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 $\kappa : E(K) \times \mathrm{Gal}(\overline{K}/K) \longrightarrow E[m]$

$$(P, \sigma) \longmapsto Q^\sigma - Q$$

where $[m]Q = P$.

DEF. The Kummer Pairing $\kappa : E(K) \times \mathrm{Gal}(\bar{K}/K) \longrightarrow E[m]$

$$(P, \sigma) \longmapsto Q^{\sigma} - Q$$

where $[m]Q = P$.

PROP (a) κ is well-defined. ✓

(b) κ is bilinear. ✓

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

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

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

Hence, κ induces a perfect bilinear pairing

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

DEF. $\varphi : A \times B \to C$ is perfect if $A \xrightarrow{\varphi_A} \mathrm{Hom}(B, C)$ are injective.

AB. GPS.

$a \longmapsto \varphi(a, \cdot)$

$B \xrightarrow{\varphi_B} \mathrm{Hom}(A, C)$

$b \longmapsto \varphi(\cdot, b)$

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

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

  then $K(P,\sigma) = Q^\sigma - Q = \mathcal{O} \quad \forall \sigma \in Gal(\bar{k}/k) \Rightarrow P \in \ker$.

- $P \in \ker \Rightarrow K(P,\sigma) = \mathcal{O} \quad \forall \sigma$. Let Q s.t. $[m]Q = P$

  $K(P,\sigma) = Q^\sigma - Q \Rightarrow Q^\sigma = Q \quad \forall \sigma \rightarrow Q \in E(K) \rightarrow P \in mE(k)$. ▨

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

- $\sigma \in Gal(\bar{K}/L)$ then $K(P,\sigma) = Q^\sigma - Q$ and $Q \in E(L)$

  $= \mathcal{O} \quad \forall P \in E(k) \Rightarrow \sigma \in \ker$.

- $\sigma \in Gal(\bar{K}/k)$ in kernel $\Rightarrow K(P,\sigma) = \mathcal{O} \quad \forall P \in E(k)$

  $Q^\sigma - Q \Rightarrow Q^\sigma = Q \quad \forall Q$ s.t. $[m]Q \in E(k)$

  $\Rightarrow \sigma$ fixes $K(Q)$

  $\Rightarrow \sigma$ fixes L. $\Rightarrow \sigma \in Gal(\bar{K}/L)$ ▨

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

$\cong$

$Gal(L/k)$

is perfect!

- $\varphi : E(k)/mE(k) \longrightarrow Hom(Gal(L/k), E[m])$

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

If $\kappa(P, \cdot)$ in kernel $\Rightarrow \kappa(P, \cdot) = 0 \ \forall \sigma$

non deg $\rightarrow P \in mE(k) \rightarrow P \equiv 0$ in $E(k)/mE(k)$ ✓

NOTE: If $\varphi : A \times B \to C$ is perfect w/ C finite.

then A is finite $\iff$ B is finite b/c

$A \hookrightarrow Hom(B, C)$

$B \hookrightarrow Hom(A, C)$

▨

UPSHOT: $\kappa : E(k)/mE(k) \times Gal(L/k) \longrightarrow E[m]$ is perfect

$\Longrightarrow$ $E(k)/mE(k)$ is finite iff $Gal(L/k)$ is finite

iff L/k is a finite extension

iff $K([m]^{-1}E(k))/K$ is finite.

$$\begin{array}{ccc} L & G_L & \mathfrak{P}G_L = (\mathfrak{Q}_1 \cdots \mathfrak{Q}_r)^e \\ | & | & | \\ k & G_k & \mathfrak{p} \end{array}$$

unramified $\Leftrightarrow e=1$.

PROP Let $L = K([m]^{-1}E(k))$. $(E[m] \subseteq E(k))$ $G_{L/k}$

(a) L/k is an abelian extension of exponent m, i.e., $Gal(L/k)$ is abelian and every element of G_L has order dividing m.

