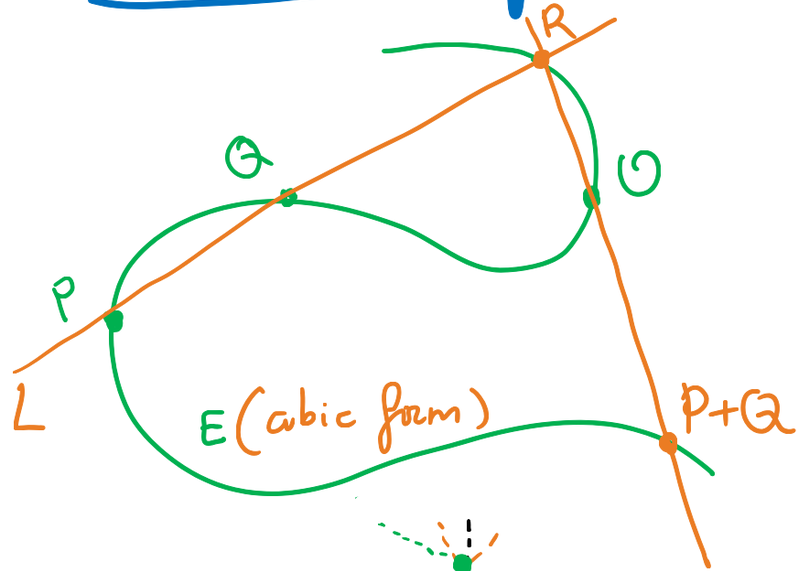
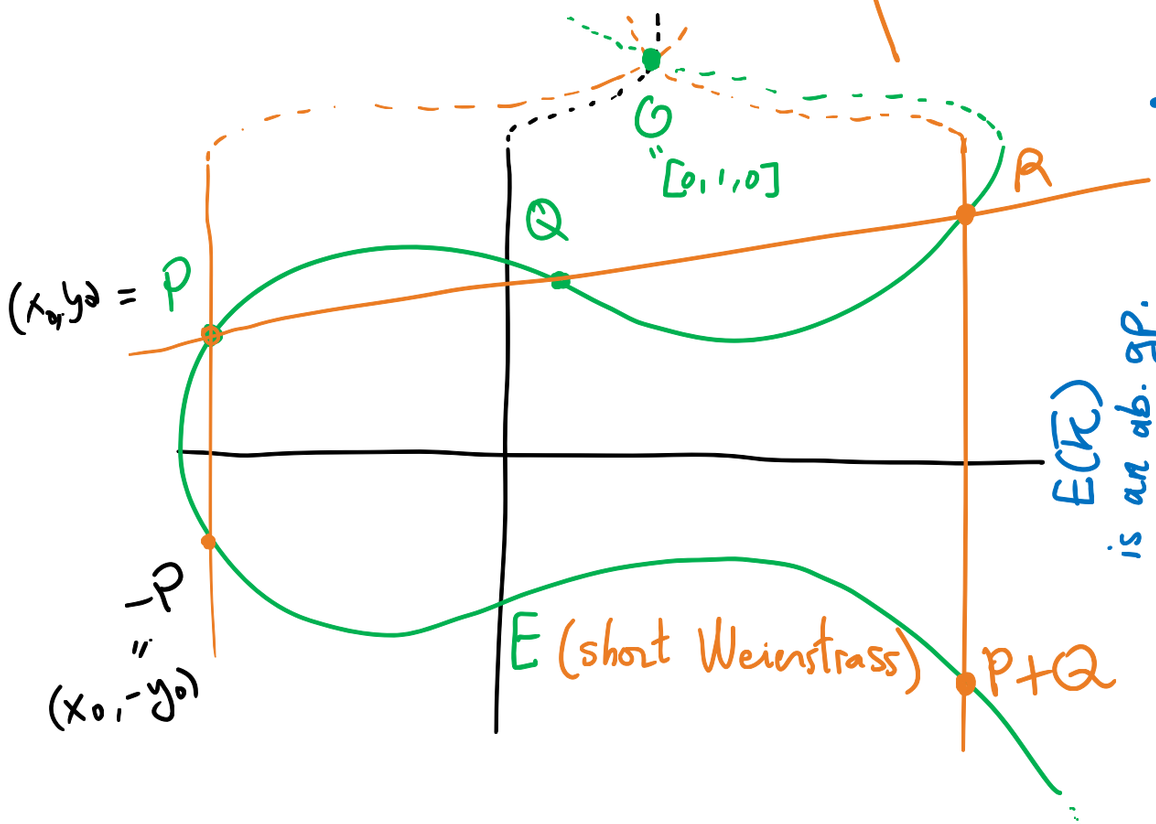
§2. The Group Law





L : line thru P, Q, and R

L′ : line thru R, O, and P+Q.

