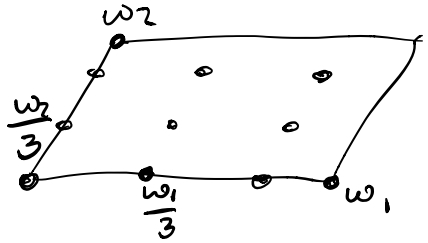
## Last time

$E = \mathbb{C}/\Lambda$

- Isogenies $\varphi: E \longrightarrow E'$
  - mult-by-$N$: $[N]: E \longrightarrow E$
  - $E[N] = \ker [N]$

$E[N] \cong (\mathbb{Z}/N\mathbb{Z})^2$

$N = 3$




- Tate module of $E$. $\ell$: prime

$$\cdots \longrightarrow E[\ell^3] \xrightarrow{[\ell]} E[\ell^2] \xrightarrow{[\ell]} E[\ell]$$

$$\cdots \longrightarrow \mathbb{Z}/\ell^3\mathbb{Z} \longrightarrow \mathbb{Z}/\ell^2\mathbb{Z} \longrightarrow \mathbb{Z}/\ell\mathbb{Z}$$

$T_\ell E = \varprojlim_{n \geq 1} E[\ell^n]$ : rank 2 $\mathbb{Z}_\ell$-module.

$\varprojlim_{n \geq 1} \mathbb{Z}/\ell^n\mathbb{Z}$

## The Weil pairing

There is an alternating, nondegenerate, bilinear pairing

$$E[N] \times E[N] \longrightarrow \mathbb{Z}/N\mathbb{Z}.$$

Let $\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ $\left(\frac{\omega_1}{\omega_2} \in \mathcal{H}\right)$.

This choice of basis gives $E[N] = \left\langle \frac{\omega_1}{N} \right\rangle \times \left\langle \frac{\omega_2}{N} \right\rangle$.

For $P, Q \in E[N]$, have $\gamma \in M_2(\mathbb{Z}/N\mathbb{Z})$ s.t.

$$\begin{pmatrix} P \\ Q \end{pmatrix} = \gamma \begin{pmatrix} \omega_1/N \\ \omega_2/N \end{pmatrix}.$$

Define $e_N : E[N] \times E[N] \longrightarrow \mathbb{Z}/N\mathbb{Z}$

$$(P, Q) \longmapsto \det \gamma$$

Prop

(1) $e_N$ does not depend on the choice of $\{\omega_1, \omega_2\}$

(2) $e_N$ is bilinear:

$$e_N(P+P', Q) = e_N(P, Q) + e_N(P', Q)$$
$$e_N(P, Q+Q') = e_N(P, Q) + e_N(P, Q')$$

(3) $e_N$ is alternating: $e_N(P, Q) = -e_N(Q, P)$

(4) $e_N$ is nondegenerate:

$$e_N(P, Q) = 0 \quad \forall Q \in E[N] \iff P = 0$$
$$e_N(P, Q) = 0 \quad \forall P \in E[N] \iff Q = 0.$$

Pf.

(1) Any other basis $\{\omega_1', \omega_2'\}$ is given by

$$\begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix} = \gamma \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} \quad \text{some } \gamma \in SL_2(\mathbb{Z}).$$

(2) $P = \dfrac{aw_1 + bw_2}{N}$ $\qquad P' = \dfrac{a'w_1 + b'w_2}{N}$

$Q = \dfrac{cw_1 + dw_2}{N}$

$e_N(P,Q) = ad - bc \qquad e_N(P',Q) = a'd - b'c$

$e_N(P+P', Q) = (a+a')d - (b+b')c.$

(3) $\begin{pmatrix} Q \\ P \end{pmatrix} = \underbrace{\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}}_{\det -1} \begin{pmatrix} P \\ Q \end{pmatrix}$

(4) $P = 0 \Longrightarrow e_N(P,Q) = 0 \quad \forall Q$ ✓

$\Leftarrow$ : $P = \dfrac{aw_1 + bw_2}{N}$

If $a, b$ not both $0$, then can pick $c, d \in \mathbb{Z}/N\mathbb{Z}$ s.t. $\det\begin{pmatrix} a & b \\ c & d \end{pmatrix} \neq 0$

Take $Q = \dfrac{cw_1 + dw_2}{N}$, □

$$E[N] \times E[N] \xrightarrow{e_N} \mathbb{Z}/N\mathbb{Z} \xrightarrow[\exp]{\sim} \mu_N$$

$$a \longmapsto e^{2\pi i a/N}$$

This composition is called the <u>Weil pairing</u> and also denoted $e_N$.

