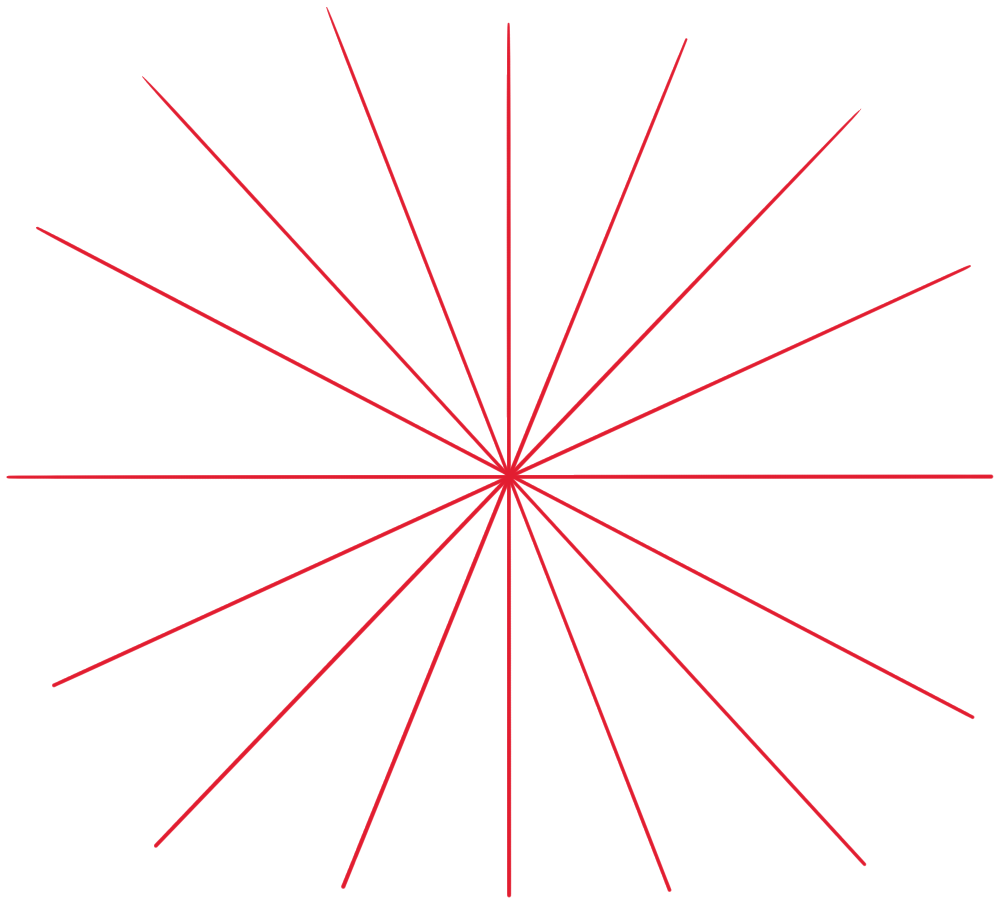


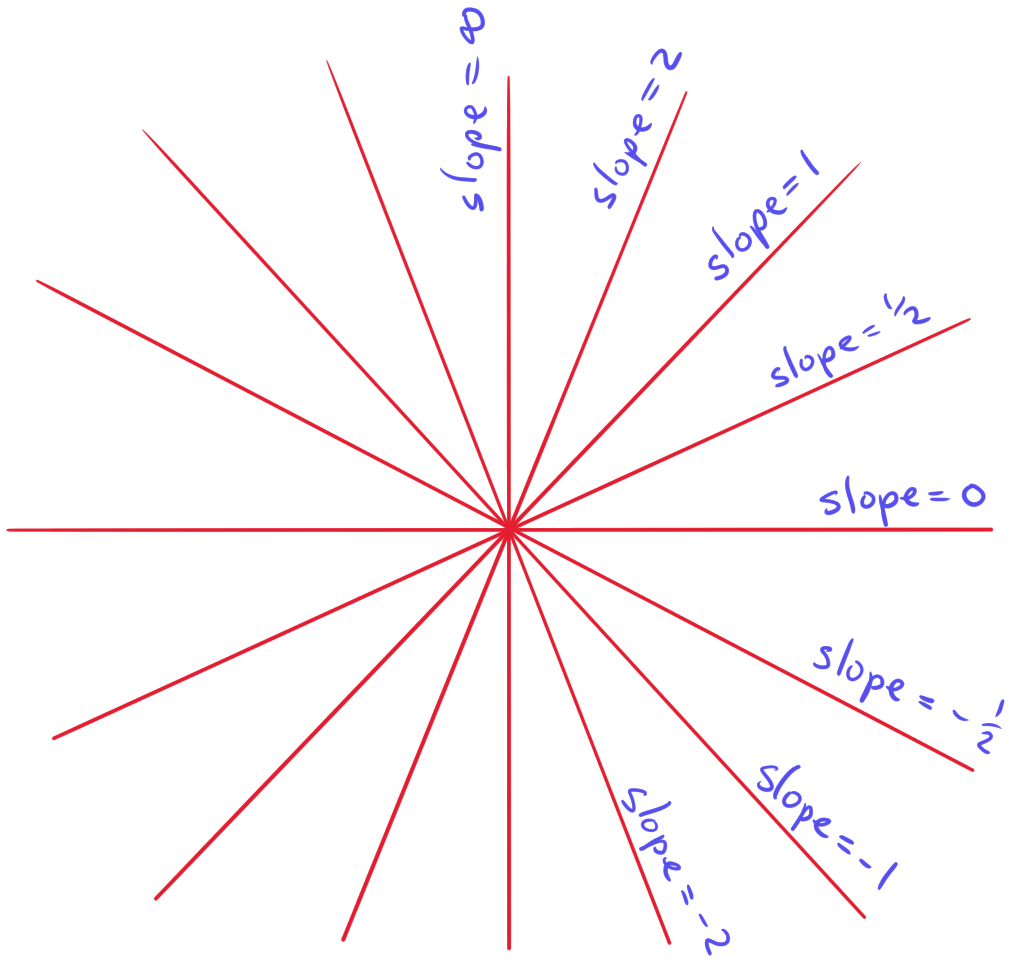
$$\{\text{lines through the origin}\}$$

$$\updownarrow$$

$$\{\text{slopes}\}$$

$$\updownarrow$$

$$\mathbb{R} \cup \{\infty\}$$



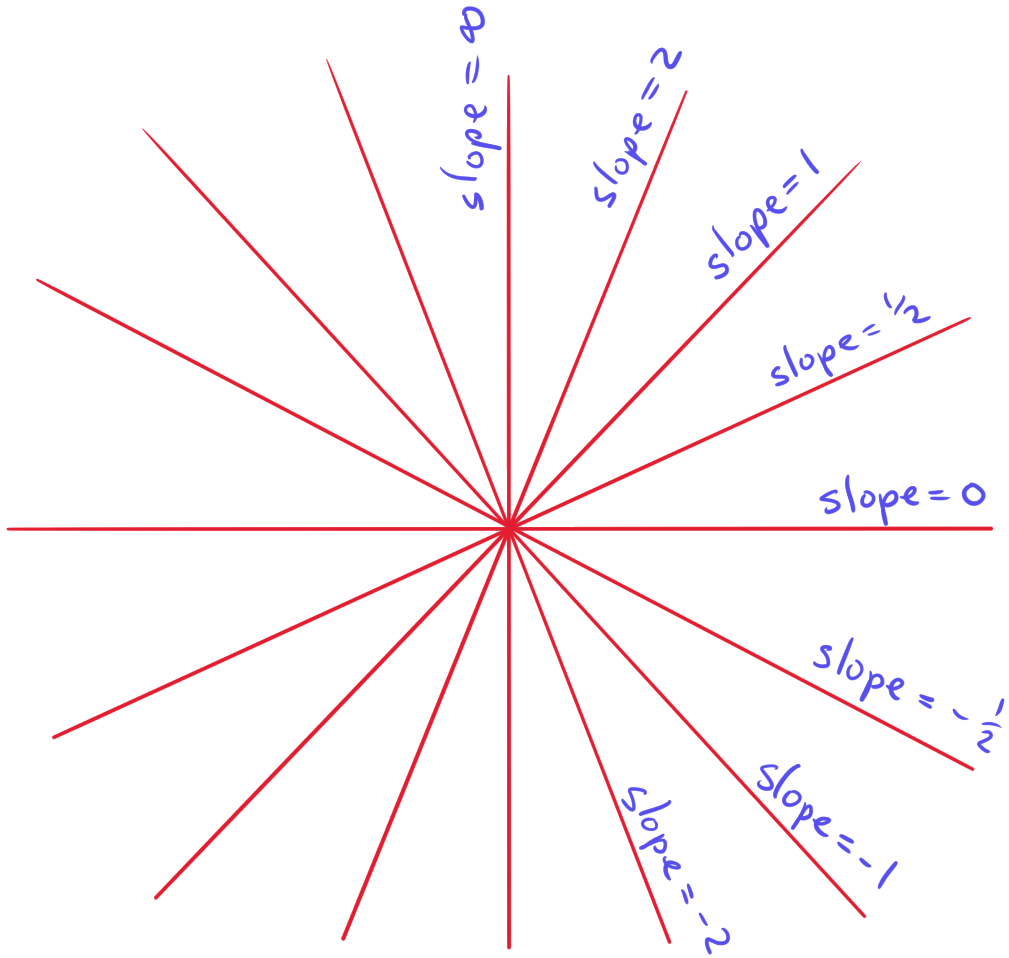
{ lines through the origin }

↕

{ slopes }

↕

$\mathbb{R} \cup \{\infty\}$



{ lines through the origin }

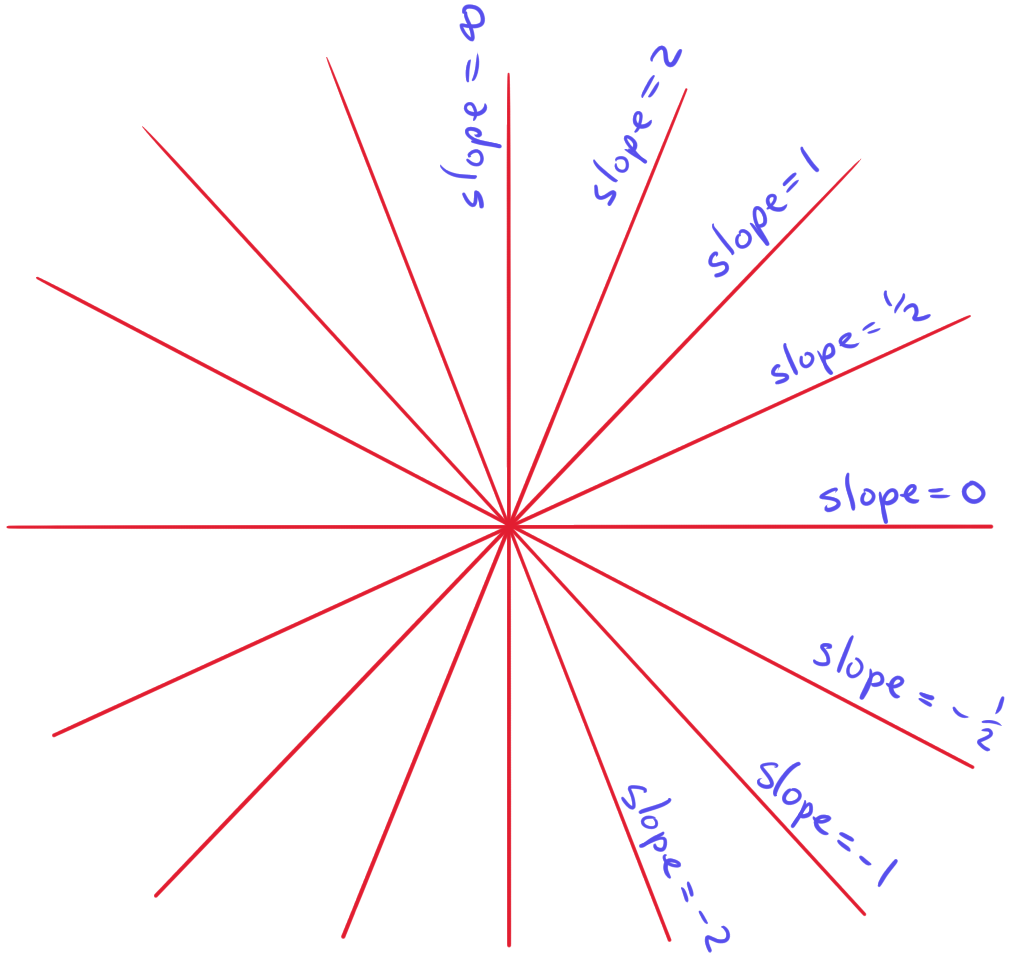
$\Leftrightarrow$

{ slopes }

$\Leftrightarrow$

$\mathbb{R} \cup \{\infty\}$

The projective line, denoted $\mathbb{P}^1_{\mathbb{R}}$



