Modular Forms (by Eyal Goren)

• Sphere Packing

Consider the problem of packing "spheres" (solid balls) of radius r, in $\mathbb{R}^n$. So $\mathbb{R}^n \supseteq \coprod_{\alpha}' S_\alpha$, S_α = ball of radius r, the $'$ means "allow intersection only on boundary".

Define the density as $\lim\limits_{N\to\infty} \dfrac{\mathrm{vol}(\coprod' S_\alpha \cap [-N,N]^n)}{\mathrm{vol}([-N,N]^n)}$.

To have it always defined, we can look at lim sup or lim inf.

This is <u>too hard</u>!

Therefore, consider lattice packing:

• Lattices:

<u>Def</u>: $L \subseteq \mathbb{R}^n$ is a <u>(full) lattice</u> if it is a <u>discrete</u> subgroup of $\mathbb{R}^n$ that contains a basis (of $\mathbb{R}^n$).

(<u>Discrete</u>: A ball around 0 contains only finitely-many points of L $\overset{\text{exercise}}{\equiv}$ <u>any</u> ball...)

<u>Equivalently</u>, L is of rank n (as an abelian group) and contains a basis of $\mathbb{R}^n$.

<u>Exercise 1</u>: Prove these equivalences.

<u>Example</u>: $L = \mathbb{Z}^n \subseteq \mathbb{R}^n$

<u>Example</u>: $d \in \mathbb{Z}$, $d > 0$ squarefree. Consider $K = \mathbb{Q}(\sqrt{-d})$, and $\mathcal{O}_K$ its ring of int.

So $\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{-d}] & -d \equiv 2,3 \pmod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{-d}}{2}\right] & -d \equiv 1 \pmod 4 \end{cases}$ $\Rightarrow \mathcal{O}_K \cong \mathbb{Z} \oplus \mathbb{Z}\delta$

$\delta = \sqrt{-d}$ or $\frac{1+\sqrt{-d}}{2}$

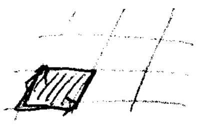
(cont example)
Choose some $\sqrt{-d} \in \mathbb{C}$. Then $L \subseteq \mathbb{C} \cong \mathbb{R}^2$ by $x+iy \mapsto (x,y)^T$

Then L is spanned by $1, \delta$, i.e. by $\begin{pmatrix}1\\0\end{pmatrix}$ and $\begin{cases}\begin{pmatrix}0\\\sqrt{d}\end{pmatrix}\\ \begin{pmatrix}\frac{1}{2}\\ \sqrt{d}/2\end{pmatrix}\end{cases}$

<u>Def (Fundamental parallelotope of L)</u>:

Let $l_1, \dots, l_n$ be a basis for L over $\mathbb{Z}$

Then a fund. parallelotope P for L would be $P := \left\{ \sum_{i=1}^{n} a_i l_i \mid 0 \leq \underset{\mathbb{R}}{a_i} \leq 1 \ \forall i \right\}$



or many other choices!!
(depends on the chosen basis).

The volume of P is $|\det(l_1 | \cdots | l_n)|$.

The matrix $M = (l_1 | \cdots | l_n)$ is called a <u>generator matrix</u> for L

So that $L = \left\{ M \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} : \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \in \mathbb{Z}^n \right\}$.

Any other basis for L has the form $M \cdot B$, $B \in GL_n(\mathbb{Z})$

$\Rightarrow \operatorname{vol}(P)$ is <u>independent</u> of the choice of basis (as $|\det(B)| = 1$).

- <u>The Gram matrix of L</u>

It is $A := {}^tM \cdot M = (l_i \overset{\text{inner product}}{\cdot} l_j)_{i,j}$

- The <u>determinant</u> of L is defined as $\det(A) = \det({}^tM \cdot M) = (\det M)^2 = \operatorname{vol}(P)^2$.

<u>Example</u>: $L = \mathbb{Z}^n$, $M = I_n$. Then $\det(L) = 1$. (and $A = M$).

- $M = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{d} \end{pmatrix}$. $A = \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix}$ and $\det(L) = d$ (sic!)
- $M = \begin{pmatrix} 1 & \frac{1}{2} \\ 0 & \frac{\sqrt{d}}{2} \end{pmatrix}$ $A = \begin{pmatrix} 1 & 1/2 \\ 1/2 & \frac{1+d}{4} \end{pmatrix}$ and $\det(L) = \frac{d}{4}$

Def The <u>dual lattice</u> of a lattice L, written $L^\vee$ is

$$L^\vee = \{ \ell \in \mathbb{R}^n \mid \ell\cdot\ell' \in \mathbb{Z} \ \forall \ell' \in L \} = \{ \ell \in \mathbb{R}^n \mid \ell \cdot \underset{\text{elts. of basis for } L}{\ell_i} \in \mathbb{Z} \ \forall i = 1..n \}$$

Let $\ell_1^*, \dots, \ell_n^*$ be the basis of $(\mathbb{R}^n)^*$ dual to $\ell_1, \dots, \ell_n$

(so that $\ell_i^* \cdot \ell_j = \delta_{ij}$), then each $\ell_i^* \in L^\vee$.

Also, if $\ell \in L^\vee$ and $\ell \cdot \ell_i = \alpha_i \in \mathbb{Z}$, then $\ell = \sum \alpha_i \ell_i^*$.

So $L^\vee = \mathbb{Z}\ell_1^* \oplus \dots \oplus \mathbb{Z}\ell_n^*$ (direct sum b/c $\ell_1^*, \dots, \ell_n^*$ are l. indep).

Also, $\begin{pmatrix} {}^t\ell_1^* \\ \vdots \\ {}^t\ell_n^* \end{pmatrix} \left(\ell_1 | \cdots | \ell_n \right) = I_n \Rightarrow \left(\ell_1^* | \cdots | \ell_n^* \right) = {}^tM^{-1}$

<u>So</u>: the generator matrix of the dual lattice is ${}^tM^{-1}$.

Def A lattice L is <u>integral</u> if $L^\vee \supseteq L$.

<u>equiv</u>: if $\forall \ell \in L, \forall \ell' \in L$, $\ell \cdot \ell' \in \mathbb{Z}$

<u>Exercise 2</u>: L is integral $\Leftrightarrow$ its gram matrix A has integer coefficients.

Def: L is <u>unimodular</u> if $L^\vee = L$.

L is <u>even</u> (or of type II) if it is unimodular and $\ell\cdot\ell \in 2\mathbb{Z}$ $\forall \ell \in L$ ($\Leftrightarrow$ diagonal entries of A are even)

L is <u>odd</u> (or of type I) if it is not even. ☺

<u>Example</u>: $L = \mathbb{Z}^n$ is odd unimodular.

Example ($\mathbb{Q}(\sqrt{-d}) = K$, $\mathcal{O}_K$ ..)

Suppose that L has gen. matrix M. So $L^\vee$ has gen. matrix ${}^tM^{-1}$.

We can always write $M = {}^tM^{-1} \cdot N$, $N \in GL_n(\mathbb{R})$.

So L unimodular $\Leftrightarrow N \in GL_n(\mathbb{Z}) \Leftrightarrow N = {}^tM \cdot M = A \in GL_n(\mathbb{Z})$.

For $M = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{d} \end{pmatrix}$, $L^\vee$ has gen. matrix $\begin{pmatrix} 1 & 0 \\ 0 & \frac{1}{\sqrt{d}} \end{pmatrix} = {}^tM^{-1}$

$$\begin{pmatrix} 1 & 0 \\ 0 & \frac{1}{\sqrt{d}} \end{pmatrix} \underbrace{\begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix}}_{N} = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{d} \end{pmatrix} \Rightarrow L \text{ is integral but not unimodular.}$$

(unless $\mathbb{Q}(\sqrt{-d}) = \mathbb{Q}(i)$!)

For $M = \begin{pmatrix} 1 & \frac{1}{2} \\ 0 & \frac{\sqrt{d}}{2} \end{pmatrix} \Rightarrow L^\vee$ has ${}^tM^{-1} = \begin{pmatrix} 1 & 0 \\ \frac{-1}{\sqrt{d}} & \frac{2}{\sqrt{d}} \end{pmatrix}$, $N = \begin{pmatrix} 1 & 1/2 \\ 1/2 & \frac{1+d}{4} \end{pmatrix}$ not integral!

Assume that L is integral. We are interested in the index of $L \subseteq L^\vee$.

$$[L^\vee : L] = \frac{\mathrm{vol}(P_L)}{\mathrm{vol}(P_{L^\vee})} = \frac{|\det(M)|}{|\det({}^tM^{-1})|} = \det(M)^2 = \det(L).$$

So the finite group $L^\vee/L$ (called the discriminant group) has order $\det(L)$.

- Lattice packing.

Def (packing radius of L, $\rho(L)$): $2\rho(L)$ = minimal length of a non-zero vector in L.

A lattice induces a lattice packing: $\bigsqcup_{\ell \in L}' (\ell + S(\rho(L)))$ sphere ball of radius $\rho(L)$ around 0

$$\mathrm{vol}(S(1)) = \begin{cases} \dfrac{\pi^{n/2}}{(n/2)!} & n \text{ even} \\[2ex] \dfrac{2^n \pi^{\frac{n-1}{2}} \left(\frac{n-1}{2}\right)!}{n!} & n \text{ odd.} \end{cases}$$

n	$\mathrm{vol}(S(1))$
1	2
2	π
3	$4\pi/3$
4	$\pi^2/2$

The density of the packing can be computed, and turns out to be:

$$\Delta(L) = \frac{vol(S(\rho(L)))}{vol(P_L)} = \frac{\rho(L)^n}{\sqrt{|A|}} \cdot vol(\rho(S(1)))$$

Up to scalar factor, we can disregard $vol(\rho(S(1)))$, and define the center density: $\delta(L) = \dfrac{\rho(L)^n}{\sqrt{|A|}}$.

To an integral lattice L we can associate a theta function:

$$\Theta_L(z) = \sum_{l \in L} e^{\pi i z\, l \cdot l} = \sum_{n=0}^{\infty} r_L(n)\, e^{\pi i n z} \quad ; \quad r_L(n) = \#\{l \in L : l \cdot l = n\}$$

Let $q = e^{2\pi i z}$. Then $\Theta_L(z) = \sum_{n \geq 0}^{\infty} r_L(n)\, q^{n/2}$ (everything formal, for now).

Rk: Θ_L depends only on A:

if $l = M \cdot x$, then $l \cdot l = x^t M^t M x = x^t A x =: A[x]$

So one can rewrite $\Theta_L(z) = \sum_{x \in \mathbb{Z}^n} q^{\frac{1}{2}A[x]} = \sum_{n=0}^{\infty} r_A(n)\, q^{n/2}$, $r_A(n) = \#\{x \in \mathbb{Z}^n : A[x] = n\}$

Note that $r_A(n) = \#$ times that the integral quadratic form $\sum a_{ij} x_i x_j$ represents n.

Write $\Theta_L(q) = 1 + \tau(L)\, q^{2\rho(L)^2} + h.o.t.$

where $\tau(L) = \#$ of nonzero vectors of L having the minimal length $2\rho(L)$ (also called the "kissing number": $\#$ spheres touching the one centered at the origin).

Example: $L = \mathbb{Z}^n \subseteq \mathbb{R}^n$. $M = I_n = A$, $x_1^2 + x_2^2 + \dots + x_n^2$, $\det(L) = \det(A) = 1$; $vol(P_L) = 1$; $\rho(L) = \frac{1}{2}$

$\Theta_L(q) = \sum_{m=0}^{\infty} r(m)\, q^{m/2}$ where $r(m) = \#$ reps of m as the sum of n squares.

Also, $\delta(L) = \dfrac{(\frac{1}{2})^n}{1} = \dfrac{1}{2^n}$, $\tau(L) = 2 \cdot n$

A little table:

n	1	2	...	8	...	24
$\delta(\mathbb{Z}^n)$	1	1/4	...	≈ 0.0039	...	$\approx 5.96\times 10^{-8}$
$\tau(\mathbb{Z}^n)$	2	4	...	16	...	48

Exercise 3: Prove that the densest lattice packing in $\mathbb{R}^2$ is the hexagonal packing: associated with the lattice $\mathbb{Z}[\omega]$, $\omega = \frac{1+\sqrt{-3}}{2}$

Prove that $\Delta(L) = \frac{\pi}{2\sqrt{3}} \approx 0.9068\ldots$

$\delta(L) = \frac{1}{2\sqrt{3}} > 1/4$ $0.28868\ldots$

$\tau(L) = 6$ $(\rho(L) = 1/2)$.

Reading: Hales, "Cannonballs and honeycombs", Notices AMS 47, no. 4 April 2000.

Sphere packing problem was put by Sir Walter Rayley to Thomas Harriot in the late 1590's (packing cannonballs in a ship). Harriot put it to Johannes Kepler, who published it as a conjecture in "The six-cornered snowflake" (1611).

- How to construct lattices?
  - * root lattices (related to Lie groups and repn theory).
  - * laminated lattices (inspired by 3-dim'l fcc packing, looking as layers of hexagonal packing)
  - * Codes ("construction A")
  - * Mordell-Weil lattices: $E(\mathbb{Q})/E(\mathbb{Q})_{tors}$ is a lattice with norm = canonical height.

  (Elkies constructed the Leech lattice from an elliptic curve over function field.

- Laminated Lattices (following Conway-Sloan, chapter 6)

Idea: construct lattices by an inductive procedure on the dimension.

Define $\Lambda_1 = 2\mathbb{Z}$, a lattice of minimal norm 2 $(\rho(\Lambda_1) = 1)$.

Define now inductively Λ_n (n^{th} laminated lattice):

take all lattices of dimension n, containing Λ_{n-1} (say, via the embedding $\mathbb{R}^{n-1} \to \mathbb{R}^n$, $x \mapsto (x,0)$) having minimal norm 2 and such that lattice $\cap \mathbb{R}^{n-1} \cong \Lambda_{n-1}$.

Among those, choose the ones having minimal determinant (so to optimize density).

Then $\delta(\Lambda_n) = \frac{1}{\sqrt{|A_n|}}$ where A_n = Gram matrix of Λ_n.

Rk: in general, Λ_n is not unique.

Constructing Λ_2: ($\Lambda_1 = 2\mathbb{Z}$).

Suppose $\begin{pmatrix} 2 & a \\ 0 & b \end{pmatrix}$ is a generator matrix for Λ_2. $\|(a,b)\|^2 = a^2+b^2$.

Can always modify a by $2\mathbb{Z}$ to get $-1 \leq a \leq 1$

For such a, we want $a^2+b^2 \geq 4$

and then to minimize $\left|\det\begin{pmatrix} 2 & a \\ 0 & b \end{pmatrix}\right| = 2b$

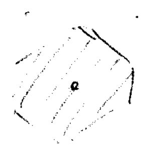
in this way, any element of the lattice has norm ≥ 2.

Solution: make b minimal subject to $\begin{cases} a \in [-1,1] \\ a^2+b^2 \geq 4 \end{cases}$ (e.g. $\begin{pmatrix} 1 \\ \sqrt{3} \end{pmatrix}$ will do).

Voronoi cells:

L lattice, $\ell \in L$. Define the Voronoi cell:

$C(\ell) := \{ x \in \mathbb{R}^n : \|x-\ell\| \leq \|x-\ell'\| \ \forall \ell' \in L \}$.



Exercise 4: Calculate Λ_3.

(Hint: look for a vector $\begin{pmatrix} a \\ b \\ c \end{pmatrix}$ s.t $\begin{pmatrix} a \\ b \end{pmatrix}$ are minimized relative to translations by Λ_2 (put it in the Voronoi cell for Λ_2)

Then $\begin{pmatrix} 2 & 1 & a \\ 0 & \sqrt{3} & b \\ 0 & 0 & c \end{pmatrix}$ s.t $a^2+b^2+c^2 \geq 4$

+ minimize $2\sqrt{3}\cdot c$, relative to

Fact: $\Lambda_2 \simeq A_2$ $\quad\Lambda_6 \simeq E_6$ $\quad$ (A_n, D_n are root lattices)

$\Lambda_3 \simeq A_3$ $\quad\Lambda_7 \simeq E_7$

$\Lambda_4 \simeq D_4$ $\quad\Lambda_8 \simeq E_8$

$\Lambda_5 \simeq D_5$ $\quad\Lambda_{24} \simeq$ Leech lattice $\leftarrow$ we'll see more on this.

Codes and Lattices. (only binary-linear)

C = code = a subspace of $\mathbb{F}_2^n$ $\quad$ (n = length of the code).

Define k = dimension of the code $C = \dim_{\mathbb{F}_2}(C)$.

Hamming distance : $d(\underline{u},\underline{v}) :=$ # places where $\underline{u},\underline{v}$ differ $= d(u-v,0)$

Hamming weight : $w(\underline{u}) = d(\underline{u},0)$ = # nonzero entries of $\underline{u}$.

Let d = minimal distance of $C = \min_{\substack{\underline{u}\in C \\ \underline{u}\neq 0}} w(\underline{u})$

The code C can detect $d-1$, and correct $\left\lfloor \frac{d-1}{2} \right\rfloor$ errors.

Goal: find codes with large d and large rate $R = \frac{k}{n}$ $\quad$ ($0 \leq R \leq 1$).

Given a code C, let its dual code $C^{\perp} := \{ u \in \mathbb{F}_2^n : u\cdot v = 0 \ \forall v \in C \}$.

$\dim(C^{\perp}) = n-k$.

Remark: an easy inequality is $d \leq n-k+1$. :

Pf/ Suppose $d-1 > n-k = \operatorname{codim}_{\mathbb{F}_2^n}(C)$

Let $V = \{ (\underbrace{*,\dots,*}_{d-1}, 0, 0, \dots 0) \}$ (subspace of $\mathbb{F}_2^n$, of dim $d-1$).

Then $V \cap C \neq \{0\} \Rightarrow \exists$ nonzero element of C of weight $\leq d-1 \Rightarrow$!! //

Def (Hamming's weight enumerator polynomial):

$$W_C(x,y) := \sum_{m=0}^{n} N(m)\, x^{n-m} y^m \qquad N(m) = \#\{c \in C : \omega(c) = m\}$$

Examples:

1) Z = the zero code : $[n,0,0]$, $W(x,y) = x^n$

2) $\mathcal{U}$ = the universal code $= \mathbb{F}_2^n = Z^\perp$ $[n,n,1]$. $W(x,y) = \sum_{m=0}^{n} \binom{n}{m} x^{n-m} y^m = (x+y)^n$

3) $\mathcal{R}$ = the repetition code : $\{(0,\dots,0),(1,1,\dots,1)\}$. $[n,1,n]$ $W(x,y) = x^n + y^n$

4) P = parity check code : $\{u \in \mathbb{F}_2^n : \sum u_i \equiv 2 \pmod 2\}$

$P = R^\perp$. $W(x,y) = x^n + \binom{n}{2} x^{n-2} y^2 + \binom{n}{4} x^{n-4} y^4 + \dots + y^n = \frac{1}{2}\left((x+y)^n + (x-y)^n\right)$

Rk: In these examples, we can see that $W_{C^\perp}(x,y) = \frac{1}{|C|} W_C(x+y, x-y)$
$\quad\uparrow$ cardinality of the code.

Theorem: $W_{C^\perp}(x,y) = \frac{1}{|C|} W_C(x+y, x-y)$

Pf/ Ommited //

Def A code $C \subseteq \mathbb{F}_2^n$ is called *cyclic* if $[(u_0, u_1, \dots, u_{n-1}) \in C \Rightarrow (u_{n-1}, u_0, u_1, \dots, u_{n-2}) \in C]$.

To a code $u \in C$, associate a polynomial :

$\underline{u} = (u_0, \dots, u_{n-1}) \longrightarrow g_{\underline{u}}(t) = u_0 + u_1 t + \dots + u_{n-1} t^{n-1}$.

Prop: (1) There's a bijection $\{\text{cyclic codes in } \mathbb{F}_2^n\} \xleftrightarrow{1:1} \{\text{ideals in the ring } \mathbb{F}_2[t]/(t^n-1)\}$.

(2) Any ideal of $\mathbb{F}_2[t]/(t^n-1)$ is generated by a (unique) polynomial dividing $t^n - 1$, say $g(t)$

(3) The dim. of the code corresp. to $g(t)$ is $k = n - \deg(g)$, and a basis is given by $\{g(t), t g(t), \dots, t^{n-\deg(g)-1} g(t)\}$.

