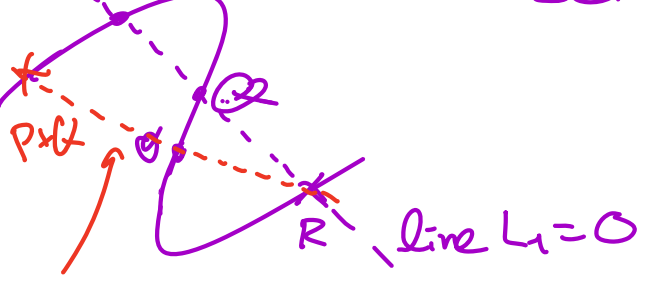

regarded as an element of $\bar{K}(E)$.

$$\operatorname{div}(f) = [P]+[Q]+[R] - ([P+Q]+[\mathcal{O}]+[R])$$
$$= [P]-[\mathcal{O}]+[Q]-[\mathcal{O}]-([P+Q]-[\mathcal{O}])$$

Thus in $\mathrm{Pic}^0(E)$, $J(P)+J(Q)-J(P+Q)=\mathcal{O}$. ∎

Our goal in the next two weeks: prove the Mordell-Weil Theorem: Let K be a number field. Let $(E,\mathcal{O})$ be an elliptic curve over K. Then the abelian group $E(K)$ is finitely-generated. (Hence $\cong$ (finite torsion group) $\times \mathbb{Z}^r$ some $r \geq 1$).

Isogenies:

Defn: Let $(E,\mathcal{O})$ and $(E',\mathcal{O}')$ be elliptic curves over k. An isogeny from $(E,\mathcal{O})$ to $(E',\mathcal{O}')$ is a non-constant (hence surjective) morphism

$$\phi: E \longrightarrow E' \text{ such that}$$
$$\phi(\mathcal{O}) = \mathcal{O}'$$

Key example: $m \in \mathbb{Z}\setminus 0$. The multiplication by m isogeny: $[m]: E \longrightarrow E$

- For $m > 0$, $[m]P = \underbrace{P + P + \cdots + P}_{m \text{ } P\text{'s}}$
- For $m < 0$, $[m]P = -[-m]P$
- Clearly $[m]$ is a morphism and a group hom.
- For $m \neq \pm 1$, $[m]$ is not an isomorphism

Ex: Suppose $\mathrm{char}\, k \neq 2$, and for $\lambda_1, \lambda_2, \lambda_3$ distinct $E: y^2 = (x-\lambda_1)(x-\lambda_2)(x-\lambda_3)$. $\mathcal{O} = [0,1,0]$

Then $[2]P = \mathcal{O} \iff P = \mathcal{O}$ or $P = (\lambda_i, 0)$ for some i.

Notation: We write $E[m]$ for $\ker([m])$ $(= \{P \in E \mid [m]P = \mathcal{O}\})$.

and write $E[m](k)$ (or $E(k)[m]$) for $E(k) \cap E[m]$.

Important exercise: $[m]$ is actually non-constant! See PSet 5 when $\mathrm{char}\, k \neq 2$ (sufficient for our proof of M-W).

- We won't need other isogenies, but they are important in the general theory. We'll sketch

one nice general fact, though:

Prop: Every isogeny $\phi : E \to E'$ is a group homomorphism.

Sketch:

$$\begin{array}{ccc} J: E & \xrightarrow{P \mapsto [P]-[\mathcal{O}]} & \mathrm{Pic}^0(E) \\ \phi \downarrow & & \vdots \\ J': E' & \xrightarrow{\sim} & \mathrm{Pic}^0(E') \\ & P' \longmapsto & [P]-[\mathcal{O}'] \end{array}$$

define a map $\phi_* : \mathrm{Pic}^0(E) \to \mathrm{Pic}^0(E')$ by

$$\phi_*\left(\sum_{P \in E} c_P \cdot [P]\right) = \sum c_P [\phi(P)]$$

This is obviously a gp hom $\mathrm{Div}^0(E) \to \mathrm{Div}^0(E')$

Must check that ϕ_* descends to $\mathrm{Pic}^0(E) \to \mathrm{Pic}^0(E')$. ∎

With this defn, the diagram commutes since ϕ is an isogeny.

