Lecture 3: Fields and Modular Arithmetic

Field: A field is a set F with two binary operations addition (denoted $+$) and multiplication (denoted $\cdot$). These operations satisfy the following axioms:

1. Addition is associative: If $a, b, c \in F$ then
$$a+(b+c)=(a+b)+c$$
2. There is an identity for addition, denoted 0. It satisfies for all $a \in F$:
$$0+a=a+0=a$$
3. Every element $a \in F$ has an additive inverse $-a \in F$ which satisfies $a+(-a)=0$ and $(-a)+a=0$.
4. Addition is commutative: If $a, b \in F$, then
$$a+b=b+a$$
5. Multiplication is associative: If $a, b, c \in F$, then
$$a \cdot (b \cdot c)=(a \cdot b) \cdot c$$
6. There is an identity for multiplication, denoted $1 \neq 0$. It satisfies for all $a \in F$:
$$1 \cdot a=a \cdot 1=a$$
7. Every element $a \in F$, except 0, has a multiplicative inverse a^{-1} which satisfies
$$a \cdot a^{-1}=1 \text{ and } a^{-1} \cdot a=1$$
8. Multiplication is commutative: If $a, b \in F$, then
$$a \cdot b=b \cdot a$$
9. Multiplication distributes over addition: If $a, b, c \in F$ then
$$a \cdot (b+c)=a \cdot b+a \cdot c$$

A field is the type of number system in which row reduction can occur and thus linear algebra can be done

Subtraction: If $a, b \in F$, then $a - b = a + (-b)$

Division: If $a, b \in F$ and $b \neq 0$, then $a/b = a \cdot b^{-1}$.

Example:

1. $\mathbb{N}$ is not a field since $3 \in \mathbb{N}$, but $-3 = (-3) \notin \mathbb{N}$.
2. $\mathbb{Z}$ is not a field since $3 \in \mathbb{Z}$, but $3^{-1} = 1/3 \notin \mathbb{Z}$.
3. $\mathbb{Q}$ is a field
4. $\mathbb{R}$ is a field
5. $\mathbb{C}$ is a field

Definition: The integers mod n is the set

$$\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$$

$n \in \mathbb{N}$ is called the modulus.

Example:

1. $\mathbb{Z}_2 = \{0, 1\}$
2. $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$

Definition:

1. To add x and y mod n, add $x+y$ as integers, divide by n and take the remainder and call it r. Then, for $x, y \in \mathbb{Z}_n$
$$x + y = r.$$
2. To multiply x and y mod n, multiply $x \cdot y$ as integers, divide by n and take the remainder and call it r. Then, for $x, y \in \mathbb{Z}_n$
$$x \cdot y = r.$$

Example:

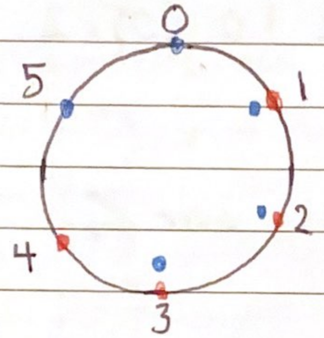
Suppose $n = 6$, so the set is $\mathbb{Z}_6$. Therefore, $4, 5 \in \mathbb{Z}_6$ and

$$4 + 5 = 9 \quad \text{(add as integers)}$$
$$= 3 \quad \text{(divide by 6 and take remainder).}$$

We also have that

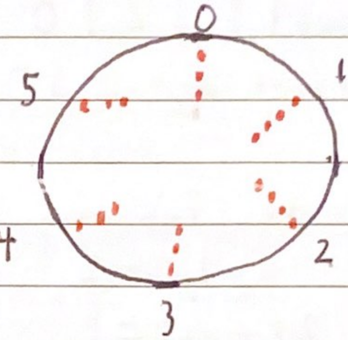
$$4 \cdot 5 = 20 \text{ (multiply as integers)}$$
$$= 2 \text{ (divide by 6 and take the remainder).}$$

Lets see how to visualize this



4 red dots
+
5 blue dots
⇓
ends at 3

$4+5=3$



last dot ends at 2.

$$4 \cdot 5 = 20 = \underbrace{3}_{\text{three rotations}} \cdot 6 + \underbrace{2}_{\text{extra steps}}$$

Example:

Again suppose $n=6$, so the set is $\mathbb{Z}_6$.

1. What is -2? Well, $2+4=0=2+(-2)$ and thus $-2=4$ in $\mathbb{Z}_6$.
2. $5^{-1}=5$ in $\mathbb{Z}_6$ since $5 \cdot 5 = 25 = 6 \cdot 4 + 1$
3. Therefore, $3/5 = 3 \cdot 5 = 15 = 6 \cdot 2 + 3 = 3$.
4. What about 4^{-1}?

$$4 \cdot 0 = 0$$
$$4 \cdot 1 = 4$$
$$4 \cdot 2 = 8 = 2$$
$$4 \cdot 3 = 12 = 0$$
$$4 \cdot 4 = 16 = 4$$
$$4 \cdot 5 = 20 = 2$$

$\Rightarrow \mathbb{Z}_6$ is not a field!!