(b) Let $S = \{v \in M_K^0 : E \text{ has bad red'n at } v\} \cup \{v \in M_k^0 : v(m) \neq 0\} \cup M_k^\infty$

Then L/k is unramified outside of S (i.e., if $v \in M_k$ and $v \notin S$ then L/k is unramified at v.)

Prop Let $L = K([m]^{-1}E(K)).$ $(E[m] \subseteq E(K))$ $G_{L/K}$

(a) L/K is an abelian extension of exponent m, i.e., $\mathrm{Gal}(L/K)$ is abelian and every element of G_L has order dividing m.

(b) Let $S = \{v \in M_K^0 : E \text{ has bad redn at } v\} \cup \{v \in M_K^0 : v(m) \neq 0\} \cup M_K^\infty$

Then L/K is unramified outside of S (i.e., if $v \in M_K$ and $v \notin S$ then L/K is unramified at v.)

abelian, exponent m!

Proof.

(a) K is perfect $\Rightarrow$ $\mathrm{Gal}(L/K) \hookrightarrow \mathrm{Hom}\left(E(K)/mE(K), E[m]\right)$

$\sigma \longmapsto k(\cdot, \sigma)$

finite!

$\square$

(b) Let $v \in M_K$, $v \notin S$, let $Q \in E(\overline{K})$ w/ $[m]Q \in E(K)$, let $K' = K(Q)$.

Suffices to show K'/K is unramified at v b/c L is comp. of all such K'.

Let $v' \in M_{K'}$ be a place above v, let $K'_{v'}/K_v$ be the extension of completions and let $k'_{v'}/k_v$ be the ext'n of residue fields.

Since E/K_v has good redn at v $(v \notin S)$, $E/K'_{v'}$ has good redn at v'.

stable!

Now let $I_{\nu'/\nu} \subseteq \mathrm{Gal}(K'_{\nu'}/K_\nu)$ be inertia for ν'/ν

and let $\sigma \in I_{\nu'/\nu}$.

By defn of inertia, $\tilde{\sigma}$ acts as $\mathrm{Id} \in \mathrm{Gal}(\bar{k}'_{\nu'}/k'_{\nu'})$ so

$$\widetilde{Q^\sigma - Q} = \tilde{Q}^{\tilde{\sigma}} - \tilde{Q} = \tilde{Q} - \tilde{Q} = \tilde{\mathcal{O}}$$

and $[m](Q^\sigma - Q) = ([m]Q)^\sigma - [m]Q = [m]Q - [m]Q = \mathcal{O}$

($[m]Q \in E(k)$)

Thus $Q^\sigma - Q \in E[m]$ AND $Q^\sigma - Q \in$ Kernel of red'n.

But $E(K'_{\nu'})[m] \longrightarrow \tilde{E}_{\nu'}(k'_{\nu'})$ is injective! (b/c $\nu'(m) = 0$ b/c $\nu \notin S$)

$\Rightarrow Q^\sigma - Q = \mathcal{O} \quad \forall \sigma \in I_{\nu'/\nu} \Rightarrow Q^\sigma = Q \quad \forall \sigma \in I_{\nu'/\nu}$

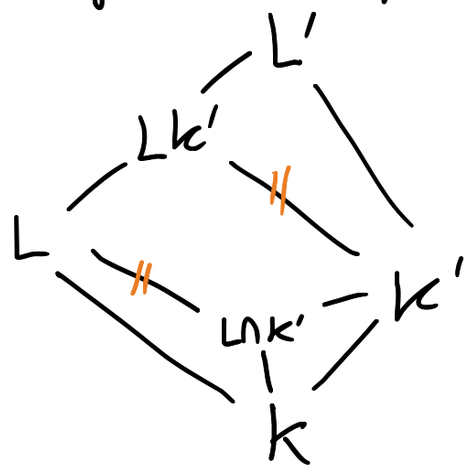
$\Rightarrow K_\nu(Q) \subseteq K_\nu^{nr} \Rightarrow K_\nu(Q)$ is unramified at ν

$\Rightarrow K' = K(Q)/K$ is unramified at ν $\Rightarrow$ K'/K unramified outside of S. ▨

Algebraic Number Theory Intermission

Prop Let K be a number field, $S \subseteq M_K$ a finite set of places containing M_K^∞, and let $m \geq 2$ be an integer. Let L/K $(L = K_{S,m}^{ab})$ be the maximal abelian extension of K having exponent m which is unramified outside of S. Then, L/K is a finite extension.