KEY: Tangent line at O in a Weier. model is $\{Z=0\}$ and it has a triple point of intersection at O. (exercise)

Prop.

(a) If O is an inflection pt, and if L intersects E on P, Q, R, then $(P+Q)+R = O$.

(b) $P+O = P$ for all $P \in E$.

(c) $P+Q = Q+P$ for all $P, Q \in E$.

(d) $\forall P \in E$, $\exists (-P) \in E$ st. $P+(-P) = O$.

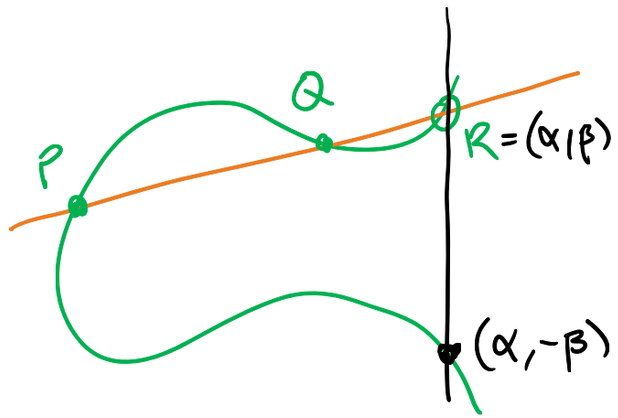
(e) $(P+Q)+R = P+(Q+R)$ $\forall P,Q,R \in E$

(f) $(E(K),+)$ is a subgp of $(E(\bar{K}),+)$.

(8) $(E(k),+) \underset{\text{subgp}}{\subseteq} (E(\bar{k}),+)$

$E: y^2 = x^3 + Ax + B \ /k$, $A, B \in k$, $P, Q \in E(k)$ ($P=(c,d)$, $Q=(e,g)$)

Q: $R \overset{?}{\in} E(k)$.



L: line thru $P, Q/k$: $y = ax + b$, $a, b \in k$

$$\begin{cases} y^2 = x^3 + Ax + B \\ y = ax + b \end{cases} \Rightarrow (ax+b)^2 = x^3 + Ax + B \quad (g(x))$$

$$\Rightarrow x^3 - (ax+b)^2 + Ax + B = 0$$

cubic poly /k and $x = c$, $x = e$ are roots!

$$\Rightarrow (x-c)(x-e) \mid x^3 \ldots = 0$$

$$\Rightarrow g(x) = (x-c)(x-e)(x-\alpha)$$

and $\alpha \in k$, $\beta = a\alpha + b \in k$

$\Rightarrow R \in E(k)$ ▨

In fact: $k \subseteq L \underset{\text{subfield}}{\subseteq} \bar{k}$

then $(E(L),+)$ is also a subgp of E.

Group law algorithm:

$E: \quad y^2 = x^3 + a_4 x + a_6 \qquad (a_1 = a_2 = a_3 = 0)$

$\Rightarrow b_2 = 4a_4, \; b_4 = 2a_4, \; b_6 = 4a_6, \; b_8 = -a_4^2$

(a) $P = (x, y)$ then $-P = (x, -y)$

(b) If $P_2 \neq \pm P_1$, then $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$

then $$x(P_1 + P_2) = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2 .$$

If $$x([2]P) = \frac{x^4 - b_4 x^2 - 2b_6 x - b_8}{4x^3 + b_2 x^2 + 2b_4 x + b_6} .$$

ex $y^2 + y = x^3 - 7x + 6$ "the Gauss elliptic curve", 5077a1.

