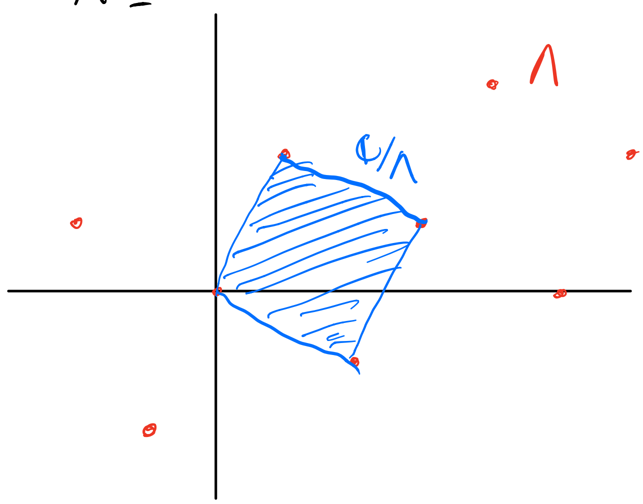
Last time

Elliptic curves a complex tori

$\mathbb{C}/\Lambda \qquad \Lambda \subseteq \mathbb{C}$ lattice



Maps as R.S.'s of complex tori $f: \mathbb{C}/\Lambda \longrightarrow \mathbb{C}/\Lambda'$ all of the form

$$f(z+\Lambda) = mz + b + \Lambda' \qquad m, b \in \mathbb{C}$$

$$f(z) = mz + b \qquad m\Lambda \subseteq \Lambda'$$

Moreover, f is bijective $\Longleftrightarrow m\Lambda = \Lambda'$.

Prop Let $f(z) = mz + b : \mathbb{C}/\Lambda \longrightarrow \mathbb{C}/\Lambda'$.

TFAE:

(1) f is a grp homomorphism

(2) $b \in \Lambda'$

(3) $f(0) = 0$

Pf. (1) $\Rightarrow$ (3) $\Rightarrow$ (2) $\Rightarrow$ (1)

if $b \in \Lambda'$ then

$$f(z+z'+\Lambda) = m(z+z') \cancel{+b} + \Lambda'$$
$$= mz + mz' + \Lambda'$$
$$= f(z+\Lambda) + f(z'+\Lambda) \qquad \square$$

Cor $\mathbb{C}/\Lambda \cong \mathbb{C}/\Lambda'$ as grps + R.S.'s (complex Lie grps)

$\iff \exists m \in \mathbb{C}^\times$ s.t. $m\Lambda = \Lambda'$.

$$\{\text{elliptic curves}\}/\text{isomorphism} \longleftrightarrow \{\text{lattices } \Lambda \subseteq \mathbb{C}\}/\text{homothety}$$

Defn Λ and Λ' are homothetic if $\exists \lambda \in \mathbb{C}^\times$ s.t. $\lambda\Lambda = \Lambda'$.

In particular, any lattice $\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ can be scaled to $\Lambda = \frac{\omega_1}{\omega_2}\mathbb{Z} + 1\mathbb{Z}$ with $\tau = \frac{\omega_1}{\omega_2} \in \mathcal{H}$.

But some distinct $\tau \in \mathcal{H}$ might determine the same lattice

$$\Lambda_\tau = \tau\mathbb{Z} + 1\mathbb{Z} = \tau'\mathbb{Z} + 1\mathbb{Z} = \Lambda_{\tau'}.$$

Prop Let $\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$, $\Lambda' = \omega_1'\mathbb{Z} + \omega_2'\mathbb{Z}$ with $\frac{\omega_1}{\omega_2}, \frac{\omega_1'}{\omega_2'} \in \mathcal{H}$.

Then $\Lambda = \Lambda' \iff \begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix} = \gamma \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}$ for some $\gamma \in SL_2(\mathbb{Z})$.

Pf. ($\Rightarrow$) Since $\omega_1', \omega_2' \in \Lambda$, we have

$$\begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix} = \gamma \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} \quad \gamma \in M_2(\mathbb{Z}).$$

Symmetrically, $\begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = \gamma' \begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix} \quad \gamma' \in M_2(\mathbb{Z})$

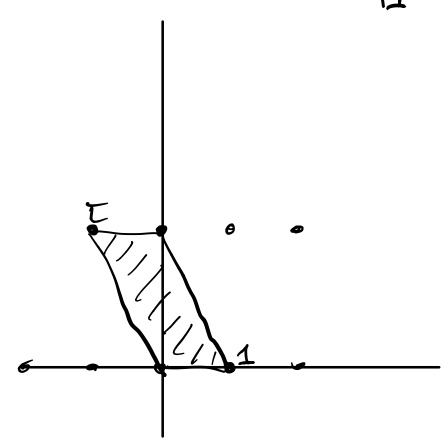
So $\begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = \gamma'\gamma \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}$ and $\{\omega_1, \omega_2\}$ is a basis,

so γ is invertible w/ $\gamma^{-1} \in M_2(\mathbb{Z})$.