$$\mathbb{P}^1_{\mathbb{R}} = \text{vectors in plane modulo length}$$

$$= \{ \vec{v} \in \mathbb{R}^2 \setminus \{\vec{0}\} \} / \sim$$

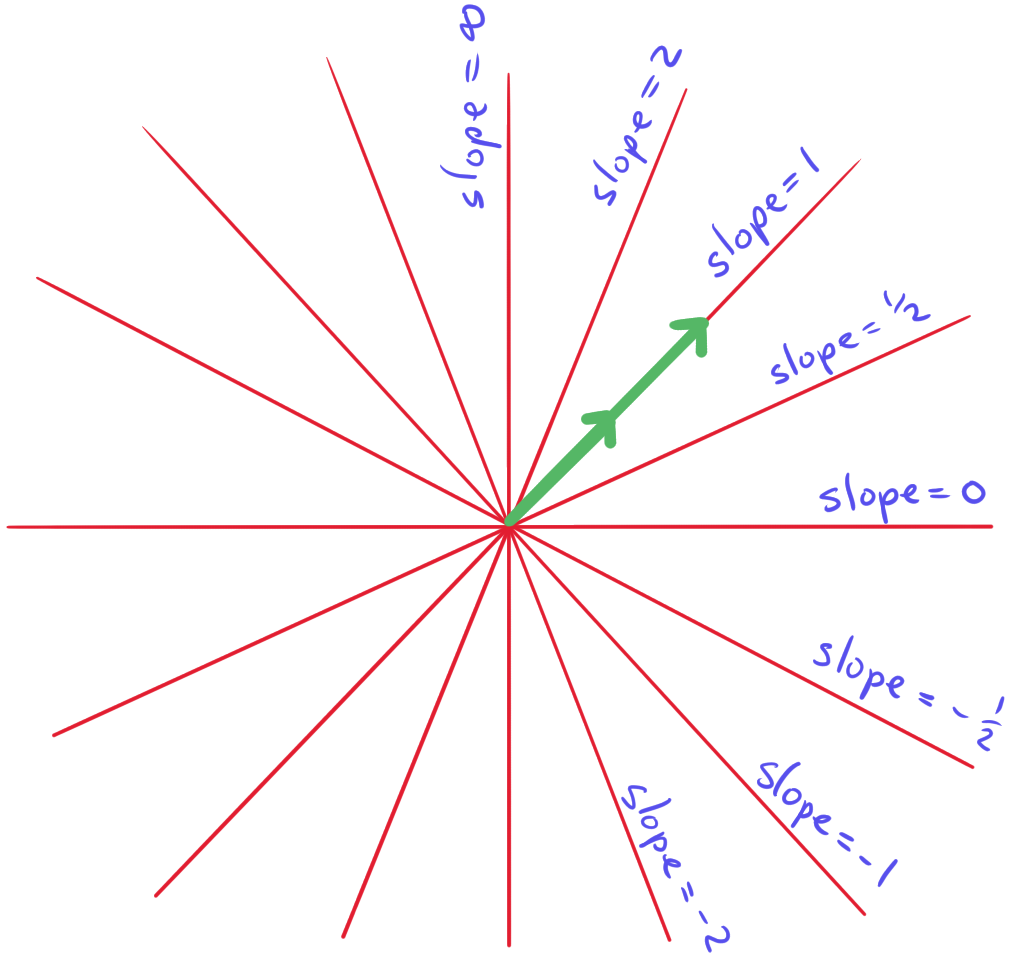
where

$\vec{v}_1 \sim \vec{v}_2$ iff

$\vec{v}_1 = \lambda \vec{v}_2$

for some $\lambda \in \mathbb{R}^* = \mathbb{R} \setminus \{0\}$

The projective line, denoted $\mathbb{P}^1_{\mathbb{R}}$



$$\mathbb{P}^1_{\mathbb{R}} = \text{vectors in plane modulo length}$$

$$= \{ \vec{v} \in \mathbb{R}^2 \setminus \{\vec{0}\} \} / \sim$$

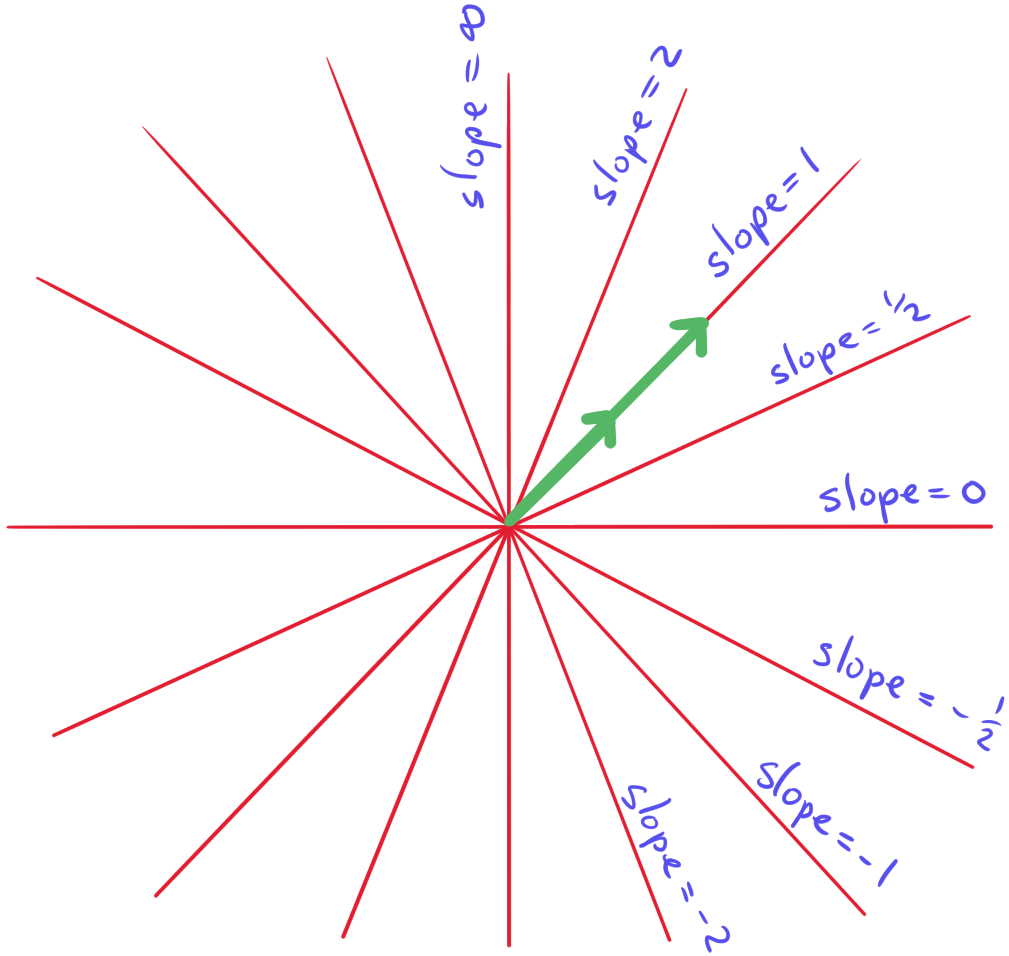
where

