2

2020年6月22日 15:50

下周一6月29日 临时调整上课时间：9:30-11:00

$K = \mathbb{Q}$ $\mathbb{Q}_p$ $\mathbb{P}^n$

p-adic 数

$\mathbb{N} \cup \{0\} \hookrightarrow \mathbb{Z} \hookrightarrow \mathbb{Q} \hookrightarrow \mathbb{R}$ 完备

3.
3.1
3.14
3.141
⋮

$(\mathbb{R}, |\cdot|)$ $\mathbb{Q} \subseteq \mathbb{R}$ 稠密

$\mathbb{Q} \hookrightarrow$ 拓扑 $\hookrightarrow$ 完备（所有 Cauchy 列均是收敛的）

实数的构造：$\mathbb{Q} \rightsquigarrow \mathbb{R}$

- 给定 $\mathbb{Q}$ 上一个"绝对值"
- 在 $\mathbb{Q}$ 中加入所有 $\mathbb{Q}$-值的 Cauchy 列 $(r \in \mathbb{Q} \quad (r, r, r, \cdots))$
- 作等价关系 $(x_n)_{n\in\mathbb{N}} \sim (y_n)_{n\in\mathbb{N}}$ 若 $|x_n - y_n| \to 0$ $(n \to +\infty)$
  $\mathbb{Q}$
- 求出等价关系的商 $\square/\sim = \mathbb{R}$

"绝对值"指：映射 $\varphi: \mathbb{Q} \to \mathbb{R}^+$ 满足：

- ✓① $\forall x \in \mathbb{Q}$ $\varphi(x) \geq 0$ 且 "=" iff $x=0$
- ✓② $\forall x, y \in \mathbb{Q}$ $\varphi(x)\varphi(y) = \varphi(xy)$
- ③a $\varphi(x+y) \leq \varphi(x) + \varphi(y)$ 三角不等式

$\Downarrow$

$(\mathbb{Q}, |\cdot|_{\mathbb{R}})$

- ✓③ $\exists C > 0$ 常数，使 $\varphi(x+y) \leq C \max(\varphi(x), \varphi(y))$

Q. $\mathbb{Q}$ 上有其它非平凡的绝对值吗？ $\varphi(x) = \begin{cases} 1 & x \neq 0 \\ 0 & x = 0 \end{cases}$

Rk. ③作定义的好处：若 $|\cdot|$ 是满足①②③的，$\forall \alpha \in \mathbb{R}^+$ $|\cdot|^\alpha$ 也满足①②③

C $|z|$ $|z|^2 = z\bar{z}$

取定素数 $p \in \mathbb{Z}$

取定素数 $p\in\mathbb{Z}$

$\forall\, 0\neq x\in\mathbb{Z}$ 定义 $v_p(x)$ = 整除 x 的最大的 p 的幂次

即 $0\neq x\in\mathbb{Z}$ $\quad x=p^{\alpha}\cdot p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s}$ $\quad p, p_i$ 互异素数

$v_p(x)=\alpha$ $\quad$ p-adic 赋值 (p-进)

$p^{\alpha}\mid x$ 但 $p^{\alpha+1}\nmid x$

约定 $\quad x=0 \quad v_p(x)=+\infty \quad p^{\infty}\mid 0$

p-adic 绝对值 $\quad |\cdot|_p:\mathbb{Z}\longrightarrow\mathbb{R}^+$

$$x\longmapsto \left(\frac{1}{p}\right)^{v_p(x)}$$

$$0\longmapsto 0$$

超距三角不等式.

exer 验证这是 $\mathbb{Z}$ 上一个绝对值 (3b): $|x+y|_p\le\max(|x|_p,|y|_p)$

$\Rightarrow$ (3)

exer 满足 (3b) 时，所有三角形均是等腰三角形.

很容易扩展到 $\mathbb{Q}$ 上：

$\forall\, x=\frac{m}{n}\in\mathbb{Q}$ $\quad$ 定义 $v_p(x)=v_p\left(\frac{m}{n}\right)=v_p(m)-v_p(n)$

$m,n\in\mathbb{Z}$ $\quad$ 良定义. $\frac{m}{n}=\frac{m'}{n'}$

同理定义 $|\cdot|_p$ $\quad \left|\frac{m}{n}\right|_p=\frac{|m|_p}{|n|_p}$.