$\det \gamma \in \mathbb{Z}^\times = \{\pm 1\}$.

Then $\det \gamma = 1$ because γ is orientation-preserving.

($\Leftarrow$) Run this in reverse. $\square$



Let $\Lambda_\tau = \tau\mathbb{Z} + 1\mathbb{Z}$, $\Lambda_{\tau'}$.

$$\mathbb{C}/\Lambda_\tau \cong \mathbb{C}/\Lambda_{\tau'} \iff \Lambda_\tau \text{ is homothetic to } \Lambda_\tau$$

$$\iff \exists \lambda \in \mathbb{C}^\times,\ \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \text{ s.t.}$$

$$\begin{pmatrix} \tau' \\ 1 \end{pmatrix} = \lambda\, \gamma \begin{pmatrix} \tau \\ 1 \end{pmatrix} = \lambda \begin{pmatrix} a\tau + b \\ c\tau + d \end{pmatrix}$$

$$\iff \begin{pmatrix} \tau' \\ 1 \end{pmatrix} = \begin{pmatrix} (a\tau+b)/(c\tau+d) \\ 1 \end{pmatrix}$$

$$\iff \tau' = \frac{a\tau+b}{c\tau+d} \quad \text{some } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}).$$

<u>Recall</u> Action of $SL_2(\mathbb{Z})$ on $\mathcal{H}$:

$$\gamma\tau = \frac{a\tau+b}{c\tau+d} \quad \text{for} \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}).$$

<u>Prop</u> $\mathbb{C}/\Lambda_\tau \cong \mathbb{C}/\Lambda_{\tau'} \iff \tau' = \gamma\tau$ some $\gamma \in SL_2(\mathbb{Z})$.

In other words,

$$\{\text{elliptic curves}\}/_{\text{isom.}} \longleftrightarrow \mathcal{H}/SL_2(\mathbb{Z}).$$

This is an example of a <u>moduli space</u> of elliptic curves, or a <u>modular curve</u>.

Monday's lecture: Possible topics:

- Representable functors.
- Weierstrass $\wp$-function (CJ) ✓

<u>Defn</u> An <u>isogeny</u> of complex tori is a

<u>nonzero</u> holomorphic homomorphic map.

If $\varphi : \mathbb{C}/\Lambda \longrightarrow \mathbb{C}/\Lambda'$ is an isogeny then

$$\varphi(z) = mz \qquad m \in \mathbb{C}^\times \qquad m\Lambda \subseteq \Lambda'.$$

Define $\deg \varphi = \# \operatorname{Ker} \varphi = \# \varphi^{-1}(\{a\})$ any $a \in \mathbb{C}/\Lambda'$.

<u>Ex.</u> Let $0 \neq N \in \mathbb{Z}$. We have a mult-by-N map

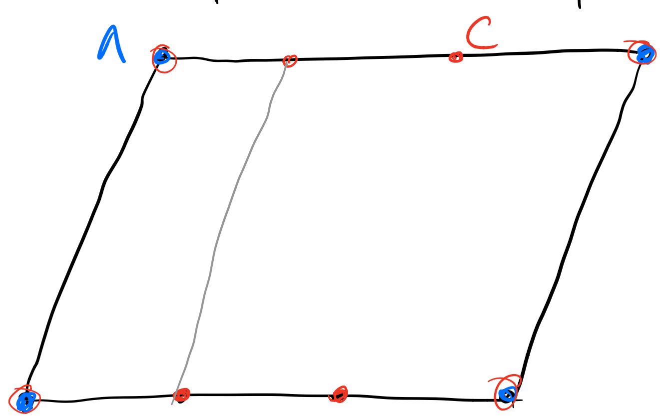
$$[N] : \mathbb{C}/\Lambda \longrightarrow \mathbb{C}/\Lambda.$$

$$\ker [N] = (\mathbb{Z}/N\mathbb{Z})^2$$

If E is an ell. curve, write $E[N] = \ker [N]$.

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

<u>Ex.</u> Let $C \subseteq E[N]$ be a cyclic subgp of order N. C corresponds to a superlattice $C \supseteq \Lambda$

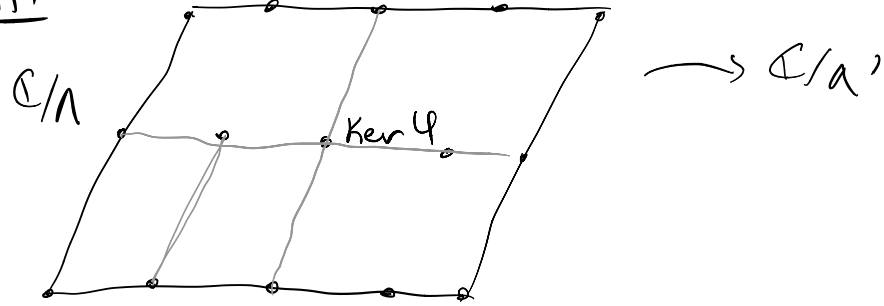


get a quotient map $\mathbb{C}/\Lambda \to \mathbb{C}/C$ with kernel C.