**Prop** $e_N$ is compatible with change in $N$, i.e.

$$\begin{array}{ccc} E[nN] \times E[nN] & \xrightarrow{e_{nN}} & \mathbb{Z}/nN\mathbb{Z} \\ \downarrow [n]\times[n] & & \downarrow \bmod N \\ E[N] \times E[N] & \xrightarrow{e_N} & \mathbb{Z}/N\mathbb{Z} \end{array}$$

commutes.

**Pf.**

$$\begin{array}{ccc} \left(\frac{aw_1+bw_2}{nN}, \frac{cw_1+dw_2}{nN}\right) & \longmapsto & ad-bc \\ \downarrow & & \downarrow \\ \left(\frac{aw_1+bw_2}{N}, \frac{cw_1+dw_2}{N}\right) & \longmapsto & ad-bc \end{array}$$

□

$$e_{\ell^n} : E[\ell^n] \times E[\ell^n] \longrightarrow \mathbb{Z}/\ell^n\mathbb{Z}$$

**Cor** We have an alternating, nondegenerate, bilinear pairing

$$T_\ell E \times T_\ell E \longrightarrow \mathbb{Z}_\ell .$$

**Rmk** Once we've introduced a Gal. action on $T_\ell E$, this pairing will be Galois-compatible w.r.t. the cyclotomic character on $\mathbb{Z}_\ell$.

# Reminders on algebraic geometry

Let $K$ be an alg. closed field.

- $\mathbb{P}^n = \mathbb{P}^n_K = K^{n+1} \setminus \{0\} \Big/ (x \sim \lambda x : \lambda \in K^\times)$

  - write pts. in homogeneous coordinates

    $[x_0 : x_1 : \cdots : x_n] \qquad x_i \in K$

- Projective variety is a subset of $\mathbb{P}^n$ given by the vanishing locus of some homogeneous polynomials

