Northeastern University, Department of Mathematics

MATH 5110: Applied Linear Algebra and Matrix Analysis.

• Instructor: **He Wang**   Email: **he.wang@northeastern.edu**

§1. Linear system and Gaussian elimination over fields

Topics: 1. Linear system; 2. Sets, groups, fields and more; 3. Gaussian elimination.

1. Background:

Definition 1. (1) A **linear equation** in variables $x_1, x_2, \dots, x_n$ is of the form

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b.$$

Here, $a_1, a_2, \dots, a_n \in \mathbb{R}$ (or a field $\mathbb{F}$) are **coefficients**.
(2) A **system of linear equations** (or **linear system**) is a collection of linear equations in the same variables.

$$\left\{\begin{array}{l} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2 \\ \qquad\vdots \qquad \vdots \qquad \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = b_m \end{array}\right.$$

$[A \mid \vec{b}]$

Matrix/vector notation:

$$A = [a_{ij}] = \underbrace{\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}}_{m\times n} \qquad \vec{b} = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{bmatrix}$$

Goal: Find the set of all solutions.

Math 2331

Method: Gauss-Jordan elimination (Gaussian elimination).

Theorem 2. *A linear system (matrix equation $A\vec{x} = \vec{b}$) has either no solution, or exactly one solution, or infinitely many solutions.*

$I = \{x \in \mathbb{R} \mid a \le x \le b\}$

2. Sets and functions

Definition 3. A set S is a *well-defined*, *unordered* collection of *distinct* elements.

Non-well-defined example, (Russell' s paradox): $S \in S \Leftrightarrow S \notin S$

$S = \{x \mid x \notin x\}$, i.e., set of all sets that are not members of themselves.

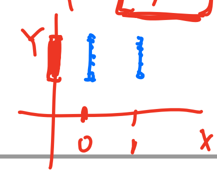
The teacher that teaches all who don't teach themselves. A

A teaches A $\Leftrightarrow$ A not teach A

Review of set operations:

- **Union** $A \cup B = \{x \mid x \in A \text{ or } x \in B\}$
- **Intersection** $A \cap B = \{x \mid x \in A \text{ and } x \in B\}$
- **Complement** of $A \subset S$, $A^c = \{x \in S \mid x \notin A\}$
- **(Cartesian) Product** $X \times Y = \{(x, y) \mid x \in X, y \in Y\}$.

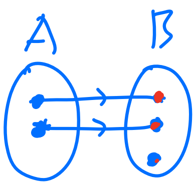
Ex $X = \{0, 1\}$ $Y = [1, 2]$

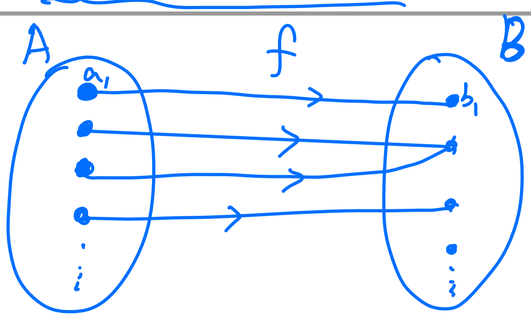


Definition 4. A **function**(map) f between two sets A and B is a rule

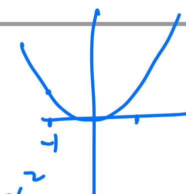
$$f : A \to B$$

sending "every" $a \in A$ to an element $f(a) \in B$.





$f(a_1) = b_1$

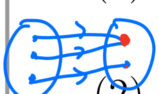


$f(x) = x^2$

$f(-1) = 1$

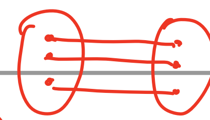
Definition 5. Let $f : A \to B$ be a function.

(1) f is called **injective (one-to-one)**, if $f(x) = f(y) \overset{\text{implies}}{\Longrightarrow} x = y$ for any $x, y \in A$



(2) f is called **surjective (onto)**, if $\underset{\text{For any}}{\forall}\, b \in B$, $\underset{\text{there exist}}{\exists}\, x \in A$ $\underset{\text{such that}}{\text{s.t.}}$ $f(x) = b$.