$\vec{v}_1 \sim \vec{v}_2$ iff

$\vec{v}_1 = \lambda \vec{v}_2$

for some $\lambda \in \mathbb{R}^* = \mathbb{R} \setminus \{0\}$

Example: $(1,1) \sim (2,2)$



$$\mathbb{P}^1_{\mathbb{R}} = \text{vectors in plane modulo length}$$

$$= \{ \vec{v} \in \mathbb{R}^2 \setminus \{\vec{0}\} \} / \sim$$

where

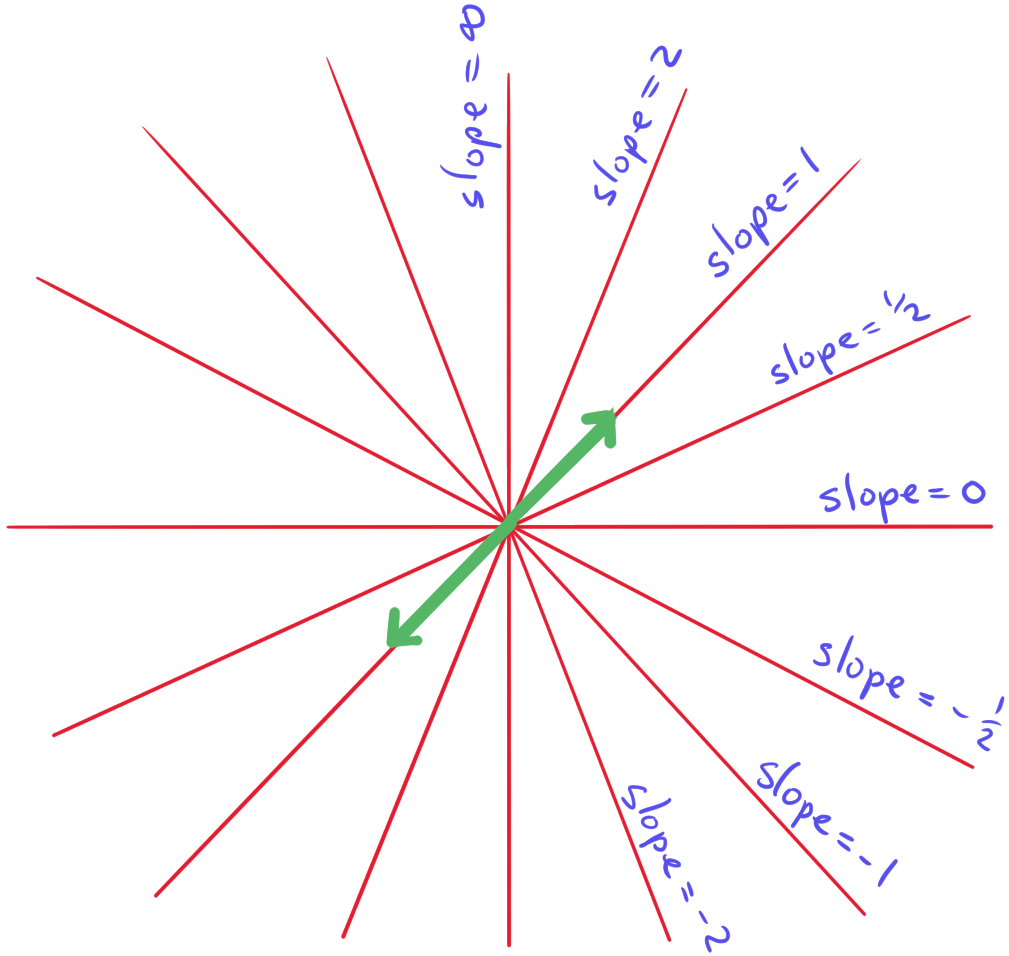
$\vec{v}_1 \sim \vec{v}_2$ iff

$\vec{v}_1 = \lambda \vec{v}_2$

for some $\lambda \in \mathbb{R}^* = \mathbb{R} \setminus \{0\}$

Example: $(1,1) \sim (2,2)$

notation: $[1,1] = [2,2]$