Proof

1) Sps C cyclic. $\{g_{\underline{u}} : \underline{u} \in C\}$ is an ideal in $\mathbb{F}_2[t]/(t^n-1)$:

$g_{\underline{u}} + g_{\underline{v}} = g_{\underline{u}+\underline{v}}$ ✓. 0 is there, and $g_{\underline{u}} + g_{\underline{u}} = g_{2\underline{u}} = 0$ ✓.

Just remains to show that the set is closed under multiplication by t :

$$t \cdot g_{\underline{u}} = u_0 t + u_1 t^2 + \dots + u_{n-1} t^n \underset{\uparrow \text{ in } \mathbb{F}_2[t]/(t^n-1)}{=} u_{n-1} + u_0 t + \dots + u_{n-2} t^{n-2} = g_{(u_{n-1}, u_0, \dots, u_{n-2})} \in C \ ✓.$$

Conversely, given $I \subseteq \mathbb{F}_2[t]/t^n-1$ an ideal,

for $h \in I$ write $h = g + f(t^n-1)$, $\deg g < n$. Write $g = u_0 + u_1 t + \dots + u_{n-1} t^{n-1}$.

Then to h associate the code word $(u_0, u_1, \dots, u_{n-1})$.

etc...

Remark: in all previous examples, the codes were cyclic:

$Z \to (t^n-1)$

$U \to 1$

$R \to 1+t+t^2+\dots+t^{n-1} = \frac{t^n-1}{t-1}$

$P \to t-1$

Prop Let C cyclic with generator $g(t) \mid t^n-1$

Let $h(t) = \frac{t^n-1}{g(t)}$, $f(t) = t^{\deg(h)} h\left(\frac{1}{t}\right)$.

Then $C^\perp$ is also cyclic, with generator $f(t)$.

Will be restated (and proven) later!

Example: The Hamming code H_7: The cyclic code associated to $1+t+t^3 \mid t^7-1$.

In fact, $t^7-1 = (1+t+t^3)(1+t+t^2+t^4)$.

A basis is $(1,1,0,1,0,0,0)$ and its cyclic permutations:

$(0,1,1,0,1,0,0)$

$(0,0,1,1,0,1,0)$

$(0,0,0,1,1,0,1)$

Exercise 5.
i) Find the weight enumerator polynomial of H_7.
ii) Conclude that H_7 is a $[7,4,3]$ - code.
iii) Prove that H_8 is an $[8,4,4]$ code with weight enumerator $x^8 + 14x^4y^4 + 8$.

Explanation: if $C \subseteq \mathbb{F}_2^n$ is a code, we can define C^e (extended code), $C^e \subseteq \mathbb{F}_2^{n+1}$ by adding a check digit:

$$C^e = \{(u_1, \dots, u_n, u_{n+1}) : (u_1, \dots, u_n) \in C,\ u_{n+1} = u_1 + \dots + u_n\}.$$

Then, H_8 is defined to be H_7^e.

Def: A code C is called self-dual if $C^\perp = C$. In this case, every codeword has even weight: $u \cdot u = \sum_{i=1}^n u_i^2 = \sum_{i=1}^n u_i \equiv 0 \Rightarrow$ even weight.

Def: A self-dual code is called doubly-even or type II if every code word has weight divisible by 4. Otherwise, it's called of type I.

Example: H_8 is a self-dual of type II.

Proposition: Let $C \subseteq \mathbb{F}_2^n$ be a cyclic code associated with the poly'l $g(t) \mid t^n - 1$.
Let $h(t) = \frac{t^n - 1}{g(t)}$. $f(t) = t^{\deg h} h\left(\frac{1}{t}\right)$.
Then $C^\perp$ is the cyclic code associated with $f(t)$.

Remark: it is clear (why?) that $C^\perp$ is cyclic, and that $f(t) \mid t^n - 1$.

$$\Big[\ h(t)\, g(t) = t^n - 1 \Rightarrow \cancel{h^{rec}(t)\, g^{rec}(t) = (t^n - 1)^{rec}}$$
$$h\left(\tfrac{1}{t}\right) g\left(\tfrac{1}{t}\right) = t^{-n} - 1 \Rightarrow t^n h\left(\tfrac{1}{t}\right) g\left(\tfrac{1}{t}\right) = 1 - t^n \Rightarrow$$
$$\Rightarrow f(t)\, t^{\deg g} \cdot g\left(\tfrac{1}{t}\right) = 1 - t^n = -(t^n - 1) \Rightarrow f(t) \mid t^n - 1\ \Big]$$

Pf (of Prop):

Let $g(t) = g_0 + g_1 t + \dots + g_d t^d$. Let $e = n-d = \deg(h)$.

C is generated by $g, tg, \dots, t^{e-1}g$.

Let $h(t) = h_e t^e + \dots + h_1 t + h_0$. Then $f(t) = h_e + h_{e-1} t + \dots + h_0 t^e$.

It generates a code C_1 with basis $f, tf, \dots, t^{d-1} f$.

Note that $\dim C_1 = d = \dim C^\perp$. So it's enough to show that $C_1 \subseteq C^\perp$. It's enough to show that:

$$(0, \dots, 0, g_0, g_1, \dots, g_d, 0, \dots, 0) \cdot (0, \dots, 0, h_e, \dots, h_1, h_0, 0, 0, \dots, 0) = 0 \pmod 2.$$

The inner product is $\sum_{i+j=N} g_i h_j$ (for some $N \in \mathbb{Z}$, and extend g_i, h_i by 0 to all $i \in \mathbb{Z}$)

(actually, check that $0 < N < n$).

This is also the coeff t^N in the polynomial $g(t) \cdot h(t) = t^n - 1$ ✓

Exercise 6: Discuss self dual cyclic codes.

- The Golay codes C_{23}, C_{24}.

Let α be a primitive 23^{rd} root of 1. (i.e. any root of $\frac{t^{23}-1}{t-1}$).

Note that $|\mathbb{F}_{2^{11}}^\times| = 2^{11} - 1 = 2047 = 23 \cdot 89 \Rightarrow$ all 23^{rd} roots of 1 are in $\mathbb{F}_{2^{11}}$ (in particular, $\alpha \in \mathbb{F}_{2^{11}}$). (and not in $\mathbb{F}_{2^n}$ $n < 11$).

$\Rightarrow$ the minimal poly. of α over $\mathbb{F}_2$, say $g(t)$, is $g(t) = \prod_{\sigma \in Gal(\mathbb{F}_{2^{11}}/\mathbb{F}_2)} (t - \sigma(\alpha)) =$

$$= \prod_{i=0}^{10} (t - \alpha^{2^i}) = \begin{cases} 1 + t^2 + t^4 + t^5 + t^6 + t^{10} + t^{11} & \leftarrow \text{call it } g(t) \\ 1 + t + t^5 + t^6 + t^7 + t^9 + t^{11} & \leftarrow \text{call it } h(t) \end{cases}$$

$g(t) \cdot h(t)(t-1) = t^{23} - 1$.

The code defined by $h(t)$ is called Golay code C_{23}.

(used by Voyager I and II in 1979/1980).

C_{23} is a $[23,12,7]$-code

C_{24} is defined as C_{23}^e (extended just add parity check)

C_{24} is a $[24,12,8]$, which is self-dual doubly-even (type II).

Also, $W_{C_{24}}(x,y) = x^{24} + 759x^{16}y^{8} + 2576x^{12}y^{12} + 759x^{8}y^{16} + y^{24}$.

C_{23} is also the cyclic code associated to

$$h_1(t) = t + t^2 + t^3 + t^4 + t^6 + t^8 + t^9 + t^{12} + t^{13} + t^{16} + t^{18} = \sum_{\substack{i = \text{non-zero square} \\ \text{mod } 23}} t^i$$

Why? $(h_1(t), t^{23}-1) = h(t)$, so h and h_1 define the same code.

C_{23} gives a discrete sphere packing of radius $3 = \frac{7-1}{2}$ of $\mathbb{F}_2^{23}$.

\# points in a ball of radius $3 = 1 + \binom{23}{1} + \binom{23}{2} + \binom{23}{3} = 2^{11}$.

\# spheres $= 2^{\dim(C_{23})} = 2^{12}$

\# pts in packing $= 2^{12} \cdot 2^{11} = 2^{23} = |\mathbb{F}_2^{23}| \Rightarrow C_{23}$ is a perfect code!

- **Construction A.**

Let C be a binary $[n,k,d]$-code

$N(m)$ = # code words of weight m.

Let $L(C) \subseteq \mathbb{Z}^n$, $L(C) := \{x \in \mathbb{Z}^n : x \bmod 2 \in C\} \supseteq (2\mathbb{Z})^n$

Then $L(C)$ is a lattice! Let $\Lambda(C) := \frac{1}{\sqrt{2}} L(C)$ (another lattice).

Prop: $\tau(\Lambda(C)) = \begin{cases} 2^d N(d) & \text{if } d<4 \\ 2n + 16N(4) & \text{if } d=4 \\ 2n & \text{if } d>4 \end{cases}$ (kissing number)

(distance $\sqrt{d}$ to 0)
(distance 2 to 0)
(distance 2 to 0)

$\rho(\Lambda(C)) = \begin{cases} \frac{1}{2}\sqrt{\frac{d}{2}} & \text{if } d<4 \\ \frac{\sqrt{2}}{2} & \text{if } d=4 \\ \frac{\sqrt{2}}{2} & \text{if } d>4 \end{cases}$

Pf/ We will work with $L(C)$ instead of $\Lambda(C)$.
If $d<4$, the vectors closest to the origin are the $2^d N(d)$ vectors with coordinates in $\{-1,0,1\}$ that lift the vectors of weight d in C.
If $d>4$, then any vector of $L(C)$ reducing to a nonzero element of C, has at least d nonzero coordinates. But the vectors $\pm 2e_i$ have distance ~~$\sqrt{2}$ to the origin, and $\sqrt{2}<\sqrt{d}$~~ 2 to the origin, and $2<\sqrt{d}$ for $d>4$. So the closest vectors are $\pm 2e_i$, $i=1..n$.
Finally, for $d=4$ both sets of vectors contribute.

Thm: Let C be an $[n,k,d]$-code, $\Lambda(C)$ has the following properties:

i) $\det(\Lambda(C)) = 2^{n-2k}$.

ii) $\Lambda(C^\perp) = \Lambda(C)^\perp$

iii) $\Lambda(C)$ is integral $\Leftrightarrow C \subseteq C^\perp$

iv) $\Lambda(C)$ is type II $\Leftrightarrow$ C is type-II (self-dual doubly-even).

v) $\Theta_{\Lambda(C)}(q) = W_C\left(\Theta_3(q^2), \Theta_2(q^2)\right)$

where $\Theta_3(q^2) = \sum_{m=-\infty}^{+\infty} q^{m^2}$, $\Theta_2(q^2) = \sum_{m=-\infty}^{+\infty} q^{(m+\frac{1}{2})^2}$

Proof (of Thm): (we use column vectors for $\mathbb{F}_2^n$)

WLOG (why?) C has a generator matrix of the form $\begin{pmatrix} I_k \\ \hline B \end{pmatrix}$

1. $M = n \times k$ -matrix
2. column reduction to get M in Row echelon form
3. Perform $\mathbb{F}_2$ permutation automorphisms, which lift to orthogonal transformations $\Rightarrow$

$\Rightarrow$ give isomorphic lattices!

Then $C^\perp$ has a generator matrix $\overbrace{\begin{pmatrix} -B^t \\ \hline I_{n-k} \end{pmatrix}}^{n-k} \Big\} n$

(because it spans a $(n-k)$-dim'l space, and hence enough to show that the columns are all $\perp$ to columns of $\begin{pmatrix} I_k \\ B \end{pmatrix}$): $(I_k \ B^t)\begin{pmatrix} -B^t \\ I_{n-k} \end{pmatrix} = (0)$. ✓

Now, $C \subseteq C^\perp \iff \begin{bmatrix} I_k & B^t \end{bmatrix}\begin{bmatrix} I_k \\ B \end{bmatrix} \equiv 0 \pmod 2 \iff I_k + B^t B \equiv 0 \iff B^t B \equiv I_k \pmod 2$

(we'll use this later in the proof)

The generator matrix for $\Lambda(C)$ is $\frac{1}{\sqrt{2}}\begin{pmatrix} I_k & 0 \\ B & 2I_{n-k} \end{pmatrix}$

For $\Lambda(C^\perp)$, a gen. matrix is $\frac{1}{\sqrt{2}}\begin{pmatrix} -B^t & 2I_k \\ I_{n-k} & 0 \end{pmatrix}$

(i) $\det(\Lambda(C)) = \det\left(\frac{1}{\sqrt{2}}\begin{pmatrix} I_k & 0 \\ B & 2I_{n-k} \end{pmatrix}\right)^2 = \left(2^{n-k}\, 2^{-\frac{n}{2}}\right)^2 = 2^{n-2k}$.

(ii) $\Lambda(C)^*$ has a generator matrix $\left({}^tM^{-1}\right) = \frac{1}{\sqrt{2}}\begin{pmatrix} 2I_k & -B^t \\ 0 & I_{n-k} \end{pmatrix}$ ✓.

(iii) $\Lambda(C)$ integral $\iff$ its Gramm matrix $A = {}^tMM$ is integral.

$${}^tMM = \begin{pmatrix} \frac{I_k + B^t B}{2} & B^t \\ B & 2I_{n-k} \end{pmatrix}$$ integral $\Rightarrow I_k + B^t B \equiv 0 \pmod 2$

$\iff$ (seen before) $C \subseteq C^\perp$.

(iv) $\Lambda(C)$ is type II $\iff I_k + B^t B \equiv 0 \pmod 4 \iff$ each basis elt. of C has wt divisible by 4.

To prove: $\Theta_{\Lambda(C)} = W(\theta_3(q^2), \theta_2(q^2))$:

For $u \in C$, the corresponding elements of $\Lambda(C)$ are: $(u = (u_1, \ldots, u_n),\ u_i \in \{0,1\})$.

$$\Lambda(u) = \{(y_1, \ldots, y_n) : y_r \in \frac{1}{\sqrt{2}} u_r + \sqrt{2}\,\mathbb{Z},\ 1 \le r \le n\}$$

So $\Lambda(C) = \bigsqcup_{u \in C} \Lambda(u)$

Recall that $\Theta_L(q) = \sum_{\ell \in L} q^{\ell \cdot \ell / 2}$, $q = e^{\pi i \tau}$

Note that $\Theta_{\sqrt{2}\mathbb{Z}}(q) = \Theta_{\mathbb{Z}}(q^2) = \sum_{m \in \mathbb{Z}} q^{m^2}$

$$\Theta_{\frac{1}{\sqrt{2}} + \sqrt{2}\mathbb{Z}}(q) = \Theta_{\frac{1}{2} + \mathbb{Z}}(q^2) = \theta_2(q^2)$$

Now, $\Lambda(u) = \bigoplus_{i=1..n} \left(\frac{1}{\sqrt{2}} u_i + \sqrt{2}\,\mathbb{Z}\right)$. So

$$\Theta_{\Lambda(u)} \underset{\substack{\uparrow \\ \Theta_{M \oplus N} = \Theta_M \cdot \Theta_N}}{=} \Theta_{\sqrt{2}\mathbb{Z}}(q)^{n - wt(u)} \cdot \Theta_{\frac{1}{\sqrt{2}} + \sqrt{2}\mathbb{Z}}(q)^{wt(u)} = \theta_3(q^2)^{n - w(u)}\, \theta_2(q^2)^{w(u)}.$$

$$\Theta_{\Lambda(C)}(q) = \sum_{u \in C} \Theta_{\Lambda(u)} = \sum_{u \in C} \theta_3(q^2)^{n - w(u)}\, \theta_2(q^2)^{w(u)} = \sum_{m=0}^{n} N(m)\, \theta_3(q^2)^{n-m}\, \theta_2(q^2)^{m} \quad //$$

<u>Example</u>: The E_8 (or Gosset) lattice.

Apply Construction A to the Hamming code $H_8 = H_7^e$.

H_8 is an $[8,4,4]$-code, $W(x,y) = x^8 + 14x^4y^4 + y^8$.

H_8 is a type II code. The lattice E_8 is defined as $\Lambda(H_8)$.

It has generator matrix:

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1&0&0&0&2&0&0&0 \\ 1&1&0&0&0&2&0&0 \\ 0&1&1&0&0&0&2&0 \\ 1&0&1&1&0&0&0&2 \\ 0&1&0&1& & & & \\ 0&0&1&0& & O & & \\ 0&0&0&1& & & & \\ 1&1&1&1&0&\cdots&&0 \end{pmatrix}$$

(cont example):

$$\Theta_{E_8}(q) = 1 + \tau q^{2\rho^2} + \text{h.o.t} = 1 + 240q + \text{h.o.t.}$$

Later we will show that Θ_{E_8} is the Eisenstein series E_4 for $SL_2(\mathbb{Z})$.

$$\Rightarrow \Theta_{E_8}(q) = 1 + 240 \sum_{n=1}^{\infty} \sigma_3(n) q^n \quad \text{with } \sigma_3(n) = \sum_{1 \le d | n} d^3$$

Remark:

1) In fact $\exists$ a unique (up to $\cong$) unimodular lattice of rk 8. We will just show that there is a unique Θ-function.

2) In dim 16, $\exists$ precisely two iso. classes, with the same Θ-function.

Exercise 7: Calculate τ, ρ, det, Θ for $\Lambda(C)$ where $C = Z, U, R, P, C_{24}$
(for Θ, write $\Theta = A + Bq + Cq^2 + \cdots$ and calculate A, B (C if possible))

Example: The Leech lattice Λ_{24}. (Λ_{24} = 24th laminated lattice)

Let $C_{24} = C_{23}^e$ be the Golay code of length 24. (C_{23} cyclic assoc. to $\sum_{\substack{i \neq 0 \\ i = \square \bmod 23}} t^i$).

C_{24} is $[24, 12, 8]$ self-dual of Type II.

Define $\Lambda^0 = \{ \frac{1}{\sqrt{2}} v : \sum_{i=1}^{24} v_i \equiv 0 \pmod 4 \} \overset{\text{index } 2}{\subsetneq} \Lambda(C_{24})$

It can be proven (using Niemeier's thm below) that: $\Lambda_{24} = \langle \Lambda^0, t \rangle$

where $t = \frac{1}{\sqrt{2}} \left(\frac{-3}{2}, \frac{1}{2}, \frac{1}{2}, \dots, \frac{1}{2} \right)$

If the coordinates of the vectors are called $0, 1, 2, \dots, 22, \infty$, then:

one sees in the literature Λ_{24} is spanned by $\frac{1}{\sqrt{8}}(2^{12}, 0^{12})$

(23 vectors supported on $(Q+i) \cup \{\infty\}$, $0 \le i \le 22$. Q = non-zero quad. residue mod 23.

$+ \frac{1}{\sqrt{8}}(-3, 1^{23})$ $(= t)$ $+ \frac{1}{\sqrt{8}}(4, 0^{23})$ $\leftarrow$ enough to give all even translations used in Λ^0.

Note: Λ_{24} is a lattice: $2t \in \Lambda^0$, so $\operatorname{rk} \Lambda_{24} = 24$.

$$\begin{array}{l} \Lambda^0 \overset{2}{\subseteq} \Lambda(C_{24}) \\ \ \ \overset{2}{\cap} \\ \ \ \Lambda_{24} \end{array} \quad \Rightarrow \Lambda_{24} \text{ has determinant } 1.$$

One shows that Λ_{24} is an even unimodular lattice (enough to see that it is integral)

Integral: • $\frac{1}{\sqrt{2}}v, \frac{1}{\sqrt{2}}w \in \Lambda^0$, $\frac{1}{\sqrt{2}}v \cdot \frac{1}{\sqrt{2}}w = \frac{1}{2}\overbrace{v \cdot w}^{\equiv 0 \pmod 2}$ because C_{24} is self-dual

(actually $\frac{1}{\sqrt{2}}v \cdot \frac{1}{\sqrt{2}}v = \frac{1}{2} v \cdot v \equiv 0 \bmod 2$ because C is doubly-even.

• $t \cdot t = 4$

• $\frac{1}{\sqrt{2}}v \cdot t = \cancel{\frac{1}{4}v \cdot (-\frac{3}{2}, \frac{1}{2}, \dots, \frac{1}{2})}\ \frac{1}{4}v \cdot (-3, 1, 1, \dots, 1) = \frac{1}{4}\left(\sum v_i - 4v_1\right) \equiv \frac{0 \bmod 4}{4}$ ✓.

