

# THE WEAK! MORDELL-WEIL THEOREM

Thm Let  $K$  be a number field, and  $m \geq 2$ , and  $E/K$  an ell. curve.

Then,  $E(K)/mE(K)$  is finite.

Lemma If  $K'/K$  is finite Galois, and  $E(K')/mE(K')$  is finite, then  $E(K)/mE(K)$  is finite.

**UPSHOT:** ASSUME  $E[m] \subseteq E(K)$ .

DEF. The Kummer Pairing  $\kappa : E(K) \times \text{Gal}(\bar{K}/K) \longrightarrow E[m]$   
 $(P, \sigma) \longmapsto \sigma^m P - P$   
where  $[m]Q = P$ .

DEF. The Kummer Pairing  $\kappa : E(K) \times \text{Gal}(\bar{K}/K) \rightarrow E[m]$   
 $(P, \sigma) \mapsto \sigma^m - P$   
 where  $[m]Q = P$ .

PROP (a)  $\kappa$  is well-defined. ✓

(b)  $\kappa$  is bilinear. ✓

(c) Kernel on the left is  $mE(K)$ .

(d) Kernel on the right is  $\text{Gal}(\bar{K}/L)$  where  $L = \kappa([m]^{-1}E(K))$

= composition of  $\kappa(Q)$   
 s.t.  $[m]Q \in E(K)$ .

Hence,  $\kappa$  induces a perfect bilinear pairing

$$E(K)/mE(K) \times \text{Gal}(L/K) \rightarrow E[m].$$

DEF.  $\varphi : A \times B \rightarrow C$  is perfect if  $A \xrightarrow{\varphi_A} \text{Hom}(B, C)$  and  $B \xrightarrow{\varphi_B} \text{Hom}(A, C)$  are injective.  
 $a \mapsto \varphi(a, \cdot)$   
 $b \mapsto \varphi(\cdot, b)$

↑ ↑ ↗  
 AB. GPS.

Proof (c) (Kernel on the left of  $K$  is  $mE(K)$ )

•  $P \in mE(K)$ ,  $P = [m]Q$ ,  $Q \in E(K)$

then  $K(P, \sigma) = Q^\sigma - Q = 0 \quad \forall \sigma \in \text{Gal}(\bar{K}/K) \Rightarrow P \in \text{Ker}.$

•  $P \in \text{Ker} \Rightarrow K(P, \sigma) = 0 \quad \forall \sigma$ . Let  $Q$  s.t.  $[m]Q = P$

$$\begin{aligned} & \text{"} \\ & Q^\sigma - Q \Rightarrow Q^\sigma = Q \quad \forall \sigma \Rightarrow Q \in E(K) \Rightarrow P \in mE(K). \end{aligned}$$

(d) (Kernel on the right  $\Rightarrow L = \text{comp. of } K(Q) \text{ for all } [m]Q \in E(K)$ ).  
 $\text{Gal}(\bar{K}/L)$  where)

•  $\sigma \in \text{Gal}(\bar{K}/L)$  then  $K(P, \sigma) = Q^\sigma - Q$  and  $Q \in E(L)$   
 $= 0 \quad \forall P \in E(K) \Rightarrow \sigma \in \text{Ker}.$

•  $\sigma \in \text{Gal}(\bar{K}/K)$  in kernel  $\Rightarrow K(P, \sigma) = 0 \quad \forall P \in E(K)$

$$\begin{aligned} & \text{"} \\ & Q^\sigma - Q \Rightarrow Q^\sigma = Q \quad \forall Q \text{ s.t. } [m]Q \in E(K) \\ & \Rightarrow \sigma \text{ fixes } K(Q) \\ & \Rightarrow \sigma \text{ fixes } L \Rightarrow \sigma \in \text{Gal}(\bar{K}/L) \end{aligned}$$

Then:  $\kappa : \frac{E(k)}{mE(k)} \times \frac{\text{Gal}(\bar{k}/k)}{\text{Gal}(\bar{k}/L)} \longrightarrow E[m]$

is perfect!

$\cong$   
 $\text{Gal}(L/k)$

•  $\varphi : \frac{E(k)}{mE(k)} \longrightarrow \text{Hom}(\text{Gal}(L/k), E[m])$

$\rho \longmapsto \kappa(\rho, \cdot)$  is injective!

















