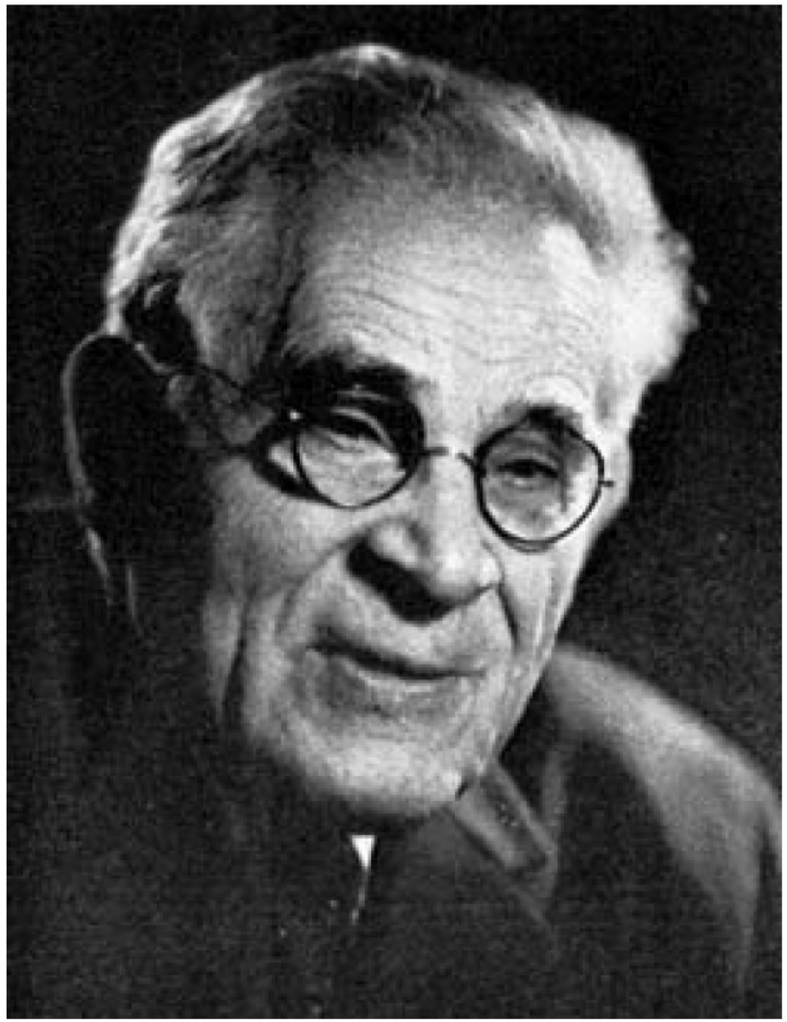
THE MORDELL-WEIL THEOREM



Louis Mordell
1888 – 1972

/ ⊘ (1922)

André Weil
1906 – 1998

/ ab vars over # flds (1928)

Thm Let E/K be an elliptic curve, where K is a number field.

Then, $E(K)$ is a finitely generated abelian group.

i.e., $E(K) = \langle P_1, \dots, P_n \rangle_{\mathbb{Z}}$ for some $P_i \in E(K)$

In particular,

$$E(K) \cong E(K)_{tors} \oplus \mathbb{Z}^{R_{E/K}}$$

where $E(K)_{tors}$ is a finite subgp formed by points of finite order

and $R_{E/K}$ is a non-neg. integer, called the rank of E/K.

$$(R_{E/K} = \operatorname{rank}_{\mathbb{Z}} E(K).)$$

Strategy.

- **Weak Mordell-Weil thm:**

  (NOTE: If $E(k) \cong T \oplus \mathbb{Z}^R \Rightarrow m \geq 2 \quad E(k)/mE(k) \cong \underbrace{T/mT \oplus (\mathbb{Z}/m\mathbb{Z})^R}_{\text{is finite}}$)

  k a number field, $m \geq 2$, then $E(k)/mE(k)$ is a finite gp.

- **Descent procedure:**

  Let A be an abelian gp w/ a "height" function, and there is $m \geq 2$ s.t. A/mA is finite. Then, A is finitely generated.

Notation

K a number field

M_K a complete set of inequivalent absolute values on K.

- M_K^∞ the archimedean abs. values on K

  $\left([K:\mathbb{Q}] = r_1 + 2r_2 \,,\; K \underset{r_1}{\hookrightarrow} \mathbb{R} \,,\; K \underset{2r_2}{\hookrightarrow} \mathbb{C} \right)$

- M_K^0 the non-archimedean abs values on K

  $\left(\mathfrak{p} \subseteq \mathcal{O}_K \text{ then } |\alpha|_{\mathfrak{p}} = \frac{1}{p^{\nu_{\mathfrak{p}}(\alpha)}} \right)$

$\nu(x) = -\log |x|_\nu$ for abs. values $\nu \in M_K$

ord_ν normalized val. for $\nu \in M_K^0$ (i.e. $\mathrm{ord}_\nu(K^*) = \mathbb{Z}$)

R or $\mathcal{O}_K$ ring of integers of $K = \{x \in K : v(x) \geq 0 \quad \forall v \in M_K^0\}$

$R^\times$ or $\mathcal{O}_K^\times$ unit gp of $R = \{x \in K : v(x) = 0 \quad \forall v \in M_K^0\}$

K_v completion of K at v, for $v \in M_K$.

