Last time

Let X be a cmpct R.S, $\mathbb{C}(X)$ field of mero fns on X.

Divisors on X: $D = \sum_{x \in X} n_x \, (x) \in \mathrm{Div}(X)$

$\deg(D) = \sum n_x$, $\mathrm{Div}^0(X)$

$f \in \mathbb{C}(X)^\times$, then $\mathrm{div}(f) = \sum \mathrm{ord}_x f \; (x) \in \mathrm{Div}^0(X)$ (principal divisors)

$\mathrm{Pic}(X) = \mathrm{Div}(X) / \text{principal divisors}$

Differentials on X: df, $f \in \mathbb{C}(X)^\times$

If z is a local coordinate at $x \in X$, then any $\omega \in \Omega'_x$

$\omega = f\,dz$ some $f \in \mathbb{C}(X)$, $\mathrm{ord}_x(\omega) = \mathrm{ord}_x(f)$.

$\mathrm{div}(\omega) = \sum_x \mathrm{ord}_x(\omega) \; (x)$.

Prop If $0 \neq \omega, \omega' \in \Omega'(X)$ then $\omega = f\omega'$ for some $f \in \mathbb{C}(X)^\times$.

(In other words $\dim_{\mathbb{C}(X)} \Omega'(X) = 1$).

Cor $\mathrm{div}(\omega) \in \mathrm{Pic}(X)$ is well-defined, indep of choice of $\omega \in \Omega'(X)$.

Defn $K_X = \mathrm{div}(\omega) \in \mathrm{Pic}(X)$ is the canonical class.

Linear systems + Riemann-Roch

Defn

(1) If $D_1 = \sum m_x (x)$, $D_2 = \sum n_x (x) \in \mathrm{Div}(X)$, we write $D_1 \geq D_2$ if $m_x \geq n_x$ $\forall x \in X$.

(2) If $D \in \mathrm{Div}(X)$, let

$$\mathcal{L}(D) = \{ f \in \mathbb{C}(X)^\times : \mathrm{div}(f) \geq -D \} \cup \{0\}.$$

This $\mathbb{C}$-vector space is the <u>linear system of D</u>.

(3) Write $\ell(D) = \dim_{\mathbb{C}} \mathcal{L}(D)$.

Ex. $D = (0) - (1) \in \mathrm{Div}(\mathbb{P}^1)$, then

$0 \neq f \in \mathcal{L}(D) \iff \mathrm{div}(f) \geq -(0) + (1)$

$\iff$ f has a zero at $1 \in \mathbb{P}^1$, at most a simple pole at 0, no other poles

$\iff$ f has a zero at 1, a simple pole at 0, no other poles

$\iff f = \lambda \dfrac{z-1}{z}$ some $\lambda \in \mathbb{C}^\times$

So $\ell(D) = 1$.

Prop

(1) If $\deg D < 0$ then $\ell(D) = 0$.

(2) $\ell(D) < \infty$ $\quad \forall D \in \mathrm{Div}(X)$.

(3) If $D = D'$ in $\mathrm{Pic}(X)$ then

$$\mathcal{L}(D) \cong \mathcal{L}(D').$$

Pf.

(1) If $f \neq 0$ then $\deg \mathrm{div}(f) = 0$. But $\deg(-D) > 0$,

so $\quad \mathrm{div}(f) \not\geq -D$.

(2) Done for $\deg D < 0$. Proof by induction on $\deg D \geq 0$.

If $\deg D = 0$, if $\mathrm{div}(f) \geq -D$ then $\mathrm{div}(f) = -D$.

If $0 \neq f, g \in \mathcal{L}(D)$ then

$$\mathrm{div}\left(\frac{f}{g}\right) = 0, \quad \text{so} \quad \frac{f}{g} \in \mathbb{C}^\times. \quad \text{Hence } \ell(D) \leq 1.$$

Suppose true for $\deg D = n$. Let

$D = D' + (x)$ have degree $n+1$.

$$\underset{(n_x+1)(x) + (*)}{\overset{\shortparallel}{D}}$$

$D' = n_x(x) + (*)$.

Note that $\mathcal{L}(D') \subseteq \mathcal{L}(D)$. Suppose

$0 \neq f, g \in \mathcal{L}(D) \setminus \mathcal{L}(D')$. Then

$$\mathrm{ord}_x(f) = \mathrm{ord}_x(g) = n_x.$$

Hence, $\quad f - cg \in \mathcal{L}(D')$ for some $c \in \mathbb{C}$.

