18.781 — 23 Apr 2003

Arithmetic of Curves / Elliptic curves

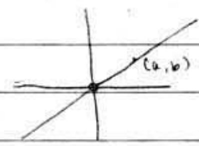
Projective space

$\mathbb{P}^1(\mathbb{R}) \leftrightarrow \mathbb{R} \cup \{\infty\}$

consider pairs $[a:b]$ $a, b \in \mathbb{R}$ not both 0

$[a:b] \sim [\lambda a : \lambda b]$ $\lambda \in \mathbb{R} - \{0\}$

Then $\mathbb{P}^1(\mathbb{R})$ is the set of equivalence classes of pairs $[a:b]$



$\mathbb{P}^1(\mathbb{R})$ is set of all lines through $(0,0)$

Look at $[a:b]$ $b \neq 0$.

$[a:b] \sim [a/b : 1]$

so every pair $[a:b]$, $b \neq 0$ is equiv. to $[a':1]$ for some unique a'.

We identify $\mathbb{R}$ with the set of equiv. classes with $b \neq 0$.

$a \longmapsto [a:1]$

Extra point: Class of $[1:0]$. call this ∞

$\mathbb{P}^2(\mathbb{R})$: Triples $[a:b:c]$ $a, b, c \in \mathbb{R}$ not all zero

$[a:b:c] \sim [\lambda a : \lambda b : \lambda c]$. $\lambda \in \mathbb{R} - \{0\}$

$\mathbb{P}^2(\mathbb{R})$ = eq. classes of such triples.

$\mathbb{P}^2(\mathbb{R}) = \mathbb{R}^2 \cup \{$a little extra$\}$

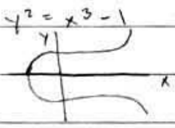
$\mathbb{R}^2$ — {eq. classes of triples $[a:b:c]$ with $c \neq 0$}

$(a,b) \longmapsto [a:b:1]$

"extra stuff": {eq. classes of $[a:b:0]$}

which is $\mathbb{P}^1(\mathbb{R})$.

Ex: $y^2 = x^3 - 1$



$y^2 z = x^3 - z^3$

$y^2 z - (x^3 - z^3) = 0$.

say $[a:b:c]$ s.t. $b^2 c - (a^3 - c^3) = 0$.

consider $[\lambda a : \lambda b : \lambda c]$ $(\lambda b)^2 (\lambda c) - ((\lambda a)^3 - (\lambda c)^3) = \lambda^3 (b^2 c - (a^3 - c^3))$

so $[\lambda a : \lambda b : \lambda c]$ satisfies eqn iff $[a:b:c]$ does

Thus it makes sense to talk about a point (i.e. elt) of $\mathbb{P}^2(\mathbb{R})$

to satisfy $y^2 z = x^3 - z^3$.

Let $V \subset \mathbb{P}^2(\mathbb{R})$ be pts that satisfy eqn.

Points of V which lie in $\mathbb{R}^2 \subset \mathbb{P}^2(\mathbb{R})$. $\mathbb{R}^2 = \{[a:b:1]\}$

$= \{$pairs (a,b) s.t. $b^2(1) - (a^3 - 1^3) = 0\} = \{$pairs (a,b) satisfying

$y^2 = x^3 - 1\}$.

Let's compute $V \cap \{\text{a little extra}\}$. $\{\text{a little extra}\} = \{[a:b:0]\}$

$y^2 z - (x^3 - z^3) = 0$

$b^2(0) - (a^3 - 0^3) = 0 \Rightarrow a = 0$

Thus $V \cap \{\text{a little extra}\} = [0:b:0]$ (which is 1 extra point)

$V = \{\text{sol'ns to } y^2 - (x^3 - 1) = 0\} \cup \{\overset{\infty}{[0:1:0]}\}$