R_v, $\mathfrak{m}_v$, k_v.

Thm (Weak Mordell-Weil) K a number field and E/K ell. curve.
Then for every $m \geq 2$, $E(K)/mE(K)$ is finite.

Lemma L/k finite Galois, and if $E(L)/mE(L)$ is finite, then $E(k)/mE(k)$ is finite.

Proof Let $\Phi = \ker\left(E(k)/mE(k) \longrightarrow E(L)/mE(L) \right)$

NOTE $0 \to \Phi \to E(k)/mE(k) \longrightarrow E(L)/mE(L)$ so if is finite then is finite and

i.e., if Φ is finite and $E(L)/mE(L)$ is finite then $E(k)/mE(k)$ is finite.

need to prove this.

For each $P \in \Phi = (E(k) \cap mE(L))/mE(k)$, we can choose $Q_P \in E(L)$ w/ $[m]Q_P = P$. Define a map of sets:

$$\lambda_P : Gal(L/k) \longrightarrow E[m]$$
$$\sigma \longmapsto Q_P^\sigma - Q_P$$

$P \in \Phi \to \exists\, Q_P \in E(L)$ s.t. $[m]Q_P = P$

$\lambda_P : G_{L/k} \longrightarrow E[m]$

$\sigma \longmapsto Q_P^\sigma - Q_P$

cohomology

$[m]/k$ $\qquad$ $P \in E(k)$

- Well-def: $[m](Q_P^\sigma - Q_P) = ([m]Q_P)^\sigma - [m]Q_P = P^\sigma - P = \mathcal{O}$.

Suppose $\lambda_P = \lambda_{P'}$ for $P, P' \in E(k) \cap mE(L)$. Then

$Q_P^\sigma - Q_P = Q_{P'}^\sigma - Q_{P'} \Rightarrow (Q_P - Q_{P'})^\sigma = Q_P - Q_{P'} \quad \forall \sigma \in G_{L/k}$

$\Rightarrow Q_P - Q_{P'} \in E(k) \Rightarrow P - P' = [m]Q_P - [m]Q_{P'} = [m](Q_P - Q_{P'}) \in mE(k)$

$\Rightarrow P \equiv P' \bmod mE(k)$

$\Rightarrow \Phi \longrightarrow Map(G_{L/k}, E[m])$, $P \longmapsto \lambda_P$ is one-to-one.

fin. $\quad$ fin

finite

$\Rightarrow \Phi$ is finite. $\blacksquare$

Use Lemma: $K(E[m])/K$ is a finite Galois extension.

$Q \in E[m]$, then $Q^\sigma \in E[m]$ for all $\sigma \in \mathrm{Gal}(\bar{K}/K)$

$\Longrightarrow K(E[m])/K$ is Galois.

$\deg [m] = m^2 \Rightarrow K(E[m])/K$ is finite.

Using the lemma we can assume $E[m] \subseteq E(K)$ (or replace K by $K(E[m])$).

The Kummer Pairing

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

$P \in E(K)$, choose $Q \in E(\bar{K})$ s.t. $[m]Q = P$

then $\kappa(P, \sigma) = Q^\sigma - Q$.

$$\kappa : E(k) \times G_{\bar{k}/k} \longrightarrow E[m]$$

$$(P, \sigma) \longmapsto Q^{\sigma} - Q \quad \text{where } [m]Q = P.$$

Prop (a) Well-defined

(b) Bilinear

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

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

L = compositum of $K(Q)$ w/ $Q \in E(\bar{k})$ s.t. $[m]Q \in E(k)$.

Hence κ induces a perfect bilinear pairing:

$$E(k)/mE(k) \times G_{L/k} \longrightarrow E[m]$$

Proof $k(P,\sigma) = Q^\sigma - Q$ w/ $[m]Q = P$.

(a)
- $[m](Q^\sigma - Q) = ([m]Q)^\sigma - [m]Q = P^\sigma - P = \mathcal{O}$.
- $\rightarrow k(P,\sigma) \in E[m]$.

- $Q' \in E(\bar{k})$ s.t. $[m]Q' = P \Rightarrow Q' = Q + T$ for some $T \in E[m]$

$$k_{Q'}(P,\sigma) = Q'^\sigma - Q' = (Q+T)^\sigma - (Q+T) = Q^\sigma - Q + T^\sigma - T$$

$E[m] \subseteq E(k)$ $\rightarrow T^\sigma = T \ \forall \sigma$

$$= Q^\sigma - Q = k_Q(P,\sigma). \quad \blacksquare$$

(b) $P, P' \in E(k)$, Q, Q' s.t. $[m]Q = P$, $[m]Q' = P' \Rightarrow [m](Q+Q') = P+P'$

left
- $k(P+P', \sigma) = (Q+Q')^\sigma - (Q+Q') = Q^\sigma - Q + Q'^\sigma - Q' = k(P,\sigma) + k(P',\sigma)$.

right
- $\sigma, \tau \in G_k$, $k(P, \sigma\tau) = Q^{\sigma\tau} - Q = (Q^\sigma - Q)^\tau + Q^\tau - Q$

$$= k(P,\sigma)^\tau + k(P,\tau) = k(P,\sigma) + k(P,\tau) \quad \blacksquare$$

$k(P,\sigma) \in E[m]$, $E[m] \subseteq E(k)$