(sketch) Proof • If k'/k is finite and result is true for k', then it is true for k.



b/c $L \subseteq Lk' \subseteq L'$

$\Rightarrow$ L'/k' and k'/k are finite

$\rightarrow$ L/k is finite.

So assume $\mu_m \subseteq K$ (or replace K by $k' = k(\mu_m)$).

- May increase S b/c $K^{ab}_{S,m} \subseteq K^{ab}_{S',m}$ (allow MORE ramification)

  L_S " $S \subseteq S'$ " $L_{S'}$

  - Increase S so that

$$R_S = \{a \in K : v(a) \geq 0 \ \ \forall v \in M_K, v \notin S\}$$ S-units

    is a PID.

    FACT: This can be done b/c $Cl(K)$ is a finite group.

  - Enlarge S so that $v(m) = 0 \ \ \forall v \notin S$.

- FACT: KUMMER THEORY: if $\mu_m \subseteq K$, then the maximal abelian ext'n of K of exp. m must be obtained by adj. m-th roots of elts in K.

$$K^{ab}_m = K(\sqrt[m]{a} : a \in K)$$

$\Rightarrow L = K^{ab}_{S,m}$ is the largest subfield of K^{ab}_m unramified outside S.

- $K(\sqrt[m]{a})/K \quad a \in K$.

  $X^m - a = 0$, $\nu \in M_K$, $\nu \notin S$, $\nu(m) = 0$.

  FACT: $K_\nu(\sqrt[m]{a})/K_\nu$ unramified $\iff ord_\nu(a) \equiv 0 \bmod m$

- Thus, $L = K(\sqrt[m]{a} : a \in T_S)$

  where $T_S = \{ a \in K^\times/(K^\times)^m : ord_\nu(a) \equiv 0 \bmod m \ \forall \nu \in M_K, \nu \notin S \}$

- Need to prove T_S is finite.

  There is a map $R_S^\times \longrightarrow T_S$, $u \longmapsto u \in K^\times/(K^\times)^m$

  Prove surjective: Let $a \in T_S$, then aR_S is an ideal and it is the m-th power of an ideal in R_S! R_S is a PID!

  $aR_S = \mathfrak{b}^m = (b)^m \Rightarrow aR_S = b^m R_S \Rightarrow u \in R_S^\times$ s.t. $a = u \cdot b^m$

  and $u \in R_S^\times \longrightarrow a \in T_S$ ✓

- Recap: $L = K^{ab}_{S,m} \Longrightarrow L \subseteq K(\sqrt[m]{a} : a \in K)$

$$\Longrightarrow L = K(\sqrt[m]{a} : a \in T_S)$$

$$T_S = \{ a \in K^\times/(K^\times)^m : \mathrm{ord}_v(a) \equiv 0 \ (m) \ \forall v \in M_K, v \notin S \}$$

and $R_S^\times \xrightarrow{\psi} T_S$

Moreover $(R_S^\times)^m$ is in kernel of $\psi \Longrightarrow R_S^\times/(R_S^\times)^m \twoheadrightarrow T_S$

- **DIRICHLET'S S-UNIT THM:** $R_S^\times/_{\text{TORSION}}$ is free of rank $|S| - 1$. $(M_K^\infty \subseteq S)$

$\Rightarrow R_S^\times/(R_S^\times)^m$ is finite! $\Rightarrow T_S$ is finite $\Rightarrow L/K$ is FINITE! ∎