$$\mathbb{P}^1_{\mathbb{R}} = \text{vectors in plane modulo length}$$

$$= \{ \vec{v} \in \mathbb{R}^2 \setminus \{\vec{0}\} \} / \sim$$

where

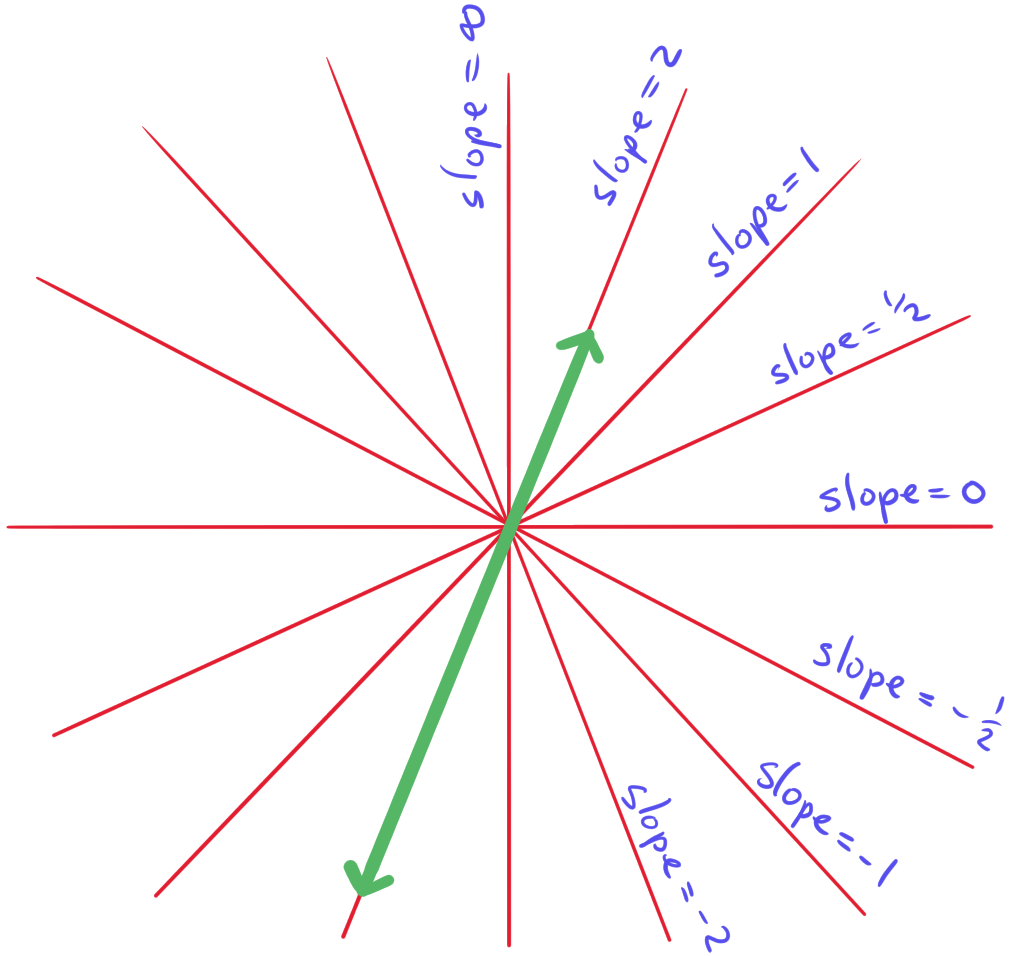
$\vec{v}_1 \sim \vec{v}_2$ iff

$\vec{v}_1 = \lambda \vec{v}_2$

for some $\lambda \in \mathbb{R}^* = \mathbb{R} \setminus \{0\}$

Example: $(1,1) \sim (-1,-1)$

notation: $[1,1] = [2,2] = [-1,-1]$



$$\mathbb{P}^1_{\mathbb{R}} = \text{vectors in plane modulo length}$$

$$= \{ \vec{v} \in \mathbb{R}^2 \setminus \{\vec{0}\} \} / \sim$$

where

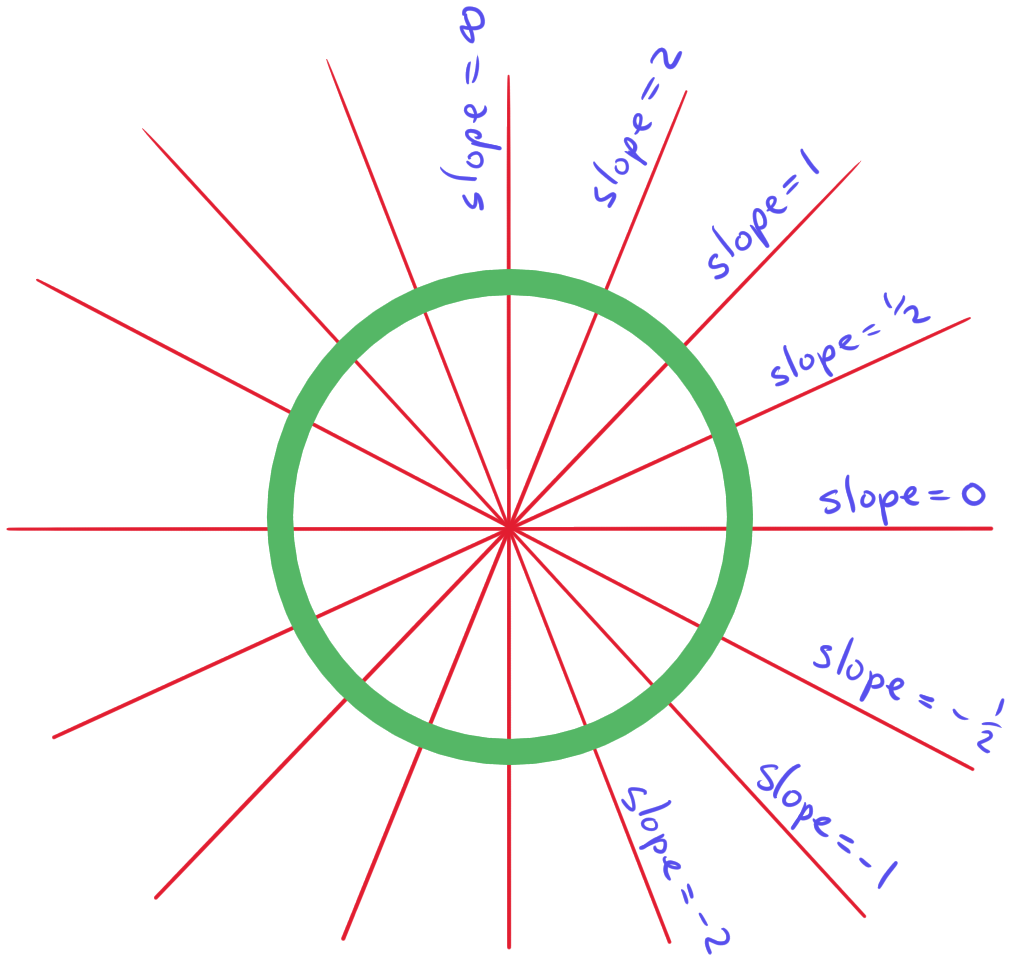