$P = (-2, 3)$, $Q = (-1, 3)$, $R = (0, 2)$

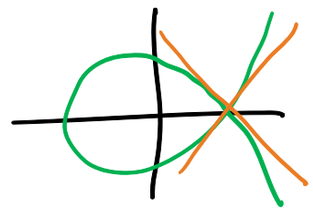
$P + Q = (3, -4)$, $P + R = \left(\frac{9}{4}, -\frac{15}{8}\right)$, $Q + R = (2, -1)$ ...

PROP 2.5

Let E be a curve given by a Weierstrass eq'n with $\Delta = 0$, so that E has a singular pt S, and let

$$E_{ns} = \{\text{non-sing. pts of } E\} \qquad E_{ns} = E_{ns}(\bar{K})$$

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



(a) Suppose E has a node ($c_4 \neq 0$), and let

$y = \alpha_1 x + \beta_1$, $y = \alpha_2 x + \beta_2$ be the two tangent lines at S.

$y^2 = x^3 + Ax + B$ / $\mathbb{Q}$
$A, B \in \mathbb{Z}$
↓ mod p
$y^2 = x^3 + Ax + B$ / $\mathbb{F}_p$
p prime
may be singular!

Then:

$$E_{ns} \longrightarrow \bar{K}^*$$

$$(x,y) \longmapsto \frac{y - \alpha_1 x - \beta_1}{y - \alpha_2 x - \beta_2}$$

is an isom. of ab. gps.

multiplicative red'n.

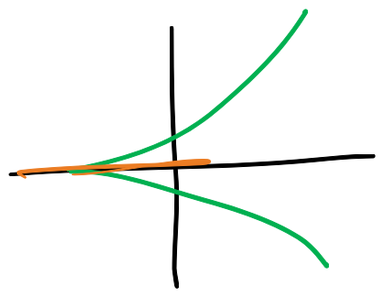
(b) E has a cusp, $y = \alpha x + \beta$ be the tangent at S.

$$E_{ns} \longrightarrow (\bar{K}^+, +)$$

$$(x,y) \longmapsto \frac{x - x(S)}{y - \alpha x - \beta}$$

is an isom of ab gps.

additive reduction.



Exercise: #3.5, this can be done over K $\quad E_{ns}(K) \cong K^*$ or K^+

Group Law and the Picard Group

Lemma 3.3. Let C be a curve of genus 1, and let $P, Q \in C$.
Then $(P) \sim (Q) \iff P = Q$.

Pf $(P) \sim (Q) \iff \exists\, f \in \overline{K}(C)$ s.t. $\operatorname{div}(f) = (P) - (Q)$.

$\Rightarrow f \in \mathcal{L}((Q))$ and $RR \to \dim \mathcal{L}((Q)) = 1$ and $\overline{K} \subseteq \mathcal{L}((Q))$ (eq!)

$\Rightarrow f \in \overline{K}$, $\operatorname{div}(f) = 0 = (P) - (Q) \Rightarrow (P) = (Q) \Rightarrow P = Q$ ▨

Prop 3.4. Let $(E, \mathcal{O})$ be an ell. curve.

(a) $\forall D \in \operatorname{Div}^0(E)$, $\exists!\, P \in E$ s.t. $D \sim (P) - (\mathcal{O})$. Define $\sigma : \operatorname{Div}^0(E) \to E$, $D \mapsto P$.

(b) σ is surjective.

(c) $D_1, D_2 \in \operatorname{Div}^0(E)$ then $\sigma(D_1) = \sigma(D_2) \iff D_1 \sim D_2$.

In other words: $\sigma : \operatorname{Pic}^0(E) \leftrightarrow E$ is a bijection of sets.

(d) With inverse $\kappa : E \xrightarrow{\sim} \operatorname{Pic}^0(E)$, $P \mapsto \kappa(P) = [(P) - (\mathcal{O})]$

(e) The (geometric) gp law on E coincides w/ the (algebraic) gp law on $\operatorname{Pic}^0(E)$.

Proof. Let $D \in \mathrm{Div}^0(E)$, recall RR $\Rightarrow \mathcal{L}(D) = \deg D$ if $\deg D > 0$.

(a) $\left(\forall D \ \exists! P \in E \text{ s.t. } D \sim (P) - (O).\right)$ NOTE: $D = 0$, pick $P = O$.

$\dim_{\bar{k}} \mathcal{L}(D + (O)) = \deg D + (O) = 1$, $D \neq 0$.

