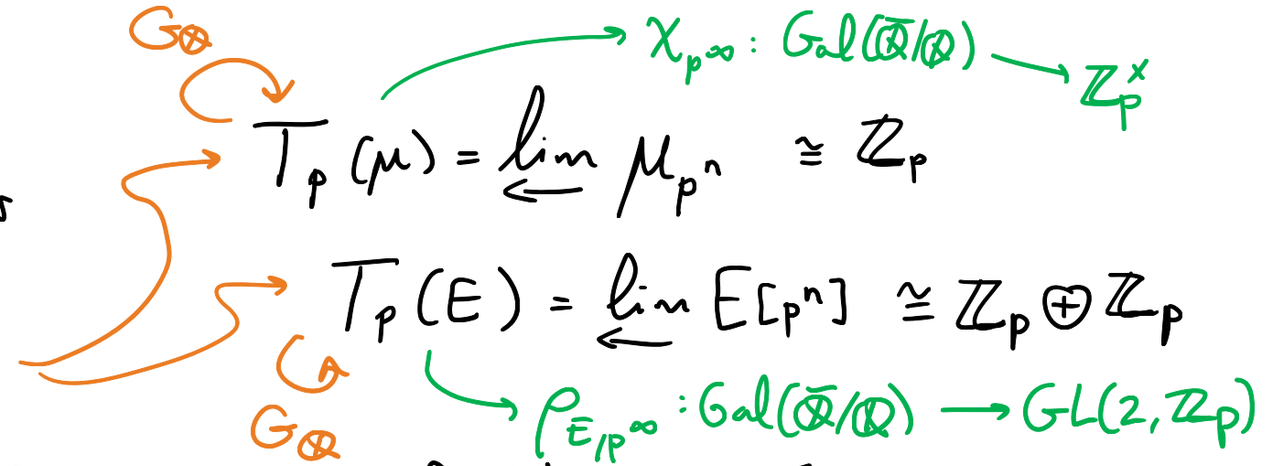
# PREVIOUSLY...

- Weierstrass models
- Isogenies
- The Tate module




**Theorem** Let $E/K$ be an elliptic curve, and let $m \geq 2$. There is a pairing

(The Weil pairing!) $e_m : E[m] \times E[m] \longrightarrow \mu_m$ $\left( (S,T) \longmapsto e_m(S,T) = \frac{g_T(X+S)}{g_T(X)} \right)$

s.t. $e_m$ is:

(a) Bilinear: $e_m(S_1+S_2, T) = e_m(S_1, T) \cdot e_m(S_2, T)$

$e_m(S, T_1+T_2) = e_m(S, T_1) \cdot e_m(S, T_2)$

(b) Alternating: $e_m(T,T) = 1$, $e_m(S,T) = e_m(T,S)^{-1}$.

(c) Non-degenerate: $e_m(S,T) = 1 \quad \forall S \in E[m] \Rightarrow T = 0$

(d) Galois-invariant: $\forall \sigma \in \mathrm{Gal}(\overline{K}/K) \quad e_m(S,T)^\sigma = e_m(S^\sigma, T^\sigma)$

(e) Compatible: if $S \in E[mm']$ and $T \in E[m]$, then

$e_{mm'}(S,T) = e_m([m']S, T)$

**Corollary** Let $K$ be a field, let $E/K$ be an ell. curve, and let $m \geq 2$. Define:

$$K(E[m]) = K\left(\{x(P), y(P)\} : P \in E[m]\right) \subseteq \overline{K}$$

the $m$-th "division field" or field of definition of $E[m]$.

(a) There are $S, T \in E[m]$ s.t. $e_m(S,T)$ is a primitive $m$-th root of unity.

(b) If $K(E[m]) \subseteq K$, then $\mu_m \subseteq K^*$. $\Rightarrow E(K) \supseteq E[m]$.

**Proof.**

(a) Consider $\{e_m(S,T) : S, T \in E[m]\} = \mu_d \subseteq \mu_m$ for some $d \mid m$. ($\mu_d$ is a subgroup of $\mu_m$)

(In general, $K(E[m])/K$ is an extension of degree $\#GL(2, \mathbb{Z}/m\mathbb{Z})$)

$\Rightarrow 1 = e_m(S,T)^d = e_m([d]S, T)$ (bilinearity) Fix $S$, this is true $\forall T \in E[m]$.

$\Rightarrow [d]S = O \quad \forall S$ but if $S$ is of exact order $m$ then $\Rightarrow d = m$.

∎

(b) If $K(E[m]) \subseteq K$ then $\mu_m \subseteq K^*$.

$$\forall \sigma \in G_{\bar{K}/K},\ e_m(S,T)^\sigma = e_m(S^\sigma, T^\sigma) = e_m(S,T) = \zeta$$

$e_m(S,T)^\sigma$: Gal inv

$e_m(S^\sigma, T^\sigma)$: $E[m] \subseteq E(K)$

then $\zeta^\sigma = \zeta$ for all $\sigma \in G_{\bar{K}/K}$ then $\sigma(S) = S$, $\sigma(T) = T$

If we pick $S, T$ so that $\zeta = \text{prim } m$