Theorem - $\mathbb{Z}_n$ is a field if and only if n is prime.

Example:

1. Find the roots of x^2+5x+6 in $\mathbb{Z}_{10}$

x	0	1	2	3	4	5	6	7	8	9
x^2+5x+6	6	2	0	0	2	6	2	0	0	2

The roots are 2, 3, 7, 8 (4 roots!!)

2. Solve the following system of equations over $\mathbb{Z}_3$:

$$\begin{aligned} x+2y &= 2 \\ 2x+y+z &= 1 \\ 2x+z &= 2 \end{aligned}$$

Since $\mathbb{Z}_3$ is a field row reduction should work

$$\left[\begin{array}{ccc|c} 1 & 2 & 0 & 2 \\ 2 & 1 & 1 & 1 \\ 2 & 0 & 1 & 2 \end{array}\right]\begin{array}{l} \\ +R1 \\ +R1 \end{array} \rightarrow \left[\begin{array}{ccc|c} 1 & 2 & 0 & 2 \\ 0 & 0 & 1 & 0 \\ 0 & 2 & 1 & 1 \end{array}\right]\begin{array}{l} \\ \\ \times 2 \end{array} \rightarrow \left[\begin{array}{ccc|c} 1 & 2 & 0 & 2 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 2 & 2 \end{array}\right]$$

$$\rightarrow \left[\begin{array}{ccc|c} 1 & 2 & 0 & 2 \\ 0 & 1 & 2 & 2 \\ 0 & 0 & 1 & 0 \end{array}\right]\begin{array}{l} +R2 \\ \\ \\ \end{array} \rightarrow \left[\begin{array}{ccc|c} 1 & 0 & 2 & 1 \\ 0 & 1 & 2 & 2 \\ 0 & 0 & 1 & 0 \end{array}\right]\begin{array}{l} +R3 \\ +R3 \\ \\ \end{array} \rightarrow \left[\begin{array}{ccc|c} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 0 \end{array}\right]$$

Therefore, $x=1$, $y=2$, $z=0$.

3. Solve the following system over $\mathbb{Z}_5$.

$$\begin{aligned} w+x+y+2z &= 1 \\ 2x+2y+z &= 0 \\ 2w+2y+z &= 1 \end{aligned}$$

$$\left[\begin{array}{cccc|c} 1 & 1 & 1 & 2 & 1 \\ 0 & 2 & 2 & 1 & 0 \\ 2 & 0 & 2 & 1 & 1 \end{array}\right]\begin{array}{l} \\ \\ +3R1 \end{array} \rightarrow \left[\begin{array}{cccc|c} 1 & 1 & 1 & 2 & 1 \\ 0 & 2 & 2 & 1 & 0 \\ 0 & 3 & 0 & 2 & 4 \end{array}\right]\begin{array}{l} \\ \times 3 \\ \\ \end{array} \rightarrow \left[\begin{array}{cccc|c} 1 & 1 & 1 & 2 & 1 \\ 0 & 1 & 1 & 3 & 0 \\ 0 & 3 & 0 & 2 & 4 \end{array}\right]\begin{array}{l} +4R2 \\ \\ +2R2 \end{array}$$

$$\rightarrow \left[\begin{array}{cccc|c} 1 & 0 & 0 & 4 & 1 \\ 0 & 1 & 1 & 3 & 0 \\ 0 & 0 & 2 & 3 & 4 \end{array}\right]\begin{array}{l} \\ \\ \times 3 \end{array} \rightarrow \left[\begin{array}{cccc|c} 1 & 0 & 0 & 4 & 1 \\ 0 & 1 & 1 & 3 & 0 \\ 0 & 0 & 1 & 4 & 2 \end{array}\right]\begin{array}{l} \\ +4R3 \\ \\ \end{array} \rightarrow \left[\begin{array}{cccc|c} 1 & 0 & 0 & 4 & 1 \\ 0 & 1 & 0 & 4 & 3 \\ 0 & 0 & 1 & 4 & 2 \end{array}\right]$$

$$\begin{aligned} w+4z &= 1 \\ x+4z &= 3 \\ y+4z &= 2 \end{aligned}$$

Since $5z = 0$ we have that

$$w = 1 + z$$
$$x = 3 + z$$
$$y = 2 + z$$

Therefore, we have five cases to check:

$z=0$,	$z=1$,	$z=2$,	$z=3$,	$z=4$
$w=2$	$w=2$	$w=3$	$w=4$	$w=0$
$x=3$	$x=4$	$x=0$	$x=1$	$x=2$
$y=2$	$y=1$	$y=4$	$y=0$	$y=1$