Cor 2.8.3 Let $V, W$ be normal projective varieties over a number field $K$ and let $\varphi: V \to W$ be a dom. finite unram. morphism. Then, there is a finite set $S$ of primes of $K$ such that the field of def. $K'$ of any $P \in V(\overline{K})$ with $Q := \varphi(P) \in W(K)$ is unramified at all primes $\mathfrak{p} \notin S$.

Pf Let $S_{ij}$ be the set from Thm 2.8.2 for the restriction $\varphi : \varphi^{-1}(W \cap H_i) \cap H_j \to W \cap H_i$.

Let $S = \bigcup_{i,j} S_{i,j}$.

Write $Q = [y_0 : \cdots : y_m]$ and $\mathfrak{p} \notin S$.

W.l.o.g. $v_{\mathfrak{p}}(y_0) \leq v_{\mathfrak{p}}(y_1) \leq \dots$

Dividing by $y_0$, we can arrange that $v_{\mathfrak{p}}(y_i) \geq 0 \ \forall i$ and $y_0 = 1$.

$\Rightarrow$ By Thm 2.8.2, $K'$ is unram. at $\mathfrak{p}$.

$\square$

$y_1, \dots, y_m$ are the coord. of $Q$ in the affine chart $W \cap H_0 \cong \mathbb{A}^n$

## 2.9. Proof of weak Mordell-Weil

**Weak M-W** Let $K$ be a number field, $\phi: E_1 \to E_2$ a nonzero isogeny between ell. curves over $K$ with $\ker(\phi) \subseteq E_1(K)$. Then, the group $E_2(K)/\phi(E_1(K))$ is finite.

**Pf** Apply Cor 2.8.3 to $\phi$. Let $S$ be the resulting set of primes.

By Hermite's thm., there are only fin. many field ext. $K'|K$ of degree $\leq \deg(\phi)$ unramified at all primes $\mathfrak{q} \notin S$.

Let $L$ be the Galois closure of their compositum.

The field of def. of any $P \in E_1(\bar{K})$ with $Q := \phi(P) \in E_2(K)$ is unram. at all primes $\mathfrak{q} \notin S$ and has degree $\leq \deg(\phi)$.

$\Rightarrow \phi^{-1}(E_2(K)) \subseteq E_1(L)$.

Let $G := \mathrm{Gal}(L|K)$.

Claim: We obtain an injective group homomorphism

$$E_2(K)/\phi(E_1(K)) \hookrightarrow \mathrm{Hom}(G, \ker(\phi))$$
$$Q \longmapsto (\sigma \mapsto \sigma(P)-P)$$

for any $P \in \phi^{-1}(Q) \subset E_1(L)$

Pf $\sigma(P)-P \in \ker(\phi)$:

$$\phi(\sigma(P)-P) = \phi(\sigma(P))-\phi(P)$$
$$= \sigma(\underbrace{\phi(P)}_{Q}) - \underbrace{\phi(P)}_{Q}$$
$$= Q - Q = O$$

$\sigma(P)-P$ is indep. of the choice of $P$

$R \in \ker(\phi) \subseteq E_1(K)$

$\Rightarrow \sigma(R)-R = R-R = O$

$\Rightarrow$ If $P, P' \in \phi^{-1}(Q)$, then $P-P' \in \ker(\phi)$,

so $(\sigma(P)-P)-(\sigma(P')-P')$

$= \sigma(P-P')-(P-P') = O$.

hom. in $\sigma$

$$\sigma_1\sigma_2(P)-P = \sigma_1(\underbrace{\sigma_2(P)-P}_{\in \ker(\phi)\subseteq E_1(K)})+(\sigma_1(P)-P)$$

$-: E\times E \to E$ is def. over $K$

$$=(\sigma_2(P)-P)+(\sigma_1(P)-P)$$

hom. in P

$\phi(P_1) = Q_1$, $\phi(P_2) = Q_2$

$\Rightarrow \phi_1(P_1+P_2) = Q_1 + Q_2$

$\sigma(P_1+P_2) - (P_1+P_2) = (\sigma(P_1) - P_1) + (\sigma(P_2) - P_2)$

$\phi(E_1(K)) \longmapsto O$

$Q \in \phi(E_1(K))$

$\Rightarrow$ can take $P \in E_1(K)$.

$\Rightarrow \sigma(P) - P = O$.

injective.

If $\sigma(P) - P = O \ \forall \sigma \in G = Gal(L|K)$,

then $\sigma(P) = P \ \forall \sigma$, so $P \in E_1(K)$.

$\Rightarrow Q = \phi(P) \in \phi(E_1(K))$. $\square$

$G$ and $ker(\phi)$ are finite.