Check that it is of type II, again by direct verification.

Further, Λ_{24} has no vector of norm $\sqrt{2}$.

Theorem (Niemeier): up to $\cong$, $\exists$ 24 even unimodular lattices in $\mathbb{R}^{24}$. Λ_{24} is the unique one not having a vector of norm $\sqrt{2}$.

This will allow us to compute parameters for Λ_{24}: $\tau = 196560$, $\delta = 1$

Theorem (Minkowski-Siegel): Let Ω be the set of all inequivalent even unimodular lattices in dimension $n = 2k \equiv 0\ (8)$ (later we'll prove that $8 | n$) (equivalent: up to rescaling + orthogonal transformations).

Then $$\sum_{\Lambda \in \Omega} \frac{1}{|\mathrm{Aut}(\Lambda)|} = \underbrace{\frac{B_k}{2k} \cdot \prod_{j=1}^{k-1} \frac{B_{2j}}{4j}}_{\text{Minkowski-Siegel constant}}$$ where B_i = Bernoulli numbers ($B_0 = 1$, $B_1 = -\frac{1}{2}$, $B_2 = 6$, $B_4 = \frac{1}{30}, \dots$ $B_3 = B_5 = B_7 = \dots = 0$.)

Example:

$n=8 \rightsquigarrow \frac{1}{696729600}$

$n=16 \rightsquigarrow \sim 2.489 \cdot 10^{-18}$

$n=24 \rightsquigarrow \sim 7.937 \cdot 10^{-15}$

$n=32 \rightsquigarrow \sim 4.031 \cdot 10^{7}$ ← !!

It turns out that $\mathrm{Aut}(E_8) = \underset{\text{Weyl gp}}{W(E_8)}$, $\# W(E_8) = 696729600 = 2^{14} \cdot 3^5 5^2 \cdot 7$

$\Rightarrow$ uniqueness of even unimodular lattices in dim. 8.

(easier proof: in Serre's Course in Arithmetic).

For $n=16$, exactly 2: $E_8 \oplus E_8$ and D_{16} (with same θ-function!)

For $n=24$, by Niemeier's thm there are exactly 24. $E_8^3, D_{16}^+ \oplus E_7, A_{24}, \Lambda(C_{24}), \ldots$

For $n=32$, since $|\mathrm{Aut}(\Lambda)| \geq 2$, the number of isoeq. lattices is at least 8×10^7.

Root Lattices

Let E be an Euclidean vectorspace (ℓ-dim'l /$\mathbb{R}$ with a given inner-product (α, β)).

A reflection of E is a linear transformation $E \to E$ fixing a hyperplane H, and taking a vector α orthogonal to H to $-\alpha$.

So given $\alpha \neq 0$, define $\sigma_\alpha(\beta) := \begin{cases} \beta & \text{if } \beta \in \langle\alpha\rangle^\perp \\ -\alpha & \text{if } \beta = \alpha \end{cases}$ + extend linearly.

Note: $\sigma_\alpha(\beta) = \beta - \frac{2(\beta,\alpha)}{\|\alpha\|^2} \alpha$

Notation: $\langle \beta, \alpha \rangle := \frac{2(\beta,\alpha)}{\|\alpha\|^2}$ ($\neq \langle \alpha, \beta \rangle$ usually !).

we can write $\sigma_\alpha(\beta) = \beta - \langle \beta, \alpha \rangle \alpha$

Def A <u>root system</u> $\Phi \subseteq E$ is a subset s.t.

(1) Φ is finite, $0 \notin \Phi$ and $\langle \Phi \rangle = E$ (spans E).

(2) If $\alpha \in \Phi$, $\mathbb{R}\cdot\alpha \cap \Phi = \{\alpha, -\alpha\}$.

(3) If $\alpha \in \Phi$, then $\sigma_\alpha(\Phi) = \Phi$.

(4) If $\alpha, \beta \in \Phi$, then $\langle \alpha, \beta \rangle \in \mathbb{Z}$

(root systems arise in studying the classification of Lie groups and their representations)

(Ref: Humphreys, Fulton & Harris "Rep. Theory")
on Lie groups & their reps.

We say that Φ has rank n if $\dim(E) = n$.

One says that $(\Phi, E) \cong (\Phi', E')$ if $\exists$ isomorphism $f : E \to E'$

(not necessarily an isometry!) s.t. • $f(\Phi) = \Phi'$

• $\langle f(\alpha), f(\beta) \rangle = \langle \alpha, \beta \rangle \quad \forall \alpha, \beta \in \Phi$.

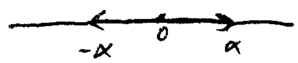
(So note that $(\Phi, E) \cong (f(\Phi), E)$ for $f \in \mathbb{R}^\times \cdot \underbrace{O_n(\mathbb{R})}_{\text{orthogonal matrices}}$)

Def A <u>root lattice</u> is a lattice spanned by a root system.

(so if $L \subseteq \mathbb{R}^n$ is a root lattice, $f(L)$ is so for $f \in \mathbb{R}^\times \times O_n(\mathbb{R})$).

Examples:

<u>Rank 1</u>: $\langle \alpha, \alpha \rangle = 1$
$\langle \alpha, -\alpha \rangle = -2$

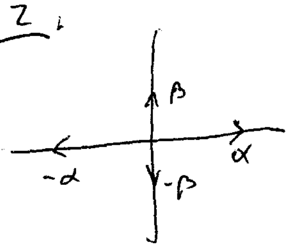


A_1 $\quad (\Phi = \{\alpha, -\alpha\})$

<u>Exercise</u>: if (Φ_i, E_i) $i = 1, 2$ are root systems, then $(\Phi_1 \cup \Phi_2, E_1 \oplus E_2)$ is also a root system. These are called the reducible root systems

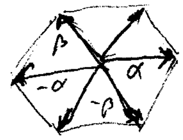
(i.e. $\Phi = \Phi_1 \sqcup \Phi_2$ s.t. $\Phi_i \neq \emptyset$, $(\Phi_1, \Phi_2) = 0$). ($\Rightarrow$ each Φ_i is a root system (on $\langle \Phi_i \rangle$)

Rank 2:



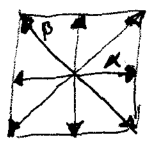
(note, the two axes can be rescaled independently, getting isomorphic root systems!) $A_1 \times A_1$

Also we have A_2:

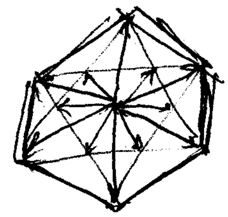


$\langle \alpha, \beta \rangle = -1$

Next is B_2:

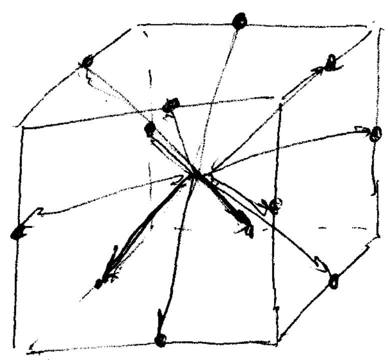


G_2:



Rank 3:

A_3 (FCC packing):



... (there are more root systems of rk 3!)

The formula $\cos \theta_{\alpha\beta} = \frac{(\alpha,\beta)}{\|\alpha\|\|\beta\|}$ gives $\overbrace{\langle \alpha, \beta \rangle \langle \beta, \alpha \rangle}^{2 \text{ integers}} = \frac{2(\alpha,\beta)}{\|\beta\|^2} \cdot \frac{2(\alpha,\beta)}{\|\alpha\|^2} = 4\cos^2 \theta_{\alpha,\beta}$

is an integer in the set $\{0,1,2,3,4\}$

Now, $\cos \theta_{\alpha\beta} = \pm 1 \iff \mathbb{R}\alpha = \mathbb{R}\beta$. Otherwise, $\cos(\theta_{\alpha\beta}) \in \left\{0, \pm\frac{1}{2}, \pm\frac{\sqrt{2}}{2}, \pm\frac{\sqrt{3}}{2}\right\}$

If $\theta_{\alpha,\beta} \neq \pm\frac{\pi}{2}$, then $\left(\frac{\|\beta\|}{\|\alpha\|}\right)^2 = \frac{\langle \beta, \alpha \rangle^2}{4\cos^2 \theta_{\alpha,\beta}}$

$\langle \alpha,\beta \rangle$	$\langle \beta,\alpha \rangle$	$\theta_{\alpha,\beta}$	$\left(\frac{\|\beta\|}{\|\alpha\|}\right)^2$
0	0	$\pi/2$	?
1	1	$\pi/3$	1
−1	−1	$2\pi/3$	1
1	2	$\pi/4$	2
−1	−2	$3\pi/4$	2
1	3	$\pi/6$	3
−1	−3	$5\pi/6$	3

A subset $\Delta \subseteq \Phi$ is called a <u>base</u> if

i) Δ is a basis for E.

ii) Each $\mu \in \Phi$ can be written as $\mu = \sum_{\alpha \in \Delta} k_\alpha \alpha$, where $k_\alpha \in \mathbb{Z}$ and either all $k_\alpha \geq 0$ or all $k_\alpha \leq 0$.

In this case, the elements of Δ are called "simple roots".
(note that this concept depends on the choice of Δ!)
If all $k_\alpha \geq 0$ we say α is positive; if all $k_\alpha \leq 0$, α is negative.

We can write $\Phi = \Phi^+ \sqcup \Phi^-$, and $\Delta \subseteq \Phi^+$.

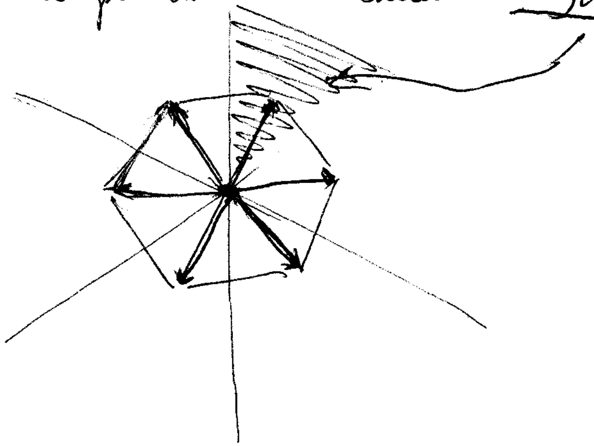
Let $\gamma \in E$ s.t. $\gamma \notin \bigcup_{\alpha \in \Phi} \{\alpha\}^\perp$. Such γ is called <u>regular</u>.

Given $\gamma \in E$ regular, let
$$\Phi^+(\gamma) := \{\alpha \in \Phi : (\alpha, \gamma) > 0\}$$
$$\Phi^-(\gamma) := \{\alpha \in \Phi : (\alpha, \gamma) < 0\}$$

So $\Phi = \Phi^+ \sqcup \Phi^-$.

The collection of regular vectors is $E \setminus \bigcup_{\alpha \in \Phi} \{\alpha\}^\perp$, which is a disjoint union of connected components such that γ, γ' are in the same connected component $\iff$ they lie on the same side of every hyperplane $\{\alpha\}^\perp$, $\alpha \in \Phi$ $\iff$
$\iff$ $\mathrm{Sign}(\gamma, \alpha) = \mathrm{Sign}(\gamma', \alpha)$ $\forall \alpha \in \Phi$ (a little argument is needed for this).

These components are called <u>Weyl chambers</u>.



A vector $\alpha \in \Phi^+(\gamma)$ is <u>decomposable</u> if $\alpha = \beta_1 + \beta_2$, $\beta_1, \beta_2 \in \Phi^+(\gamma)$.
Otherwise, call α <u>indecomposable</u>.

Let $\Delta(\gamma) = \{\alpha \in \Phi^+(\gamma) : \alpha \text{ indecomposable}\}$.

Note that $\Delta(\gamma)$ only depends on which Weyl chamber γ lies.

<u>Theorem</u>: Let $\gamma \in E$ be a <u>regular</u> vector. Then $\Delta(\gamma)$ is a base.
Moreover, every base of Φ is obtained in this way.

Proof

<u>Step 1</u>: Each root in $\Phi^+(\gamma)$ is a non-negative integral combination of $\Delta(\gamma)$:

Pf Suppose not. Choose among the exceptions a vector $\alpha \in \Phi^+(\gamma)$ s.t. (α, γ) is minimal. Then $\alpha = \beta_1 + \beta_2$, $\beta_i \in \Phi^+(\gamma)$.

Then $(\alpha,\gamma) = \underset{\vee 0}{(\beta_1,\gamma)} + \underset{\vee 0}{(\beta_2,\gamma)} > 0 \Rightarrow$ contradiction unless each β_i is a non-exception. So each β_i is a non-negative integral combination of elts. in $\Delta(\gamma) \Rightarrow$ so is $\alpha \Rightarrow$!! again, so α doesn't exist.

Note that $\Phi^-(\gamma) = -\Phi^+(\gamma)$, and so every element of Φ is of the form $\sum_{\alpha \in \Delta(\gamma)} k_\alpha \cdot \alpha$ $\quad k_\alpha \in \mathbb{Z}\ \forall \alpha$ and $\begin{cases} \text{all } k_\alpha \geq 0 \\ \text{or all } k_\alpha \leq 0 \end{cases}$ (property (2) for $\Delta(\gamma)$ to be a base)

Since Φ spans E, so does $\Delta(\gamma)$. It just remains to show that $\Delta(\gamma)$ is a linearly-indep. set.

<u>Step 2</u>: $\Delta(\gamma)$ is linearly-independent.

<u>Lemma</u>: Spse $\alpha, \beta \in \Phi$, $\alpha \neq \pm\beta$. Then $\begin{cases} \text{if } (\alpha,\beta) > 0, \text{ then } \alpha - \beta \text{ is a root.} \\ \text{if } (\alpha,\beta) < 0, \text{ then } \alpha + \beta \text{ is a root.} \end{cases}$

pf (of lemma).

The first claim $\Rightarrow$ second (replace β by $-\beta$).

Now, if $(\alpha,\beta)>0$, then either $\langle\alpha,\beta\rangle$ or $\langle\beta,\alpha\rangle$ is 1 (check the table).

So if $\langle\alpha,\beta\rangle=1$, then $\sigma_\beta(\alpha)=\alpha-\langle\alpha,\beta\rangle\cdot\beta=\alpha-\beta\in\Phi$

if $\langle\beta,\alpha\rangle=1$, then $\sigma_\alpha(\beta)=\beta-\langle\beta,\alpha\rangle\cdot\alpha=\beta-\alpha\in\Phi$, and $-(\beta-\alpha)$ $=\alpha-\beta\in\Phi$ //

(cont pf of thm)

From the lemma, if $\alpha,\beta\in\Delta(\gamma)$, $\alpha\neq\beta$, then:

$(\alpha,\beta)\leq 0$ (angle is not acute). Otherwise, $(\alpha,\beta)>0\Rightarrow\alpha-\beta\in\Phi\Rightarrow$

$\Rightarrow$ either $\alpha-\beta$ or $\beta-\alpha$ are in $\Phi^+(\gamma)$ $\Rightarrow$ either $\alpha=(\alpha-\beta)+\beta$ or $\beta=(\beta-\alpha)+\alpha$ are decomposable $\Rightarrow$!!

Now, suppose $\sum_{\alpha\in\Delta(\gamma)} r_\alpha\cdot\alpha=0$. Then, for some disjoint sets $I,J\subseteq\Delta(\gamma)$,

we have $\varepsilon=\sum_{\alpha\in I}s_\alpha\cdot\alpha=\sum_{\alpha\in J}t_\alpha\cdot\alpha$, each $s_\alpha>0$, each $t_\alpha>0$ (allow $I=\emptyset$ or $J=\emptyset$) empty set

$$0\leq(\varepsilon,\varepsilon)=\sum_{\substack{\alpha\in I\\ \beta\in J}}\overset{\geq 0}{s_\alpha}\,\overset{\geq 0}{t_\beta}\underbrace{(\alpha,\beta)}_{\leq 0}\Rightarrow\varepsilon=0\Rightarrow\text{each } s_\alpha=0$$

(else $(\gamma,\varepsilon)>0\Rightarrow$!!)

Similarly, each $t_\alpha=0$. So all the $r_\alpha=0$. //

To finish the proof of the theorem, we need to see that any base is of this form. So given any base Δ, (to Φ), choose any γ regular s.t $(\gamma,\alpha)>0$ $\forall\alpha\in\Delta$ (this is possible!)

Now, $\Delta\subseteq\Phi^+(\gamma)\Rightarrow\exists$ matrix $M\in GL_n(\mathbb{Z})$, with all entries ≥ 0, taking Δ to $\Delta(\gamma)$

Also, $\exists N=M^{-1}$ s.t $N\in GL_n(\mathbb{Z})$ with all entries ≥ 0 taking $\Delta(\gamma)$ to Δ.

Exercise: prove that such M is a permutation matrix. ($\Rightarrow\Delta=\Delta(\gamma)$) //

The Weyl Group.

Def: Let $W = W(\Phi) = \langle \sigma_\alpha : \alpha \in \Phi \rangle \subseteq \mathrm{Aut}(E)$.

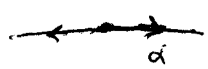
Prop: Φ a root system, W its Weyl group.

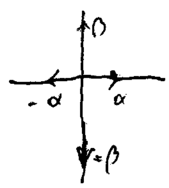
If $\sigma \in GL(E)$ (as a vectorspace only!) leaves Φ invariant, then $\langle \sigma(\beta), \sigma(\alpha) \rangle = \langle \beta, \alpha \rangle$ $\left(\text{recall } \langle \beta, \alpha \rangle = 2\dfrac{(\beta,\alpha)}{\|\alpha\|^2}\right)$

(that is, $\sigma \in \mathrm{Aut}(\Phi, E)$.)

Furthermore, $W \triangleleft \mathrm{Aut}(\Phi, E)$. In fact, $\sigma \cdot \sigma_\alpha \cdot \sigma^{-1} = \sigma_{\sigma(\alpha)}$

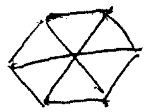
Examples:

-  A_1 $W = \langle \sigma_\alpha \rangle = \{\pm 1\} = \mathrm{Aut}(A_1, \mathbb{R})$

-  $W = \langle \sigma_\alpha, \sigma_{-\alpha}, \sigma_\beta, \sigma_{-\beta} \rangle \simeq \left(\mathbb{Z}/2\mathbb{Z}\right)^2$.

  But $\mathrm{Aut}(A_1 \times A_1, \mathbb{R}^2) \ni \tau$, $\tau(\alpha) = \beta$, $\tau(\beta) = \alpha$.

  Actually, $\mathrm{Aut}(A_1 \times A_1, \mathbb{R}^2) = \langle \tau, \sigma_\alpha, \sigma_\beta \rangle \simeq D_{2\cdot 4}$ (symmetries of $\diamond$).

-  $W \simeq D_{2\cdot 3}$. $\mathrm{Aut} \simeq D_{2\cdot 6}$ (symmetries of the hexagon).

Pf (of prop): Let τ be the linear map $\tau = \sigma \sigma_\alpha \sigma^{-1}$ $(\alpha \in \Phi)$.

For $\beta \in \Phi$, $\sigma \sigma_\alpha \sigma^{-1}(\underbrace{\sigma(\beta)}_{\in\Phi}) = \sigma \underbrace{\sigma_\alpha(\beta)}_{\in\Phi} \in \sigma(\Phi) = \Phi$. So τ preserves Φ.

Further,

1) $\tau(\sigma(\alpha)) = \sigma \sigma_\alpha(\alpha) = \sigma(-\alpha) = -\sigma(\alpha)$.

2) for $\beta \in \alpha^\perp$, $\tau(\sigma(\beta)) = \sigma \sigma_\alpha(\beta) = \sigma(\beta) \Rightarrow \tau$ preserves $\sigma(\alpha^\perp)$

Let $\tilde{\tau} = \underbrace{\sigma_{\sigma(\alpha)}}_{= \sigma_{\sigma(\alpha)}^{-1}} \cdot \tau$. We want to show that $\tilde{\tau} = id$.