Thus, $\ell(D) \leq \ell(D') + 1$.

(Note: we've shown $\ell(D) \leq \deg D + 1$.)

(3) Let $D = D' + \mathrm{div}(f)$. Define

$$\mathcal{L}(D) \longrightarrow \mathcal{L}(D')$$
$$g \longmapsto fg$$

$$\mathrm{div}(g) \geq -D \iff \mathrm{div}(fg) \geq \mathrm{div}(f) - D = -D'$$

so this map is an iso. $\square$

Thm (Riemann-Roch)

Let X be a cmpt R.S. of genus g. Then $\forall D \in \mathrm{Div}(X)$,

$$\ell(D) - \ell(K_X - D) = \deg D - g + 1.$$

Ex.

(1) $D = 0 \implies \underbrace{\ell(0)}_{1} - \ell(K_X) = -g + 1$

$$\implies \ell(K_X) = g$$

(This is one way of defining the genus)

(2) $D = K_X \implies \ell(K_X) - \ell(0) = \deg K_X - g + 1$

$$g - 1 = \deg K_X - g + 1$$
$$\deg K_X = 2g - 2.$$

(3) $X = \mathbb{P}^1$: $\quad K_X = \mathrm{div}(dx) = -2(\infty)$

$X = E$: $\quad K_X = \mathrm{div}(dz) = 0$

(4) On pset: if $P, Q \in E$ then
$(P) = (Q)$ in $\mathrm{Pic}(X) \Longleftrightarrow P = Q$.

Pf.

If $(P) = (Q) + \mathrm{div}(f)$ some $f \in \mathbb{C}(E)$, then $f \in \mathcal{L}((Q))$.

$$\ell((Q)) - \ell(0 - (Q)) = \deg(Q) - 1 + 1$$
$$\ell(Q) - 0 = 1$$

But $\mathbb{C} \subseteq \mathcal{L}((Q))$, so $f \in \mathbb{C}$.

Thus

$(P) = (Q) + 0 \Longrightarrow P = Q$. $\square$

Rmk We will use Riemann-Roch theorem to compute dimensions of spaces of mod forms. To what R.S.'s?

Modular curves

Recall: The space $SL_2(\mathbb{Z}) \backslash \mathcal{H} = \{ SL_2(\mathbb{Z}) \tau : \tau \in \mathcal{H} \}$

classifies ell. curves up to isomorphism.

$$SL_2(\mathbb{Z}) \backslash \mathcal{H} \longrightarrow \{ \text{ell. curves} \} / \text{iso}.$$
$$\tau \longmapsto E_\tau = \mathbb{C} / \Lambda_\tau = \mathbb{C} / \tau\mathbb{Z} + \mathbb{Z}$$

Defn For $N \geq 1$ let ...

(1)
$$S_0(N) = \frac{\left\{ (E,C) \;:\; \begin{array}{l} E \text{ ell. curve} \\ C \leq E[N] \text{ cyclic subgp} \\ \text{of order } N \end{array} \right\}}{\begin{array}{l} (E,C) \sim (E',C') \text{ if } \exists \varphi : E \xrightarrow{\sim} E' \\ \qquad \varphi(C) = C' \end{array}}$$

$$\Gamma_0(N) = \left\{ \gamma \in SL_2(\mathbb{Z}) \;:\; \gamma \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod N \right\} \leq SL_2(\mathbb{Z})$$

(2)
$$S_1(N) = \frac{\left\{ (E,Q) \;:\; \begin{array}{l} E \text{ ell curve} \\ Q \in E[N] \text{ of order } N \end{array} \right\}}{\begin{array}{l} (E,Q) \sim (E',Q') \text{ if } \exists \varphi : E \xrightarrow{\sim} E' \\ \qquad \varphi(Q) = Q' \end{array}}$$

$$\Gamma_1(N) = \left\{ \gamma \in SL_2(\mathbb{Z}) \;:\; \gamma \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod N \right\}$$

(3)
$$S(N) = \frac{\left\{ (E,P,Q) \;:\; \begin{array}{l} E \text{ ell curve} \\ P,Q \text{ basis for } E[N] \\ \text{with } e_N(P,Q) = e^{2\pi i/N} \end{array} \right\}}{\begin{array}{l} (E,P,Q) \sim (E',P',Q') \text{ if } \exists \varphi : E \xrightarrow{\sim} E' \\ \qquad \varphi(P) = P',\ \varphi(Q) = Q' \end{array}}$$

$$\Gamma(N) = \left\{ \gamma \in SL_2(\mathbb{Z}) \;:\; \gamma \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod N \right\}$$