$\vec{v}_1 \sim \vec{v}_2$ iff

$\vec{v}_1 = \lambda \vec{v}_2$

for some $\lambda \in \mathbb{R}^* = \mathbb{R} \setminus \{0\}$

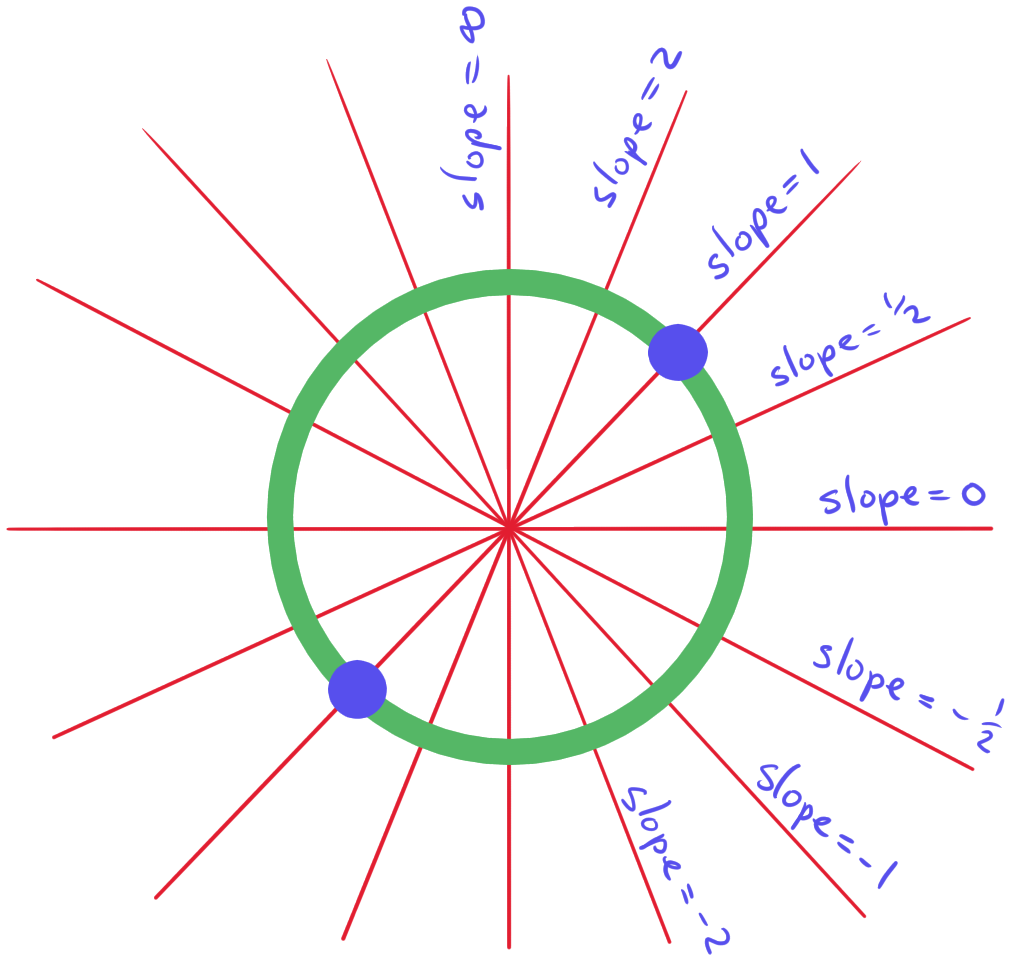
Example: $(\frac{1}{2}, 1) \sim (-1, -2)$

notation: $[\frac{1}{2}, 1] = [-1, -2] = [1, 2]$



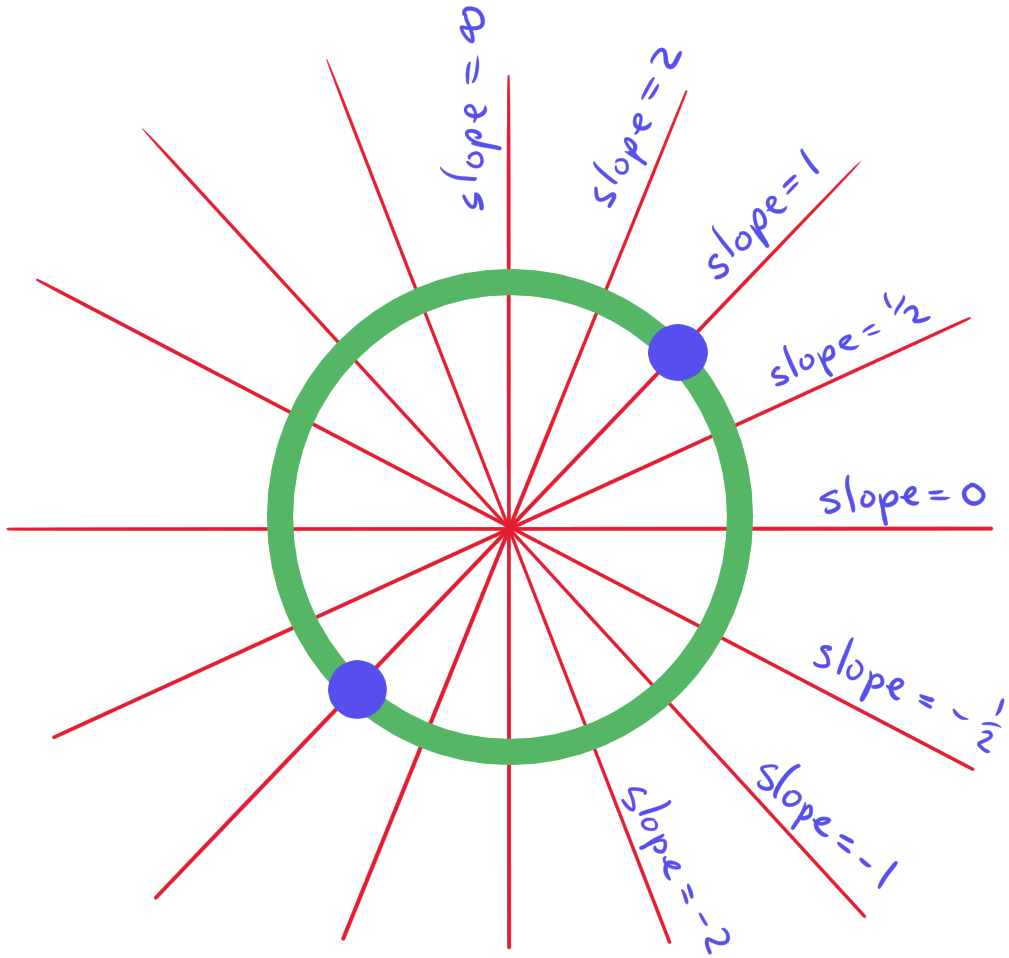
$$\mathbb{P}^1_{\mathbb{R}} = \text{vectors in plane modulo length}$$

$$= \{ \vec{v} \in \mathbb{R}^2 \setminus \{\vec{0}\} \} / \sim$$



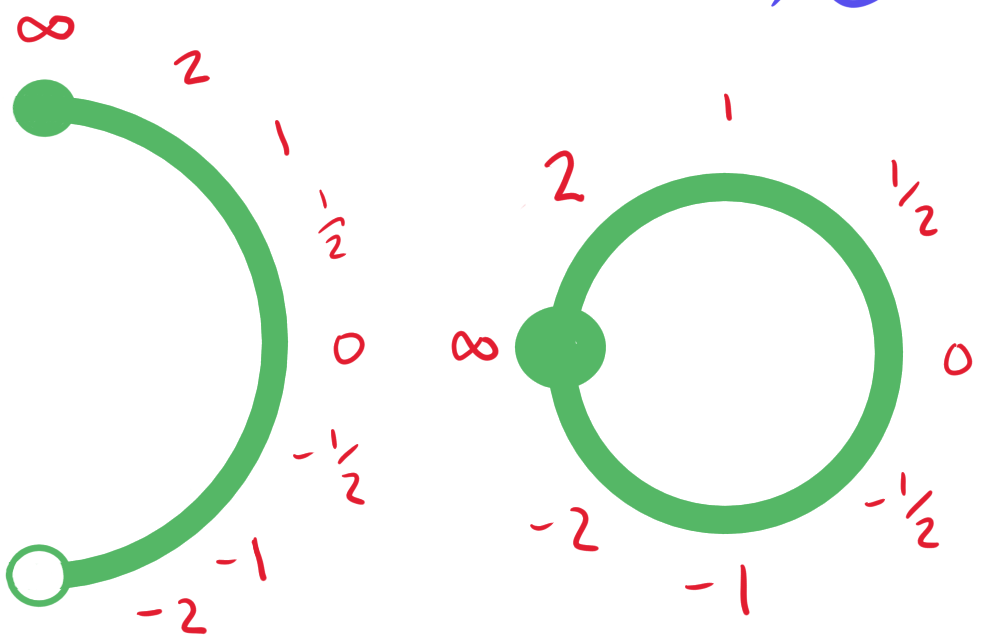
$$\mathbb{P}^1_{\mathbb{R}} = \text{vectors in plane modulo length}$$