(3) f is called **bijective**, if f is surj and inj.



Consider a function $f : A \to B$ and the equation $f(x) = b$ for every $b \in B$.

Proposition 6.

- *f is injective $\Leftrightarrow$ $f(x) = b$ has* at most one *solution.*
- *f is surjective $\Leftrightarrow$ $f(x) = b$ has* at least one *solution.*
- *f is bijective $\Leftrightarrow$ $f(x) = b$ has* exactly one. *solution.*

Example 7. Consider functions $f : [0, 1] \to \mathbb{R}$ defined by $f(x) = x$.

$g : \mathbb{R} \to [0, \infty)$ defined by $g(x) = x^2$.

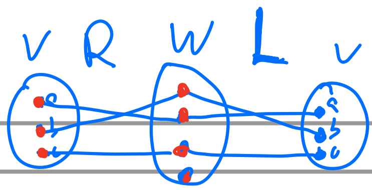
$h : \mathbb{R} \to \mathbb{R}$ defined by $h(x) = 2x + 1$.

"map"

Definition 8. The **composition** $T \circ S$ of two functions $S : U \to V$ and $T : V \to W$

$$T\circ S : U \xrightarrow{S} V \xrightarrow{T} W$$

$$u \longrightarrow S(u) \longrightarrow T(S(u))$$



$$\begin{tikzcd} V \arrow[r, bend right, "R"'] & W \arrow[l, bend right, "L"'] \end{tikzcd}$$

Theorem 9. *Consider functions $R : V \to W$ and $L : W \to V$. If*

left-inverse of R   right inverse of L

$$L \circ R = \mathrm{id}_V$$

$\mathrm{id}_V(x) = x$

①

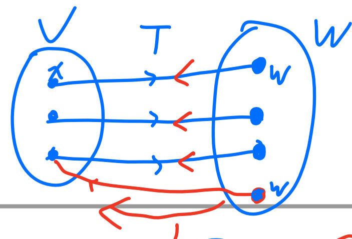
then L is surjective and R is injective. (That is $V \overset{R}{\hookrightarrow} W \overset{L}{\twoheadrightarrow} V$)

$$\underbrace{\quad\quad\quad\quad}_{L\circ R}$$

Right-invertible

Proof. ①: For any $v \in V$, $L\circ R(v) = \mathrm{id}_V(v)$, then $L\big(R(v)\big) = v$.

②



$$V \xrightarrow{T} W \xrightarrow{L} V$$

Theorem 10.
(1) A map $T : V \to W$ is injective if and only if it has a left-inverse.
(2) A map $T : V \to W$ is surjective if and only if it has a right-inverse.

$\Longleftrightarrow$ $L\circ T = \mathrm{id}_V$

(1) "$\Leftarrow$" ✓ Thm 9

"$\Rightarrow$" T is injective $\Longleftrightarrow$ $T(x) = w$ has (at most) one solution for any $w \in W$

· Define: $L : W \to V$ ① If $w = T(x)$ has a unique soln, then define $L(w) = x$

② If $w = T(x)$ has no soln, then define $L(w) = y$ for some $y \in V$.

· Check: $L\circ T = \mathrm{id}_V$

$$\begin{tikzcd} W \arrow[r, "R"] \arrow[rr, bend left, "\mathrm{id}_W"] & V \arrow[r, "T"] \arrow[rr, bend left, "\mathrm{id}_V"] & W \arrow[r, "L"] & V \end{tikzcd}$$

$R=L$

Theorem 11. *Suppose a function $T : V \to W$ has both a left-inverse L and a right-inverse R. Then*

$$\boxed{L = R} : W \to V$$

$L \circ T = id_V$

$T \circ R = id_W$

For any $w \in W$. $L(w) = L(T \circ R(w)) = L \circ T(R(\vec{w})) = R(\vec{w})$ $\quad T \circ R(w) = id_W(w) = w$

Def: We call T is "invertible" and $L=R$ is the inverse of T.

