Review

- integers $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \dots\}$

  rationals $\mathbb{Q} = \{\frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0\}$

  real numbers $\mathbb{R}$: $\longleftrightarrow$ number line.

  complex numbers $\mathbb{C} = \{a+bi \mid a, b \in \mathbb{R}, i^2 = -1\}$

* $\mathbb{Z}_n$ is the set of integers mod n

$\mathbb{Z}_n$ Let $n \in \mathbb{Z}$, $n \geq 2$,

Given, $a, b \in \mathbb{Z}$ we write $\underbrace{a \equiv b \pmod n}_{\text{"a congruent to b modulo n"}}$ if $n \underset{\uparrow \text{ divides}}{\mid} (a-b)$

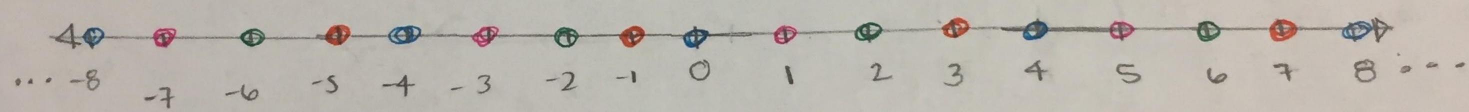
Example: $n = 4$ $a = 3, b = 11$

$3 - 11 = -8 = 4(-2)$ so $3 \equiv 11 \pmod 4$

The distance between 3 and 11 is a multiple of 4.

- $3 \not\equiv 9 \pmod 4$

  $3 - 9 = -6 \leftarrow$ 4 does not divide -6



Let $x \in \mathbb{Z}$, let $n \in \mathbb{Z}$, $n \geq 2$

Def The equivalence class of x mod n is

$$\bar{x} = \{y \in \mathbb{Z} \mid x \equiv y \pmod n\}$$

$$\mathbb{Z}_n = \{\bar{x} \mid x \in \mathbb{Z}\} = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}\}$$

Example: $(n = 4)$

- $\bar{0} = \{\dots, -8, -4, 0, 4, 8, \dots\}$

  $\bar{1} = \{\dots, -7, -3, 1, 5, 9, \dots\}$

  $\bar{2} = \{\dots, -6, -2, 2, 6, \dots\}$

  $\bar{3} = \{\dots, -5, -1, 3, 7, \dots\}$

* $\bar{a} = \bar{b}$ iff $a \equiv b \pmod n$

$\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$

Adding / Multiplying in $\mathbb{Z}_n$

Recall the following operations are well-defined on $\mathbb{Z}_n$

Given $\bar{a}, \bar{b} \in \mathbb{Z}_n$

Define $\bar{a} + \bar{b} = \overline{a+b}$

$\bar{a} \cdot \bar{b} = \overline{ab}$

Example: $(n=4)$

$\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$

- $\bar{3} \cdot \bar{2} = \bar{6} = \bar{2}$
- $\bar{3} + \bar{2} = \bar{5} = \bar{1}$
- $\bar{3} \cdot \bar{3} = \bar{9} = 1$
- $\bar{2} \cdot \bar{2} = \bar{4} = \bar{0}$

Rings and Fields

Def ① A **Ring** R is a set with binary operations $+$ and $\cdot$ satisfying:

(i) R is an abelian group under $+$

(ii) R is closed under $\cdot$ ← If $a, b \in R$, then $a \cdot b \in R$

(iii) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ $\forall a, b, c \in R$ (associativity)

(iv) $\forall a, b, c \in R$ we have $a \cdot (b+c) = a \cdot b + a \cdot c$.
(distributive) $(a+b) \cdot c = a \cdot c + b \cdot c$

elaborate on (i)

- If $a, b \in R$, then $a+b \in R$
- If $a, b, c \in R$, then $(a+b)+c = a+(b+c)$
- $\exists$ an elemen 0 (additive identity) where $0+a = a+0 = a$ $\forall a \in R$
- For every $a \in R$ $\exists$ $-a$ (additive inverse of a) where $a+(-a) = (-a)+a = 0$
- For every $a, b \in R$ we have $a+b = b+a$

② A ring is called **commutative** if $a \cdot b = b \cdot a$ $\forall a, b \in R$

3. A ring R is said to have an <u>identity</u> (or contain a 1) if there is an element $1 \in R$ with

$$1 \cdot a = a \cdot 1 = a$$

for all $a \in R$.

4. Let R be a ring with identity $1 \neq 0$. Let $x \in R$. We say that y is a <u>multiplicative inverse</u> of x if $x \cdot y = y \cdot x = 1$. If x has a multiplicative inverse then we call x a <u>unit</u> of R.

5. F is a <u>field</u> if

   (i) F is a ring

   (ii) F is commutative with identity $1 \neq 0$.

   (iii) every $a \in F$ with $a \neq 0$ has a multiplicative inverse.

<u>Notation:</u> We will write xy instead of $x \cdot y$.