$\tilde{\tau}(\sigma(\alpha)) = \sigma_{\sigma(\alpha)}(-\sigma(\alpha)) = \sigma(\alpha)$ $\rightsquigarrow$ $\tilde{\tau}$ induces a well-defined linear transformation on $E/_{\mathbb{R}\cdot\sigma(\alpha)}$.

$\sigma(\alpha)^{\perp} \twoheadrightarrow E/_{\mathbb{R}\cdot\sigma(\alpha)}$ and $\sigma(\alpha^{\perp}) \twoheadrightarrow E/_{\mathbb{R}\sigma(\alpha)}$.

So both τ and $\sigma_{\sigma(\alpha)}$ are the identity on $E/_{\mathbb{R}\sigma(\alpha)}$ $\Rightarrow \tilde{\tau} = id$.

So far, we have that $\sigma\sigma_\alpha\sigma^{-1} = \sigma_{\sigma(\alpha)}$.

$\sigma\sigma_\alpha\sigma^{-1}(\sigma(\beta)) = \sigma\sigma_\alpha(\beta) = \sigma(\beta - \langle\beta,\alpha\rangle\alpha) = \sigma(\beta) - \langle\beta,\alpha\rangle\sigma(\alpha)$

On the other hand,

$\sigma\sigma_\alpha\sigma^{-1}(\sigma(\beta)) = \sigma_{\sigma(\alpha)}(\sigma(\beta)) = \sigma(\beta) - \langle\sigma(\beta),\sigma(\alpha)\rangle\cdot\sigma(\alpha)$

$\Rightarrow \langle\beta,\alpha\rangle = \langle\sigma\beta,\sigma\alpha\rangle$.

<u>Theorem</u>: Let Φ be a root system, with Weyl group W.
Then W acts transitively on the bases of Φ.

Pf/ Because W preserves inner-products, it acts on bases and also on Weyl chambers (it is an easy check). In fact, $\sigma(\Delta(\gamma)) = \Delta(\sigma(\gamma))$ (for $\sigma \in W$)

It is enough to check that W permutes the Weyl chambers transitively.

<u>Lemma</u>: Let Δ be a basis, and $\alpha \in \Delta$. Then ~~$\sigma(\alpha)$~~ σ_α permutes $\Phi^+ - \{\alpha\}$.

Pf/ Let $\Phi^+ \ni \beta = \sum_{\gamma\in\Delta} r_\gamma\cdot\gamma$, each $r_\gamma \geq 0$. If $\beta \neq \alpha$, also $\beta \notin \mathbb{R}\alpha$ and so some r_{γ_0} (for $\gamma_0 \neq \alpha$) is $r_{\gamma_0} \neq 0$ (hence $r_{\gamma_0} > 0$).

$\sigma_\alpha(\beta) = \sum_{\gamma\in\Delta-\{\alpha\}} r_\gamma\cdot\sigma_\alpha(\gamma) + (r_\alpha - 1)\cdot\alpha$ $\rightarrow$ all coeffs are positive $\Rightarrow \sigma_\alpha(\beta) \in \Phi^+$.

(cont pf of thm)

Corollary (to lemma): Let $\delta = \frac{1}{2}\sum_{\beta\in\Phi^+}\beta$ and $\alpha\in\Delta$. Then $\sigma_\alpha(\delta) = \delta-\alpha$.

So if Δ is a base, and γ a regular vector.

Choose $\sigma\in W$ s.t. $(\sigma(\gamma),\delta)$ is maximal.

Let $\alpha\in\Delta$. Then $(\sigma(\gamma),\delta)\geq(\sigma_\alpha\sigma(\gamma),\delta) = (\sigma(\gamma),\sigma_\alpha(\delta)) =$

$= (\sigma(\gamma),\delta-\alpha) = (\sigma(\gamma),\delta) - (\sigma(\gamma),\alpha) \Rightarrow (\sigma(\gamma),\alpha)\geq 0 \;\; \forall\alpha\in\Delta.$

As γ is regular, we have actually $(\sigma(\gamma),\alpha) > 0 \;\; \forall\alpha\in\Delta$.

$\Rightarrow \Delta = \Delta(\sigma(\gamma))$.

If $\Delta = \Delta(\gamma')$, then $\}$ $\Rightarrow$ $\sigma(\gamma)$ and γ' belong to the same Weyl chamber $\Rightarrow W$ acts transitively on the Weyl chambers //

Remarks:

* W (the Weyl group) acts simply-transitively on bases (and on Weyl chambers)
* W is generated by $\langle\sigma_\alpha : \alpha\in\Delta\rangle$ where Δ is any fixed base.
* any root $\alpha\in\Phi$ is part of some base.

The Cartan matrix.

Let Φ be a root system of rank n, $\Delta := \{\alpha_1,\dots,\alpha_n\}$ a base.

Define $C := (\langle\alpha_i,\alpha_j\rangle)_{i,j} \in M_n(\mathbb{R})$

Properties:

- $C\in M_n(\mathbb{Z})$
- $c_{ii} = 2 \;\; \forall i$
- for $i\neq j$, $c_{ij}c_{ji} = 0,1,2,3$ $\quad (c_{ij}c_{ji} = 4\cos^2\theta_{ij})$
- C is symmetric if all roots have the same length.

(more properties of C):

- C, up to a permutation $c_{ij} \sim c_{\sigma(i)\sigma(j)}$ (arising from re-ordering the basis elements) depends only on Φ, not Δ.
  (this is because W preserves $\langle\,,\,\rangle$ and is transitive on bases).

- C determines the root system (Humphries explains it...)
  This is done by first constructing vectors giving C, and then acting on them by the Weyl group.
  Therefore, to classify root systems it's enough to classify Cartan matrices.

Given C, we construct a "Dynkin diagram":

- The nodes are the simple roots (elements of Δ)
- Connect the i^{th} node j^{th} node by $c_{ij} \cdot c_{ji}$ $(i \neq j)$. edges.
  If $c_{ij} \neq c_{ji}$, we put an arrow pointing to the shorter root.

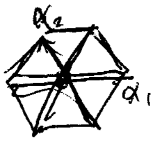
The diagram determines C and viceversa.

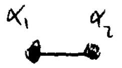
<u>Examples</u>:

A_1 $\longleftrightarrow$ $\sim$ $\bullet$ (2)

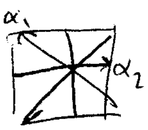
$A_1 \times A_1$ 

$\sim$ $\bullet\ \bullet$ $\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$

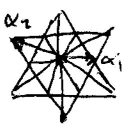
A_2 

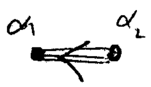
$\sim$ 

$\begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix}$

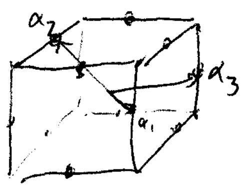
B_2 

$\begin{pmatrix} 2 & -2 \\ -1 & 2 \end{pmatrix}$

G_2 



$\begin{pmatrix} 2 & -1 \\ -3 & 2 \end{pmatrix}$

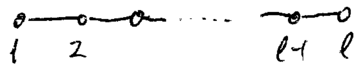



$\begin{pmatrix} 2 & -1 & 0 \\ -1 & 2 & -1 \\ 0 & -1 & 2 \end{pmatrix}$

Theorem: Let Φ be an irreducible root system ($\Leftrightarrow$ Dynkin diagram is connected)

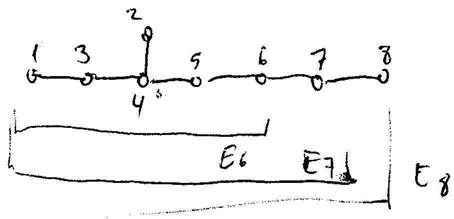
Then its Dynkin diagram is one of the following:

$A_\ell \ (\ell \geq 1)$



$D_\ell \ (\ell \geq 4)$

E_6, E_7, E_8



and B_ℓ, C_ℓ, F_4, G_2.

Proof (sketch):

It is convenient to initially allow a more general setting: E Euclidean space, of arbitrary dimension (but finite).

$A = \{\varepsilon_1, \dots, \varepsilon_n\} \subseteq E$ is <u>admissible</u> if:

1) ε_i are independent unit vectors.

2) $(\varepsilon_i, \varepsilon_j) \leq 0 \quad \forall i \neq j$ (not acute angles).

3) $4 \cdot (\varepsilon_i, \varepsilon_j)^2 \in \{0, 1, 2, 3\}$ for $i \neq j$.

We associate a diagram Γ_A to A in the same way as before.

If $A' \subseteq A$, then A' is also admissible, and $\Gamma_{A'}$ is the corresponding full subgraph of Γ_A.

Claim: The number of pairs of vertices of Γ_A connected by at least one edge is strictly less than n.

Pf Let $\varepsilon = \varepsilon_1 + \dots + \varepsilon_n$. $\varepsilon \neq 0$, so $(\varepsilon, \varepsilon) > 0$. $0 < (\varepsilon, \varepsilon) = n + 2 \sum_{i<j} (\varepsilon_i, \varepsilon_j)$.

If $i < j$ are connected, then $(\varepsilon_i, \varepsilon_j) < 0$. So $4(\varepsilon_i, \varepsilon_j)^2 \in \{1, 2, 3\}$.

(cont pf of claim). $4(\varepsilon_i,\varepsilon_j)^2 \in \{1,2,3\} \Rightarrow 2(\varepsilon_i,\varepsilon_j) \leq -1$.

So $0 < n + 2\sum_{i<j}(\varepsilon_i,\varepsilon_j) \Rightarrow \#\{(i,j) : i<j, (\varepsilon_i,\varepsilon_j)\neq 0\} < n$. // (claim)

__Corollary__: Γ_A contains no cycles.

(the nodes in such a cycle gives A' and $\Gamma_{A'}$ would violate the claim)

__Claim__: no more than 3 edges can originate at a vertex (here we __do__ count multiple edges).

(So for instance the only Dynkin diagram with $\equiv$ is $\circ\!\Rrightarrow\!\circ$).

Pf Let $\varepsilon \in A$. Let $\eta_1,\dots,\eta_k$ be the vectors connected to ε (by 1, 2, 3 edges).

Then $(\varepsilon,\eta_i) < 0 \ \forall i$, and $(\eta_i,\eta_j) = 0$ for $i \neq j$ (otherwise we'd have a triangle)

$\varepsilon \notin \mathrm{Span}\{\eta_1,\dots,\eta_k\}$, so $\exists$ unit vector η_0 in $\mathrm{Span}\{\varepsilon,\eta_1,\dots,\eta_k\}$ s.t.

$\eta_0 \perp \eta_i \ \forall i = 1..k$, i.e. $\{\eta_0,\dots,\eta_k\}$ is orthonormal.

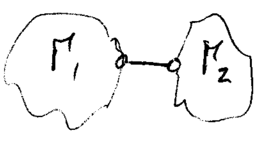
So $\varepsilon = \sum_{i=1}^{k}(\varepsilon,\eta_i)\eta_i$.

$(\varepsilon,\eta_0) = 0 \Rightarrow \varepsilon \in \mathrm{Span}\{\eta_1,\dots,\eta_n\}$

$$1 = (\varepsilon,\varepsilon) = (\varepsilon,\eta_0)^2 + \sum_{i=1}^{k}(\varepsilon,\eta_i)^2 \Rightarrow 1 > \sum_{i=1}^{k}(\varepsilon,\eta_i)^2 \Rightarrow$$

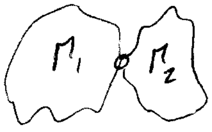
$$\Rightarrow \sum_{i=1}^{k} 4(\varepsilon,\eta_i)^2 < 4$$ (and $4(\varepsilon,\eta_i)^2 = \#$ edges b/w ε and η_i) //

__Exercise__ (next step in proof): if A is admissible with diagram



, then $\exists\, B$ admissible in some Euclidean space

with diagram

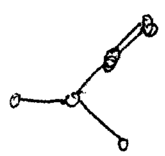
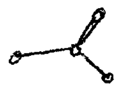


.

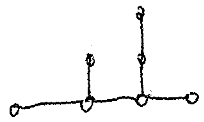
(cont. proof)

Now, what we know so far from the diagram?

- Connected "tree" on n-vertices (by "tree" we think ⊗ as "one vertex")

For instance  is NOT possible. If it was so, then contract to get  which is not possible.

Hence • multiple edges ⇒ "line".

 not possible b/c contracting gives also 4 edges out of a vertex.

Need to be finished ... but just rule out some cases and get it.

<u>Exercise</u>: Let C be the Cartan matrix of a Dynkin diagram $A_\ell, D_\ell, E_6, E_7, E_8$

Prove that C is a symmetric, positive definite matrix.

Prove that $\exists$ a matrix M s.t. ${}^tMM = C$.

Conclude that C is the Gramm matrix of some lattice L.

Calculate $\det(L)$ directly as $\det(C)$.

(Note that L is even integral).

* A concrete model for D_n:

Consider the lattice $\{(x_1, \ldots, x_n) \in \mathbb{Z}^n : \sum x_i \equiv 0 \bmod 2\}$.

Show that $M = \begin{pmatrix} -1 & 0 & \cdots & 0 & 0 \\ 1 & -1 & & \vdots & \vdots \\ 0 & 1 & & & \\ \vdots & \vdots & & -1 & -1 \\ 0 & 0 & & 1 & -1 \end{pmatrix}$ is a generator matrix for this lattice.

Check that ${}^tMM$ is the Cartan matrix of the root system D_n.

(continues exercise)

* A concrete model for the root lattice A_n:

Consider the lattice given by $\{(x_0,\dots,x_n) : x_i \in \mathbb{Z}, \sum x_i = 0\} \subseteq \mathbb{R}^{n+1}$

Prove that $M = \begin{pmatrix} -1 & 0 & \cdots & 0 \\ 1 & -1 & & \vdots \\ 0 & 1 & & \\ \vdots & 0 & & -1 \\ 0 & 0 & & 1 \end{pmatrix}$ is a generator matrix for it.

Prove that ${}^t M \cdot M$ is the Cartan matrix of A_n.

Conclude the following table:

	det	ρ	τ	δ
A_n	$n+1$	$\frac{1}{\sqrt{2}}$	$n(n+1)$	$2^{-\frac{n}{2}}(n+1)^{-\frac{1}{2}}$
D_n	4	$\frac{1}{\sqrt{2}}$	$2n(n-1)$	$2^{-\frac{(n+2)}{2}}$

The lattices D_n^+:

Let $[\tfrac{1}{2}] := (\tfrac{1}{2}, \tfrac{1}{2}, \dots, \tfrac{1}{2}) \in \mathbb{R}^n$.

Let $D_n^+ := D_n \amalg ([\tfrac{1}{2}] + D_n)$.

D_n^+ is a lattice $\iff$ n even (b/c need that $[1] \in D_n$)

Integral? Need that $v \in D_n \Rightarrow v \cdot [\tfrac{1}{2}] \in \mathbb{Z}$ and $[\tfrac{1}{2}]\cdot[\tfrac{1}{2}] \in \mathbb{Z}$.

the condition $v \cdot [\tfrac{1}{2}] \in \mathbb{Z}$ is always true. $[\tfrac{1}{2}]\cdot[\tfrac{1}{2}] = \frac{n}{4} \in \mathbb{Z} \iff 4 \mid n$.

Even? $\iff 8 \mid n$ (check that if $8 \mid n$, $v \in D_n \Rightarrow v \cdot v \in 2\mathbb{Z}$)

Conclusion: if $8 \mid n$, then D_n^+ is an even integral unimodular lattice

(unimodular b/c $[D_n^+ : D_n] = 2 \Rightarrow \det D_n^+ = \frac{\det D_n}{2^2} = \frac{4}{4} = 1$)

($\Rightarrow \Theta_{D_n^+}$ is a modular form for $SL_2(\mathbb{Z})$ of weight $\frac{n}{2}$) ($\Rightarrow D_{16}^+$ and $E_8 \oplus E_8$ have the same Θ-function)

The length of a minimal vector in D_n is $\sqrt{2}$. (e.g. $(1,1,0,\dots,0)$).
This is also the length of a minimal vector in D_n^+
(enough to calculate $\|[\tfrac{1}{2}]\| = \sqrt{\tfrac{n}{4}} \geq \sqrt{2}$ b/c $n \equiv 0\ (8)$).

- <u>The theta function of a lattice and the basic functional equation</u>

Let $L \subseteq \mathbb{R}^n$ a lattice which is integral.
M = generator matrix for L ; $A = {}^tM M$ → gram matrix.
A : symmetric positive-definite matrix, $a_{ij} \in \mathbb{Z}$
(any such arises from an integral lattice) (*)
Define $A[x] := {}^t x A x$.

$$\Theta_L(q) = \sum_{\ell \in L} q^{\ell\cdot\ell/2} = \sum_{x \in \mathbb{Z}^n} q^{\frac{1}{2}A[x]} = \sum_{m=0}^{\infty} r_A(m) q^{m/2} \quad \left(r_A(m) = \#\{\underline{x} \in \mathbb{Z}^n \mid \textstyle\sum a_{ij}x_ix_j = m\}\right)$$

One could just consider as $\Theta_A(q)$ (only depends on A).
But this is no restriction, by (*)
If we let $Q(x) := \frac{1}{2}A[x]$, then $\Theta_A(q) = \sum_{\underline{x} \in \mathbb{Z}^n} q^{Q(x)}$
The function $x \mapsto \sqrt{Q(x)}$ is a norm in $\mathbb{R}^n$.
All norms in $\mathbb{R}^n$ are equivalent, so $\exists\, c > 0$ s.t. $Q(x) \geq c \sum_{i=1}^{n} x_i^2 \ \forall \underline{x} \in \mathbb{R}^n$
$\ulcorner$ Let $c = \min\{Q(x) : \|x\| = 1\} > 0$. If $\|x\| = 1$, then $Q(x) \geq c$.
Now use that both $\sqrt{Q(x)}$ and $\|x\|$ are homogeneous of wt 1 $\lrcorner$

Let $q = e^{2\pi i \tau}$, and then we want to show

$\Theta_A : \mathcal{H} \to \mathbb{C}$ is <u>analytic</u>, where $\mathcal{H} = \{ z \in \mathbb{C} : \operatorname{Im} z > 0 \}$.

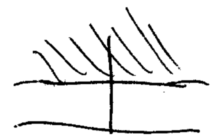
Let $\tau = x + iy$, $x, y \in \mathbb{R}$, $y > 0$.

Then $e^{2\pi i \tau} = \underbrace{e^{2\pi i x}}_{|\cdot| = 1} e^{-2\pi i}$

$$\sum_{x \in \mathbb{Z}^n} |q^{Q(x)}| = \sum_{x \in \mathbb{Z}^n} e^{-2\pi y Q(x)} \leq \sum e^{-2\pi y \cdot c \sum_{i=1}^{n} x_i^2} =$$

$$= \left(\sum_{x \in \mathbb{Z}} e^{-2\pi y c x^2} \right)^n$$

The series $\sum_{x \in \mathbb{Z}} e^{-2\pi y c x^2}$ converges on any compact set in $\mathcal{H}$

(in fact, uniformly on any set of the form ).

Let $S_N(\tau) := \sum_{\substack{x \in \mathbb{Z}^n \\ |x_i| \leq N}} q^{Q(x)}$. Then the sequence of complex-analytic

function $S_1, S_2, S_3, \dots$ converges absolutely-uniformly on every compact

set in $\mathcal{H}$. $\Rightarrow$ the limit (i.e. $\Theta_A(\tau)$ is an analytic function on $\mathcal{H}$).

<u>Recall</u>: Fourier series:

Consider the space $L_2(0,1)$ of complex functions $f : [0,1] \to \mathbb{C}$ s.t $\int_0^1 |f(x)|^2 dx < \infty$

Also, $f_1 = f_2$ if $\mu(f_1 \neq f_2) = 0$

Then $L_2^*(0,1)$ is a Hilbert space (∞-dim inner-product space in which every Cauchy sequence converges), with respect to

$$\langle f, g \rangle := \int_0^1 f(x)\overline{g(x)}\,dx$$

<u>Notation</u>: For $n \in \mathbb{Z}$, define $e(n,x) = e^{2\pi i n x} \in L_2(0,1)$

The set $T = \{e(n,x) : n \in \mathbb{Z}\}$ is orthonormal:

$$\langle e(n,x), e(m,x) \rangle = \int_0^1 e^{2\pi i n x} e^{-2\pi i m x} = \begin{cases} 1 & n = m \\ 0 & n \neq m \end{cases}$$

<u>Thm</u> (Stone-Weierstrass):
Let K be a cpt. ~~topological~~ Hausdorff space (eg $[0,1]$, $[0,1]^n$), and A a $\mathbb{C}$-algebra of continuous functions, $f : K \to \mathbb{C}$, s.t.