Proposition 12. *A map $T : V \to W$ is bijective if and only if it is invertible.*

3. Algebraic objects: Set → Monoid → Group→ Ring→ Field

Ex1 $S = \mathbb{N} = \{0, 1, 2, \ldots\}$

$* =$ product, $e = 1$

or

Ex2 $* =$ sum, $e = 0$

Definition 13. A **binary operation** on a set S is

a function $* : S \times S \longrightarrow S$

Definition 14. A **monoid** is a set M with a binary operation $* : M \times M \to M$ satisfying two axioms:

(1) (Identity) $\exists\, e \in M$ s.t. $e * m = m$ and $m * e = m$. for any $m \in M$.

(2) (Associativity) $a * (b * c) = (a * b) * c$ for any $a, b, c \in M$.

Proposition 15. *Identity is "unique" in a monoid.*

Proof: Suppose $\exists$ two identities e and e'

$$e' = e * e' = e$$

Ex: {all 2x2 matrices} $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$

$* =$ product

$\times, +$

Definition 16. A monoid $(M, *)$ is called a **commutative** (or abelian), if

$a * b = b * a$ for any $a, b \in M$

Definition 17. A **group** is a monoid $(G, *)$ satisfies

(3) (Inverse) $\forall\, g \in G,\ \exists\, h \in G$ s.t. $g*h = h*g = e$ identity.

Proposition 18. *In a group G, inverse is unique in for any $g \in G$.*

Ex: $G = \{$all 2x2 matrices$\}$ with sum ($* = +$) is a abelian group.

Ex: $R = \{$all 2x2 matrices$\}$ $*_1 = +$, $*_2 = \times$ ring

Denote commutative (abelian) group as $(G, \underset{*}{+}, \overset{=e_0}{0})$; inverse of a as $-a$.

$R = \mathbb{Z}$ $\quad e_1 = 0,\ *_1 = +,\ *_2 = \times,\ e_2 = 1$

Definition 19. A **ring** (with unit/identity) is a set R with two binary operations $*_1 = +$ and $\cdot = *_2$ s.t.

$e_0 * a = a * e_0 = a$

(1) $(\underset{*_1}{R, +})$ is an abelian group. $= \{$identity, associative, commutative, inverse$\}$

(2) (multiplicative identity) ($*_2 = \cdot$) $\quad e_1 \cdot a = a \cdot e_1 = a$ for any $a \in R$

(3) (multiplicative associative) $\quad (a \cdot b) \cdot c = a \cdot (b \cdot c)$

(4) (Distributivity) $\quad a \cdot (b + c) = a \cdot b + a \cdot c$

and $(b + c) \cdot a = b \cdot a + c \cdot a$

Definition 20. A ring R is called a **commutative** if $\forall a, b \in R$, $a \cdot b = b \cdot a$.

(Denote e_2 as 1 in commutative ring.)

Example 21. Integers $\mathbb{Z}$ is a commutative ring.

Example 22. Set of all polynomials $\mathbb{R}[t]$ with sum and product is a commutative ring.

Example 23. Set of all polynomials $\mathbb{R}[x_1, x_2, \ldots, x_n]$ is a commutative ring.

Example 24. $2\mathbb{Z}$ is a ring (without identity).

$2\mathbb{Z} = \{\ldots -4, -2, 0, 2, 4 \ldots\}$ $\quad *_1 = +,\ *_2 = \times$

$$\mathbb{Z}_6 = \{[0], [1], [2], [3], [4], [5]\}$$

$$[0] := \{0, \pm 6, \pm 12, \dots\} = 0 + 6\mathbb{Z}$$

$$[1] := \{1, 1\pm 6, 1\pm 12, \dots\} = \underline{1 + 6\mathbb{Z}}$$

$$\vdots$$

$$[5] := \{5, 5\pm 6, \dots\} = 5 + 6\mathbb{Z}$$

$$\dots \quad -3 \quad -2 \quad -1 \quad 0 \quad 1 \quad 2 \quad 3 \quad 4 \quad 5 \quad \dots$$

$e_1 = [0] = a$

$e_2 = [1] = b$

X_1	a	b
a	a	b
b	b	a

X_2	a	b
a	a	a
b	a	b

$$[x] + [y] := [x+y]$$

$$[x] \cdot [y] := [xy]$$

Definition 25. A **field** $\mathbb{F}$ is a commutative ring $(\mathbb{F}, \overset{*_1}{+}, \overset{*_2}{\cdot})$ such that
(5) any non-zero element has a multiplicative inverse.

