \in I$)
2) $\forall x \in m.\ r \in R.\ r \cdot x \in m$

- **R/m**

A quotient of R by m is a set R/m of elements $r+m$
$(r+m) + (t+m) = (r+t+m)$
$(r+m) \cdot (t+m) = (rt+m)$

- **Maximal Ideal**

I is a maximal ideal in R. there are no $J \lneq R$ s.t. $I \lneq J \lneq R$

- **Prime Ideal**

$I \trianglelefteq S$ is prime iff $ab \in I$ then $a \in I$ or $b \in I$

- **Principal Ideal**

R = commutative ring with 1_R. $x \in R$
$(x) = \{r \cdot x \mid r \in R\}$ is principle ideal generated by x

- **Ideal Generation**

R = commutative ring with 1_R. $x_1, x_2 \cdots x_k \in R$
$(x_1, x_2 \cdots x_k) = \langle x_1, x_2 \cdots x_k \rangle$
$= \{r_1 \cdot x_1 + r_2 \cdot x_2 + \cdots + r_k \cdot x_k \mid r_1, r_2 \cdots r_k \in R\}$
is an ideal generated by $x_1, x_2 \cdots x_k$.

Ring Theory

- **Ideal Multiplication**

R = commutative ring with 1_R. $I, J \trianglelefteq R$

$$I \cdot J = \{ i_1 j_1 + i_2 j_2 + \cdots + i_m j_m \mid i_1 \cdots i_m \in I, \; j_1 \cdots j_m \in J \}$$

this is multiplication of ideals.

- **Vector Space.**

A vector space V or F is:

1. an abelian group
2. a multiplication by scalar.

here F = field = $(F, +, \times)$

$- \cdot - : F \times V \to V$ s.t.

1) $\alpha(\beta v) = (\alpha\beta)v$
2) $(\alpha+\beta)v = \alpha v + \beta v$
3) $\alpha(v+u) = \alpha v + \alpha u$
4) $1_F \cdot v = v$

- **Linear Map**

$A : (V, +) \to (W, +)$ is a linear map.

V, W are F-vector spaces maps from V to W (matrices)

1. homomorphism of abelian groups
2. $A(\alpha \cdot_V v) = \alpha \cdot_W A(v)$

- **Basis**

A basis of V of F is a set of vectors $e_1, e_2 \cdots e_n$ s.t.

1. $V = \langle e_1, e_2 \cdots e_n \rangle = \alpha_1 e_1 + \cdots \alpha_n e_n$
2. $e_1, e_2 \cdots e_n$ are linearly independent

- **subring**

A subset S of a ring R is a subring of R if:

1. $S \leq (R, +)$
2. S is closed under multiplication in R

- **Simple**

A ring R is called simple if its only ideals are 0 and R.

- **associates**

$x, y \in R$ are associates if $a = ub$ for a unit u of R.

- **irreducible**

A nonunit $x \in R := R \setminus \{0\}$ is irreducible if whenever $x = uv$ in R, then either u or v is a unit.

Field Theory

- **Field**

  Field F is ①~⑧ s.t. $a \in F$ and $a \neq 0_F$ has multiplicative inverses.

  A Field F is a non-zero commutative ring with identity such that all non-zero elements of F are units.

- **Extension Fields**

  $F \leq K$: F is subfield of K

  A containment of fields $F \subseteq E$ is called field extension.

- **principle ideal domain (PID)**

  An integral domain R is called priciple ideal domain if every ideal of R is principle.

- **prime ideal (II)**

  The ideal I is prime iff if $ab \in I$ implies $a \in I$ or $b \in I$

- **maximal ideal (II)**

  The ideal I is maximal iff any ideal J containing I either equals I or R.

- **prime element**

  The element r is prime iff the ideal rR is a prime ideal

- **UFD (Unique Factorization Domain)**

  A unique factorization domain is an integral domain R in which every non-zero element $r \in R$ can be written in the form

  $$r = p_1 p_2 \cdots p_n$$

  where p_i are irreducible, and such a factorization is unique up to permutation of the p_i and multiplying the p_i by a unit.

- **Euclidean Norm**

  A Euclidean Norm on an integral domain R is a function: $v(R \setminus \{0\}) \longrightarrow \mathbb{Z}_{\geq 0}$ satisfying the following:

  1) For all $a, b \in R$ with $b \neq 0$. $\exists q, r \in R$. s.t. $a = bq + r$. where either $r = 0$ or $v(r) < v(b)$

  2) $\forall$ non-zero $a, b \in R$. we have $v(a) < v(ab)$

- **Euclidean Domain**

  If an integral domain R admits a Euclidean norm, then R is called Euclidean Domain.

- **Degree**

  $K \subseteq L$, $[L:K]$ equals the dimension of L as K-vector space.