• Points of order 2

$y^2 = f(x) = x^3 + ax^2 + bx + c$ $\quad O = (0:1:0)$

$2P = O \iff P = -P$, $\quad (x,y) = P \Rightarrow -P = (x,-y) = P \iff y = 0$ $\quad f(x) = 0$.

$\Rightarrow P_i = (\alpha_i, 0) \in E(\bar{K})$ and $\alpha_1 + \alpha_2 = \alpha_3$ as $\Delta \neq 0$.

Might happen: a) over $\mathbb{C}$: 3 affine points, 4 proj

b) over $\mathbb{R}$: 1 affine / 3 affine

2 proj / 4 proj.

c) over $\mathbb{Q}$: 0 affine / 1 affine / 3 affine

1 proj / 2 proj / 4 proj.

↳ same over $\mathbb{F}_q$

over $\overline{\mathbb{F}_q}$ $(q,2) = 1$: 4 proj.

over $\mathbb{F}_2$: $0, 2$ (not in book)

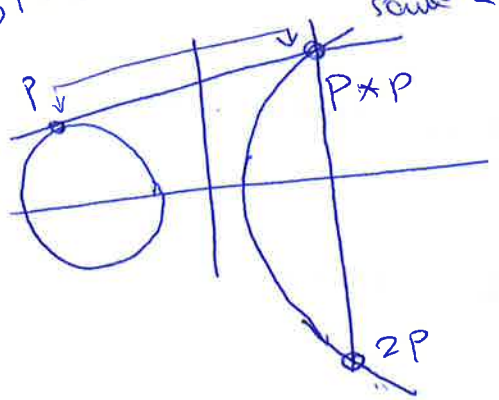
↑ no Weierstrass.

$\Rightarrow E[2](K) = \{O\}, C_2, V$ $\quad V = C_2 \oplus C_2$

• Points of order 3

$3P = O \iff 2P = -P \Rightarrow x(2P) = x(-P) = x(P)$

same $\iff T_P C$ cuts C at P with mult 3 $\iff P$ inflection



$\times 1 \quad \dfrac{x^4 - 2bx^3 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c} = x$

$\iff \dfrac{3x^4 + 4ax^3 + 6bx^2 + 12cx + (4ac - b^2)}{4(x^3 + 4ax^2 + 4bx + 4c)} = 0$

$\psi_3(x)$

(3)

$E[3](\bar{K}) = C_3 \oplus C_3$.

Must check : $\psi_3(x)$ has 9 distinct roots over $\bar{K}$.

$\psi_3'(x) = 12 f(x)$ ← check.

$\psi_3(x_0) = 0$, $\psi_3'(x_0) = f(x_0) = 0$ $\Rightarrow$ $f(x_0) = 0$!!

$\Rightarrow$ φ $f(x_0) \neq 0$

$\psi_3(x) = 2f(x)f''(x) - f'(x)^2$ ← check.

Now: β_i roots of $\psi_3(x)$ in $\bar{K}$. $\delta_i^2 = \beta_i$

$\Rightarrow$ $\{(\beta_i, \pm\delta_i)\}$ affine 3-torsion. $\delta_i \neq 0$ (otherwise order 2).

$\Rightarrow$ 8 points of order 3

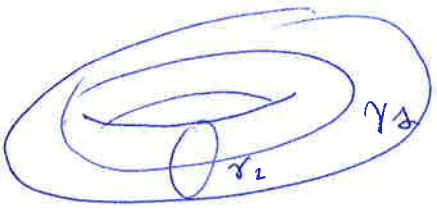
There exist a unique abelian group G of order 9 s.t $\forall g \in G$, $\mathrm{ord}(g) = 3$ $g \neq e$.

- Complex points

$E : y^2 = f(x) = x^3 + ax^2 + bx + c$

$\{\infty\} \subseteq E(\mathbb{Q}) \subseteq E(\mathbb{R}) \subseteq E(\mathbb{C})$

$x \leftrightarrow x - \frac{1}{3}a$: $y^2 = 4x^3 - g_2 x - g_3$.



$\omega_E = \dfrac{dz}{\sqrt{f(z)}}$ $\omega_i = \int_{\gamma_i} \omega_E$ $L = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$.

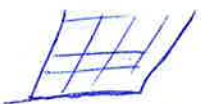
$\Rightarrow g_2 = 60 \sum_{\omega \in L^*} \frac{1}{\omega^4}$, $g_3 = 140 \sum_{\omega \in L^*} \frac{1}{\omega^6}$.

$\wp_E = \frac{1}{u^2} + \sum_{\omega \in L^*} \frac{1}{(u-\omega)^2} - \frac{1}{\omega^2}$, $\wp, \wp'$ doubly periodic

$\mathbb{C} \xrightarrow{\text{exp}} E(\mathbb{C})$

$z \longmapsto (\wp(z), \wp'(z))$

$\mathbb{C}/L \to E(\mathbb{C})$



$E[m](\mathbb{C}) \simeq C_m \oplus C_m$.

• Points of finite order / $\mathbb{Q}$.

$D = \Delta_E = \prod_{i \neq j} (\alpha_i - \alpha_j)^2 \neq 0.$

Thm (Lutz, Nagel). $E/\mathbb{Q}$ an elliptic curve ($\Leftrightarrow E/\mathbb{Z}$).
Let $(x,y) \in E[m](\mathbb{Q})$. Then $b)\ y=0$ and $m=2$ or $y \mid D$.

$a)\ (x,y) \in E[m](\mathbb{Z})$.

Lem: $D = r(x)f(x) + s(x)f'(x) = \mathrm{Res}(f(x), f'(x))$.

Lemme: Let $P = (x,y) \in E(\mathbb{Q})$ s.t. P and $2P \in E(\mathbb{Z}) \Rightarrow y=0$ or $y \mid D$.

(homw)