1) A is "self-dual" $f \in A \Rightarrow \bar{f} \in A$ (where $\bar{f}(x) := \overline{f(x)}$)
2) A separates points: $x \neq y \in K$, $\Rightarrow \exists f \in A$ s.t. $f(x) \neq f(y)$
3) $1_K \in A$.

<u>Then</u> A is dense in $\mathscr{C}_{\mathbb{C}}(K) = \{$continuous complex functions on $K\}$. (with respect to the sup-norm).

<u>Corollary</u>: $sp(T)$ is dense in $C_{\mathbb{C}}(S^1) \leftarrow$  $0=1$ continuous <u>periodic</u> functions on $[0,1]$.

As $C_{\mathbb{C}}(S^1)$ is dense in $L_2(0,1)$ (wrt $\langle \cdot, \cdot \rangle$), we get $sp(T)$ dense in $L_2(0,1)$ (wrt $\langle , \rangle$)

In a Hilbert space, any dense orthonormal set is a basis.

This last sentence means really that, $\forall h \in H$,

$$h \text{ "=" } \sum_{i=1}^{\infty} c_i t_i \quad \left(\text{in the sense that } \sum_{i=1}^{N} c_i t_i \xrightarrow[N\to\infty]{\text{in the norm } \langle\cdot,\cdot\rangle} h \right).$$

Moreover, $c_i = \langle h, t_i \rangle$, and $\|h\|^2 = \sum_{i=1}^{\infty} |c_i|^2$

$\Rightarrow$ any $f \in L_2(0,1)$ is equal (in the L_2-sense) to its Fourier series:

$$\star \quad f = \sum_{n\in\mathbb{Z}} \hat{f}(n) e(n,x) \overset{(\ast)}{\underset{a.e}{\frown}} \qquad \underset{\mathbb{C}}{\hat{f}(n)} = \langle f, e(n,x)\rangle = \int_0^1 f(x)\, e(-n,x)\,dx$$

Suppose that f is periodic, with continuous derivative f':

Then $\widehat{f'}(n) = \int_0^1 f'(x) e^{-2\pi i n x}\,dx \overset{\text{by parts}}{=} 2\pi i n \int_0^1 f(x) e^{-2\pi i n x}\,dx = 2\pi i n \hat{f}(n)$

So $f'(x) = \sum_{n\in\mathbb{Z}} 2\pi i n \hat{f}(n) e(n,x)$.

$$\sum_{k=-n}^{n} |\hat{f}(k) e(k,x)| = \sum_{k=-n}^{n} |\hat{f}(k)| = |\hat{f}(0)| + \sum_{\substack{k=-n\\k\neq 0}}^{n} \frac{1}{2\pi|k|} |\widehat{f'}(k)| \leq$$

$$\underset{\text{Cauchy-Schwartz}}{\leq} |\hat{f}(0)| + \left(\sum_{k=1}^{n} \frac{1}{2\pi^2 k^2}\right)^{\frac12} \left(\sum_{k=-n}^{n} |\widehat{f'}(k)|^2\right)^{\frac12} \leq |\hat{f}(0)| + C \cdot \|f'\|_{L_2} < \infty$$

$\Rightarrow \sum_{k=-n}^{n} \hat{f}(k) e(k,x)$ converges $(n\to\infty)$ uniformly on any compact set in $[0,1]$

$\Rightarrow$ RHS of $(\ast)$ is continuous, too.

<u>Conclusion</u>: if f has continuous derivative, then f <u>equals</u> (pointwise) to its Fourier series.

Consider $\mathcal{L}^2([0,1]^n)$ = complex square-integrable functions on $[0,1]^n$.

with $\langle f, g\rangle := \int_{[0,1]^n} f(x)\overline{g(x)}\,dx$.

Note: if $\left.\begin{aligned} f(x_1,\dots,x_n) &= \prod_{i=1}^n f_i(x_i) \\ g(x_1,\dots,x_n) &= \prod_{i=1}^n g_i(x_i)\end{aligned}\right\} \Rightarrow \langle f, g\rangle = \prod_{i=1}^n \langle f_i, g_i\rangle$.

Let $T := \{e(m,x) : m \in \mathbb{Z}^n\}$, $e(m,x) := e^{2\pi i\, {}^t m \cdot x}$

Then T is orthonormal.

By the Stone-Weierstrass theorem, Span(T) is dense in $L^2([0,1]^n)$

$\Rightarrow f(x) = \sum_{a\in\mathbb{Z}^n} \hat{f}(a)\, e(a,x)$ a.e. , $\hat{f}(a) = \langle f, e(a,x)\rangle = \int_{[0,1]^n} f(x)\, e(-a,x)\,dx$

Exercise: Suppose that all mixed derivatives of f of all orders exist.
Then $f(x) = \sum_{a\in\mathbb{Z}^n} \hat{f}(a)\, e(a,x)$ everywhere.

- Poisson summation Formula

Let $f: \mathbb{R}^n \to \mathbb{C}$ be a Schwarz function, that is,
all partials of all orders exist, and

$$\left| x^b \frac{\partial^{|a|}}{\partial x^a} f(x)\right| \text{ is bounded, for all } \begin{array}{ll} b=(b_1,\dots,b_n) & b_i \geq 0 \\ a=(a_1,\dots,a_n) & a_i \geq 0. \end{array}$$

(where $x^b = x_1^{b_1}\cdots x_n^{b_n}$ and $\dfrac{\partial^{|a|}}{\partial x^a} = \dfrac{\partial^{\sum a_i}}{\partial x_1^{a_1}\cdots\partial x_n^{a_n}}$).

Example:

1) $x^b e^{-\alpha\|x\|^2}$ is Schwarz.

2) If f is Schwarz, $x^b f$ and $\dfrac{\partial^{(a)}}{\partial x^a} f$ are Schwarz.

3) any $f \in \mathcal{C}_c^\infty(\mathbb{R}^n)$ with compact support is Schwarz.

Example: If f is Schwartz, then define $\tilde{f} = \int_{\mathbb{R}^n} f(y)\, e(-x,y)\, dy$,
its continuous Fourier transform. Then $\tilde{f}$ is Schwartz.

Thm (Poisson Summation): Let f be Schwartz on $\mathbb{R}^n$, with continuous Fourier transform $\tilde{f}$.

Then: $$\sum_{a\in\mathbb{Z}^n} f(x+a) = \sum_{a\in\mathbb{Z}^n} \tilde{f}(a)\, e(a,x) \qquad \forall x\in\mathbb{R}^n.$$

Pf/ Let $g(x) = \sum_{a\in\mathbb{Z}^n} f(x+a)$, a periodic C_c^∞-function on $\mathbb{R}^n$.

And so $g(x) = \sum_{a\in\mathbb{Z}^n} \hat{g}(a)\, e(a,x)$ everywhere.

$$\hat{g}(a) = \langle g(x), e(a,x)\rangle = \int_{[0,1]^n} g(x)\, e^{-2\pi i\, {}^t a x}\, dx =$$

$$= \int_{[0,1]^n} \Big(\sum_{b\in\mathbb{Z}^n} f(x+b)\Big) e(-a,x)\, dx = \sum_{b\in\mathbb{Z}^n} \int_{[0,1]^n+b} f(x)\, e(-a,x)\, dx =$$

$$= \sum_{b\in\mathbb{Z}^n} \int_{[0,1]+b} f(x)\, e(-a,x)\, dx = \tilde{f}(a).$$

Corollary (set $x=0$): $$\sum_{a\in\mathbb{Z}^n} f(a) = \sum_{a\in\mathbb{Z}^n} \tilde{f}(a).$$

The group $\mathbb{T} = SO_2(\mathbb{R})$ = unit circle (a compact abelian gp). It acts on $L^2(\mathbb{T})$ by "translation". ($L^2(\mathbb{T})$ = periodic square-integrable functions on $[0,1]$)

The functions $e(n,x)$ are eigenforms for this action:
$$(\xi \cdot e(n,\cdot))(x) = e(n, x+\xi) = e(n,\xi)\, e(n,x) \Rightarrow \xi\cdot e(n,\cdot) = e(n,\xi)\, e(n,\cdot)$$
so the eigenvalue is $\chi_n(\xi) := e(n,\xi)$.

We have then:

$$\chi_n : \mathbb{T} \to \mathbb{C}^\times \qquad \text{a unitary character of } \mathbb{T}$$
$$\xi \mapsto e(n,\xi)$$

Satisfying
- $\chi_n(\xi+\xi') = \chi_n(\xi)\chi_n(\xi')$
- $\chi_1^n = \chi_n$.

These characters are $\cong \mathbb{Z}$ as abelian group.

<u>Exercise</u>: 1) prove that every character unitary (cont. hom. $\mathbb{T} \to \{|z|=1\}$) is χ_n for some n.

By Fourier series expansion, $L^2(\mathbb{T}) \cong \bigoplus_{n\in\mathbb{Z}} \mathbb{C}_n$ ← corresp. to $e(n,x)$.

The group $\mathbb{R}$ acts by translations on itself, and induces an action on functions:

$(\xi \cdot f)(x) := f(x+\xi)$ for f a Schwartz function.

Then the functions $e(u,x) = e^{2\pi i u x}$, $u \in \mathbb{R}$ are eigenforms.

So again $\xi \mapsto e(u,\xi)$ gives a unitary character of $\mathbb{R}$.

<u>Exercise</u>: 2) Prove that every unitary character of $\mathbb{R}$ is of the form $e(u,\cdot)$, for some $u \in \mathbb{R}$.

• <u>Fourier Theory</u>:

Informally, "$L^2(\mathbb{R}) \cong \int^{\oplus}_{h\in\mathbb{R}} \mathbb{C}_h$" (direct integral, instead of sum!)

the Fourier transform can be extended to $L^2(\mathbb{R})$. (Plancherel's theorem).

Moreover, these are isometric: $\|f\| = \|\hat{f}\|$.

Note: there's no reason to expect $f \underset{ae}{=} \tilde{f}$,

$$\left[f(x) = \begin{cases} 1 & |x|<1 \\ 0 & \text{otherwise} \end{cases} \Rightarrow \tilde{f}(x) = \frac{\sin 2\pi x}{\pi x} \right]$$

However, the poisson summation formula relates the values.

If G is a locally compact abelian top group, there is a complete theory.

(see Katz, Nelson; "Intro. to Harmonic Analysis").

Q: What about G = locally compact top group, but not abelian?

- G compact → also done
- $G = \Gamma(\mathbb{R})$, Γ a reductive algebraic group (eg $GL_n, Sp_{2n}, SO_n, E_8, G_2$)
  This is the theory of Automorphic Forms
  (Proceedings of Sym. in Pure Math, vol 61).

Let $L \subseteq \mathbb{R}^n$ be a lattice, with generator matrix M. $(L = \{Ma : a \in \mathbb{Z}^n\})$

Let f be a Schwartz function on $\mathbb{R}^n$, and let $F(x) := f(M.x)$.

Then $$\sum_{\lambda \in L} f(\lambda) = \sum_{a \in \mathbb{Z}^n} F(a) \overset{\text{Poisson}}{=} \sum_{a \in \mathbb{Z}^n} \hat{F}(a).$$

$$\hat{F}(a) = \int_{\mathbb{R}^n} F(x) e(-a,x)\, dx = \int_{\mathbb{R}^n} f(Mx)\, e(-{}^tM^{-1}a, Mx)\, dx = \frac{1}{|\det M|} \int_{\mathbb{R}^n} f(x) e(-{}^tM^{-1}a, x)\, dx$$

Note: ${}^tM^{-1}$ is a generator matrix for the dual lattice $L^\vee$, so:

$$\sum_{a \in \mathbb{Z}^n} \hat{F}(a) = \frac{1}{|\det M|} \sum_{\lambda \in L^\vee} \hat{f}(\lambda).$$

If A = Gram matrix $= {}^tM \cdot M$, then $$\sum_{\lambda \in L} f(\lambda) = \frac{1}{\sqrt{\det A}} \sum_{\lambda \in L^\vee} \tilde{f}(\lambda).$$

Example: $\mathbb{R}^1 \supseteq L = \sqrt{t}\cdot\mathbb{Z}$. $M = (\sqrt{t})$, $A = (t)$, $L^\vee = \frac{1}{\sqrt{t}}\mathbb{Z}$.

Then, $f = e^{-\pi x^2}$, $f = \hat{f}$, $\displaystyle\sum_{n\in\mathbb{Z}} e^{-\pi t n^2} = \frac{1}{\sqrt{t}} \sum_{n\in\mathbb{Z}} e^{-\pi n^2/t}$

Recall: $\displaystyle\Theta_L(z) = \sum_{\lambda\in L} q^{\lambda\cdot\lambda/2} = \sum_{a\in\mathbb{Z}^n} q^{\frac{1}{2}A[a]}$.

Let $\displaystyle F_L(t) = \sum_{a\in\mathbb{Z}^n} e^{-\pi t A[a]}$: $\mathbb{R}^+ \to \mathbb{R}$.

Theorem: $\displaystyle\Theta_L(z) = \frac{1}{\sqrt{\det A}}\left(\frac{i}{z}\right)^{n/2}\Theta_{L^\vee}\left(\frac{-1}{z}\right)$

Pf Both sides are analytic function of $z\in\mathcal{H}$.

Therefore, it's enough to show for $z = it$, $t > 0$.

$\Theta_L(it) = F_L(t)$.

Let $f(x) = e^{-\pi x\cdot x}$, then $f = \hat{f}$.

$$\Theta_L(it) = F_L(t) = \sum_{a\in\mathbb{Z}^n} e^{-\pi t A[a]} = \sum_{\lambda\in L} e^{-\pi t\|\lambda\|^2} \overset{\text{poisson}}{=} \sum_{\lambda\in\sqrt{t}L^\vee} \hat{f}(\lambda)\cdot\frac{1}{\sqrt{\det(A\cdot t)}}$$

$$= (\det A)^{-\frac{1}{2}}\, t^{-n/2} \sum_{a\in\mathbb{Z}^n} e^{-\pi A^{-1}[a]/t} = (\det A)^{-1/2}\, i^{n/2}(it)^{-n/2}\sum e^{\frac{t\pi i A^{-1}[a]}{2}\frac{-1}{it}}$$

$$= \frac{1}{\sqrt{\det A}}\left(\frac{i}{it}\right)^{n/2}\Theta_{L^\vee}\left(\frac{-1}{it}\right). \quad //$$

Corollary: If L is integral unimodular ($\det A = 1$), then $\Theta_L(z) = \left(\frac{i}{z}\right)^{n/2}\Theta_L\left(\frac{-1}{z}\right)$

In this case, Θ_L satisfies a functional equation for $z \mapsto \frac{-1}{z}$.

Also, it satisfies one for $z \mapsto z+1$ $\left(\Theta_L(z) = \Theta_L(z+1)\right)$.

$\Rightarrow$ functional equation with all the group $PSL_2(\mathbb{Z})$ (gen by $z\mapsto z+1$, $z\mapsto\frac{-1}{z}$).

We want to understand all analytic functions $\mathcal{H} \to \mathbb{C}$ with such a functional equation.

• The upper-half-plane and its quotients.

Lemma: Let $\gamma \in GL_2(\mathbb{R})^+$, $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ act on $z \in \mathcal{H}$ by $\gamma z = \frac{az+b}{cz+d}$.

1) $\operatorname{Im}(\gamma z) = \frac{\det(\gamma)}{|cz+d|^2} \cdot \operatorname{Im}(z)$.

2) $GL_2(\mathbb{R})^+$ acts on $\mathcal{H}$ transitively, and the center $\left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} : a \in \mathbb{R}^\times \right\}$ acts trivially, so $PGL_2(\mathbb{R})^+ \cong SL_2(\mathbb{R}) / \{\pm I\} = PSL_2(\mathbb{R})$ acts on $\mathcal{H}$. (transitively).

Pf.

Stabilizer of i in $SL_2(\mathbb{R})$:

$$\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{R}) : ai+b = (ci+d)i \right\} = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in SL_2(\mathbb{R}) : a^2+b^2=1 \right\} \simeq S^1.$$

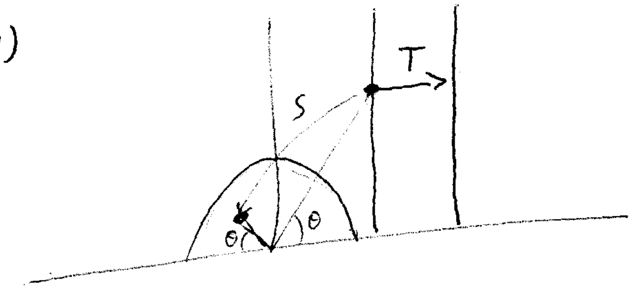
Corollary: $\mathcal{H} \simeq SL_2(\mathbb{R}) / SO_2(\mathbb{R})$ (as topological spaces).

Define the matrices $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, so that

$S \cdot z = \frac{-1}{z}$, $T \cdot z = z+1$. Also, $S^2 = I$ in $PSL_2(\mathbb{R})$.

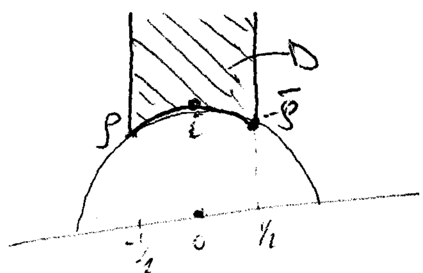
Moreover, $ST = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$, and $(ST)^3 = I$ in $PSL_2(\mathbb{R})$.

If $z = re^{i\theta}$, $S \cdot z = \frac{1}{r} e^{i(\pi - \theta)}$



Let $D = \{ z \in \mathcal{H} \mid |\mathrm{Re}\, z| \leq \frac{1}{2},\ |z| \geq 1 \}$.

Let $\rho = e^{2\pi i/3}$



__Theorem__: i) $\forall z \in \mathcal{H}$, $\exists g \in SL_2(\mathbb{Z})$ s.t. $gz \in D$.

ii) Suppose $z \neq z'$ are both in D and $\exists g \in SL_2(\mathbb{Z})$ st $gz = z'$.

__Then__: $z = z' \pm 1$ (so $\mathrm{Re}(z) = \pm 1/2$)

or $|z| = 1$, $z' = -1/z$

iii) Let $G = PSL_2(\mathbb{Z})$. The stabilizer of any point of D in G is trivial, except for $i, \rho, -\bar{\rho}$, where:

$\mathrm{Stab}(i) \cong \mathbb{Z}/2\mathbb{Z} = \langle S \rangle$

$\mathrm{Stab}(-\bar{\rho}) \cong \mathrm{Stab}(\rho) \cong \mathbb{Z}/3\mathbb{Z} = \begin{cases} \langle TS \rangle & (-\bar{\rho}) \\ \langle ST \rangle & (\rho) \end{cases}$

iv) G is generated by S, T.

Proof (of Thm):

Let $G' = \langle S, T \rangle \subseteq G$.

For $z \in \mathcal{H}$, $g \in G$: $\mathrm{Im}(gz) = \dfrac{\mathrm{Im}(z)}{|cz+d|^2}$

For every $C > 0$, $\exists$ finitely-many $c, d \in \mathbb{Z}$ s.t. $|cz+d|^2 < C$

[Let $z = x+iy$. $|cz+d|^2 = (cx+d)^2 + (cy)^2 = (c,d) \underbrace{\begin{pmatrix} x^2+y^2 & x \\ x & 1 \end{pmatrix}}_{\text{pos. def } \left(\substack{x^2+y^2>0 \\ \text{and} \\ y^2>0}\right)} \begin{pmatrix} c \\ d \end{pmatrix}$

So $\{|cz+d|^2 < C\}$ = pts of the lattice $\mathbb{Z}^2$ in the ball for this quadratic form of radius C^2]

So $\exists g \in G'$ s.t. $\mathrm{Im}(gz)$ is the maximum possible (g runs over all G').

Choose n s.t. $|\mathrm{Re}(T^n g z)| \leq \frac{1}{2}$

Claim: $T^n g z \in D$.

pf $|T^n g z| \geq 1$?

Let $z' = T^n g z$. $\mathrm{Im}\left(\frac{-1}{z'}\right) = \mathrm{Im}(S \cdot z') = \dfrac{\mathrm{Im}(z')}{|z'|^2}$.