$\Rightarrow$ ~~Hom~~ $(G, ker(\phi))$ is finite

$\Rightarrow E_2(K)/\phi(E_1(K))$ is finite. $\square$

Rmk: If $\phi = [m]$, one can in fact take

$S = \{\mathfrak{q} \mid E$ has bad reduction at $\mathfrak{q}$ or $\mathfrak{q} \mid m\}$.

(See Silverman.)

One can use this to obtain an explicit upper bound on the size of $E(K)/mE(K)$ and (using descent) on the rank of $E$ over $K$.

Rmk: Even if $\ker(\phi) \not\subseteq E_1(K)$, we still get an injective homomorphism

$$E_2(K)/\phi(E_1(K)) \hookrightarrow H^1(G, \ker(\phi))$$
$$Q \longmapsto (\sigma \mapsto \sigma(P) - P) \quad \text{for } P \in \phi^{-1}(Q)$$

to the cohomology group $H^1(G, \ker(\phi))$.
(finite)

(Look at the exact sequence

$$0 \to \ker(\phi) \to E_1(\overline{K}) \xrightarrow{\phi} E_2(\overline{K}) \to 0$$

and the resulting long exact sequence in $G$-module cohomology:

$$\cdots \to E_1(K) \xrightarrow{\phi} E_2(K) \xrightarrow{\delta} H^1(G, \ker(\phi)) \to H^1(G, E_1(\overline{K})).)$$

Conjecture (Lang) weak variant:

Let $E = \{[x:y:z] \mid y^2 z = x^3 + a_4 x z^2 + a_6 z^3\}$ be an elliptic curve over $\mathbb{Q}$ with $a_4, a_6 \in \mathbb{Z}$ of rank $r$. For every $\varepsilon > 0$, there is a basis $P_1, \dots, P_r \in E(\mathbb{Q})$ of $E(\mathbb{Q}) \otimes_{\mathbb{Z}} \mathbb{R}$ with

$$\hat{h}(P_1), \dots, \hat{h}(P_r) \ll_{\varepsilon, r} \max\left(|a_4|^{\frac{1}{4}+\varepsilon}, |a_6|^{\frac{1}{6}+\varepsilon}\right).$$

Question: Are there elliptic curves $E$ over $\mathbb{Q}$ of arbitrarily large rank?

Conjecture (Néron, Honda, "folklore") No.

Conjecture (Cassels, Tate, "folklore") Yes.

Conjecture (Park-Poonen-Voight-Wood) No.

In fact, there are only fin. many ell. curves $E$ over $\mathbb{Q}$ of rank $> 21$.

Record (Elkies) There is an (explicit) ell. curve $E$ over $\mathbb{Q}$ of rank $\geq 28$.

Conjecture (Elkies) (?) No. Any ell. curve $E$ over $\mathbb{Q}$ has rank $\leq 28$.

# 3. Abelian varieties

References:

- Milne's notes on Abelian Varieties
- Lang, Abelian Varieties

## 3.1. Overview

Def A group variety $G$ over $K$ is a variety over $K$ and a group such that the maps $G \times G \to G$, $(g,h) \mapsto gh$ and $G \to G$, $g \mapsto g^{-1}$ are morphisms defined ~~over~~ $K$ and with identity $e \in G(K)$.

Ex
- Ell. curve $E$ over $K$
- The additive group $G_a = \mathbb{A}^1_K$ (with addition)
- The multiplicative group
$$G_m = \{(x,y) \in \mathbb{A}^2_K \mid xy = 1\} \cong \overline{K}^\times$$
$$(x,y) \mapsto x$$
with mult.

- $GL_n = \{(M,N)$ pair of $n\times n$-matrices $\mid MN = I_n\}$ with mult.
- $SL_n = \{M$ $n\times n$-matrices $\mid \det(M) = 1\}$.
- Any product of group varieties.

<u>Def</u> A variety $V$ over $K$ is <u>complete</u> if for every affine variety $W$ over $K$, the projection $V \times W \longrightarrow W$ is a closed map (so the image of any closed set is closed).

<u>Ex</u> $\mathbb{A}^1_K$ is not complete: look at $\mathbb{A}^1 \times \mathbb{A}^1 \to \mathbb{A}^1$
$$(x,y) \mapsto y$$

The image of $\{(x,y) \mid xy = 1\}$ is $\{y \mid y \neq 0\}$, which is not closed.

<u>Rmk</u> Complete var. behave like compact manifolds.

<u>Rmk</u> Any subvariety of a complete variety is complete.

Thm 3.1.1 $\mathbb{P}^n_k$ is complete.

Cor 3.1.2 Any $V \subseteq \mathbb{P}^n_k$ is complete.

(Rmk If $\varphi : V \to W$ is a morphism between varieties and $V$ is complete, then $\varphi$ is closed.)