$g *_1 h = h *_1 g = e_2$

Remark: $(F - \{0\}, \cdot)$ are abelian groups.

For $n > 0 \in \mathbb{Z}$, let $\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}$=the set of congruence classes modulo n.

Proposition 26. $(\mathbb{Z}_n, +, \times)$ *is a commutative ring.*

Example 27. $\mathbb{Z}_2$ is a field.

$\{a, b\} = \{[0], [1]\}$

$a = [0] := \{0, \pm 2, \ldots\}$

$b = [1] := \{\pm 1, \pm 3, \ldots\}$

$*_2 = \times$	$[0]$	$[1]$
$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$

$+ = *_1$	$[0]$	$[1]$
$[0]$	$[0]$	$[1]$
$[1]$	$[1]$	$[0]$

Example 28. $\mathbb{Z}_6$ is not a field. (Reason: $[2]$ has no multiplicative inverse.)

$[2] \cdot [\;\;] = [1]$

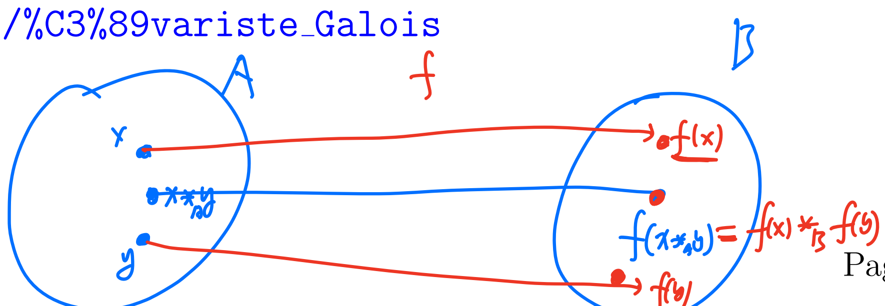
Proposition 29. $\mathbb{Z}_n$ *is a field if and only if* $n = p$ *is a prime number.*

$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are fields. Remark: $\mathbb{Q}$ is the smallest field containing $\mathbb{Z}$.

In our class, we will focus on fields $\mathbb{R}$, $\mathbb{C}$, (and $\mathbb{Z}_p$).

The idea of group and field was created by Évariste Galois (1811 – 1832).

https://en.wikipedia.org/wiki/%C3%89variste_Galois



Function between algebraic objects:

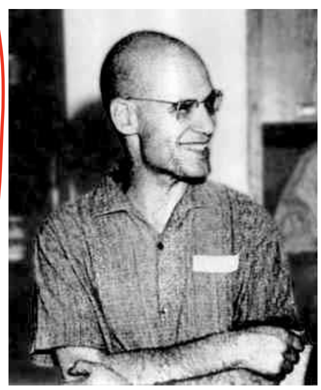
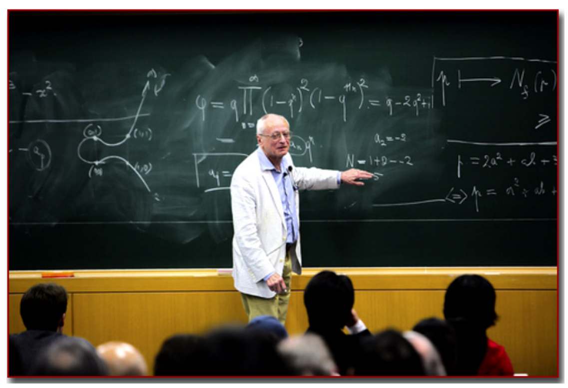
“good” map

Definition 30. A **homomorphism** $f : A \to B$ between any two algebraic objects is a function preserving all operations, i.e.,

$$f(x * y) = f(x) * f(y) \text{ for any } x, y \in A$$

For ring with identity, we also need the homomorphism sends identity to identity.