If $|z'| < 1$, then $\mathrm{Im}(ST^n g z) > \mathrm{Im}(z')$ $\Rightarrow\Leftarrow$!! . So $|z'| \geq 1$. //

This gives (i).

Let now $z \in D$, $g \in G$ s.t. $gz \in D$. WLOG assume $\mathrm{Im}(gz) \geq \mathrm{Im}(z)$.

If $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, this means that $|cz+d| \leq 1$. Write $z = x+iy$.

Then $1 \geq |(cx+d)^2 + (cy)^2|^{1/2} \geq |c|\, y \geq |c| \frac{\sqrt{3}}{2} \Rightarrow |c| \leq 1 \Rightarrow c \in \{-1, 0, 1\}$.

WLOG, $c \in \{0, 1\}$ (else multiply by $-I$, which doesn't change the action).

Case $c=0$: $g=\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in SL_2(\mathbb{Z})$. $\Rightarrow a=\pm 1$, $d=\pm 1$. WLOG, $g=\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \Rightarrow$

$\Rightarrow gz = z+b \Rightarrow b \in \{-1,0,1\}$. ($b=0$ leads to $z'=z$).

Case $c=1$:

$|cz+d| = |z+d| \leq 1$

a) $d=0$ $\quad g=\begin{pmatrix} a & b \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} a & -1 \\ 1 & 0 \end{pmatrix}$, $gz = a - \frac{1}{z}$ (and $|z|=1$).

So either $a=0$, $g=\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $gz = \frac{-1}{z}$

or $a=1$, $z=-\bar{\rho}$

or $a=-1$, $z=\rho$

$\Big\}$ $\Rightarrow |\mathrm{Re}\, z| = \frac{1}{2}$, $z' = z \pm 1$.

b) $d=1$, ($d=-1$)

$|z+d| \leq 1 \Rightarrow |z+d| \in \{\rho, -\bar{\rho}\}$ and $|z+d|=1$

Then $\mathrm{Im}\, gz = \frac{y}{|cz+d|} = \mathrm{Im}(z) \Rightarrow \mathrm{Im}(z) =$ minimal possible for $z \in D$.

$\Rightarrow gz \in \{\rho, -\bar{\rho}\}$, so $gz = -\frac{1}{z}$ (or z).

This gives (ii). Also, we have seen that $gz = z \Rightarrow \begin{cases} |z|=1 \\ z \in \{i, \rho, -\bar{\rho}\} \end{cases}$

Some calculation gives the corresponding stabilizers.

It remains to show that $G' = G$.

Choose some $z \in$ interior of D. Let $g \in G$. $\exists g' \in G'$ s.t. $g' \cdot g z \in D$.

So z and $g'g z$ are equivalent under $PSL_2(\mathbb{Z})$, and $z \notin \partial D$.

Hence $z = g'g z \Rightarrow (g')^{-1} = g \Rightarrow g \in G'$.

• Remarks about class numbers of imaginary quadratic fields (following Cohen, "A course on Computational #-theory").

Let $D<0$ be a fundamental discriminant

$\left(D \equiv 0,1 \bmod 4,\ \left(\Rightarrow [p>2 \Rightarrow p^2 \nmid D]\right)\right)$ and either $\begin{cases} 8 \| D \\ 4 \mid D \text{ and } \frac{D}{4} \equiv 3 \pmod 4 \\ 2 \nmid D \end{cases}$

Consider the class group of the ring of integers $K = \mathbb{Q}(\sqrt{D})$,

$\mathcal{O}_K = \mathbb{Z}\left[\frac{D+\sqrt{D}}{2}\right]$.

The class gp consists of fractional ideals ($I \subseteq K$ s.t $\exists m \in \mathbb{Z}$ s.t $0 \neq mI \subseteq \mathcal{O}$ ideal) up to equivalence given by $\lambda \in K^\times$ ($I \sim \lambda I = \{\lambda a : a \in I\}$).

This is a finite set with abelian group structure, induced by $I * J = \langle \{ij \mid i \in I, j \in J\}\rangle$

Any such ideal is a rank 2 abelian group, hence $I = \mathbb{Z}\alpha + \mathbb{Z}\beta$,

and one can assume that $\frac{\beta\bar{\alpha} - \alpha\bar{\beta}}{\sqrt{D}} > 0$

(i.e. $\beta\bar{\alpha} - \alpha\bar{\beta}$ purely imaginary $\Rightarrow$ quotient $\in \mathbb{R}$, and switch if necessary α, β s.t it is positive. If quot $= 0$, $\beta\bar{\alpha} = \alpha\bar{\beta} \Rightarrow \beta\bar{\alpha}$ is real $\Rightarrow \beta\bar{\alpha} - \alpha\bar{\beta}$ real $\Rightarrow$ $\Rightarrow \beta \in \mathbb{R}\alpha \cap K = \mathbb{Q}\alpha \Rightarrow \alpha, \beta$ are linear-dependent $\Rightarrow$!!)

To such a basis $\{\alpha, \beta\}$, associate the quadratic norm:

$$\frac{N(x\alpha - y\beta)}{N(I)} = ax^2 + bxy + cy^2 \quad \begin{cases} a, b, c \in \mathbb{Z} \\ a > 0 \\ b^2 - 4ac = D \end{cases}$$

depends only on the class of I and the basis.

(where $N(\gamma) = \gamma \cdot \bar{\gamma}$, $N(I) = \langle \{N(i) : i \in I\}\rangle = N(I) \cdot \mathbb{Z}$).

Conversely, given such a form, we associate to it an ideal.

If $ax^2+bxy+cy^2$ is a positive quad. form w/ $a,b,c \in \mathbb{Z}$, $b^2-4ac=D$,

we associate the ideal $\mathbb{Z} + \mathbb{Z}\dfrac{-b+\sqrt{D}}{2a}$

One shows that this produces an equivalence between:

$$\left\{\begin{array}{l}\text{ideal classes}\\ \text{of } K\end{array}\right\} \xleftrightarrow{1:1} \left\{\begin{array}{l}\text{primitive}\\ \text{pos. def quadratic}\\ \text{forms of disc. } D\end{array}\right\} \Big/ SL_2(\mathbb{Z})$$

primitive ← $\gcd(a,b,c)=1$ ← is this automatic by the conditions on D?

(where the action of $SL_2(\mathbb{Z})$ is $f(x,y) = ax^2+bxy+cy^2 \overset{M = \begin{pmatrix}\alpha & \beta \\ \gamma & \delta\end{pmatrix} \in SL_2(\mathbb{Z})}{\rightsquigarrow} f|M \to f(\alpha x+\beta y, \gamma x+\delta y)$)

Given such $f(x,y) = ax^2+bxy+cy^2$, associate to it $\tau = \dfrac{-b+\sqrt{D}}{2a} \in \mathcal{H}$ its "root".

(So $f(\tau,1) = 0 \iff f\left(\binom{\tau}{1}\right) = 0 \iff f\left(M \cdot M^{-1}\binom{\tau}{1}\right) = 0$, i.e.

the form $f|M$ has root $M^{-1}\tau$, $\dfrac{\alpha'\tau+\beta'}{\gamma'\tau+\delta'}$ $\left(M^{-1} = \begin{pmatrix}\alpha' & \beta' \\ \gamma' & \delta'\end{pmatrix}\right)$)

We have then a map (bijective)

$$\left\{\begin{array}{l}\text{primitive positive definite}\\ \text{quadratic forms}\\ \text{with disc } D\end{array}\right\} \longleftrightarrow \left\{\begin{array}{l}\text{orbits of certain } \tau\text{'s} \in \mathcal{H}\\ \text{under } SL_2(\mathbb{Z})\end{array}\right\} \quad (*)$$

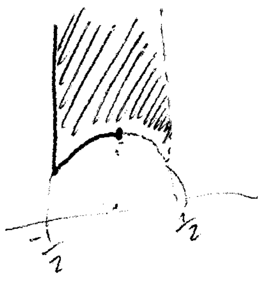
τ s.t. $\mathbb{Q}(\tau) = K$

(*) $\mathbb{Q}(\tau) = K$, so $\tau = \dfrac{-b}{2a} + \dfrac{\sqrt{D}}{2a}$ for some rational #'s a,b s.t.:

$\cdot\ a \in \mathbb{Z}$, $a>0$, $b \in \mathbb{Z}$, $c = \dfrac{b^2-D}{4a} \in \mathbb{Z} \iff b^2 \equiv D \pmod{4a}$, where $D = b^2-4ac \Rightarrow$

$\Rightarrow c = \dfrac{b^2-D}{4a}$!

The fact that every $\tau \in \mathcal{H}$ is equiv. under $SL_2(\mathbb{Z})$ to a unique element in the region:



This set of representatives translates into:

- Every primitive positive-definite quadratic form of discriminant D is equivalent to a unique quadratic form $ax^2 + bxy + cy^2$ such that: $a, b, c \in \mathbb{Z}$, $b^2 - 4ac = D$, $a > 0$, $|b| \leq a \leq c$ and if $|b| = a$ or $a = c$, then $b \geq 0$ (took the boundary of the region s.t. $\mathrm{Re}(\tau) = -\frac{1}{2}$).

These are called the <u>reduced forms.</u> $\leftarrow$ allows to calculate class numbers.

<u>Remark</u>: One can ask what is the group law in terms of quadratic forms. This is Gauss's composition law, which predates the notion of class group!

<u>Example</u>: $D = -71$, $K = \mathbb{Q}(\sqrt{-71})$. Look for reduced forms:

$$b^2 \equiv D \pmod{4a}$$

$$D = b^2 - 4ac = \underbrace{(b^2 - ac)}_{\leq 0} - 3ac \leq -3ac \quad (a \leq c)$$

$$\Rightarrow a \leq \sqrt{\frac{-D}{3}}$$

a	b	c
1	+1	18
	~~-1~~	
2	+1	9
	-1	9
	~~+2~~	
	~~-2~~	
3	+1	24
	-1	24
	~~+5~~	
	~~-5~~	
4	3	5
	-5	5

$$\Rightarrow \boxed{h(K) = 7}.$$

Generalization: look at Manjul Bhargava's ICM '06 talk. (Madrid).

• Subgroups of $SL_2(\mathbb{Z})$

Lemma: Let N be a positive integer. Then the group hom.

$$SL_2(\mathbb{Z}) \longrightarrow SL_2(\mathbb{Z}/N\mathbb{Z}) \quad \text{is \underline{surjective}.}$$

Pf/ Claim: Let (c,d,N) integers s.t. $N>0$, $\gcd(c,d,N)=1$. Then $\exists t\in\mathbb{Z}$ s.t. $\gcd(c, d+tN)=1$.

Pf/ • If $p|c$, $p|d$, then $p\nmid N$, so take $t\equiv 1 \pmod p$. Then $p\nmid tN$, so $p\nmid d+tN$.

• If $p|c$, $p\nmid d$, then take $t\equiv 0 \pmod p$. So $p\nmid d+tN$.

~~If $p\nmid c$, $p|d$~~

Let then $\begin{pmatrix}\bar a & \bar b\\ \bar c & \bar d\end{pmatrix}\in SL_2(\mathbb{Z}/N\mathbb{Z})$, lift it to $\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in M_2(\mathbb{Z})$.

If $p|c$, $p|d$ and $p|N$, then $p\,|\,ad-bc\equiv 1 \bmod N \Rightarrow !!$.

So $\gcd(c,d,N)=1$. Modify $d \rightsquigarrow d+tN$ so that $\gcd(c,d)=1$.

Then $\exists \alpha,\beta\in\mathbb{Z}$ s.t. $1=\alpha c+\beta d$. Consider $\begin{pmatrix} a-k\beta N & b+k\alpha N\\ c & d\end{pmatrix}$

(where $ad-bc=1+kN$, $k\in\mathbb{Z}$)

Then $\det(\cdot) = ad-bc-(k\beta d+ck\alpha)N = ad-bc-kN=1$

Let $\pi: SL_2(\mathbb{Z})\to SL_2(\mathbb{Z}/N\mathbb{Z})$, and define $\Gamma(N) := \pi^{-1}(\{1\}) = \ker\pi$

So $\Gamma(N) = \left\{\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in SL_2(\mathbb{Z}) : \equiv \begin{pmatrix}1&0\\0&1\end{pmatrix} \pmod N\right\}$

Unipotent sgp.

Let $\Gamma_1(N) := \left\{\begin{pmatrix}a&b\\c&d\end{pmatrix} : \equiv\begin{pmatrix}1&*\\0&1\end{pmatrix}\pmod N\right\} = \pi^{-1}\left(\left\{\begin{pmatrix}1&x\\0&1\end{pmatrix} : x\in\mathbb{Z}/N\mathbb{Z}\right\}\right)$

$\Gamma_0(N) := \left\{\begin{pmatrix}a&b\\c&d\end{pmatrix} : \equiv\begin{pmatrix}*&*\\0&*\end{pmatrix}\pmod N\right\} = \pi^{-1}\left(\left\{\begin{pmatrix}*&*\\0&*\end{pmatrix}\right\}\right)$ ← Borel sgp.

Note that by isomorphism thm:

$$\Gamma(N) \underset{N}{\subseteq} \Gamma_1(N) \underset{\phi(N)}{\in} \Gamma_0(N) \qquad \phi(N) := \#\left(\mathbb{Z}/N\mathbb{Z}\right)^\times = N \cdot \prod_{p \mid N}\left(1 - \frac{1}{p}\right).$$

Define $\Gamma := \Gamma(1) := SL_2(\mathbb{Z})$.

$[\Gamma : \Gamma(N)] = \# SL_2(\mathbb{Z}/N\mathbb{Z}) = ?$

By Chinese Remainder Theorem, $M_2(\mathbb{Z}/N\mathbb{Z}) = \prod_{p^r \| N} M_2(\mathbb{Z}/p\mathbb{Z}) \Rightarrow$ (taking units)

$$\Rightarrow GL_2(\mathbb{Z}/N\mathbb{Z}) = \prod_{p^r \| N} GL_2(\mathbb{Z}/p^r\mathbb{Z}).$$

Also, by considering the determinant condition,

$$SL_2(\mathbb{Z}/N\mathbb{Z}) = \prod_{p^r \| N} SL_2(\mathbb{Z}/p^r\mathbb{Z}).$$

From the exact sequence $1 \to SL_2 \to GL_2 \to (\mathbb{Z}/N\mathbb{Z})^\times \to 1$,

$$\# SL_2(\mathbb{Z}/N\mathbb{Z}) = \frac{\# GL_2(\mathbb{Z}/N\mathbb{Z})}{\phi(N)}.$$

Let $G = GL_2(\mathbb{Z}/p^r\mathbb{Z})$, $G_i := \{M \in GL_2(\mathbb{Z}/p^r\mathbb{Z}) : M \equiv I \pmod{p^i}\}$.

$$\{1\} = G_r \subseteq \cdots\cdots \subseteq G_2 \subseteq G_1 \subseteq G.$$

$$G/G_1 \simeq GL_2(\mathbb{Z}/p\mathbb{Z}) \Rightarrow [G : G_1] = \# GL_2(\mathbb{Z}/p\mathbb{Z}) = (p^2-1)(p^2-p)$$

<u>Lemma</u>: The map $(G_i, \cdot) \xrightarrow{\sim} M_2(p^i\mathbb{Z}/p^{i+1}\mathbb{Z}, +) \simeq (M_2(\mathbb{Z}/p\mathbb{Z}), +)$

$$\begin{pmatrix} \alpha & \beta \\ \alpha & \delta \end{pmatrix} \longmapsto \begin{pmatrix} \alpha-1 & \beta \\ \gamma & \delta-1 \end{pmatrix}$$

induces, for $i \geq 1$, a gp isomorphism $G_i/G_{i+1} \simeq (M_2(\mathbb{Z}/p\mathbb{Z}), +)$

Pf/
$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\begin{pmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{pmatrix} = \begin{pmatrix} \alpha\alpha' + \beta\gamma' & \alpha\beta' + \beta\delta' \\ \gamma\alpha' + \delta\gamma' & \gamma\beta' + \delta\delta' \end{pmatrix} \longmapsto \begin{pmatrix} \alpha\alpha' + \beta\gamma' - 1 & \alpha\beta' + \beta\delta' \\ \gamma\alpha' + \delta\gamma' & \gamma\beta' + \delta\delta' - 1 \end{pmatrix} \equiv \begin{pmatrix} \alpha\alpha' - 1 & \alpha\beta' + \beta\delta' \\ \gamma\alpha' + \delta\gamma' & \delta\delta' - 1 \end{pmatrix}$$

and note that $\alpha\alpha' - 1 \equiv (\alpha - 1) + (\alpha' - 1) \bmod p^i$. ...

To finish the lemma that $G_i \twoheadrightarrow M_2(p^i\mathbb{Z}/p^{i+1}\mathbb{Z})$ is surjective is easy. The kernel is just G_{i+1}, by definition (almost).

Conclusion:

$$\# GL_2(\mathbb{Z}/p^r\mathbb{Z}) = (p^2-1)(p^2-p)\cdot(p^4)^{r-1} = (p^r)^4 \frac{(p^2-1)(p-1)}{p^3}.$$

Hence $\# GL_2(\mathbb{Z}/N\mathbb{Z}) = N^4 \cdot \prod_{p\mid N} \frac{(p^2-1)(p-1)}{p^3}$

$\Rightarrow \# SL_2(\mathbb{Z}/N\mathbb{Z}) = N^3 \prod_{p\mid N} \frac{p^2-1}{p^2} = N^3 \prod_{p\mid N}\left(1-\frac{1}{p^2}\right).$

Hence: $[\Gamma : \Gamma(N)] = N^3 \prod_{p\mid N}\left(1-\frac{1}{p^2}\right)$

$[\Gamma : \Gamma_1(N)] = N^2 \prod_{p\mid N}\left(1-\frac{1}{p^2}\right)$

$[\Gamma : \Gamma_0(N)] = N \prod_{p\mid N}\left(1+\frac{1}{p}\right)$

We'll be interested in the degree of the map $\begin{array}{c}\Delta\backslash\mathcal{H}\\ \downarrow\\ \Gamma\backslash\mathcal{H}\end{array}$, $\Delta \subseteq \Gamma$.

This degree is not the index $[\Gamma:\Delta]$, as they do not act ~~transitively~~ faithfully.

We will then work with $\bar{\Gamma} = PSL_2(\mathbb{Z})$, $\bar{\Delta}$ = image of Δ in $PSL_2(\mathbb{Z})$.

So $[\bar{\Gamma} : \bar{\Delta}] = \begin{cases} [\Gamma:\Delta] & \text{if } -I_2 \in \Delta \\ \frac{1}{2}[\Gamma:\Delta] & \text{if } -I_2 \notin \Delta \end{cases}$

Example: $-I_2 \in \Gamma_0(N)$

$-I_2 \notin \Gamma(N)$ unless $N=2$

Next goal: understand $\Delta^{\mathcal{H}}$ as a Riemann surface in its compactification.

and interpret a function as Θ_L (L a lattice in $\mathbb{R}^n$) as "multidifferentials" on it.

Classification of elements of $GL_2(\mathbb{R})^+$:

$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $gz = \dfrac{az+b}{cz+d}$.

$$gz = z \iff az+b = (cz+d)z \iff cz^2 + (d-a)z - b = 0 \iff$$

$$\iff z = \frac{a-d \pm \sqrt{(d-a)^2+4bc}}{2c}$$

Rk: if $c=0$ and g is non-scalar, g has two fixed points: ∞, $z = \frac{b}{d-a} \in \mathbb{R}\cup\{\infty\}$ which are equal iff $d=a$.

Note: $(d-a)^2 + 4bc = (a+d)^2 - 4(ad-bc) = (\operatorname{tr} g)^2 - 4\det g$.

There are two solutions to $gz = z \iff \operatorname{tr}(g)^2 - 4\det(g) \neq 0$.

The solutions are real $\iff \operatorname{tr}(g)^2 - 4\det(g) \geq 0$.