$$= \{ \vec{v} \in \mathbb{R}^2 \setminus \{\vec{0}\} \} / \sim$$

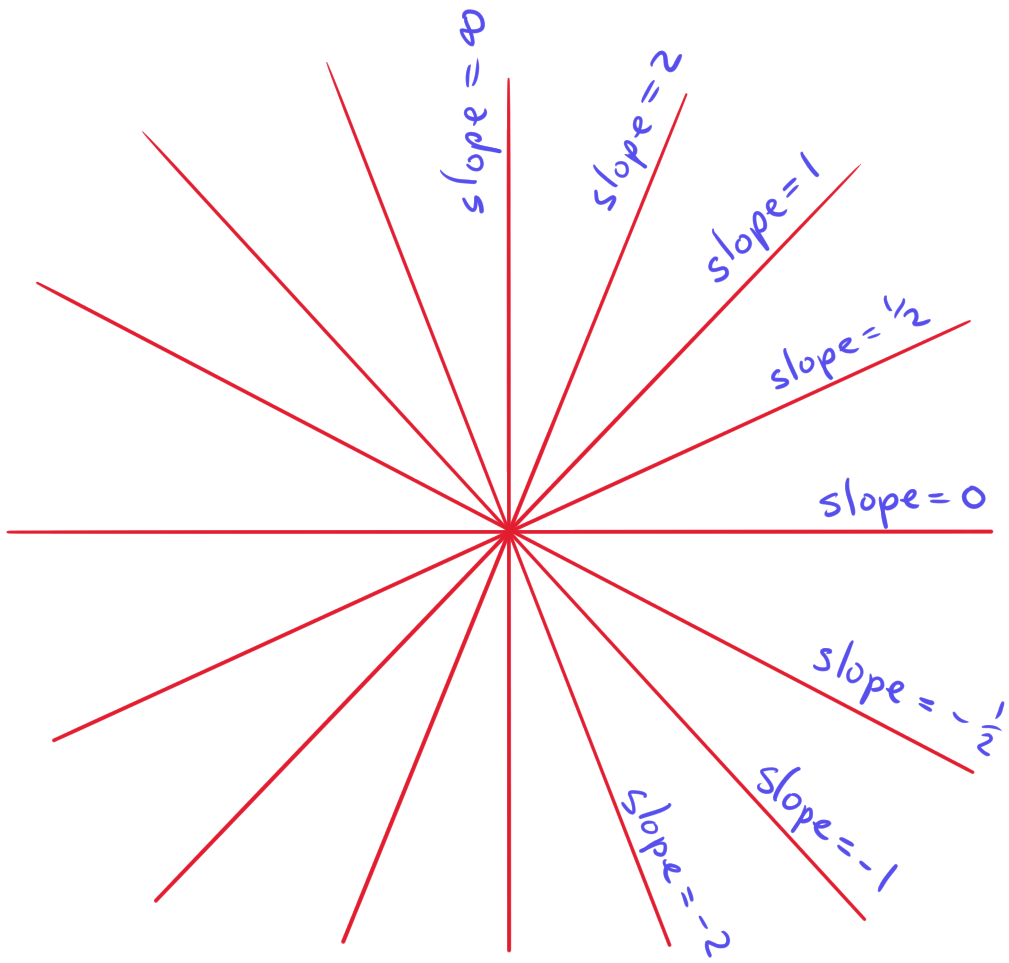


$$\mathbb{P}^1_{\mathbb{R}} = \text{vectors in plane modulo length}$$

$$= \{ \vec{v} \in \mathbb{R}^2 \setminus \{\vec{0}\} \} / \sim$$



$$\mathbb{R} \cup \{\infty\}$$



$$\mathbb{P}^1_{\mathbb{R}} = \text{vectors in plane modulo length}$$

$$= \{ \vec{v} \in \mathbb{R}^2 \setminus \{\vec{0}\} \} / \sim$$

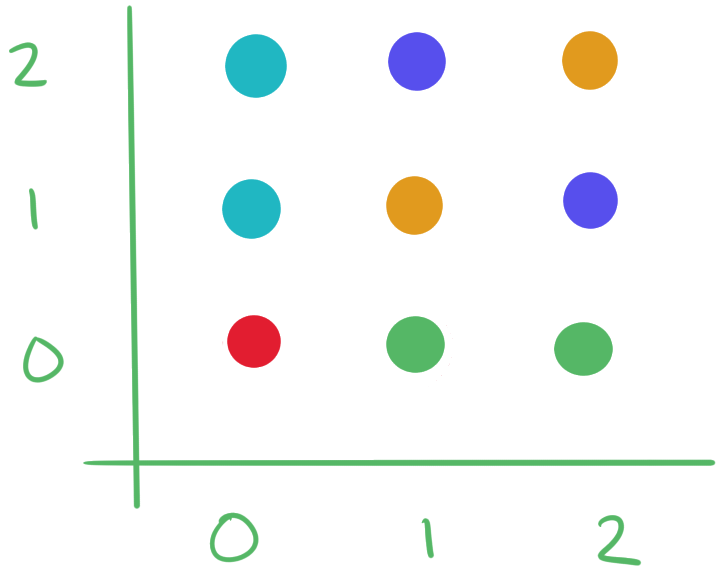
$$\mathbb{P}^1_{\mathbb{F}_p} = \text{vectors in plane modulo length}$$

$$= \{ \vec{v} \in \mathbb{F}_p^{\,2} \setminus \{\vec{0}\} \} / \sim$$

Example.

$\mathbb{P}^1_{\mathbb{F}_3}$

Note: $\mathbb{F}_3^* = \{1, 2\}$



$[1,0] = [2,0]$

$[1,1] = [2,2]$

$[2,1] = [1,2]$

$[0,1] = [0,2]$

$$\left|\mathbb{P}^1_{\mathbb{F}_3}\right| = 4$$

$$\mathbb{P}^1_{\mathbb{F}_p} = \text{vectors in plane modulo length}$$

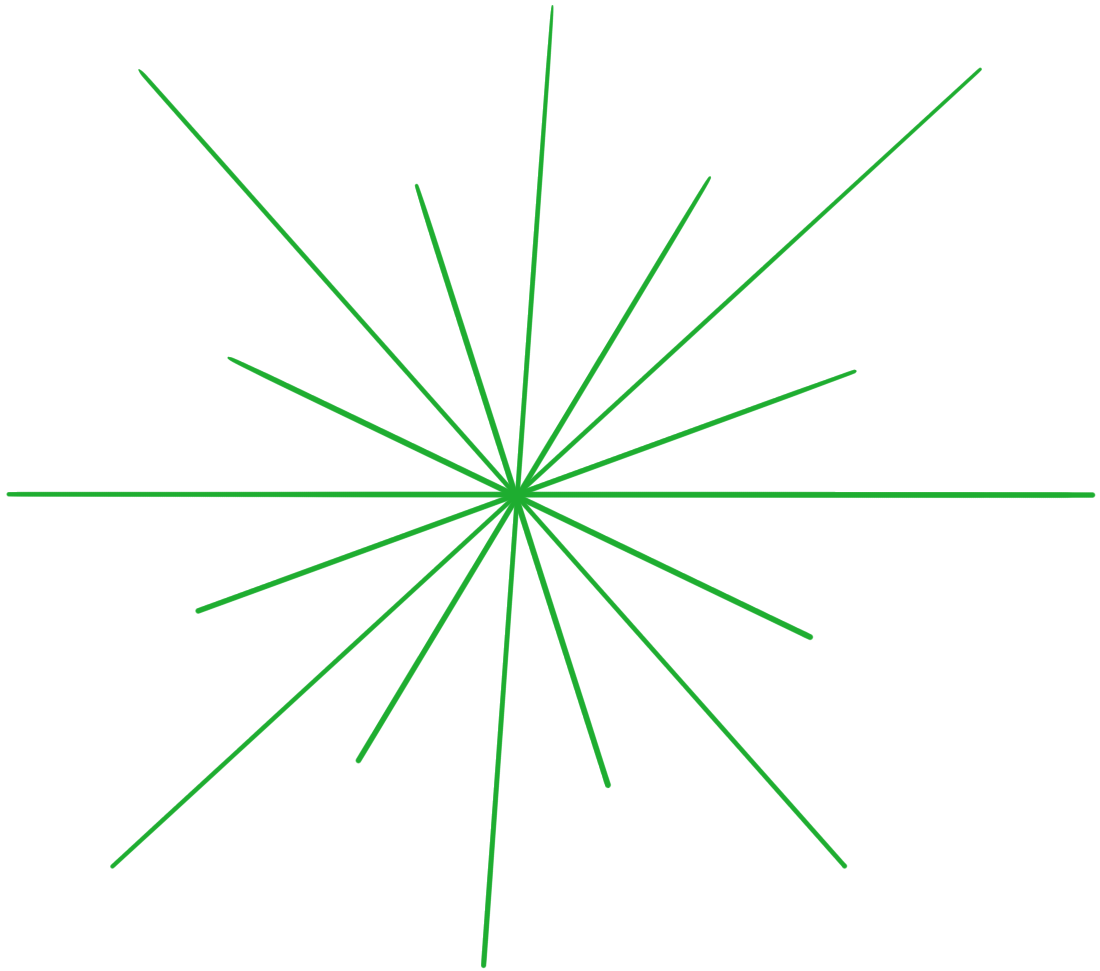
$$= \left\{ \vec{v} \in \mathbb{F}_p^{\,2} \setminus \{\vec{0}\} \right\} / \sim$$