Thus $\phi = (J')^{-1} \circ \phi_* \circ J$ is a group homomorphism since J, ϕ_*, J' are.

In particular, we can speak of the

kernel of an isogeny.

Cor: $\phi: E \to E'$ an isogeny. Then $\ker(\phi) = \phi^{-1}(\mathcal{O}')$ is a finite subgroup of E.

(eg, $E[m]$ is a finite subgp of E ($m \neq 0$))

Pf: Since $\deg(\phi) = \sum_{P \in \phi^{-1}(\mathcal{O}')} e_\phi(P)$, $\phi^{-1}(\mathcal{O}')$ is finite. ∎

Let's return to $[m]: E \to E$.

Some fundamental facts:

Theorem: Let $(E, \mathcal{O})$ be an elliptic curve over k, and let $m \in \mathbb{Z} \setminus 0$.

(1) $[m]: E \to E$ is an isogeny of degree m^2.

(2) If $(m, \mathrm{char}\, k) = 1$, then $[m]$ is separable ($k(E)/[m]^* k(E)$ is separable), and

$$E[m] := \ker([m]) \cong \mathbb{Z}/m \times \mathbb{Z}/m$$

(*) The proof of the M-W theorem will depend on an analysis of the G_k-module $E[m]$; from the exercise above, we know at least that this is finite.

(a more refined understanding of the $E[m]$ as G_k-modules is central in studying elliptic curves —)

Road to Mordell-Weil

F - number field.

E an elliptic curve over F

Thm^{MW} $E(F)$ is finitely-generated.

Two steps:

Thm^1 (Weak Mordell-Weil) For any $m \in \mathbb{Z}_{>1}$, $E(F)/mE(F)$ is finite.

Rmk: ① Without further info about $E(F)$, this doesn't guarantee finite generation. (eg $\mathbb{Q}$ or $\mathbb{Z}_p$ or ...)

② For M-W, suffices to prove for a single m (e.g., taking $m=2$ can give somewhat easier hands-on arguments, at least if you assume ... about $E[2](F)$ ...)

Thm^2 (Descent via heights) Detailed statement later. Roughly, "heights" are a way of measuring the size of elements of $E(F)$, and we show: $[m]: E(F) \to E(F)$ increases the height, and $\forall X \in \mathbb{R}$, $E(F)$ has only finitely many points with height $\leq X$.

Thm^1 + Thm^2 $\Rightarrow$ Thm^{MW}.

We'll first discuss weak Mordell-Weil. It will use a chunk of algebraic number theory & one crucial fact from the study of elliptic curves over local fields (like $\mathbb{Q}_p$ & its finite extensions.

We know $E(\bar{F}) \xrightarrow{[m]} E(\bar{F})$ is surjective

$E(F) \xrightarrow{[m]} E(F)$ is not. To show $E(F)/mE(F)$ is finite, we'll show that $\exists$ finite extension L/F such that $\forall P \in E(F)$, $[m]^{-1}(P) \in E(L)$

(clear $[L:F]$ bdd. local analysis will bound the set of ramified primes).

The local input: Let $K/\mathbb{Q}_p$ be a finite extension. The integral closure $\mathcal{O}_K$ of $\mathbb{Z}_p$ in K is still a DVR, with maximal ideal $m_K = (\pi)$ (π is a choice of uniformizer)

\varpi

$p \in m_K$, so $p = u \cdot \pi^{e_K}$ for some $u \in \mathcal{O}_K^\times$, $e_K \in \mathbb{Z}_{\geq 1}$.

e_K = the ramification index of $K/\mathbb{Q}_p$. When $e_K = 1$, we say $K/\mathbb{Q}_p$ is unramified.

The quotient $\mathcal{O}_K/m_K = k$ is called the residue field of K.

$[k:\mathbb{F}_p] < \infty$.

Ex: $K = \mathbb{Q}_p[\sqrt{p}]$ has $\mathcal{O}_K = \mathbb{Z}_p[\sqrt{p}]$, $\varpi = \sqrt{p}$, $e_K = 2$.