$\longrightarrow$ $\mathbb{Q}$ 上绝对值 $|\cdot|_p$

$\mathbb{Q}\xrightarrow[\text{完备化}]{|\cdot|_p}\mathbb{Q}_p$ 域，完备

$\cup \qquad \cup \qquad \mathbb{Q}\subseteq\mathbb{Q}_p$ 稠密.

$\mathbb{Z}\xrightarrow[\text{完备化}]{|\cdot|_p}\mathbb{Z}_p$

交换代数：$\mathbb{Z}_p$ 是 PID, UFD

唯一极大理想 $p\mathbb{Z}_p=m_p$.

素理想 $0,\ p\mathbb{Z}_p$

$I\subset\mathbb{Z}_p$ ideal $\quad I=p^n\mathbb{Z}_p$.

$\mathbb{Z}_p=\{x\in\mathbb{Q}_p \mid |x|_p\le 1\}$ "单位球"

$\mathbb{Z}_p^{\times}=\{x\in\mathbb{Q}_p \mid |x|_p=1\}$ "单位球面"

$\mathbb{Q}_p$: p-adic 数域 (拓扑域)

局部紧: 0 的邻域 $\mathbb{Z}_p$ 是紧的.

$\mathbb{Z}_p$ 局部环 $\qquad \mathbb{Q}_p$ 我们 局部域 $\qquad$ "完备-离散"

$\mathbb{Z}_p$ 局部环. $\mathbb{Q}_p$ 称作局部域 "局部-整体"

$\mathbb{Q}$: 整体域 $\mathbb{Q} \sim \mathbb{Q}_p$ 之间的关系

例. $p=3$

	通俗绝对值	$v_p(\cdot)$	$\lvert\cdot\rvert_p$	
大	$n_1 = 36 = 3^2 \cdot 2^2$	$v_p(n_1)=2$	$\lvert n_1\rvert_p = \frac{1}{9}$	中
中	$n_2 = 27 = 3^3$	$v_p(n_2)=3$	$\lvert n_2\rvert_p = \frac{1}{27}$	小
小	$n_3 = 3 = 3^1$	$v_p(n_3)=1$	$\lvert n_3\rvert_p = \frac{1}{3}$	大

即 $|\cdot| = |\cdot|_\infty$ 与 $|\cdot|_p$ 之间绝不相同

通俗的

$p \neq q$ $|\cdot|_p$ 与 $|\cdot|_q$ 也绝不相同. $p^n \xrightarrow[|\cdot|_p]{n\to+\infty} 0$

$$|p^n|_q \equiv 1 \not\to 0. \quad (q \neq p)$$

Def 称两个绝对值等价. 若 $\exists\, C>0$ 使

$$\frac{1}{C}\|x\| < |x| < C\|x\| \quad \text{对任何 } x \text{ 成立.}$$

(即给出相同的拓扑)

Th (Ostrowski) $\mathbb{Q}$ 上任何一个非平凡的绝对值必等价于 $|\cdot|_p$ 或 $|\cdot|_\infty$ 之一

(⚠ 记法 从现在起 $\Omega_{\mathbb{Q}} = \{\text{素数}\} \cup \{\infty\}$ $v \in \Omega_{\mathbb{Q}}$ $v = p$ 或 $v = \infty$)

$\mathbb{Q}_p$ $\mathbb{R}$ 是所有可能的 $\mathbb{Q}$ 的完备化. $\mathbb{Q}_\infty = \mathbb{R}$

$\mathbb{R} \rightsquigarrow$ 可作经典的数学分析. ($\lim$)

$\mathbb{Q}_p \rightsquigarrow$ p-adic 分析.

解决 $\longrightarrow$ 可以利用分析工具

例. $x^2+y^2=-1$ 在 $\mathbb{Q}$ 中有无解? 无!