  - Eg. $V(X+Y-Z) \subseteq \mathbb{P}^2$

    $\| $

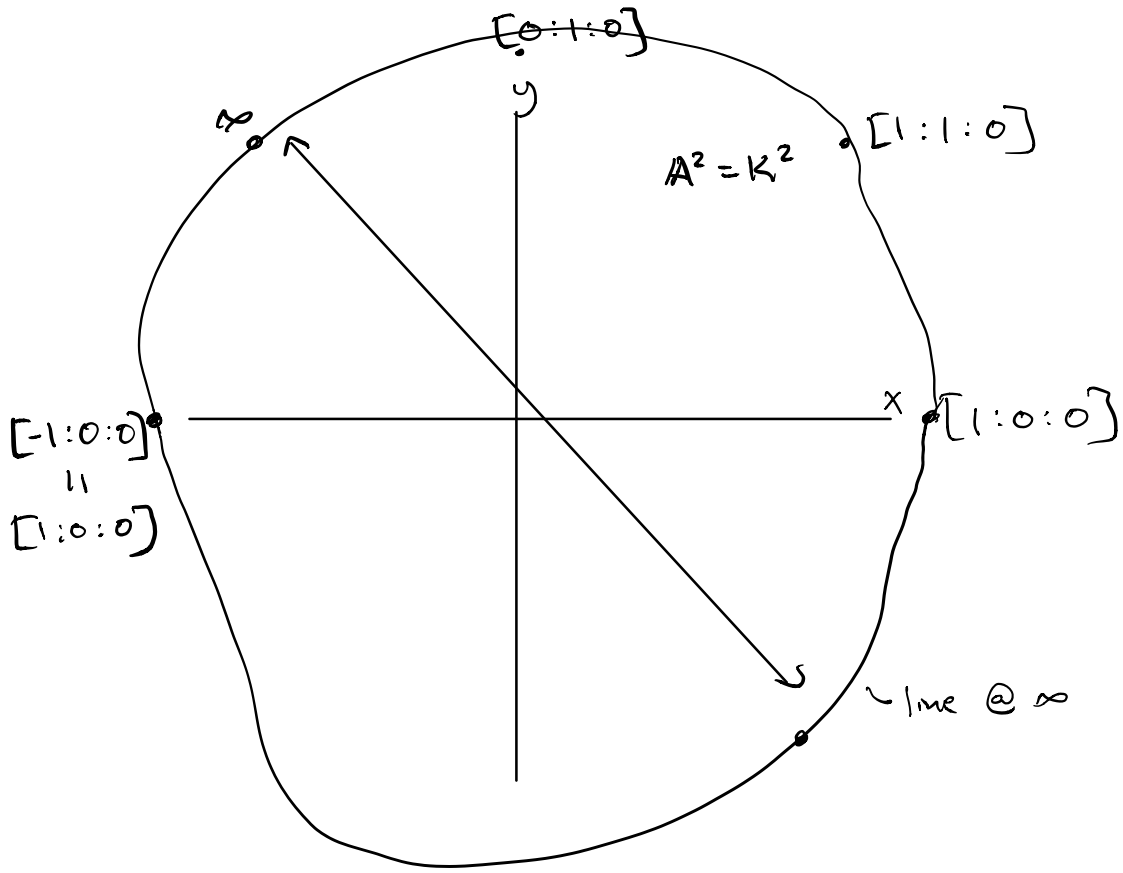
    $\{ [X:Y:Z] \in \mathbb{P}^2 : X+Y-Z = 0 \}$

- $\mathbb{P}^2 = \{ [X:Y:Z] : Z \neq 0 \} \cup \{ [X:Y:Z] : Z = 0 \}$

  $\|?$ $\uparrow$ line

  $\{ (x,y) \in K^2 \}$

  $x = \frac{X}{Z} \quad y = \frac{Y}{Z}$




$V(X+Y-Z)$ $\quad Z = X+Y$

$1 = x+y$

$Z=0$ $\quad 0 = X+Y$

$X = -Y$ $\quad [1:-1:0]$

$=$

$[-1:1:0]$

# Elliptic curves algebro-geometrically

Let $K$ be a field of char $0$, not necessarily algebraically closed.

**Defn** An **elliptic curve** is a projective variety in $\mathbb{P}^2_K$ given by

$E: Y^2Z = X^3 + aXZ^2 + bZ^3$ (in affine $Z=1$ coords. $y^2 = x^3 + ax + b$)

with $4a^3 + 27b^2 \neq 0$.

$E$ is **defined over** $K$ if $a, b \in K \subseteq \bar{K}$.

**Rmk** If $Z=0$, then $X=0$, so the only pt @ $\infty$ on $E$ is $[0:1:0] = \infty$

---

The condition $4a^3 + 27b^2 \neq 0$ is equiv to $E$ being nonsingular. Why?

$f(X,Y,Z) = Y^2Z - X^3 - aXZ^2 - bZ^3$

$P \in \mathbb{P}^2_K$

$P \in E$ and singular $\iff 0 = f(P) = \frac{\partial}{\partial X} f(P) = \frac{\partial}{\partial Y} f(P) = \frac{\partial}{\partial Z} f(P)$.