Like $\mathbb{Z}_p$, $\mathcal{O}_K$ is a complete DVR:

$$\mathcal{O}_K \xrightarrow{\sim} \varprojlim_n \mathcal{O}_K/\mathfrak{m}_K^n = \left\{ (\ldots a_n, \ldots, a_2, a_1) \;\middle|\; a_i \in \mathcal{O}_K/\mathfrak{m}_K^i \text{ and } a_{i+1} \equiv a_i \bmod \mathfrak{m}_K^i \right\}$$

Hensel's Lemma holds exactly as before.

Ex: • Let $k/\mathbb{F}_p$ be finite, $|k| = q = p^f$. Then $\exists$ an unramified extension $K/\mathbb{Q}_p$ such that $\mathcal{O}_K/\mathfrak{m}_K \simeq k$

Pf: Let $k = \mathbb{F}_p[\alpha]$ (α gen. of $k^\times$), let $\bar{f}(x) \in \mathbb{F}_p[x]$ be the min. poly. of α. Lift $\bar{f}(x)$ to a monic $f(x) \in \mathbb{Z}_p[x]$. $\bar{f}(x)$ irr. $\Rightarrow f(x)$ is irr. in $\mathbb{Z}_p[x]$ $\overset{\text{(Gauss)}}{\Rightarrow} f(x)$ is irr. in $\mathbb{Q}_p[x]$

$\Rightarrow K := \mathbb{Q}_p[x]/f(x)$ is a field extension of $\mathbb{Q}_p$ with $[K:\mathbb{Q}_p] = \deg(f) = \deg(\bar{f}) = [k:\mathbb{F}_p]$. This knows:

$$\begin{array}{ccc} \mathbb{Z}_p[x]/(f(x),p) & \xrightarrow{\sim} & k \\ \downarrow & & \downarrow \text{define this s.t. the diagram commutes} \\ \mathcal{O}_K/p\mathcal{O}_K & \longrightarrow & \mathcal{O}_K/\varpi\mathcal{O}_K \end{array} \qquad \Rightarrow k \hookrightarrow \mathcal{O}_K/\varpi\mathcal{O}_K,$$

and $[\ell : \mathbb{F}_p] = [K : \mathbb{Q}_p] \geq [\mathcal{O}_K/\varpi\mathcal{O}_K : \mathbb{Z}/p]$

Thus $\ell \xrightarrow{\sim} \mathcal{O}_K/\varpi\mathcal{O}_K$ (concretely, $K = \mathbb{Q}_p(\mu_{q-1})$).

- For any $K/\mathbb{Q}_p$ with residue field k and any ℓ/k finite, $\exists$ unramified extension L/K with residue field ℓ. (same proof)

↖ means $\mathfrak{m}_K \cdot \mathcal{O}_L = \mathfrak{m}_L$

What we'll need:

Let $K/\mathbb{Q}_p$ be a finite extension. Let E/K be an elliptic curve, given by a W.E. We may and do assume (by rescaling) that the coefficients all lie in $\mathcal{O}_K$ and are not all divisible by π. Thus the reduction mod π of the WE gives a WE, possibly singular, over $\mathcal{O}_K/\pi\mathcal{O}_K$

Ex: $y^2 = x^3 + px$ over $\mathbb{Q}_p$ (ell curve)

$\downarrow$

$y^2 = x^3$ over $\mathbb{F}_p$ (singular cubic)

$(0,0)$ is the singular point.

Defn: E/K has good reduction if it is possible to choose a W.E. for E such that the reduction $\bar{E}/(\mathcal{O}_K/\pi)$ is nonsingular (and thus is an elliptic curve over $\mathcal{O}_K/\pi$, with identity $[0,1,0] \in \mathbb{P}^2(\mathcal{O}_K/\pi)$).

(This is a little subtle — we haven't discussed how unique a W.E. for E is, but it can be extracted from

the Riemann-Roch argument.)

Lemma: Let E/F be an elliptic curve over a number field F. Then for all but finitely many ("almost all") primes $\mathfrak{p}$ of $\mathcal{O}_F$, the elliptic curve $E/F_{\mathfrak{p}}$ has good reduction.