在 $\mathbb{R}$ 中已经无解 (用到了 $\mathbb{R}$ 上分析学)

$\mathbb{Q}$ 上有解 $\Rightarrow$ $\begin{cases} \mathbb{R} \text{ 上} \\ \mathbb{Q}_p \text{ 上} \end{cases}$ 均有解

$\mathbb{Q}$ 上无解. $\Leftarrow$ $\begin{cases} \mathbb{R} \\ \mathbb{Q}_n \end{cases}$ 上无解

$\mathbb{Q}$ 上无解 $\Leftarrow$ $\begin{cases}\mathbb{R} \\ \mathbb{Q}_p\end{cases}$ 上无解

$|\cdot|$ 绝对值 $\Rightarrow$ $|\cdot|^{\alpha}$ ($\alpha \in \mathbb{R}^+$) 也是绝对值

$|x|_p = \left(\frac{1}{p}\right)^{v_p(x)}$ ← 换底.

取定 $\frac{1}{p}$ 为底 是个约定
可任取 $(0,1)$ → 如左上

Th (product formula) $\forall x \in \mathbb{Q}$, $x \neq 0$

$$\prod_{v \in \Omega} |x|_v = 1$$

Pf. 只需对 $x \in \mathbb{Z}$, $x \in \mathbb{N}$ 证明即可。 把 x 唯一分解 $x = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ 按定义算 #

以上分析角度

代数角度: $\mathbb{Z}_p := \varprojlim_n \mathbb{Z}/p^n\mathbb{Z} \subset \prod_{n=1}^{+\infty} \mathbb{Z}/p^n\mathbb{Z}$
逆极限

其中 $\varprojlim_n \mathbb{Z}/p^n\mathbb{Z} = \left\{ (a_n)_{n \geq 1} \in \prod_{n=1}^{+\infty} \mathbb{Z}/p^n\mathbb{Z} \;\middle|\; a_n \equiv a_{n+1} \bmod p^n \right\}$

然后定义 $\mathbb{Q}_p = \mathrm{Frac}(\mathbb{Z}_p)$

exer 试证明以上分析方法与代数方法定义的 $\mathbb{Z}_p$, $\mathbb{Q}_p$ 是一样的.
(提示: $x, y \in \mathbb{Z}$ $x \equiv y \bmod p^n$ n 越大 表明 $|x-y|_p$ 越小, 两者越近)

$\mathbb{Z}_p$ 上 ($\mathbb{Q}_p$ 上) 的 p-adic 分析 $\xleftrightarrow{\text{转化为}}$ $\bmod p^n$ ($n \in \mathbb{N}$) 初等数论.

求一个方程的 $\mathbb{Z}_p$ 解 ($\mathbb{Q}_p$ 解) $\longleftrightarrow$ $\bmod p^n$ 求解.

以下引理说明: 绝大部分情况下, $\bmod p$ 求解即足够

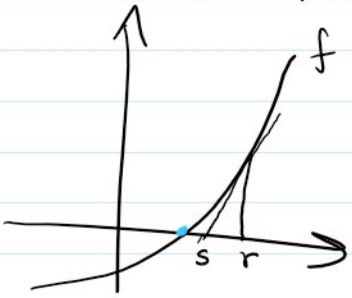
Lemma (Hensel) $f(x) \in \mathbb{Z}[x]$ $k \in \mathbb{N}$, $k \geq 1$, $r \in \mathbb{Z}$ 使

$|f(r)|_p \leq \frac{1}{p^k}$ (即 $f(r) \equiv 0 \bmod p^k$)

若(*) $|f'(r)|_p = 1$ (即 $f'(r)\not\equiv 0 \mod p$)

那么 ∃ $s\in\mathbb{Z}$ 使
$$\begin{cases} |f(s)|_p \le \frac{1}{p^{k+1}} & (\text{即 } f(s)\equiv 0 \mod p^{k+1}) \\ |s-r|_p \le \frac{1}{p^k} & (\text{即 } s\equiv r \mod p^k) \end{cases}$$

"Pf" 分析角度: Newton 迭代法 (数值分析?)