Let $f \in \bar{k}(E)$ be a gen. of $\mathcal{L}(D + (O))$.

Then since $\mathrm{div}(f) \geq \underbrace{-D - (O)}_{\deg = -1}$ and $\deg(\mathrm{div}(f)) = 0$

then $\underbrace{\mathrm{div}(f) - (-D - (O))}_{\deg 1} \geq 0 \Rightarrow \mathrm{div}(f) - (-D - (O)) = (P)$

$\Rightarrow \exists P \in E$ s.t. $\mathrm{div}(f) = -D - (O) + (P) \Rightarrow D \sim (P) - (O)$.

Uniqueness: If P' also $(P)' - (O) \sim D \sim (P) - (O)$ (Lemma 3.3)

$\Rightarrow (P) \sim D + (O) \sim (P') \Rightarrow (P) \sim (P') \Rightarrow P = P'$.

We define $\sigma : Div^0(E) \longrightarrow E$

$D \longmapsto P$

(b) σ is surjective: let $P \in E$, take $D = (P) - (O)$

then $(P) - (O) \sim (P) - (O)$

$\parallel$

$D \Longrightarrow \sigma\big((P) - (O)\big) = P.$ ✓

(c) σ is injective:

Let $P_i = \sigma(D_i)$, $i = 1, 2$. ~~Suppose $\sigma(D_1) = \sigma(D_2)$~~

s.t. $D_1 \sim (P_1) - (O)$, $D_2 \sim (P_2) - (O)$.

- If $P_1 = P_2 \Rightarrow D_1 \sim (P_1) - (O) = (P_2) - (O) \sim D_2 \Rightarrow D_1 \sim D_2$
- If $D_1 \sim D_2 \Rightarrow (P_1) - (O) \sim (P_2) - (O) \Rightarrow (P_1) \sim (P_2) \overset{\text{Lemma}}{\Longrightarrow} P_1 = P_2.$

so $\sigma(D_1) = \sigma(D_2) \Longleftrightarrow P_1 = P_2$. (d) Clear, inverse $K : E \to Pic^0(E)$, $P \mapsto (P) - (O)$.

(e) $\big(Div^0(E), +\big) \cong \big(E, +_{GEOM.}\big)$

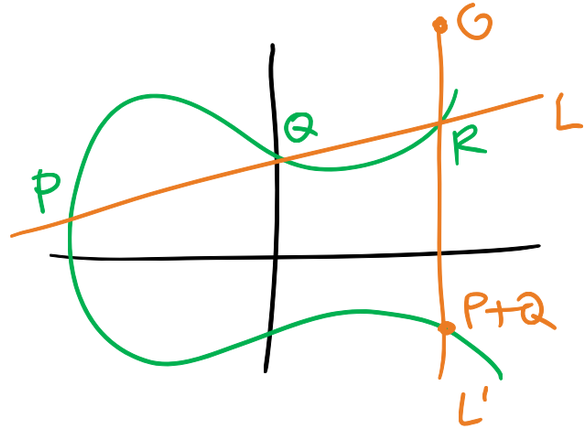
(e) $(\mathrm{Div}^0 E, +) \cong (E, +_{GEOM})$

Suffices to show $K(P +_G Q) = K(P) +_{Pic} K(Q)$

Pf. Let $L: f(X,Y,Z) = \alpha X + \beta Y + \gamma Z = 0$ line thru P, Q (R)

$L': f'(X,Y,Z) = \alpha' X + \beta' Y + \gamma' Z = 0$ line thru R, O. (and $P+Q$)

$L'': Z = 0$ (triple zero at O).



$$\mathrm{div}\left(\frac{f}{Z}\right) = (P) + (Q) + (R) - 3(O)$$

$$\mathrm{div}\left(f'/Z\right) = (R) + (O) + (P+_G Q) - 3(O)$$

$$= (R) + (P+_G Q) - 2(O)$$

Hence $(P+Q) - (P) - (Q) + (O) = \mathrm{div}(f'/f) \sim 0.$

$-(O)+(O)$

$$((P+Q)-(O)) - ((P)-(O)) - ((Q)-(O)) \sim 0$$

$$\Rightarrow \boxed{k(P+_G Q) - k(P) - k(Q) = 0}$$

$$K(P+_G Q) = K(P) +_{Pic} K(Q).$$

∎