Ex: $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \dots\}$

- abelian under +
- closure under $\cdot$
- associative under $\cdot$
- distributive

$\Big\}$ Ring axioms

$\therefore$ $\mathbb{Z}$ is a ring
- $\mathbb{Z}$ is commutative $\left(\begin{matrix} ab = ba \\ a, b \in \mathbb{Z}\end{matrix}\right)$
- $\mathbb{Z}$ has an identity 1

units of $\mathbb{Z}$

1 and -1

1 is its own mult. inverse

-1 is its own mult. inverse

for ex: 2 is not a unit since you can't solve $2 \cdot x = 1,\ x \in \mathbb{Z}$

$\mathbb{Z}$ is not a field, since $\exists$ non-zero elements without a multiplicative inverse.

<u>note</u>

$\mathbb{Z}$ is a commutative ring with identity

$\left.\begin{matrix}\mathbb{R} \\ \mathbb{Q} \\ \mathbb{C}\end{matrix}\right\}$ fields

R has a 1
R has an identity
R has unity

Question what about $\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$?

additive ident. ($\bar{0}$) mult ident. ($\bar{1}$)

Ring ✓

commutative $\bar{a}\,\bar{b} = \overline{ab} = \overline{ba} = \bar{b} \cdot \bar{a}$

✓ has a $\bar{1} \in \mathbb{Z}_4$

<u>units</u>

$\bar{1} \cdot \bar{1} = \bar{1}$	$\bar{3} \cdot \bar{3} = \bar{9} = \bar{1}$	$\bar{2} \cdot \bar{1} = \bar{2} \neq \bar{1}$
		$\bar{2} \cdot \bar{2} = \bar{4} = \bar{0} \neq \bar{1}$
$\bar{1}$ is a unit	$\bar{3}$ is a unit	$\bar{2} \cdot \bar{3} = \bar{6} = \bar{2} \neq \bar{1}$

$\bar{2}$ has no mult inverse

only units: $\bar{1}, \bar{3}$

so $\bar{2}$ is not a unit

$\mathbb{Z}_4$ is not a field, it is a commutative ring w/ $\bar{1}$

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

$\mathbb{Z}_3$ is a commutative ring with $\bar{1}$.

units of $\mathbb{Z}_3$

$\bar{1} \cdot \bar{1} = \bar{1}$ ($\bar{1}$: unit) | $\bar{2} \cdot \bar{2} = \bar{4} = \bar{1}$ ($\bar{2}$: unit) | units are $\bar{1}$ and $\bar{2}$

$\therefore \mathbb{Z}_3$ is a field

note:
we will later see that $\mathbb{Z}_n$ is a field iff n is prime

Ex: $M_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a, b, c, d \in \mathbb{R} \right\}$

$M(2, \mathbb{R})$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} a+e & b+f \\ c+g & d+h \end{pmatrix}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix}$$

Ring ✓ additive identity is $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

additive inverse $-\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}$

Check commutivity

$AB = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$ $AB \neq BA$ in this case

$BA = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$ $M_2(\mathbb{R})$ is not commutative

$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is a mult. identity.

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

units: $\underset{\uparrow}{GL}(2, \mathbb{R}) = GL_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \underbrace{ad - bc}_{\det\begin{pmatrix} a & b \\ c & d \end{pmatrix}} \neq 0 \right\}$

general linear group

P. 2 1/26

Prop: Let R be a ring then:

① $0a = a0 = 0 \ \forall a \in R$

② $(-a)b = a(-b) = -(ab) \ \forall a, b \in R$

③ $(-a)(-b) = ab \ \forall a, b, \in R$

④ If R has identity $1 \neq 0$, then the identity is unique.

⑤ $-a = (-1)a \ \forall a \in R$

⑥ If R is a ring with a $1 \neq 0$ and x is a unit, then the mult inverse of x is unique and we denote it by x^{-1}.

Proof: ① Let $a \in R$ then

$$0a = (0+0)a = 0a + 0a$$

so, $\underbrace{-(0a) + (0a)}_{0} = \underbrace{-(0a) + 0a}_{0} + 0a$

Then $0 = 0a$, same thing for $a0 = 0$

② Lets show that $(-a)b$ is the additive identity of ab. so, $(-a)b = -ab$, we have that

$$(-a)b + ab = (-a+a)b$$
$$= 0b \overset{①}{=} 0,$$ similarly, $a(-b) = -(ab)$

③ By ②, $(-a)(-b) \overset{②}{=} -(a(-b)) \overset{②}{=} -(-(ab)) = ab$

④ Suppose that 1 and 1 are both identities for R

then $1 = 1 1 = 1$

since 1 is an identity of R

since 1 is an identity of R

⑤ Let $a \in R$. Then $-a = (-a)(1) = a(-1)$

⑥ Let x be a unit in R

Suppose y_1 and y_2 are both mult. inverses of x

then $y_1 x = x y_1 = 1$ and $y_2 x = x y_2 = 1$

so $y_1 x = 1 = y_2 x$

then, $(y_1 x) y_1 = (y_2 x) y_1$, so $y_1 \cdot 1 = y_2 \cdot 1$

Hence $y_1 = y_2$ $\boxtimes$

so there's only 1 mult. inverse