Rk. 初等数论角度: 存在 mod p^k 解 r $\overset{(*)}{\Longrightarrow}$ 存在 mod p^{k+1} 解 s #

且 $r\equiv s \mod p^k$ (正是 $\mathbb{Z}_p$ 定义中要求的) $\mathbb{Z}_p = \varprojlim \cdots$

换言之 ∃ mod p 解 (在 $\mathbb{F}_p$ 中) ⟹ ∃ $\mathbb{Z}_p$ 解. ($\mathbb{Q}_p$ 解)

Rk (*) 条件: f (mod p) 的根 r 不是 f' (mod p) 的根

即 r 不是 f mod p 的重根. 几何语言: f mod p 定义的几何对象(代数簇) 是光滑的.

一般的 Hensel 引理:

假设代数簇 X mod p 是光滑的, 若 X 在 $\mathbb{F}_p$ 中有有理点, 则 X 有 $\mathbb{Z}_p$ (或 $\mathbb{Q}_p$) 有理点

※ 椭圆曲线 mod p 有好的约化时, 它的局部性质就会相对简单.
good reduction

例. $f(x)=x^2-17$

它在 $\mathbb{Q}_{13}$ 中有解: 因为 $x^2-17\equiv 0 \pmod{13}$ 解 $x=\pm 2$.

$f'=2\underset{\pm 2}{x} \mod 13$ (*) ✓.

exer $f(x)=(x^2-13)(x^2-17)(x^2-13\times 17)$ 6次

求证 f 在 所有 $\mathbb{Q}_p$ 及 $\mathbb{R}=\mathbb{Q}_\infty$ 中有解 但在 $\mathbb{Q}$ 中无解

Exer $f(x)=(x^2-13)(x^2-17)(x^2-13\times17)$ 6次

求证 f 在所有 $\mathbb{Q}_p$ 及 $\mathbb{R}=\mathbb{Q}_\infty$ 中有解，但在 $\mathbb{Q}$ 中无解.

记有6次齐次式：$F(x,y)=(x^2-13y^2)(x^2-17y^2)(x^2-13\times17y^2)$

在 $\mathbb{Q}_p$ 中恒为0解，在 $\mathbb{Q}$ 中只恒为0解.

Th (Hasse-Minkowski) K 数域，$F\in K[x_1,\cdots,x_n]$ 二次齐次多项式.

(即二次型 $F=X^tMX$ M 对称矩阵 $\in M_n(K)$，$X=\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix}\in K^n$)

则 F 在 K 上有非0解 $\Longleftrightarrow$ F 在 K_v ($\forall v\in S_K$) 中有非零解.

$K=\mathbb{Q}$ 时 $S_K=\{\mathbb{Q}_p,\mathbb{Q}_\infty\}$

称之为二次型满足 局部-整体原则 或 Hasse原则.

Rk. 其实，三次型已有反例：

Selmer： $K=\mathbb{Q}$. $F(x,y,z)=3x^3+4y^3+5z^3$ (*)

在 $\mathbb{Q}_p$ 及 $\mathbb{R}$ 均有解，但在 $\mathbb{Q}$ 中无解.

(*) 定义了 $\mathbb{P}^2$ 中一条光滑射影曲线，亏格为1，"人手"是一条椭圆曲线；它是椭圆曲线的一个主齐次空间，可看成是 Tate-Shafarevich 群中的一个典型类.

二. 椭圆曲线

1. 射影空间

只关心 $\mathbb{P}^2$ 中的 射影曲线 由一个3元齐次多项式所定义的，次数为 d 称作曲线的次数.

Def 若 $C\subset\mathbb{P}^2$ 为 光滑 射影曲线，次数为 d.

则称 $g(C)=\frac{1}{2}(d-1)(d-2)\in\mathbb{Z}$ 为 C 的亏格 genus.

例 光滑二次曲线（圆锥曲线） $g=0$

光滑三次曲线 $d=3\Rightarrow g=1$. 例 $F(x,y,z)=3x^3+4y^3+5z^3=0$

Rk. 亏格有一个"内蕴"，利用上同调和维数

Rk. 只够有一个"内蕴"，利用上同调的维数.