$\infty$ is never singular: $\frac{\partial}{\partial Z} f \Big|_{\substack{\infty \\ [0:1:0]}} = Y^2 - 2aXZ - 3bZ^2 \Big| = 1$

$$f(x,y) = y^2 - x^3 - ax - b$$

$$\frac{\partial}{\partial x} f = -3x^2 + a = 0 \implies x = \left(\frac{-a}{3}\right)^{1/2}$$

$$\frac{\partial}{\partial y} f = 2y = 0 \implies y = 0$$

$$f(x,y) = 0 \implies -b = \left(\frac{-a}{3}\right)^{3/2} + a\left(\frac{-a}{3}\right)^{1/2}$$

$$b^2 = \left(\frac{-a}{3}\right)^3 + 2a\left(\frac{-a}{3}\right)^2 + a^2\left(\frac{-a}{3}\right)$$

$$b^2 = a^3\left(\frac{-1}{27} + \frac{6}{27} - \frac{9}{27}\right)$$

$$= a^3\left(\frac{-4}{27}\right)$$

$$4a^3 + 27b^2 = 0.$$

Equivalent defn An elliptic curve is a nonsingular projective curve of genus 1, with a given pt.

Two key structures on an elliptic curve:

- Gal action
- Group law

If $E/K$ and $x \in E$, then $\forall \tau \in G_K$, $\tau(x) \in E$.

($E/K$: $E$ is defined over $K$)

So $G_K$ acts on $E$. Note

$x \in E$ is fixed by all $\tau \in G_K \iff x \in E(K)$

$$\left\{ \begin{array}{l} x \in E : x \text{ has} \\ \text{all coords in } K \end{array} \right\} = E(K) \subseteq E$$

Group law

Bezout's theorem implies that a line in $\mathbb{P}^2$ intersects $E$ at exactly 3 points (w/ multiplicity).

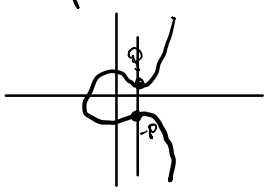
Define an addition law on $E$ with identity $\infty$ via the rule:

if $P, Q, R \in E$ are colinear pts, then

$P + Q + R = 0 (= \infty)$.

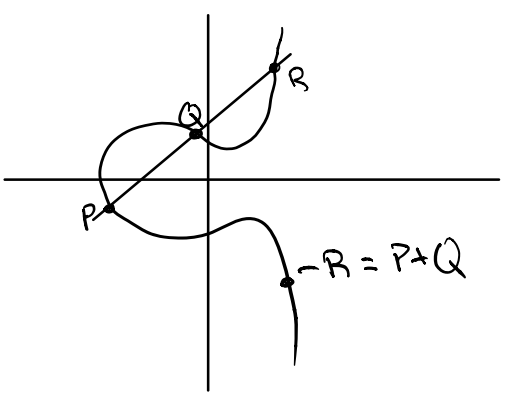
- If $P \in E$ then $-P$ is the third pt. on the line through $P, \infty$

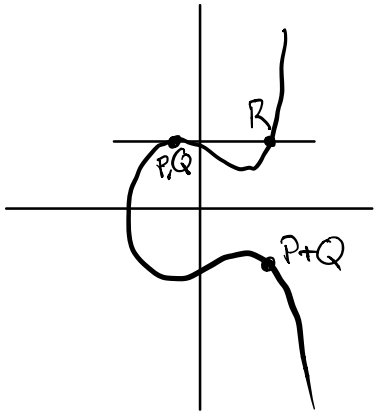
$(P + -P + \infty = P + -P = \infty)$



so $-P$ is obtained by flipping over the $x$-axis.

- If $P, Q \in E$ then $P + Q = -R$ where $R$ is colinear w/ $P, Q$.




**Prop** This group law turns $E$ into an abelian group.

Hard part: $+$ is associative

Later: different perspective on this group law that makes this obvious.

**Prop** If $E/K$, then $E(K) \subseteq E$ is a subgroup.

**Pf.** $E(K)$ clearly closed under inversion $(-)$.

Suffices to check that if $P, Q \in E(K)$ and $\ell$ is the line they span then the third intersection pt of $\ell$ with $E$ is in $E(K)$.

Pf 1: substitute eqn for $\ell$ into eqn for $E$; two roots are in $K$, so the third is too.

Pf 2: $R \in \{P, Q\}$ then we're done. Otherwise

$\forall \sigma \in G_K \quad \sigma(R) \in \ell \cap E$, so $\sigma(R) \in \{P, Q, R\}$.

But $\sigma^{-1}$ fixes $P, Q$, so $\sigma(R) = R$.