Q. Which of these has "most" structure? "least" structure?

A:

$$S_0(N) \longleftarrow S_1(N) \longleftarrow S(N)$$

$$\Gamma_0(N) \supseteq \Gamma_1(N) \supseteq \Gamma(N)$$

Rmk. When $N=1$, $S_0(N) = S_1(N) = S(N) = \{\text{ell. curves}\}/_{\text{iso}}$

$$\Gamma_0(N) = \Gamma_1(N) = \Gamma(N) = SL_2(\mathbb{Z}).$$

Prop We have bijections

$$\Gamma_0(N)\backslash\mathcal{H} \longrightarrow S_0(N)$$
$$\tau \longmapsto (E_\tau, \langle \tfrac{1}{N} \rangle)$$

$$\Gamma_1(N)\backslash\mathcal{H} \longrightarrow S_1(N)$$
$$\tau \longmapsto (E_\tau, \tfrac{1}{N})$$

$$\Gamma(N)\backslash\mathcal{H} \longrightarrow S(N)$$
$$\tau \longmapsto (E_\tau, \tfrac{\tau}{N}, \tfrac{1}{N})$$

Pf. (for $\Gamma_1(N)$).

Well-defined: Suppose $\tau' = \gamma\tau$ some $\gamma \in \Gamma_1(N)$. Then

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod N$$

$$\varphi : E_{\tau'} \longrightarrow E_\tau$$

$$z \longmapsto (c\tau + d)z$$

$$\frac{1}{N} \longmapsto \frac{c\tau}{N} + \frac{d}{N} + \Lambda_\tau = \frac{1}{N} + \Lambda_\tau$$

(If merely $\gamma \in \Gamma_0(N)$, then $\frac{1}{N} \mapsto \frac{d}{N}$ where $(d,N)=1$.
Hence, $\langle \frac{1}{N} \rangle = \langle \frac{d}{N} \rangle \subseteq E_\tau[N]$.)

Injective: suppose that

$$\varphi : E_{\tau'} \xrightarrow{\sim} E_\tau$$

$$\frac{1}{N} \longmapsto \frac{1}{N}$$

φ is mult by $c\tau + d$ some $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ s.t. $\tau' = \gamma\tau$.

$$\varphi\left(\frac{1}{N}\right) = \frac{c\tau}{N} + \frac{d}{N} = \frac{1}{N} \pmod{\Lambda_\tau}$$

so $N \mid c$, $d \equiv 1 \pmod N$, so $\gamma \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod N$.

(If merely $\langle \varphi(\frac{1}{N}) \rangle = \langle \frac{1}{N} \rangle$ then
$\varphi(\frac{1}{N}) = \frac{c\tau}{N} + \frac{d}{N} \mod \Lambda_\tau$ generates $\langle \frac{1}{N} \rangle$, so

$N \mid c$ and $(d,N)=1$, hence $\gamma \in \Gamma_0(N)$.)

Surjective: Let $(E,Q) \in S_1(N)$. Know $E = E_\tau$ some $\tau \in \mathcal{H}$.
So $Q = \frac{c\tau + d}{N}$ for $\gcd(c,d,N) = 1$.
Hence $\exists\, a,b \in \mathbb{Z}/N\mathbb{Z}$ s.t. $ad - bc \equiv 1 \pmod N$.

Ex. $SL_2(\mathbb{Z}) \longrightarrow SL_2(\mathbb{Z}/N\mathbb{Z})$, reduction mod N, is surjective.

Thus, let $\gamma \in SL_2(\mathbb{Z})$ s.t. $\gamma \equiv \begin{pmatrix} a & b \\ c & d \end{pmatrix} \pmod N$.

Let $\tau' = \gamma\tau = \frac{a\tau + b}{c\tau + d}$. Then

$$\begin{aligned} \varphi : E_{\tau'} &\longrightarrow E_\tau \\ z &\longmapsto (c\tau + d) z \\ \tfrac{1}{N} &\longmapsto \frac{c\tau + d}{N} = Q \end{aligned}$$

so $E_{\tau'} = E_\tau \in S_1(N)$ is in the image of
$\mathcal{H} \longrightarrow S_1(N)$.

(Also proves surjectivity for $S_0(N)$). $\square$