04/23 251 Lec 5

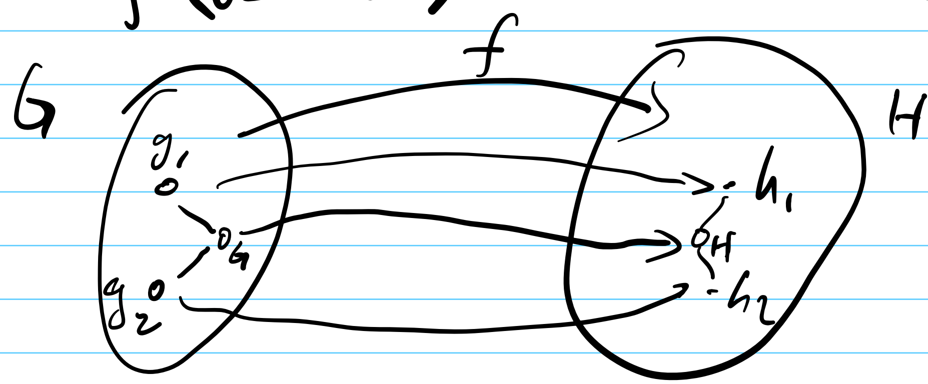
1. Group isomorphism.

· **DEF**: A function $f: G \to H$ is an <u>isomorphism</u> from G to H, if

① f is <u>bijection</u>

② $\forall g_1, g_2 \in G$

$$f(g_1 \circ_G g_2) = \underbrace{f(g_1)}_{h_1} \circ_H \underbrace{f(g_2)}_{h_2}$$



if $\exists f$ iso $G \to H$, call G & H <u>isomorphic</u>.

$$\boxed{G \cong^f H}$$

if only ② holds, call it <u>homomorphism</u>.
call G & H <u>homorphic</u>

· Direct product groups.

Let G, H be groups.

Define: $T = G \times H = \{(g, h) : g \in G, h \in H\}$.

$\times: T \times T \to T$

$(g_1, h_1), (g_2, h_2) \longmapsto (g_1 \circ_G g_2, h_1 \circ_H h_2)$

Claim: $(T, \times)$ is a group.

identity elem in T:

$e_T = (g, h) = (e_G, e_H)$

$\forall (g', h')$ $\quad \underbrace{e_T \times (g', h')}_{\shortparallel} = (g', h')$

$$\left((g \circ_G g'),\ h \circ_H h'\right) = (g', h')$$

b. Chinese Remainder Theorem (CRT)

· Thm: Let $N = p \cdot q$, $p, q > 1$ $\quad \gcd(p, q) = 1$.

then $\mathbb{Z}_N \cong \mathbb{Z}_p \times \mathbb{Z}_q$

$\mathbb{Z}_N^* \cong \mathbb{Z}_p^* \times \mathbb{Z}_q^*$

$f(x) := (x \bmod p,\ x \bmod q)$
is such an isomorphism.

· Ex: $N = 15 = 3 \times 5 \quad p = 3, q = 5$

$\mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$

$\mathbb{Z}_3^* = \{1, 2\}$ $\qquad\qquad \mathbb{Z}_5^* = \{1, 2, 3, 4\}$

By CRT: $\mathbb{Z}_{15}^* \cong \mathbb{Z}_3^* \times \mathbb{Z}_5^*$

$1 \leftrightarrow (1, 1)$, $\quad 2 \leftrightarrow (2, 2)$ $\quad 4 \leftrightarrow (1, 4)$

$7 \leftrightarrow (1, 2)$ $\quad 8 \leftrightarrow (2, 3)$ $\quad 11 \leftrightarrow (2, 1)$

$13 \leftrightarrow (1, 3)$ $\quad 14 \leftrightarrow (2, 4)$

Ex: $14 \cdot 13 \bmod 15 = 2 \bmod 15$ $\qquad \mathbb{Z}_{15}^*$

$$\mathbb{Z}_{15}^* \longrightarrow \mathbb{Z}_3^* \times \mathbb{Z}_5^*$$

$(2,4) \cdot (1,3)$

$(\mathbb{Z}_2^* \times \mathbb{Z}_5^*)$

$= (2 \cdot 1 \bmod 3,\ 4 \cdot 3 \bmod 5)$

$= (2, 2)$

$x \equiv 2 \bmod 3$

$x \equiv 3 \bmod 5 \quad \Rightarrow x = ?$

$x \equiv 2 \bmod 7$

$\mathbb{Z}_3^* \times \mathbb{Z}_5^* \times \mathbb{Z}_7^* \cong$

$(2, 3, 2) \longleftrightarrow ?$

(环) (域)

2. Rings & Fields.

a. Rings.

DEF: $(R, +, \cdot)$ binary op's. an algebra. i.e. closure under $+$ & $\cdot$

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

i.e. $\exists$ $+$ identity (denoted 0)

$\exists$ inverse,

commutative.

ii $(R,\cdot)$ is a monoid (semigroup) $\Rightarrow$ rng

$\exists$ $\cdot$ identity (denoted 1)

iii $\cdot$ is distributive over $+$

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

call $(R,+,\cdot)$ a ring.

Ex - $(\mathbb{Z}, +, \times)$

$(\mathbb{R}, +, \times)$

$(M_n, +, \times)$

M_n: n×n matrices

$(\mathbb{Z}_N, +_N, \cdot_N)$: ring of integers mod N.