A non-scalar $g \in GL_2(\mathbb{R})^+$ is called:

$\operatorname{tr}(g)^2 - 4\det(g)$	name	# fixed points	nature	Remarks
<0	elliptic	2	$\tau \in \mathcal{H}, \bar{\tau}$	$c \neq 0$ in this case
$=0$	parabolic	1	$\tau \in \mathbb{R}\cup\{\infty\}$	$c=0$, $a=d$ is possible
>0	hyperbolic	2	$\tau \in \mathbb{R}\cup\{\infty\}$	$c=0$, $a \neq d$ is possible

- Classification of non-scalar g in $\underline{SL_2(\mathbb{Z})}$

g elliptic $\underset{\det g=1}{\Longleftrightarrow}$ $|tr(g)| \in \{0,1\}$

$\Updownarrow$

$g \in Stab_{SL_2(\mathbb{Z})}(\tau)$

$\Updownarrow$

$\exists h \in SL_2(\mathbb{Z})$
$hgh^{-1} \in Stab_{SL_2(\mathbb{Z})}(\tau)$, for $\tau = i, \rho$.

$\Updownarrow$

g is conjugate to a matrix of the form $\left\{ \pm\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \pm\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}, \pm\begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix} \right\}$

<u>Fact</u>: The group $SL_2(\mathbb{Z})$ acts <u>transitively</u> on $\mathbb{Q} \cup \{\infty\}$ by $\begin{pmatrix} a & b \\ c & d \end{pmatrix} z = \frac{az+b}{cz+d}$:

Pf Given $\frac{a}{b} \neq \infty$ s.t $(a,b)=1 \Rightarrow \exists c,d : ac+bd=1$.

Then $\begin{pmatrix} c & d \\ -b & a \end{pmatrix} \in SL_2(\mathbb{Z})$ and $\begin{pmatrix} c & d \\ -b & a \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \infty$

Thus, if $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ is <u>parabolic</u>, then its (only) fixed point is in $\mathbb{Q} \cup \{\infty\}$, so $\exists h \in SL_2(\mathbb{Z})$ s.t $hgh^{-1} \in Stab_{SL_2(\mathbb{Z})}(\infty) = \left\{ \pm\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{Z} \right\}$

$\Rightarrow \exists b \neq 0$ s.t $hgh^{-1} = \pm\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$.

Let $\Gamma \leq SL_2(\mathbb{R})$ be a discrete subgroup $\left(\exists \varepsilon > 0 \text{ s.t } \Gamma \cap \left\{ \begin{pmatrix} 1+\alpha & \beta \\ \gamma & \delta+1 \end{pmatrix} : |\alpha|,|\beta|,|\gamma|,|\delta| < \varepsilon \right\} = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\} \right)$.

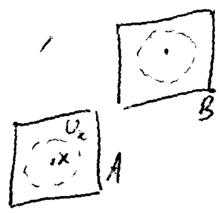
<u>Example</u>: $\Gamma \leq SL_2(\mathbb{Z}) \Rightarrow \Gamma$ discrete. (take $\varepsilon = \frac{1}{2}$).

<u>Prop</u>: Γ discrete $\Rightarrow$ it acts properly discontinuously on $\mathcal{H}$.
(i.e. $\forall x, y \in \mathcal{H}$ (equal or not) $\exists$ open sets $x \in U_x \subseteq \mathcal{H}$, $y \in U_y \subseteq \mathcal{H}$ s.t
$\#\{\gamma \in \Gamma : (\gamma U_x) \cap U_y \neq \emptyset\}$ is finite.

Corollary: The $\mathrm{Stab}_\Gamma(x)$ is finite, $\forall x \in \mathcal{H}$.
(we already know it for $\Gamma \subseteq SL_2(\mathbb{Z})$, and then $|\mathrm{Stab}_\Gamma(x)| \leq 6$)

Exercise: $\forall x, y \in \mathcal{H}$, $\exists$ open sets $x \in U_x$, $y \in U_y$ s.t.
$\forall \gamma \in \Gamma$, ~~#~~ $[\gamma U_x \cap U_y \neq \emptyset \Rightarrow \gamma x = y]$

Proof (of Prop): Enough to show: if $A = [\alpha_1, \alpha_2] \times [\alpha_3, \alpha_4] \subseteq \mathcal{H}$,
$B = [\beta_1, \beta_2] \times [\beta_3, \beta_4] \subseteq \mathcal{H}$



then $\#\{\gamma \in \Gamma : \gamma A \cap B \neq \emptyset\}$ is finite.

(need A, B just to be compact sets with nonempty interior)

Claim: Let $G_A := \{g \in SL_2(\mathbb{R}) : g(i) \in A\}$. Then G_A is compact, and
closed + bounded

$G_A \cdot i = A$

Pf/ Know that $SL_2(\mathbb{R})$ acts transitively on $\mathcal{H}$.

Given $x + iy \in A$, then $\begin{pmatrix} \sqrt{y} & x/\sqrt{y} \\ 0 & \frac{1}{\sqrt{y}} \end{pmatrix}^{\in SL_2(\mathbb{R})} i = x + iy$.

So $G_A\, i = A$, and we have a map
$$A \to G_A$$
$$x + iy \mapsto \begin{pmatrix} \sqrt{y} & x/\sqrt{y} \\ 0 & 1/\sqrt{y} \end{pmatrix}$$

Any other elt. of $SL_2(\mathbb{R})$ taking $i \mapsto x + iy$ is this matrix times a matrix in $SO_2(\mathbb{R}) \cong \{|z| = 1\}$, compact.

Hence
$$A \times SO_2(\mathbb{R}) \to G_A$$
$$(x+iy, M) \longmapsto \begin{pmatrix} \sqrt{y} & x/\sqrt{y} \\ 0 & 1/\sqrt{y} \end{pmatrix} \cdot M$$
is a continuous surjective map.

A and $SO_2(\mathbb{R})$ compact $\Rightarrow$ $A \times SO_2(\mathbb{R})$ is compact $\Rightarrow$ G_A is compact.

(claim)

(cont pf of prop):

Now, $\{\gamma\in\Gamma : \gamma A\cap B \neq \emptyset\} = \{\gamma\in\Gamma : (\gamma G_A i)\cap(G_B i)\neq\emptyset\} = \{\gamma\in\Gamma : \gamma\in G_B G_A^{-1}\} =$

$= \underbrace{\Gamma}_{\text{discrete}} \cap \underbrace{G_B G_A^{-1}}_{\text{compact}}$ ← finite set

($G_B G_A^{-1}$ is compact b/c $G_A\times G_B \to G_B G_A^{-1}$, $(M,N)\mapsto MN^{-1}$ is cont. surjective.)

- Cusps:

Let $\Gamma \subseteq SL_2(\mathbb{R})$ a discrete subgroup.

Let $P_\Gamma :=$ cusps of Γ = {points in $\mathbb{R}\cup\{\infty\}$ fixed by some parabolic element of Γ}.

Examples: $\Gamma = SL_2(\mathbb{Z})$. Then $P_\Gamma = \mathbb{Q}\cup\{\infty\}$.

Note: P_Γ is always a union of Γ-orbits [if $c\in\mathbb{R}\cup\{\infty\}$, γ parabolic (nonscalar), $\gamma c = c$, then if $\sigma\in\Gamma$, $\sigma\gamma\sigma^{-1}(\sigma c) = \sigma c$, and $\sigma\gamma\sigma^{-1}$ is parabolic (nonscalar) so σc is also a cusp].

Hence, in the example of $\Gamma = SL_2(\mathbb{Z})$, it is enough to show that ∞ is a cusp of Γ. ok, b/c $\begin{pmatrix}1&1\\0&1\end{pmatrix}\in\Gamma$ (and is ~~[illegible]~~ parabolic).

Example: if $[\Gamma:\Gamma_1]<\infty$, then $P_\Gamma = P_{\Gamma_1}$ (for any $\Gamma\leq SL_2(\mathbb{R})$).

Pf $P_{\Gamma_1}\subseteq P_\Gamma$ is clear. Now let $x\in P_\Gamma$. Then $\gamma x = x$ for some $\gamma\in\Gamma$ parabolic. ~~[illegible]~~

So $\exists N$ s.t. $\gamma^N\in\Gamma_1$, and $\gamma^N x = x$. Why is γ^N parabolic?

$\gamma\in SL_2(\mathbb{R})$, $\gamma = \begin{pmatrix}a&b\\c&d\end{pmatrix}$ is parabolic, so the eigenvalues of γ are the roots of its char. poly, $X^2-(a+d)X+(ad-bc)$, and so they are equal (disc $=0$) (and multiply to 1)

$\Rightarrow$ J.C.F of γ is either $\begin{pmatrix}1&\lambda\\0&1\end{pmatrix}$, $\begin{pmatrix}-1&\lambda\\0&-1\end{pmatrix}$, $\lambda\neq0$ b/c γ non scalar.

Then the JCF of g^N is either $\begin{pmatrix} 1 & N\lambda \\ 0 & 1 \end{pmatrix}$ or $\begin{pmatrix} (-1)^N & N\lambda \\ 0 & (-1)^N \end{pmatrix}$, still non-scalar.

(end of example)

Remark: two commensurable Γ_1, Γ_2 have the same set of cusps. (corollary to that).

Exercise: (A discrete "large" subgroup of $SL_2(\mathbb{R})$ with no cusps).

a) Prove that $x^2+y^2-3z^2-3w^2$ doesn't represent 0 over $\mathbb{Q}$

(may use that if $n=a^2+b^2$ integers, $\Leftrightarrow$ every prime $p \equiv 3\ (4)$ st $p \mid n$, divides n to an even power).

b) The vectorspace $\mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}j \oplus \mathbb{Q}k = B$ has an algebra structure under $i^2=-1$, $j^2=3$, $k^2=3$, $ij=k=-ji$

It can be realised as a subalgebra of the 2×2 matrices on $\mathbb{Q}(\sqrt{3}) \subseteq \mathbb{R}$, as follows: $a+bj+ci+dk \mapsto \begin{pmatrix} a+b\sqrt{3} & -(c-d\sqrt{3}) \\ c+d\sqrt{3} & a-b\sqrt{3} \end{pmatrix}$.

Verify this.

Note: $\det = a^2+c^2-3b^2-3d^2$.

c) Prove that B is a division algebra.

Prove that $B^\times \subseteq GL_2(\mathbb{R})$ cannot contain a parabolic element.

d) Let $\mathcal{O} = \{a+bi+cj+dk \mid a,b,c,d \in \mathbb{Z}\}$.

Prove that $\mathcal{O}_1^\times$ = units of norm (det) $= 1$ is an infinite discrete subgroup of $SL_2(\mathbb{R})$ with no cusps.

Remark: the same works for any quat. alg. $/\mathbb{Q}$, $\not\cong M_2(\mathbb{Q})$ indefinite, and for any order $\mathcal{O}$.

• Constructing $\Gamma\backslash\mathcal{H}^*$ as a Riemann surface (see Diamond & Shurman).

Assume that $\Gamma \subseteq SL_2(\mathbb{Z})$, to simplify.

<u>Lemma</u>: If $\Gamma \subseteq \Gamma_1(N)$ for some $N > 3$, then $\overline{\Gamma}$ = image of Γ in $PSL_2(\mathbb{Z})$ has no elliptic elements.

Same if $\Gamma \subseteq \Gamma(N)$ for $N \geq 3$.

Pf Let $g \in \Gamma$ be an elliptic element, $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

$tr(g)^2 < 4\det(g) = 4 \Rightarrow |tr(g)| \in \{0,1\}$.

On the other hand, $g \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod N$, so $\overset{\{-1,0,1\}}{\overbrace{a+d}} = 2 + kN$, which is not possible if $N > 3$

If $N = 3$, $\Gamma \subseteq \Gamma(3)$, then: $a + d = 2 + 3k' \in \{-1,0,1\}$.

So $a + d = -1 \Rightarrow a = -(1+d)$. Write $d = 1 + 3k$, and have:

$$g = \begin{pmatrix} -(2+3k) & 3b' \\ 3c' & 1+3k \end{pmatrix} \Rightarrow 1 = \det g = -(2+3k)(1+3k) - 9b'c' \Rightarrow$$

$$\Rightarrow 3 = -9k + 9k^2 - 9b'c' \Rightarrow !! \quad (9 \nmid 3!)$$

<u>Comment</u>: once that one has an interpretation as modular curves, one can deduce that if $\sigma \in Aut(E)$, $E/\mathbb{C}$ an elliptic curve and either σ fixes a point of order $N > 3$ or acts trivially on the 3-torsion $E[3]$, then $\sigma = id$.

For Γ with $\overline{\Gamma}$ having no elliptic elements, the action of $\overline{\Gamma}$ on $\mathcal{H}$ is <u>free</u> and, in fact, $\forall x \in \mathcal{H}$, $\exists U_x$ s.t. $\gamma U_x \cap U_x = \emptyset$ if $\gamma \neq 1$ in $\overline{\Gamma}$.

In this case, give ${}_\Gamma\backslash\mathcal{H}$ the quotient topology ($\mathcal{H}$ usual top. as metric space $\subseteq \mathbb{C}$).

So $U \subseteq {}_\Gamma\backslash\mathcal{H}$ is open iff $\pi^{-1}(U) \subseteq \mathcal{H}$ is open, where $\pi : \mathcal{H} \twoheadrightarrow {}_\Gamma\backslash\mathcal{H}$.

<u>Claim</u>: ${}_\Gamma\backslash\mathcal{H}$ is naturally a Riemann surface.

* <u>${}_\Gamma\backslash\mathcal{H}$ is Hausdorff</u> (T_2): given $\bar{x}, \bar{y} \in {}_\Gamma\backslash\mathcal{H}$, $\bar{x} \neq \bar{y}$, can separate them by open sets. Choose $x, y \in \mathcal{H}$ lifts of $\bar{x}, \bar{y}$ resp.

  Clearly, $x \neq y$. In fact, $y \notin \Gamma x$. We need $U_x \ni x$ s.t $\forall \gamma \in \Gamma$,

  $\gamma U_x \cap U_y = \emptyset$.

  We can do that by some previous remark (Γ is discrete!).

* <u>2^{nd} countable</u>: need a countable collection of open sets s.t every open is a ~~open~~ is a union of elements from that collection

  But $\mathcal{H}$ is 2^{nd}-countable: $\forall x \in \mathbb{Q}^2 \cap \mathcal{H}$, $\forall n \geq 1$, take open balls ~~$B_x(\frac{1}{n})$~~ $B_{\frac{1}{n}}(x)$

  It's not hard to show that ${}_\Gamma\backslash\mathcal{H}$ is 2^{nd} countable, too.

* <u>Complex structure</u>: given $x \in \mathcal{H}$, take <u>small</u> balls $B^\circ(x, \frac{1}{a})$ as charts around $\bar{x}$ s.t $B^\circ(x, \frac{1}{a}) \simeq \pi(B^\circ(x, \frac{1}{a}))$.

* <u>check that transition maps are (bi) holomorphic.</u>

  The transition maps are (restrictions of) maps of the form $z \mapsto \gamma z$, and $\Gamma \subseteq SL_2(\mathbb{Z}) \subseteq GL_2(\mathbb{C})$ are holomorphic on $\mathbb{C} \cup \{\infty\}$.

<u>Q</u>: What if Γ <u>does have</u> elliptic elements?

Assume furthermore that $\Gamma \leq SL_2(\mathbb{Z})$ has finite index.

If $\bar\Gamma$ has elliptic elements: Let $\Gamma' := \bar\Gamma \cap \bar\Gamma(3)$. Then Γ' has no elliptic elements, so $\Gamma' \backslash \mathcal{H}$ is defined as a Riemann surface, and $\Gamma \backslash \mathcal{H}$ is a ~~topological~~ Hausdorff 2^{nd}-countable space.

$$\begin{array}{c} \Gamma' \backslash \mathcal{H} \\ \downarrow \\ \Gamma \backslash \mathcal{H} \end{array} \quad \text{is a continuous surjective map.}$$

It is a general fact: let S_1 be a Riemann surface, which is connected (not necessarily compact). Let S_2 be a top. space 2^{nd} count. + T_2.

Let $S_1 \xrightarrow{f} S_2$ be a surjective continuous map with finite fibers.

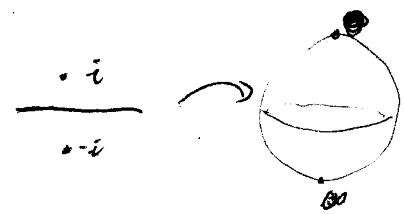
Then $\exists!$ complex structure on S_2 making f a map of R.S.'s.

In our case, any elliptic element $\neq \pm I_2$, is conjugate to $\pm\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \pm\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}, \pm(\cdot\,\cdot)$.

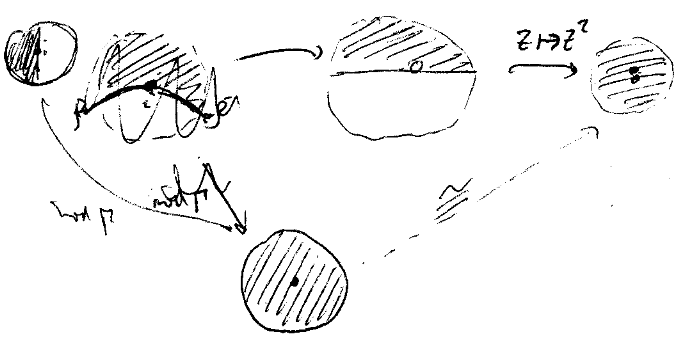
To sketch the argument, let us assume that this element is $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

The fixed points are $i, -i$.

Apply $\begin{pmatrix} 1 & -i \\ 1 & i \end{pmatrix}$, which takes $\begin{array}{l} i \mapsto 0 \\ -i \mapsto \infty \end{array}$. So



Takes also a circle around i to a circle around 0:



The induced action of $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ on the disk is:

$$z \longmapsto \begin{pmatrix} 1 & -i \\ 1 & i \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & -i \\ 1 & i \end{pmatrix}^{-1} z = -z$$

Let $\begin{matrix} S_1 \\ \pi \downarrow \\ S_2 \end{matrix}$ be a surjective map of Riemann Surfaces.

Let $s_1 \in S_1$, $s_2 \in S_2$ s.t $\pi(s_1) = s_2$.

Let t_2 be a local parameter around s_2, and t_1 a local param. around s_1.

$\pi^* t_2$ is a germ of analytic function around s_1.

So $\pi^* t_2 = t_1^e (a_0 + a_1 t_1 + a_2 t_1^2 + \cdots)$, $a_i \in \mathbb{C}$.

We know that $e \geq 1$ is the ramification index.

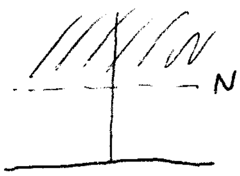
We say that π is ramified at s_1 if $e > 1$.

<u>General Lemma</u>: In this situation, we can always find local charts around s_1 and s_2 s.t the map in local coordinates is $z \mapsto z^e$.

Let now $\mathcal{H}^* := \mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})$.

$\Gamma \subseteq PSL_2(\mathbb{Z})$ acts on $\mathcal{H}^*$. We extend the topology of $\mathcal{H}$ on $\mathcal{H}^*$:

We add the following open sets:

→ For $i\infty$, a basis of nbhds is  $= \{ \mathrm{Im}(z) > N \}$.

→ For $p/q \in \mathbb{Q}$, tangent open disks $\cup \{p/q\}$:

<u>Facts</u>: $PSL_2(\mathbb{Z})$ acts continuously on $\mathcal{H}^*$ (in fact, respects these local basis)

The points in $\mathbb{P}^1(\mathbb{Q})$ (and their images in $_\Gamma\backslash^{\mathcal{H}^*}$) are called <u>cusps</u>.

In $_\Gamma\backslash^{\mathcal{H}^*}$, there are finitely-many cusps (b/c $SL_2(\mathbb{Z})$ acts <u>transitively</u> on $\mathbb{P}^1(\mathbb{Q})$).

The set $_{\Gamma}\backslash\mathcal{H}^*$ is given again the quotient topology.

It can be made into ~~an~~ Riemann Surface.

One checks that $_{\Gamma}\backslash\mathcal{H} \hookrightarrow {}_{\Gamma}\backslash\mathcal{H}^*$.

* 2^{nd} countable: just add $\{\operatorname{Im}(z) > N\}$ $N \in \mathbb{Z}_{>0}$, $\{$disks of radius $\frac{1}{N}\}$ around $p/q \in \mathbb{Q}$.
* T2: need to separate cusps, and $\bar{x} \in {}_{\Gamma}\backslash\mathcal{H}$ from a cusp.

Suppose $x \in \mathcal{H}$, and want to separate it from $i\infty$

(for other cusps, reduce to this by action of $SL_2(\mathbb{Z})$).