Pf: Choose any W.E. for E, which we may assume has the form $y^2 = x^3 + ax + b$ for some $a, b \in \mathcal{O}_F$.

$\Delta(a,b) = 4a^3 + 27b^2 \neq 0$ since E is nonsingular.

For any $\mathfrak{p} \subset \mathcal{O}_F$ prime, as long as $\mathfrak{p} \nmid 2 \cdot \Delta(a,b)$, the reduction $\overline{E}_{\mathfrak{p}}$ of E mod $\mathfrak{p}$ is still nonsingular. ∎

(*) See any of the standard references for a more thorough treatment of reduction of elliptic curves. For simplicity, since it suffices for M-W, we will restrict to:

↓↓↓ ASSUME THIS IN WHAT FOLLOWS

$K/\mathbb{Q}$ finite. E/K an elliptic curve with good reduction. $\overline{E}$ = the resulting ell. curve over $k = \mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$

We have a map (of sets)

$E(K) \longrightarrow \overline{E}(k)$ given by

$[x,y,z] \longmapsto [\bar{x},\bar{y},\bar{z}]$ where we choose

$(x,y,z) \in \mathcal{O}_K^3 \setminus \pi \mathcal{O}_K^3$ ($\bar{x} = x \bmod \pi$, etc.), and such normalization is unique up to $\mathcal{O}_K^\times$-multiple, yielding a well-defined reduction $[\bar{x},\bar{y},\bar{z}] \in \overline{E}(k) \subset \mathbb{P}^2(k)$

$E(K) \longrightarrow \overline{E}(k)$ is in fact a group homomorphism: lines reduce to lines, and $P, Q, R \in E(K)$ satisfy $P+Q+R=\mathcal{O} \Leftrightarrow P, Q, R$ colinear in $\mathbb{P}^2(K)$

$\Rightarrow \bar{P}, \bar{Q}, \bar{R}$ colinear in $\mathbb{P}^2(k) \Leftrightarrow \bar{P}+\bar{Q}+\bar{R}=\mathcal{O}$ in $\overline{E}(k)$

(check is required to see this still works when $\bar{P}, \bar{Q}, \bar{R}$ not distinct – exercise).

Lemma: Let $E_1(K) = \ker(E(K) \longrightarrow \overline{E}(k))$.

Then we have an exact sequence of abelian groups

$$0 \to E_1(K) \to E(K) \to \overline{E}(k) \to 0$$

Pf: The only thing to show is surjectivity of $E(K) \to \overline{E}(k)$

Since each point of $\overline{E}(k)$ is nonsingular, surjectivity follows from (multivariable) Hensel's Lemma as discussed at the start of the course.

Here is the input we'll need for Mordell-Weil:

Theorem: For any $m \in \mathbb{Z}$ not divisible by p,

(1) $[m]: E_1(K) \to E_1(K)$ is an isomorphism.

(2) For any $P \in E(K)$, there exists a finite unramified extension L/K and a $Q \in E(L)$ such that $[m]Q = P$.

(3) The reduction map $E(K)[m] \to \bar{E}(k)$ is injective.

Pf: (1) will take work. Let's show (1) $\Rightarrow$ ((2) and (3)).

Assume (1). (2): Take $P \in E(K)$, $\bar{P} \in \bar{E}(k)$ the reduction.

$[m]: \bar{E} \to \bar{E}$ is an isogeny, so $\exists\ k'/k$ finite and $\bar{Q} \in \bar{E}(k')$ such that $[m]\bar{Q} = \bar{P}$.

Let K'/K be the unramified extension with residue field k' (lemma start of class). Have exact sequence

$$0 \to E_1(K') \to E(K') \to \bar{E}(k') \to 0$$

$$\exists\ Q \longmapsto \bar{Q}$$

Now $[m]Q - P$ reduces to 0 in $\bar{E}(k')$, hence lies in $E_1(K') \overset{(1)}{=} [m] \cdot E_1(K')$, so $[m]Q - P = [m]Q'$, $Q' \in E_1(K')$, so

$P = [m] \cdot Q$ for some $Q' \in E(K')$.

③: $E_1(K) \cap E(K)[m] = \mathcal{O}$ by ① (inj.). ✓

Do ① next time →