In fact, these examples cover all isogenies

<u>Prop</u> Every $\varphi : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ factors as a composition of these.

<u>Pf.</u>



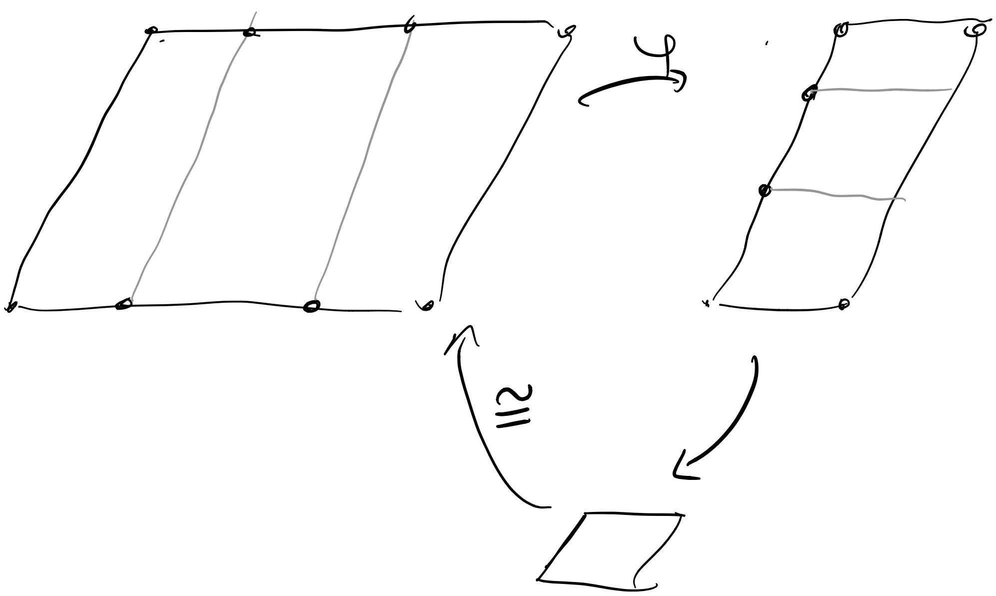
$\square$

Let $C \subset E[N]$ be a cyclic subgp of order N.
let $\varphi : \mathbb{C}/\Lambda \longrightarrow \mathbb{C}/C$.

We can pick a complementary C' s.t.

$$C \oplus C' = E[N].$$

$$\begin{tikzcd}
\mathbb{C}/\Lambda \arrow[r, "\varphi"] & \mathbb{C}/C \arrow[r] \arrow[rrr, bend right, "\hat{\varphi}"'] & \mathbb{C}/C\oplus C' = \mathbb{C}/E[N] \arrow[rr, "\cdot N", "\sim"'] & & \mathbb{C}/\Lambda
\end{tikzcd}$$



<u>Prop</u> If $\varphi : E \longrightarrow E/C$ then $\exists \hat{\varphi} : E/C \longrightarrow E$

s.t. $\hat{\varphi} \circ \varphi = [\deg \varphi]$.

Prop If $\varphi : E \to E'$ is <u>any</u> isogeny then $\exists\, \hat{\varphi} : E' \to E$ (<u>dual isogeny</u>) s.t.

$$\hat{\varphi} \circ \varphi = [\deg \varphi].$$

The Tate Module

Let $E = \mathbb{C}/\Lambda$ be a cmplx torus, ℓ a prime.

$E[\ell^n] = (\mathbb{Z}/\ell^n\mathbb{Z})^2 \quad \forall n \geq 1.$

$$\begin{array}{ccccccc} \cdots \longrightarrow & E[\ell^3] & \xrightarrow{[\ell]} & E[\ell^2] & \xrightarrow{[\ell]} & E[\ell] \\ & \circlearrowright & & \circlearrowright & & \circlearrowright \\ \cdots \longrightarrow & \mathbb{Z}/\ell^3\mathbb{Z} & \longrightarrow & \mathbb{Z}/\ell^2\mathbb{Z} & \longrightarrow & \mathbb{Z}/\ell\mathbb{Z} \end{array}$$

Thus $T_\ell E = \varprojlim_{n \geq 1} E[\ell^n]$ is a free rk 2 $\mathbb{Z}_\ell$-module.

called the <u>Tate Module</u>.

Let $V_\ell E = T_\ell E \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$.

Want: compatible actions of $G_{\mathbb{Q}}$ on $E[\ell^n]$

$\Rightarrow$ action of $G_{\mathbb{Q}}$ ~~on~~ $T_\ell E$, $V_\ell E$, so

$V_\ell E$ is a 2-dim'l ℓ-adic Gal. rep.