$\vec{v}_1 \sim \vec{v}_2$ iff $\vec{v}_1 = \lambda \vec{v}_2$ for some $\lambda \in \mathbb{F}_p^*$

$$\mathbb{P}^1_{\mathbb{R}} = \text{vectors in plane modulo length}$$

$$= \{ \vec{v} \in \mathbb{R}^2 \setminus \{\vec{0}\} \} / \sim$$

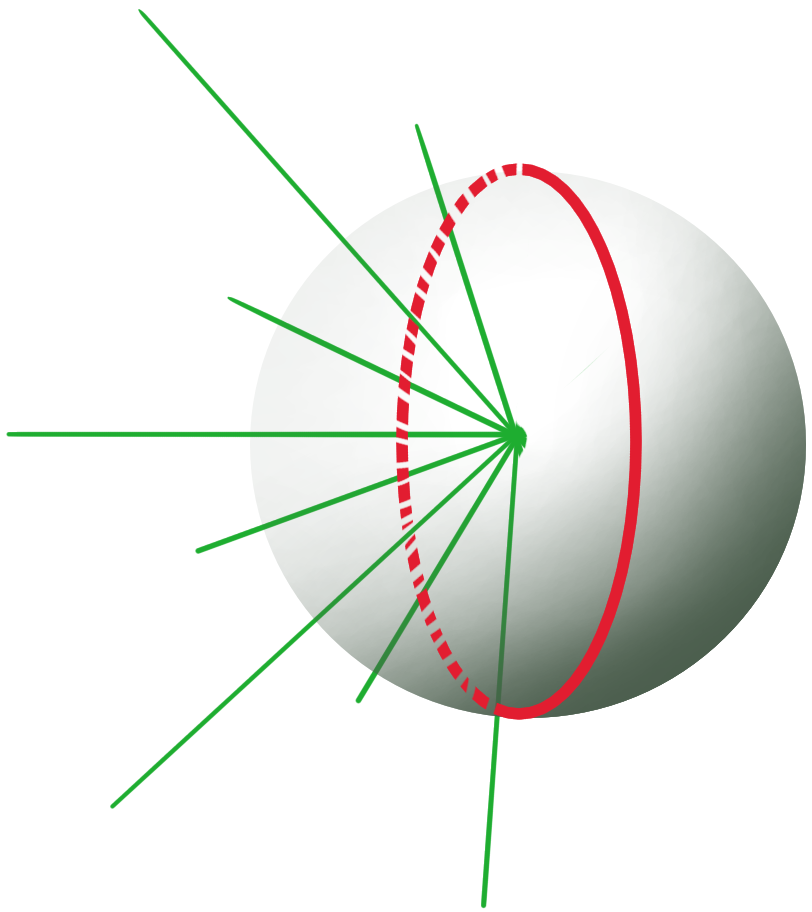
$\vec{v}_1 \sim \vec{v}_2$
iff
$\vec{v}_1 = \lambda \vec{v}_2$ for some $\lambda \in \mathbb{R}^*$



$$\mathbb{P}^2_{\mathbb{R}} = \text{vectors in space modulo length}$$

$$= \{ \vec{v} \in \mathbb{R}^3 \setminus \{\vec{0}\} \} / \sim$$

$\vec{v}_1 \sim \vec{v}_2$
iff
$\vec{v}_1 = \lambda \vec{v}_2$ for some $\lambda \in \mathbb{R}^*$



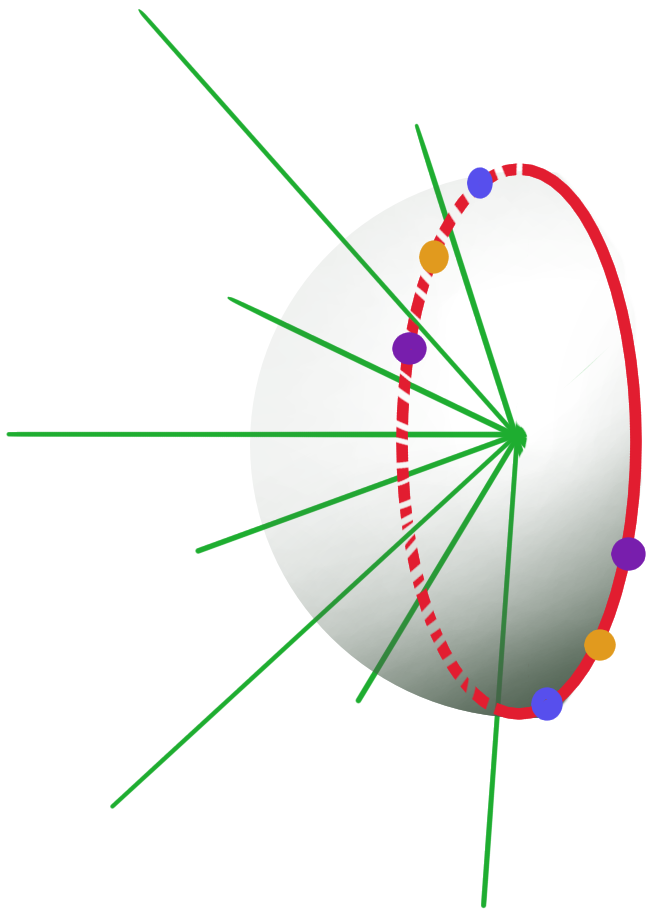
$\mathbb{P}^2_{\mathbb{R}}$ = vectors in space modulo length

$= \{ \vec{v} \in \mathbb{R}^3 \setminus \{\vec{0}\} \} / \sim$

$\vec{v}_1 \sim \vec{v}_2$

iff

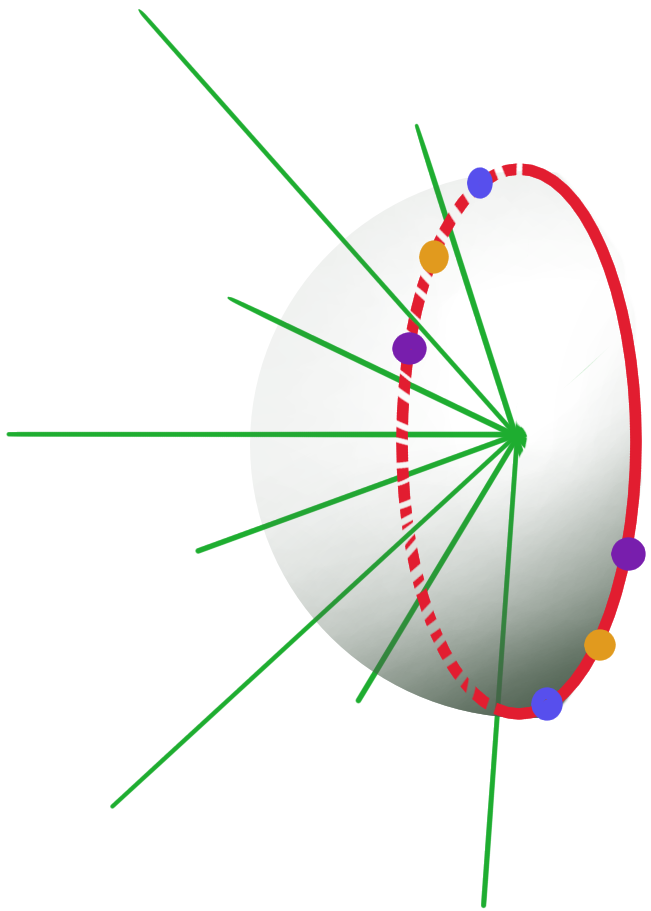
$\vec{v}_1 = \lambda \vec{v}_2$ for some $\lambda \in \mathbb{R}^*$



$$\mathbb{P}^2_{\mathbb{R}} = \text{vectors in space modulo length}$$

$$= \{ \vec{v} \in \mathbb{R}^3 \setminus \{\vec{0}\} \} / \sim$$

$\vec{v}_1 \sim \vec{v}_2$
iff
$\vec{v}_1 = \lambda \vec{v}_2$ for some $\lambda \in \mathbb{R}^*$