Definition 31. (1) An injective homomorphism is called **monomorphism**.
(2) A surjective homomorphism is called an **epimorphism**.
(3) A function $f : A \to B$ is called **isomorphism**, if it is monomorphism and epimorphism. In this case, we consider A and B are the “same”.
(Terminology first by Nicolas Bourbaki (1934-).)

https://en.wikipedia.org/wiki/Nicolas_Bourbaki

Further extended reading: 1. Classification finite fields. 2. Classification of finite abelian groups. 3. “Classification of finite groups”.

 2231

Go back to matrix $[A \mid \vec{b}]$.

The leftmost nonzero entry of a row is called **leading entry**(or **pivot**).

Definition 32. A matrix is in ***row-echelon form*** **(ref)** if
(1.) All entries in a column below a leading entry are zeros.
(2.) Each row above it contains a leading entry further to the left.
A matrix is in ***reduced row-echelon form*** **(rref)**, if it satisfies (1) (2) and
(3.) The leading entry in each nonzero row is 1.
(4.) All entries in a column above a leading entry are zeros.

Condition 2 implies that all zero rows are at the bottom of the matrix.

One example of **ref**, ($\blacksquare$: non-zero number, $*$ any number) and one example of **rref**

$$\textbf{ref} = \begin{bmatrix} \blacksquare & * & * & * & * & * \\ 0 & 0 & \blacksquare & * & * & * \\ 0 & 0 & 0 & \blacksquare & * & * \\ 0 & 0 & 0 & 0 & \blacksquare & * \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \quad \to \cdots \to \quad \textbf{rref} = \begin{bmatrix} 1 & * & 0 & 0 & 0 & * \\ 0 & 0 & 1 & 0 & 0 & * \\ 0 & 0 & 0 & 1 & 0 & * \\ 0 & 0 & 0 & 0 & 1 & * \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Examples.

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 0 & 0 & 1 & 4 & 5 \\ 0 & 0 & 1 & 0 & 5 \end{bmatrix}, \quad \begin{bmatrix} 0 & 2 & 3 & 4 & 5 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 5 \end{bmatrix}, \quad \begin{bmatrix} 0 & 0 & 3 & 4 & 5 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 5 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2 & 0 & 4 & 5 \\ 0 & 0 & 1 & 4 & 5 \\ 0 & 0 & 0 & 1 & 5 \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 & 0 & 4 & 0 \\ 0 & 0 & 1 & 7 & 0 \\ 0 & 0 & 0 & 0 & 5 \end{bmatrix}$$

Elementary Row Operations:

kR_i

(1.) **Scaling:** Multiply a row R_i by a nonzero scalar $k \neq 0$.

$R_i + kR_j$

(2.) **Replacement:** Replace a row R_i by adding a multiple of another row kR_j.

(3.) **Interchange:** Interchange two rows. $R_i \Leftrightarrow R_j$

Elementary row operations do not change solutions of the linear system.

Theorem 33. *Using the elementary row operations, one can change a matrix to a reduced row-echelon form.*

$A \to \cdots \to \mathrm{rref}(A)$

Proof. Gauss-Jordan elimination:
1. Begin with the *leftmost* ***nonzero*** column.
2. Select a *nonzero* entry as a **pivot**, and interchange its row to the first row.
3. Use ERO to create zeros in all positions below the pivot.
4. Omit the first row and repeat this process.
5. Repeat the process until the last nonzero row.
6. Scale all pivots to 1's.
7. Beginning with the **rightmost** pivot and working upward and to the left. ☐

Theorem 34. *A matrix A has a unique reduced row echelon form* $\boldsymbol{rref}(A)$.

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix} \xrightarrow{R_1 \Leftrightarrow R_2} \begin{bmatrix} 4 & 5 & 6 \\ 1 & 2 & 3 \end{bmatrix} = B$$

$A \overset{r.q.}{\sim} B$

Definition 35. If $A \xrightarrow{ERO} \cdots \xrightarrow{ERO} B$, then A is called **row-equivalent** to B.