Ex: show that $a \cdot 0 = 0 \ \forall a \in R$.

let $(-a) + a = \cancel{0}\ 1$

Pf: $\underline{a \cdot 0} = a \cdot (0+0)$

$= \underline{a \cdot 0 + a \cdot 0}$

$\Leftrightarrow \underline{(a \cdot 0) + (-a \cdot 0)} = a \cdot 0 + \underline{a \cdot 0 + (-a \cdot 0)}$

$\Leftrightarrow (a + (-a)) \cdot 0 = a \cdot 0 + (a + (-a)) \cdot 0$

$\Leftrightarrow 1 \cdot 0 = a \cdot 0 + 1 \cdot 0$

$\Leftrightarrow 0 = a \cdot 0 + \cancel{0}$

$\bigstar$

b. Special cases:

- commutative ring (交换环): $(R, \cdot)$ comm
- domain (无零因子环):

$$x \cdot y = 0_{(+\text{identity})} \Rightarrow x = 0 \text{ OR } y = 0.$$

- integral domain (整环): domain + commutative $(R, \cdot)$

Ex. $(\mathbb{Z}, +, \cdot)$ is int. domain.

$a \cdot b = 0 \Rightarrow a = 0$ OR $b = 0$.

c. Fields.

- DEF: let $(F, +, \cdot)$ being ring

if if$(F\setminus\{0\}, \cdot)$ is <u>abelain group</u>

then $(F, +, \cdot)$ is called a <u>field</u>.

<u>Ex</u>. - $(\mathbb{R}, +, \cdot)$: field ✓

- $(\mathbb{Q}, +, \cdot)$: ✓

- $(\mathbb{Z}, +, \cdot)$: ✗

$(\mathbb{Z}\setminus\{0\}, \cdot)$ NOT a group

<u>claim</u> : A <u>field</u> is an <u>int. domain</u>

$\Longrightarrow$ ✓

$\not\Longleftarrow$ $(\mathbb{Z}, +, \cdot)$

· ring
|
· domain
|
· int domain
|
· field

$\uparrow$ $\cup\!\!|$

· B
|
· A

$A \subseteq B$

3. QC

·(Impact): Treat:

Peter Shor
Alexei Kitaev '94 Quantum poly-time algs. for factoring ✓ DL.

$\Rightarrow$ Breaking RSA & DH cryptosystems!

$\downarrow$

PQC: post-quan. crypto.

(NIST ongoing effort)

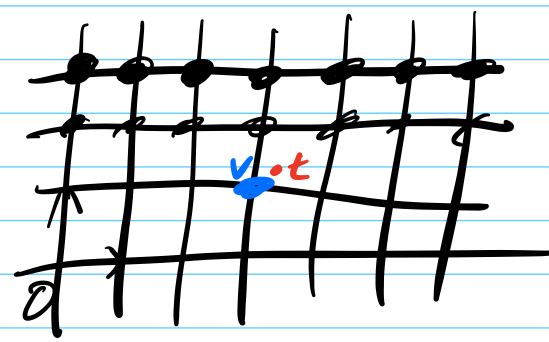
[Need hard prob's against QC.]

b. Lattice (problem) based CRYPTO.

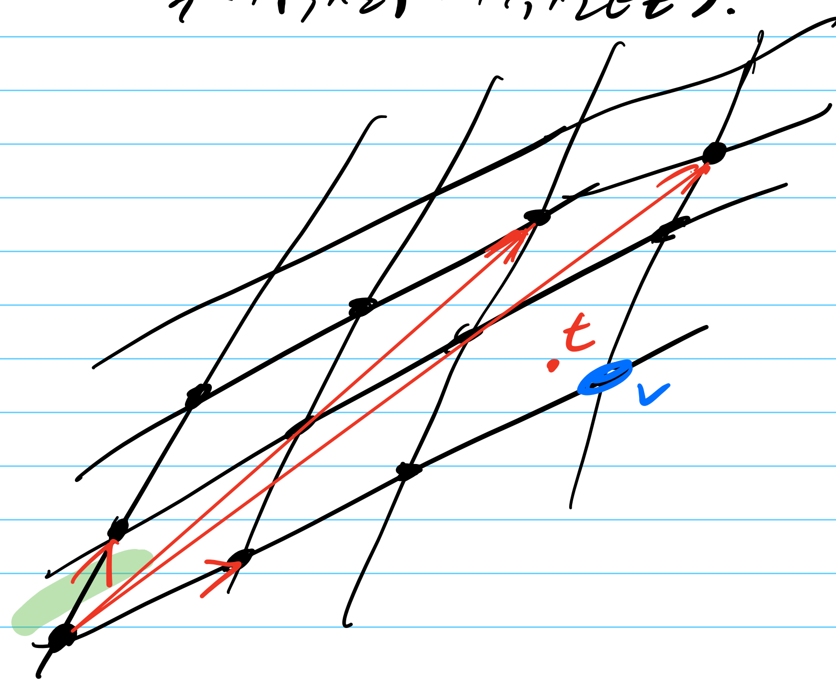
$L \subseteq \mathbb{R}^n$

$\mathbb{Z}^2$

Ex.



$\{(x_1, x_2) : x_1, x_2 \in \mathbb{Z}\}$.



$B := \{(b_1, \cdots, b_n) : b_i \in \mathbb{R}^n$ lin. indep $\}$

(Basis).

$L := \Lambda(B) = \{v : v = a_1 b_1 + \cdots + a_n b_n\}$.

$a_i \in \mathbb{Z}$.

- Important problems in lattices.

SVP (Shortest Vector problem)

Given: B for L

Goal: Find $v \neq 0$ s.t. $\|v\|$ smallest.

Hard in high. dim!

CVP (closest vector problem)

Given: B for L, $t \notin L$

Goal: Find $v \in L$ s.t. $\|v - t\|$ smallest.

BDD (Bounded distance decoding)

Given: B for L, $t = v + e$

$v \in L$. $\|e\|$ small

Goal: Find v