<u>GTLA Lecture</u> 04 August 2020

<u>Number systems</u>

$\mathbb{Z}_{>0} = \{1, 1+1, 1+1+1, 1+1+1+1, \ldots\}$

$= \{1, 2, 3, 4, \ldots\}$

$\mathbb{Z}_{\geq 0} = \{0, 1, 2, 3, 4, \ldots\}$

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

$\mathbb{Q} = \left\{ \frac{a}{b} \;\middle|\; a, b \in \mathbb{Z},\ b \neq 0 \text{ and } \frac{a}{b} = \frac{c}{d} \text{ if } ad = bc \right\}$

$\mathbb{R}$ = real numbers

$\mathbb{C}$ = complex numbers.

have addition and multiplication

Let $\mathbb{A}$ be a number system.
Let $a \in \mathbb{A}$.
Then a is <u>invertible</u> if
there exists $y \in \mathbb{A}$ such that
$a \cdot y = 1$ and $y \cdot a = 1$.

The multiples of a is the set

$a\mathbb{A} = \{ak \mid k \in \mathbb{A}\}$.

Example $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$

What are the invertible elements?

$1 \cdot 1 = 1$ so $1 \in \mathbb{Z}^\times$.

$(-1)(-1) = 1$ so $-1 \in \mathbb{Z}^\times$.

If $\mathbb{A}$ is a number system

$\mathbb{A}^\times = \{$invertible elements in $\mathbb{A}\}$.

$\mathbb{Z}^\times = \{1, -1\}$

Multiples in $\mathbb{Z}$

$0\mathbb{Z} = \{0\}$

$1 \cdot \mathbb{Z} = (-1)\mathbb{Z} = \{\ldots -3, -2, -1, 0, 1, 2, 3 \ldots\}$

$2\mathbb{Z} = -2\mathbb{Z} = \{\ldots -6, -4, -2, 0, 2, 4, 6, \ldots\}$

$3\mathbb{Z} = -3\mathbb{Z} = \{\ldots -9, -6, -3, 0, 3, 6, 9 \ldots\}$

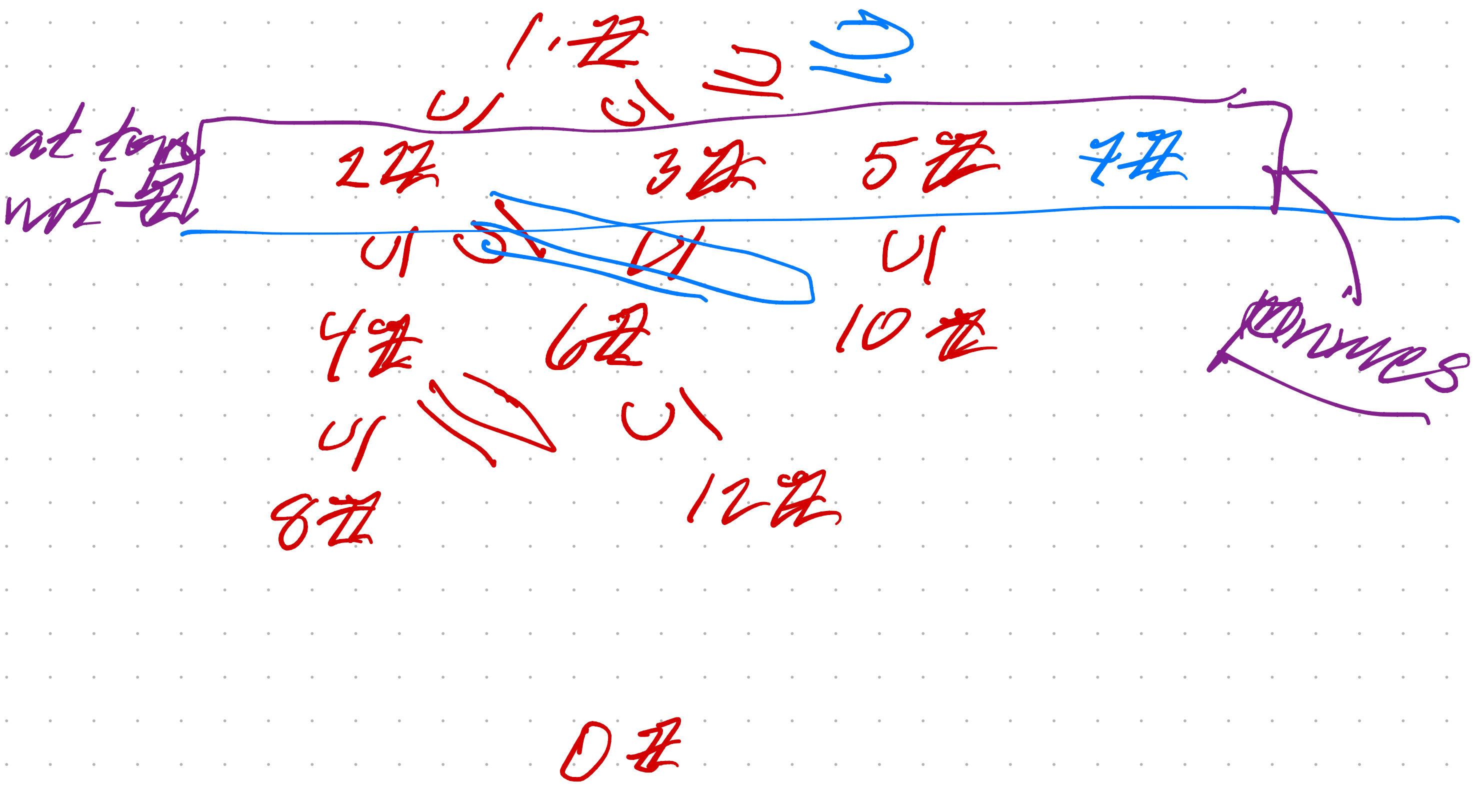
If $m \in \mathbb{Z}$ then $m\mathbb{Z} = -m\mathbb{Z}$