Proposition 36. *Row-equivalent is an equivalent relation.*

$A \sim B$

Proof. 1. (reflexive) $A \sim A$

2. (symmetric) $A \sim B \Leftrightarrow B \sim A$

3. (transitive) $A \sim B,\ B \sim C \Rightarrow A \sim C$ ☐

Theorem 37. *A linear system $[A|\vec{b}]$ is inconsistent (no solution) if and only if* $\boldsymbol{rref}([A|\vec{b}])$ *has a row*

$$[\,0\ 0\ 0\ \ldots\ 0\,|\,1\,].$$

If a linear system is consistent, it has either
- *a unique solution (no free variables), or*
- *infinitely many solutions (at least one free variable).*

Definition 38. The **rank** of a matrix A is
$$\text{rank}(A) = \text{the number of pivots in } \mathbf{rref}(A).$$

$A \overset{r.e.}{\sim} B$

Proposition 39. *Row-equivalent matrices have the same rank.*

$$\begin{array}{ccc} A & \to \cdots \to & B \\ \downarrow & & \downarrow \\ \text{rref}(A) & = & \text{rref}(B) \end{array}$$

Example 40. Suppose the coefficient matrix A is of size $m \times n$. Then,

$A = \begin{bmatrix} \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \end{bmatrix}_{m \times n}$

1. $\text{rank}(A) \leq m$ and $\text{rank}(A) \leq n$.

2. If the system is inconsistent, then $\text{rank}(A) < m$.

3. If the system has exactly one solution, then $\text{rank}(A) = n$.

4. If the system has infinitely many solutions, then $\text{rank}(A) < n$.

Definition 41. An $m \times n$ matrix A has **full rank**, if $\text{rank}(A) = \min(m, n)$.

Proposition 42. *A linear system with an $n \times n$ coefficient matrix A has exactly one solution if and only if* $\text{rank}(A) = n$ *if and only if* $\boldsymbol{rref}(A) = I_n$.

Remark:

1. We can apply Gaussian elimination over any field (including $\mathbb{Z}_p$). p prime

2. We can apply Gaussian elimination over integers $\mathbb{Z}$. However, we can not achieve **rref**. $\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}$

$\{0, \pm 3, \pm 6 \cdots\}$ $\{1, 1\pm 3, 1\pm 6 \cdots\}$ $\{2, 2\pm 3, 2\pm 6 \cdots\}$

3. Buchberger's algorithm is a generalization of Gaussian elimination to polynomials to obtain a Grobnear basis in commutative algebra.

over $\mathbb{Z}_3 = \{[0], [1], [2]\}$

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

×	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Ex1 $\begin{bmatrix} [1] & [2] & [0] & [1] & [2] \\ [0] & [0] & [1] & [1] & [2] \\ [0] & [0] & [1] & 0 & [2] \end{bmatrix}$ $R_3 + 2R_1$, $R_3 + (-1)R_1$, $\xrightarrow{R_3 - R_2}$ $\begin{bmatrix} 1 & 2 & 0 & 1 & 2 \\ 0 & 0 & 1 & 1 & 2 \\ 0 & 0 & 0 & 2 & 0 \end{bmatrix}$ $\xrightarrow{R_3 \cdot (2^{-1})}$ $\begin{bmatrix} 1 & 2 & 0 & 1 & 2 \\ \end{bmatrix}$

$R_3 \cdot 2$ $\begin{bmatrix} 0 & 0 & 1 & 1 & 2 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}$

Ex2 $\begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{bmatrix}$ over $\mathbb{Z}_2$

$R_1 - R_2$, $R_2 - R_1$ $\begin{bmatrix} 1 & 2 & 0 & 0 & 2 \\ 0 & 0 & 1 & 0 & 2 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}$

Warning: ① $\times \frac{1}{2}$ ② NOT $R_k \cdot 3$

$\mathbb{Z}_3 = \{[0], [1], [2]\}$

$\mathbb{Z} = \{\cdots -3\ -2\ -1\ 0\ 1\ 2\ 3 \cdots\}$

$0 \sim 3 \sim -3$

$\mathbb{Z}_4$ Not a field.