$\mathbb{P}^2_{\mathbb{R}}$ = vectors in space modulo length

$= \{ \vec{v} \in \mathbb{R}^3 \setminus \{\vec{0}\} \} / \sim$

$\vec{v}_1 \sim \vec{v}_2$ iff $\vec{v}_1 = \lambda \vec{v}_2$ for some $\lambda \in \mathbb{R}^*$

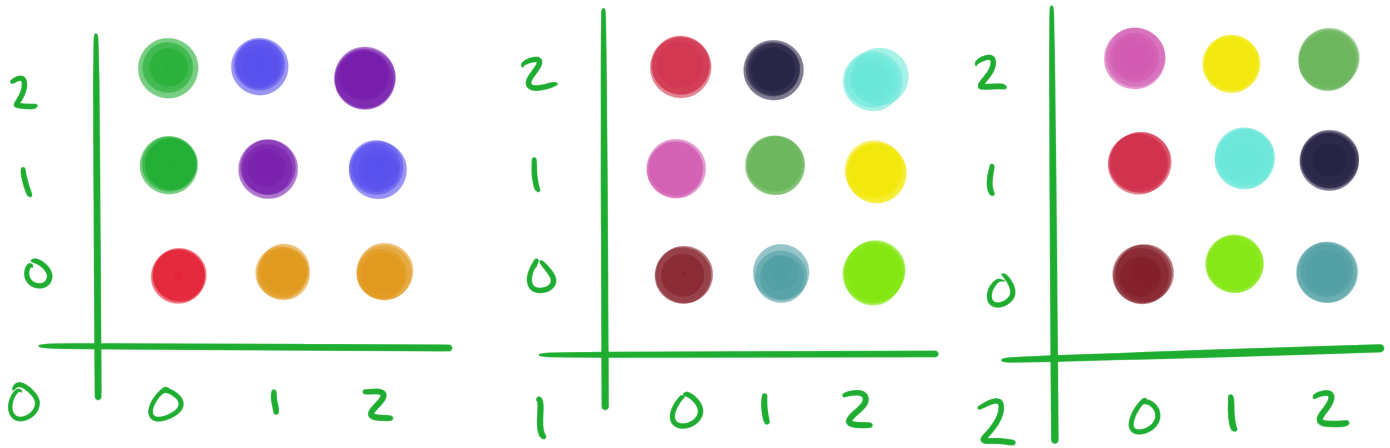
Example: $(1,0,7) \sim (2,0,14)$ notation: $[1,0,7]$

$$\mathbb{P}^2_{\mathbb{F}_p} = \text{vectors in space modulo length}$$

$$= \{ \vec{v} \in \mathbb{F}_p^{\,3} \setminus \{\vec{0}\} \} / \sim$$

$$\vec{v}_1 \sim \vec{v}_2$$
iff
$$\vec{v}_1 = \lambda \vec{v}_2 \text{ for some } \lambda \in \mathbb{F}_p^{\,*}$$

Example. $\mathbb{P}^2_{\mathbb{F}_3}$ = projective plane over $\mathbb{F}_3$



each equivalence class has 2 elements

26 nonzero vectors

$\Rightarrow$ 13 elements in $\mathbb{P}^2_{\mathbb{F}_3}$

Example: $[1,1,2] = [2,2,1]$

$$\mathbb{P}^2_{\mathbb{F}_p} = \text{vectors in space modulo length}$$

$$= \{ \vec{v} \in \mathbb{F}_p^3 \setminus \{\vec{0}\} \} / \sim$$

$\vec{v}_1 \sim \vec{v}_2$ iff

$\vec{v}_1 = \lambda \vec{v}_2$ for some $\lambda \in \mathbb{F}_p^*$



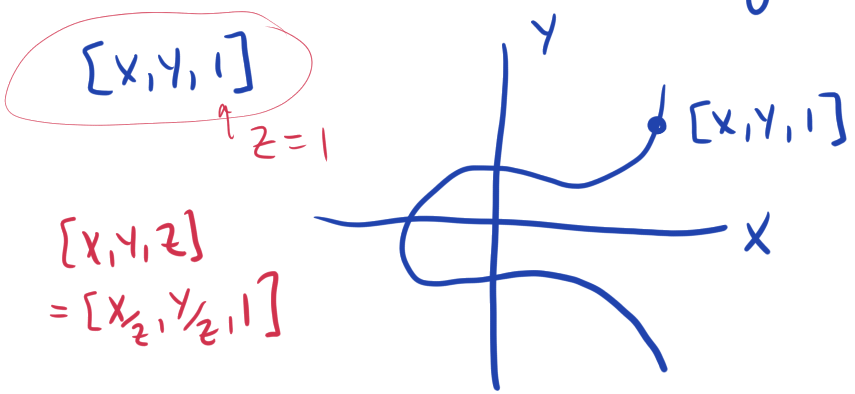
Elliptic Curve
in the
projective
plane

Elliptic Curves in projective space.

$$E: Y^2Z = X^3 + aXZ^2 + bZ^3$$

$[X,Y,Z] \in E$ if it satisfies the equation

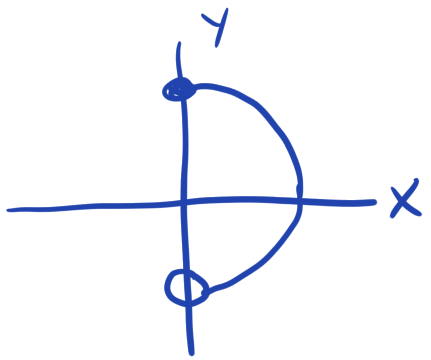
The "affine part" $Z \neq 0$ looks like a copy of $\mathbb{R}^2$



The "line at infinity" is a copy of $\mathbb{P}^1$



$\{[X,Y,0]\}$



The curve has only one pt here:

$[0,1,0]$

$=$ "∞"

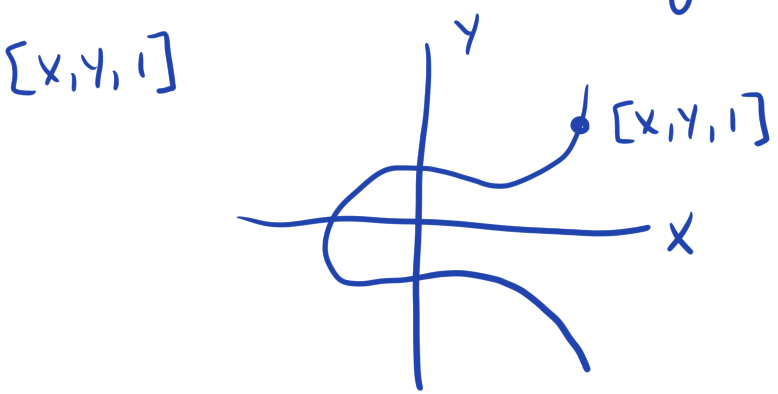
Elliptic Curves in projective space.

$$E: Y^2Z = X^3 + aXZ^2 + bZ^3$$

$[X,Y,Z] \in E$ if it satisfies the equation

The "affine part" $Z \neq 0$

looks like a copy of $\mathbb{R}^2$



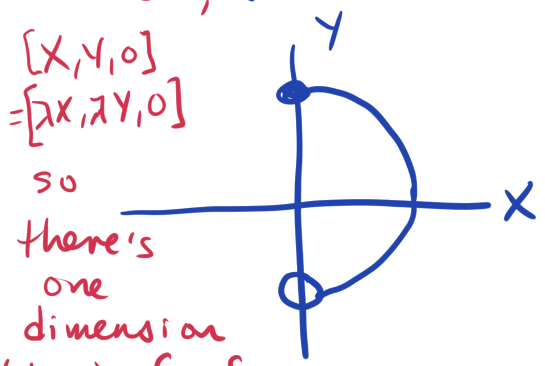
with $z=1$ fixed you can't scale X,Y so there's 2 dimensions (X,Y) of info

The "line at infinity" $Z=0$

is a copy of $\mathbb{P}^1$

$\{[X,Y,0]\}$

with $z=0$, $[X,Y,0] = [\lambda X, \lambda Y, 0]$ so there's one dimension (slope) of info



The curve has only one pt here:

$[0,1,0]$

$=$ "∞"