$F \in k[X,Y,Z]$ 齐次多项式 定义了曲线 $C \subset \mathbb{P}^2$.

$\mathbb{P}^2 = \underset{(Z\neq 0)}{\mathbb{A}^2} \sqcup \mathbb{P}^1$ 取 $Z=1$ 记 $x=\frac{X}{Z}$, $y=\frac{Y}{Z}$.

$F(X,Y,Z)$ 在 $\mathbb{A}^2$ 定义的 $\mathbb{A}^2 \cap C$ 的方程为 $= F(x,y,1)=0$

$f(x,y) \in k[x,y]$ ↳ 不必齐次

$d=3$

例. $F(X,Y,Z)=3X^3+4Y^3+5Z^3=0$: C

$\underset{(Z\neq 0)}{C\cap\mathbb{A}^2}$ $3\left(\frac{X}{Z}\right)^3+4\left(\frac{Y}{Z}\right)^3+5=0$

$f(x,y)=3x^3+4y^3+5=0$

即 $f(x,y)$ 定义了 $C\cap\mathbb{A}^2 \subseteq \mathbb{A}^2$ 是 C 的一个仿射部分

相对 $\mathbb{A}^2$ 的无穷远处 还有一些 C 上的点 $C\setminus\mathbb{A}^2$ $(Z=0)$
$\overset{\shortparallel}{C\cap\mathbb{P}^1}$

即 $3X^3+4Y^3=0$ 的解 $(X:Y)$

f : F 的去齐次化

F : f 的齐次化 (把 $x \rightsquigarrow \frac{X}{Z}$, $y \rightsquigarrow \frac{Y}{Z}$)

若考虑开覆盖 $\mathbb{P}^2 = \underset{(X\neq 0)}{\mathbb{A}^2} \cup \underset{(Y\neq 0)}{\mathbb{A}^2} \cup \underset{(Z\neq 0)}{\mathbb{A}^2}$

$C \subseteq \mathbb{P}^2$ $C_1=\mathbb{A}^2\cap C$ $C_2=\mathbb{A}^2\cap C$ $C_3=\mathbb{A}^2\cap C$

C_1, C_2, C_3 粘合成 C.

例. 抛物线 $f(x,y)=y-x^2=0$ $y=x^2$

无穷远处只有一个点

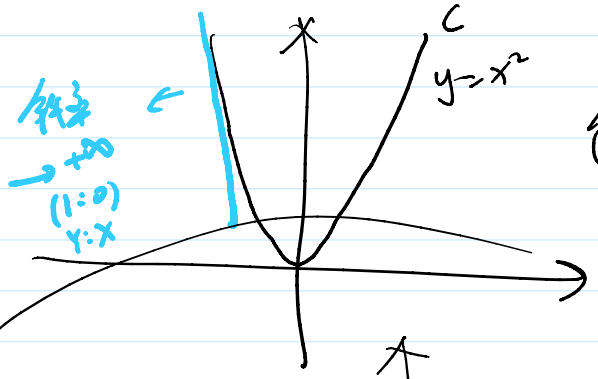
$y \rightsquigarrow \frac{Y}{Z}$ $\frac{Y}{Z}-\left(\frac{X}{Z}\right)^2=0$

$x \rightsquigarrow \frac{X}{Z}$ 即 $F(X,Y,Z)=YZ-X^2=0$

$x \rightsquigarrow \infty$　　$F(X,Y,Z) = YZ - X^2 = 0$

$Z=0 \Rightarrow (0:1:0)$ 是在 ∞ 处唯一的点.