Sets of Multiples $\longleftrightarrow$ elements $m \in \mathbb{Z}_{\geq 0}$

$m\mathbb{Z} \longleftarrow\!\shortmid\; m$

Sets $m\mathbb{Z}$ are also called **submodules of $\mathbb{Z}$** or **subgroups of $\mathbb{Z}$**

or **ideals of $\mathbb{Z}$**



Prime factorizations of 6:

$$\underbrace{6\mathbb{Z} \subseteq 2\mathbb{Z}}_{3} \underbrace{\subseteq \mathbb{Z}}_{2} \qquad 6 = 3\cdot 2$$

$$\underbrace{6\mathbb{Z} \subseteq 3\mathbb{Z}}_{2} \underbrace{\subseteq \mathbb{Z}}_{3} \qquad 6 = 2\cdot 3$$

Prime factorization of 12:

$12\mathbb{Z} \subseteq 6\mathbb{Z} \subseteq 2\mathbb{Z} \subseteq \mathbb{Z}$ $\quad 12 = 2 \cdot 3 \cdot 2$

$\underbrace{12\mathbb{Z} \subseteq 6\mathbb{Z}}_{2} \; \underbrace{\subseteq 2\mathbb{Z}}_{3} \; \underbrace{\subseteq \mathbb{Z}}_{2}$

---

gcd greatest common divisor.

Let S and T be ideals in $\mathbb{Z}$.

So $S = s\mathbb{Z}$ and $T = t\mathbb{Z}$

$$S + T = \{k + l \mid k \in S,\ l \in T\}$$

$$6\mathbb{Z} = \{\ldots -18, -12, -6, 0, 6, 12, 18, \ldots\}$$

$$8\mathbb{Z} = \{\ldots -24, -16, -8, 0, 8, 16, 24, \ldots\}$$

$$6\mathbb{Z} + 8\mathbb{Z} = \{\ldots, 12 + -16, 6 + -8, 0 + 0, -6 + 8, -12 + 16, \ldots\}$$

$$= \{\ldots, -4, -2, 0, 2, 4, \ldots\} = 2\mathbb{Z}$$

$$6\mathbb{Z} + 8\mathbb{Z} = 2\mathbb{Z}.$$

$2 = \gcd(6, 8)$

Theorem

Let $a, b \in \mathbb{Z}_{>0}$. Then there exists a unique $l \in \mathbb{Z}_{>0}$ such that

$$a\mathbb{Z} + b\mathbb{Z} = l\mathbb{Z}.$$

Theorem 1 If

$a = p_1^{a_1} \cdots p_r^{a_r}$ and $b = p_1^{b_1} \cdots p_r^{b_r}$

are prime factorizations (allowing $a_i, b_i \in \mathbb{Z}_{\geq 0}$), then

$$a\mathbb{Z} + b\mathbb{Z} = \ell\mathbb{Z}$$

if and only if

$$\ell = p_1^{\min(a_1,b_1)} \cdots p_r^{\min(a_r,b_r)}$$ and

if and only if

ℓ satisfies

(b1) ℓ divides a and ℓ divides b.

(b2) If $m \in \mathbb{Z}_{>0}$ and m divides a and m divides b (other divisor)

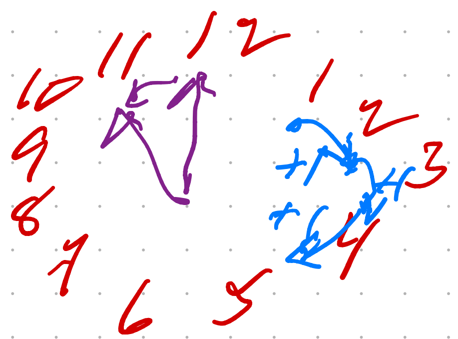
then m divides ℓ (ℓ is bigger than m)

greatest common divisor

$\ell = \gcd(a,b)$

12 clock $\mathbb{Z}/12\mathbb{Z}$

$\mathbb{Z}/12\mathbb{Z} = \{$



$\}$

+1 is one step clockwise
-1 is one step counterclockwises
$12+5=5$. Another name for 12 is 0 (in $\mathbb{Z}/12\mathbb{Z}$)
so
$12-1 = 0-1 = -1 = 11$

A ring, or a $\mathbb{Z}$-algebra, or a number system, is a set A with two functions

$$A \times A \to A \qquad\qquad A \times A \to A$$
$$(a,b) \mapsto a+b \qquad\qquad (a,b) \mapsto ab$$

such that

(1) If $a,b,c \in A$ then
$$(a+b)+c = a+(b+c)$$
(2) If $a,b \in A$ then $a+b=b+a$
(3) There exist $0 \in A$ such that if $a \in A$ then $0+a=a$ and $a+0=a$
(4) If $a \in A$ then there exists $-a \in A$ such that

$a + (-a) = 0$ and $(-a) + a = 0$

(5) If $a, b, c \in A$ then $(ab)c = a(bc)$

(6) There exist $1 \in A$ such that if $a \in A$ then $1 \cdot a = a$ and $a \cdot 1 = a$

(7) If $a, b, c \in A$ then $a(b+c) = ab + ac$ and $(a+b)c = ac + bc$.