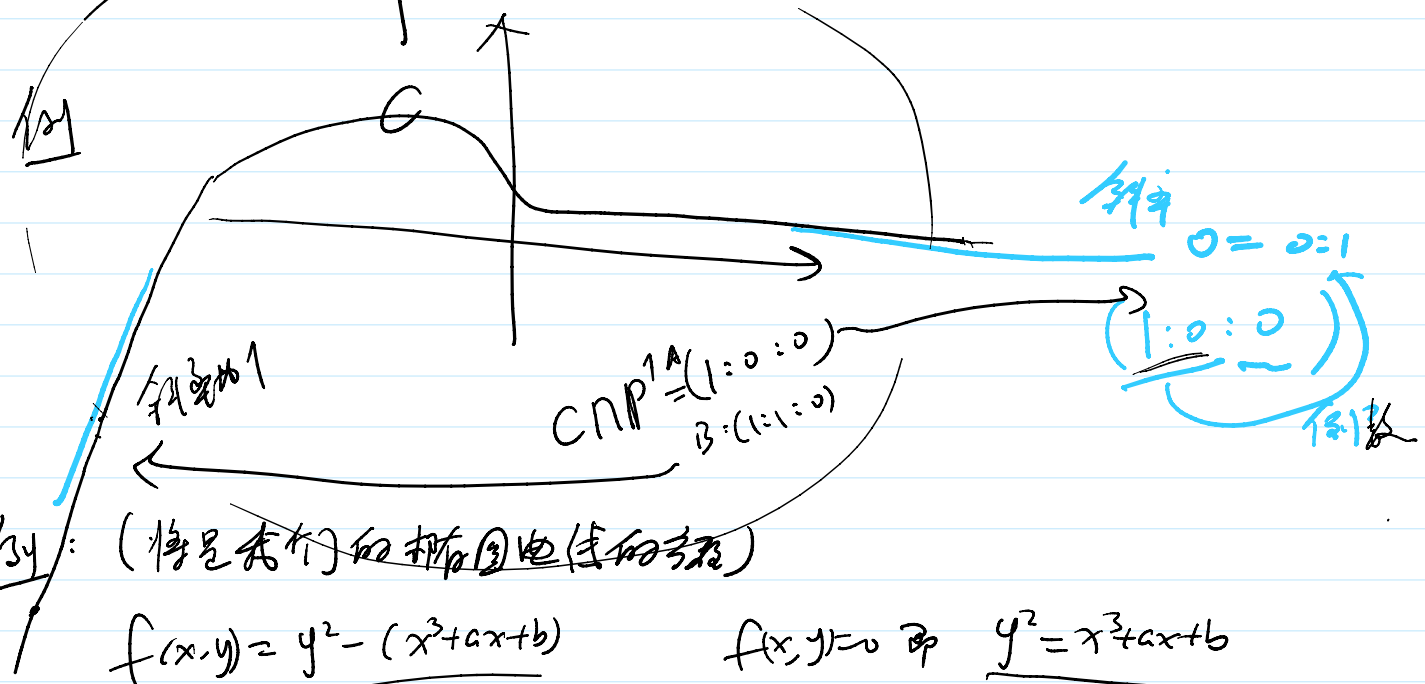
∞ 也是处于 $Z=0$



斜率 $\to +\infty$ $(1:0)$ $Y:X$

A^2 $(Z\neq 0)$

例



例：（特殊点的椭圆曲线的方程）

$f(x,y) = y^2 - (x^3+ax+b)$　　$f(x,y)=0$ 即 $y^2 = x^3+ax+b$

$\lambda=3$　　仿射曲线 $C\cap A^2$

齐次化：$F(X,Y,Z) = Y^2Z - (X^3+aXZ^2+bZ^3) = 0$

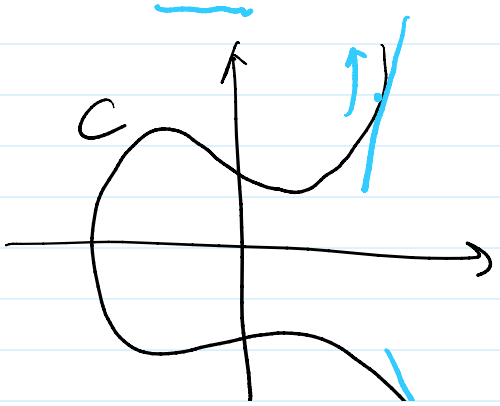
$C: Y^2Z = X^3+aXZ^2+bZ^3$

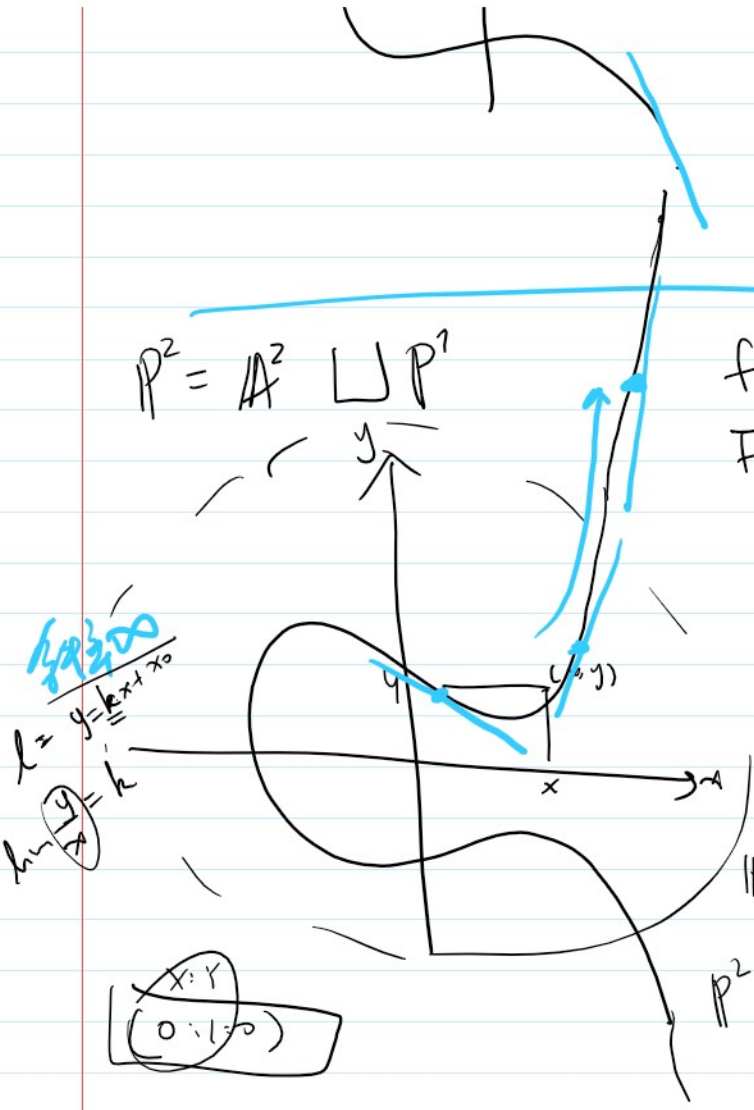
P^2：∞ "边界" 上的点：取 $Z=0 \Rightarrow X=0$

$(X:Y:Z)$ 不全为0，又有 $Y\neq 0$.

$Y=1$

$(0:1:0)$ 是 C 在无穷远处唯一的一个点





$\mathbb{P}^2 = \mathbb{A}^2 \sqcup \mathbb{P}^1$

$f(x,y)=0 \quad C \cap \mathbb{A}^2$

$F(X,Y,Z)=0 \quad C \subseteq \mathbb{P}^2$

$d=3$

$y^2 = x^3 + ax + b$

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

$X^3=0$ 且 $Z=0$

$\mathbb{A}^2: \ Z \neq 0$

$\mathbb{P}^1: \ Z=0$

$\mathbb{P}^2 \ (X:Y:Z) \begin{cases} Z \neq 0 \\ Z=0 \end{cases}$

$\frac{X}{Z} = x, \ \frac{Y}{Z} = y$

$(x,y) \in \mathbb{A}^2$

$\left(\frac{X}{Z} : \frac{Y}{Z} : 1\right)$

$(X:Y) \leftrightarrow \mathbb{P}^1$

$\lambda \to \infty$

$l: y = kx + x_0$

$k = \frac{y}{x} = k$

$(X:Y)$

$(0:1:0)$

下周一 office hour: 9:30 - 11:00