(WLOG can assume $\Gamma = SL_2(\mathbb{Z})$, as this is harder than for general Γ).

Recall that $\operatorname{Im}(\gamma x)$, $\gamma \in SL_2(\mathbb{Z})$ has a finite maximum, say N_x.

Then use $\{\operatorname{Im}(z) > N_x + 1\}$ + open disk around x, of radius $\frac{1}{2}$.

<u>Exercise</u>: Let $D_\infty = \{\operatorname{Im}(z) \geq 1\}$, $D_\infty^- = \{\operatorname{Im}(z) > 1\}$.

For $p/q \in \mathbb{Q}$, $D_{p/q} = \{\tau \in \mathcal{H} : |\tau - (p/q + \frac{i}{2q^2})| \leq \frac{1}{2q^2}\}$. closed circle of radius $\frac{1}{2q^2}$ around $\frac{p}{q} + i\frac{1}{2q^2}$

$D_{p/q}^- = \{\tau \in \mathcal{H} : |\tau - (p/q + \frac{i}{2q^2})| < \frac{1}{2q^2}\} \cup \{p/q\}$.

<u>Prove</u> that if $\gamma \in SL_2(\mathbb{Z})$ is s.t. $\gamma\infty = p/q$, then

$\gamma(D_\infty) = D_{p/q}$, $\gamma(D_\infty^-) = D_{p/q}^-$.

Deduce an action of $SL_2(\mathbb{Z})$ on $\{D_c^{(-)} : c \in \mathbb{P}^1(\mathbb{Q})\}$

Prove that if $x \neq y \in \mathbb{P}^1(\mathbb{Q})$, then $D_x^- \cap D_y^- = \emptyset$, $D_x \cap D_y$ has at most one point.

<u>Note</u>: in particular, $_{\Gamma}\backslash\mathcal{H}^*$ is T_2 for cusps.

<u>Prove</u> that if $0 \leq x < y \leq 1$, then $D_x \cap D_y \neq \emptyset \iff x, y$ are consecutive terms in some Farey series.

[Farey series: for each level $n = 1, 2, 3, \dots$

(1) $\frac{0}{1}$ $\frac{1}{1}$

(2) $\frac{0}{1}$ $\frac{1}{2}$ $\frac{1}{1}$

(3) $\frac{0}{1}$ $\frac{1}{3}$ $\frac{1}{2}$ $\frac{2}{3}$ $\frac{1}{1}$

(4) $\frac{0}{1}$ $\frac{1}{4}$ $\frac{1}{3}$ $\frac{1}{2}$ $\frac{2}{3}$ $\frac{3}{4}$ $\frac{1}{1}$

(5) $\frac{0}{1}$ $\frac{1}{5}$ $\frac{1}{4}$ $\frac{1}{3}$ $\frac{2}{5}$ $\frac{1}{2}$ $\frac{3}{5}$ $\frac{2}{3}$ $\frac{3}{4}$ $\frac{4}{5}$ $\frac{1}{1}$.

i.e. fractions $\left\{ \frac{i}{j} : \begin{array}{l} 0 \le i \le j \\ 1 \le j \le n \end{array} \right\}$, well-ordered.

Fact: $\frac{n}{k} < \frac{n+n'}{k+k'} < \frac{n'}{k'}$ $\forall n, n', k, k'$. $\Rightarrow$ recursive construction.

Fact: $\frac{n}{k}, \frac{n'}{k'}$ (in reduced form) are consecutive members of some Farey sequence if, and only if, $|nk' - kn'| = 1$.]

Hint: think that either $\begin{pmatrix} n & n' \\ k & k' \end{pmatrix}$ or $\begin{pmatrix} n' & n \\ k' & k \end{pmatrix}$ in $SL_2(\mathbb{Z})$. (for the exercise)

* Complex structure at the cusps: (more details in Diamond & Shurman).

Consider the cusp $i\infty$. For $N \gg 0$, the action of Γ on $\{\mathrm{Im}(z) > N\}$ reduces to $\mathrm{Stab}_\Gamma(i\infty) = \left\{ \pm \begin{pmatrix} 1 & Ma \\ 0 & 1 \end{pmatrix} : a \in \mathbb{Z} \right\}$ (M a positive integer).

(So the action of Γ is $z \mapsto z + M$).

The map $U_N := \{\mathrm{Im}(z) > N\} \xrightarrow[e^{2\pi i z/M}]{}$ open disk around 0 of radius $e^{-2\pi N/M}$

induces a ~~biholomorphic~~ homeomorphism map $\Gamma \backslash U_N = \mathrm{Stab}_\Gamma(\infty) \backslash U_N \longrightarrow$ open disk around 0.

<u>Theorem</u>: ${}_{\Gamma}\backslash\mathcal{H}^*$ is a <u>compact</u> R.S.

<u>Pf (sketch)</u>: $\mathcal{H}^*$ connected $\Rightarrow {}_{\Gamma}\backslash\mathcal{H}^*$ connected.

So ${}_{\Gamma}\backslash\mathcal{H}^*$ is a connected R.S.

Why is it compact?

First, let $\Gamma = SL_2(\mathbb{Z})$. In this case, ${}_{\Gamma}\backslash\mathcal{H}^* \underset{\text{homeom.}}{\cong}$  $= S^2$.

So ${}_{\Gamma}\backslash\mathcal{H}^*$ is compact, and ${}_{\Gamma}\backslash\mathcal{H}^* \cong \mathbb{P}^1(\mathbb{C})$ ($\exists!$ Riemann Surface homeom. to S^2).

For general Γ, write $PSL_2(\mathbb{Z}) = \coprod g_i \bar{\Gamma}$.

Given $z \in \mathcal{H}^*$, $\exists g_i$ and $g \in \bar{\Gamma}$ s.t. $g_i g z \in D^*$ $\longrightarrow$ ,

or equiv, $gz \in g_i^{-1} D^*$.

So $\coprod_i g_i^{-1}(D^*)$ is a "fundamental domain" for $\bar{\Gamma}$ (maybe not connected).

The map $\mathcal{H}^* \longrightarrow {}_{\Gamma}\backslash\mathcal{H}^*$ factors through $\bigcup_i g_i(D^*)$ = finite union of compact sets.

(as $D^* = D \cup \{i\infty\}$ is compact).

Therefore, the image ${}_{\Gamma}\backslash\mathcal{H}^*$ is compact.

<u>Hurwitz's genus formula</u>:

Let S_1, S_2 be cpct Riemann surfaces of genus g_1, g_2, resp. Then if $\pi: S_1 \to S_2$ is a surjective morphism,

$$2(g(S_1)-1) = \deg(\pi)\cdot 2(g(S_2)-1) + \sum_{i=1}^{n}(e_i - 1)$$

where $\alpha_1, \ldots, \alpha_n$ are the ramification points of π of indexes $e_1, \ldots, e_n$.

Remarks.

- There are only finitely-many ramification points.
- The degree of π is $\#\{\pi^{-1}(z)\}$ for a "general" $z \in S_2$.

  More generally, if $\pi^{-1}(z) = \{p_1, \dots, p_g\}$ of ramification order $e_1, \dots, e_g$,

  then $e_1 + e_2 + \dots + e_g = \deg \pi$.

Example: $S_1 = S_2 = \mathbb{P}^1(\mathbb{C})$, $\pi(z) = z^n$.

$$\pi^{-1}(z) = \{\mu z : \mu = e^{2\pi i a/n}, \ 0 \leq a < n\}.$$

There are no ramification points besides points mapping to 0 and ∞ (which are 0 and ∞, actually).

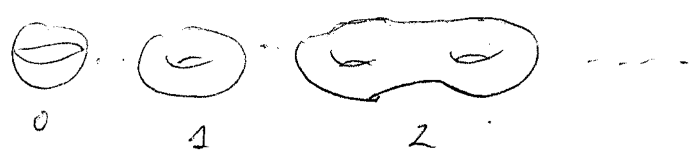
So $\deg \pi = n$, $\pi^{-1}(0) = 0$, and $\pi^* z = z^{n} \Rightarrow n$ is the ram. order of 0.

$\frac{1}{z}$ and $\frac{1}{z}$ are local params. at ∞, as $\pi^*\left(\frac{1}{z}\right) = \frac{1}{z^n} = \left(\frac{1}{z}\right)^n \Rightarrow n$ is ram. index at ∞.

Then $2 \cdot 0 - 2 = n \cdot (2 \cdot 0 - 2) + (n-1) + (n-1)$ ✓.

Q: What is the genus?

A (misleading): every R.S. is homeom. to a compact oriented surface, so it is homeom. to:



The complex solutions to a non-singular homog. equ^{n} $f(x,y,z) = 0$ in $\mathbb{P}^2(\mathbb{C})$.

This meets any line, so it's not that similar to the models drawn above...

If f has degree d, then this has genus $\frac{(d-1)(d-2)}{2}$.

Also, $H_1(S, \mathbb{Z}) \simeq \mathbb{Z}^{2g}$

$H^0(S, \Omega^1_S) =$ space of global holo. differential forms on $S \simeq \mathbb{C}^g$.

Exercise: $\Gamma \leq SL_2(\mathbb{Z})$ of finite index, $d = [PSL_2(\mathbb{Z}) : \bar{\Gamma}]$.

$X(\Gamma) = {}_{\Gamma}\backslash \mathcal{H}^*$, $Y(\Gamma) = {}_{\Gamma}\backslash \mathcal{H}$.

$d = \text{degree}\left(X(\Gamma) \to X(SL_2(\mathbb{Z}))\right)$.

Let ε_2 (resp ε_3) be the number of elliptic points of Γ of order 2 (resp. 3): the points in ${}_{\Gamma}\backslash \mathcal{H}$ whose stabilizer in Γ is of order 2 (resp. 3).

Let ε_∞ = number of cusps of Γ = $\#\left(X(\Gamma) \setminus Y(\Gamma)\right)$ = # orbits of Γ in $\mathbb{P}^1(\mathbb{Q})$

Prove: $g(X(\Gamma)) = 1 + \frac{d}{12} + \frac{1}{4}\varepsilon_2 - \frac{1}{3}\varepsilon_3 - \frac{1}{2}\varepsilon_\infty$

Exercise: The case of $X_0(p) = X(\Gamma_0(p))$.

1) Find coset reps for $\Gamma_0(p)$ in $SL_2(\mathbb{Z})$.
(verify again that $[PSL_2(\mathbb{Z}) : \overline{\Gamma_0(p)}] = p+1$)

2) Prove that $\varepsilon_\infty = 2$ (in fact, 0 and ∞ are the two cusps).

3) Calculate $\varepsilon_2, \varepsilon_3$ using (1).

4) Deduce that $X_0(2), X_0(3)$ have genus 0, and for $p > 3$, $g(X_0(p)) = \cancel{\frac{p+1}{12}}$ is

$$\frac{p+1}{12} - \frac{1}{4}\left(1 + \left(\frac{-1}{p}\right)\right) - \frac{1}{3}\left(1 + \left(\frac{-3}{p}\right)\right).$$

5) Find all $X_0(p)$ of genus 0 or 1.

• The modular curve $X(N) = X(\Gamma(N))$.

$\Gamma(N) = \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod N \} \trianglelefteq SL_2(\mathbb{Z})$.

Lemma: Let A be a group acting transitively on a set S. Let $s_0 \in S$. Let $B \trianglelefteq A$. Then the number of orbits of B in S is

$$[A : \Gamma B] \quad \text{where } \Gamma = \mathrm{Stab}_A(s_0).$$

Pf A acts on the orbits of B by: $a * (Bs) := B(as)$ (thanks to $B \trianglelefteq A$).

This action is transitive. By general theory,

$$\text{Orbits of } B \overset{1:1}{\Longleftrightarrow} \text{cosets of } \mathrm{Stab}_A(\text{particular orbit}) \Longleftrightarrow \text{Cosets of } \mathrm{Stab}_A(B \cdot s_0) \overset{\text{check}}{=} \Gamma B = B\Gamma.$$

Now consider $A = SL_2(\mathbb{Z})$, $B = \Gamma(N)$, $S = \mathbb{P}^1(\mathbb{Q})$. Let $s_0 = \infty$.

Then $\varepsilon_\infty = [SL_2(\mathbb{Z}) : \{ \pm \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} : a \in \mathbb{Z} \} \cdot \Gamma(N)] = [SL_2(\mathbb{Z}) : \{\pm I\} \cdot \Gamma_1(N)] =$

$$= [PSL_2(\mathbb{Z}) : \overline{\Gamma_1(N)}] = \begin{cases} 3 & N = 2 \\ \frac{1}{2} N^2 \prod_{p \mid N} \left(1 - \frac{1}{p^2}\right) & N \neq 2 \end{cases}$$

Now, $\varepsilon_2 = \varepsilon_3 = 0$ because if x is elliptic point of order 2 (resp 3)

$\exists \gamma$ s.t. $x = \gamma i$ (resp $x = \gamma \rho$) and
$$\begin{cases} \gamma \{ \pm \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \} \gamma^{-1} \subseteq \Gamma(N) & (2) \\ \gamma \{ \pm \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \} \gamma^{-1} \subseteq \Gamma(N) & (3) \end{cases}$$

$$\Leftrightarrow \begin{cases} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in \gamma^{-1} \Gamma(N) \gamma \overset{\Gamma(N) \trianglelefteq SL_2(\mathbb{Z})}{=} \Gamma(N) \\ \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \in \gamma^{-1} \Gamma(N) \gamma = \Gamma(N) \end{cases} \quad \text{which is never true.}$$

Using the previous exercise and that $[PSL_2(\mathbb{Z}) : \Gamma(N)]$ is known,

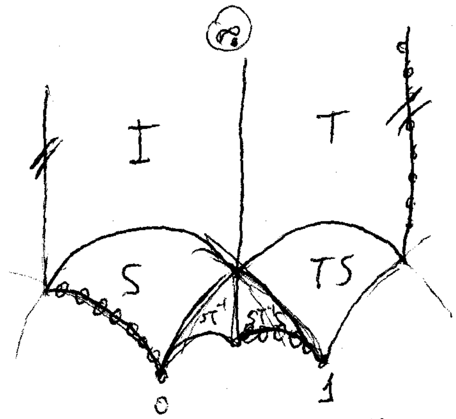
we conclude that

$$\mathrm{genus}(X(N)) = \begin{cases} 0 & N = 2 \\ 1 + \frac{N-6}{12N} \overbrace{N^3 \prod_{p \mid N} \left(1 - \frac{1}{p^2}\right)}^{\text{degree}} & N \geq 3 \end{cases}$$

Example: $X(2)$

The cosets of $\Gamma(2)$ in $PSL_2(\mathbb{Z})$ have reps given by:

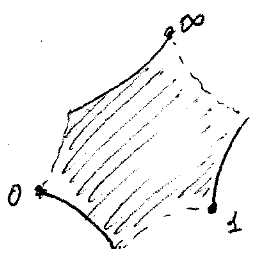
$I=\begin{pmatrix}1&0\\0&1\end{pmatrix}$ $T=\begin{pmatrix}1&1\\0&1\end{pmatrix}$ $S=\begin{pmatrix}0&-1\\1&0\end{pmatrix}$ $TS=\begin{pmatrix}1&-1\\1&0\end{pmatrix}$ $ST^{-1}=\begin{pmatrix}0&-1\\1&-1\end{pmatrix}$ $ST^{-1}S=\begin{pmatrix}-1&0\\-1&-1\end{pmatrix}$



Fundamental domain for $\Gamma(2)$

line excluded

$T^2\in\Gamma(2)$. Q: what about the other edges? How are they identified?



Modular Forms

Let $\gamma=\begin{pmatrix}a&b\\c&d\end{pmatrix}\in SL_2(\mathbb{R})$. We call the function $j(\gamma,\tau)=c\tau+d$,

$$j: SL_2(\mathbb{R})\times\mathcal{H}\to\mathbb{C}$$

a factor of automorphy.

It satisfies: $j(\gamma_1\gamma_2,\tau)=j(\gamma_1,\gamma_2\tau)\cdot j(\gamma_2,\tau)$ (just check it!)

Let $\Gamma\subseteq SL_2(\mathbb{Z})$ be a subgroup of finite index.

A holomorphic function $f:\mathcal{H}\to\mathbb{C}$ is called a "very weak modular form" of weight $k\in\mathbb{Z}$ if $f(\gamma\tau)=j(\gamma,\tau)^k f(\tau)$ $\forall\gamma\in\Gamma$.

Notation: $(f|_k\gamma)(\tau) := j(\gamma,\tau)^{-k} f(\gamma\tau)$.

The rule $f \rightsquigarrow f|_k\gamma$ defines a group action of Γ on the holomorphic functions $f: \mathcal{H} \to \mathbb{C}$

The "very weak modular forms of weight k for Γ" are the fixed functions under Γ acting by $|_k\gamma$.

- Check that $f \rightsquigarrow f|_k\gamma$ is a group action:

$$((f|\gamma_1)|\gamma_2)(\tau) = (f|\gamma_1)(\gamma_2\tau)\cdot j(\gamma_2,\tau)^{-k} = f(\gamma_1\gamma_2\tau)\, j(\gamma_1,\gamma_2\tau)^{-k} j(\gamma_2\tau)^{-k}$$
$$= f(\gamma_1\gamma_2\tau)\cdot j(\gamma_1\gamma_2,\tau)^{-k} = (f|(\gamma_1\gamma_2))(\tau) \quad //$$

The cusps of Γ are the same as those of $SL_2(\mathbb{Z})$ (the fun grps are commensurable). So $i\infty$ is a cusp of Γ, whose stabilizer in $\bar{\Gamma} \subseteq PSL_2(\mathbb{Z})$ has the form $\left\{\begin{pmatrix} 1 & a\mathbb{Z} \\ 0 & 1\end{pmatrix}\right\}$ for some $a \in \mathbb{Z}_{>0}$.

The positive integer a is called the fun width of the cusp $i\infty$.

$$\begin{pmatrix} 1 & a \\ 0 & 1\end{pmatrix} \in \Gamma \Rightarrow f|_k\gamma = f \Rightarrow f(\tau+a) = f(\tau) \quad \forall \tau \in \mathcal{H}.$$

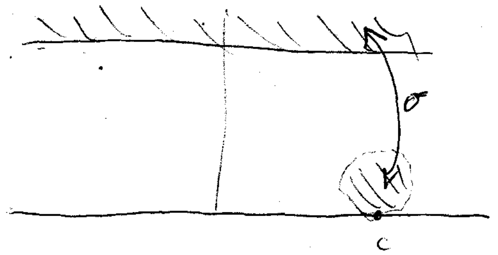
Then f has a Fourier expansion in the variable $q^{\frac{1}{a}}$, $q = e^{2\pi i\tau}$.

$$f(\tau) = \sum_{n\in\mathbb{Z}} a_n(f)\left(q^{\frac{1}{a}}\right)^n.$$

Let c be any other cusp of Γ. Choose $\sigma \in SL_2(\mathbb{Z})$ s.t. $c = \sigma\cdot(i\infty)$.

Consider $f|_k\sigma$. Its behavior near $i\infty$ is the behavior of f near c.

In other words, there is a conformal mapping



Further, $f|_k\sigma$ is very weakly modular relative to $\sigma^{-1}\Gamma\sigma \underset{\text{finite index}}{\subseteq} SL_2(\mathbb{Z})$

Let a_σ be the width of $i\infty$ relative to $\sigma^{-1}\Gamma\sigma$

(which we also call the width of c relative to Γ).

$\left(a_\sigma = [\mathrm{Stab}_{PSL_2(\mathbb{Z})}(c) : \mathrm{Stab}_{\overline{\Gamma}}(c)]. \right)$

Then $f|_k\sigma$ has a Laurent expansion at $i\infty$ in the variable $q^{\frac{1}{a_\sigma}}$

$$(f|_k\sigma)(\tau) = \sum_{n=-\infty}^{+\infty} a_{n,\sigma}(f)\left(q^{1/a_\sigma}\right)^n .$$

The coefficients $a_{n,\sigma}(f)$ do depend on σ (not just on c).

But: $\inf_n \{a_{n,\sigma} \neq 0\}$ does not.

Why: σ is well-defined up to $\mathrm{Stab}_{PSL_2(\mathbb{Z})}(i\infty) = \{\begin{pmatrix} 1 & \mathbb{Z} \\ 0 & 1 \end{pmatrix}\}$.

$f|_k(\sigma\gamma) = f|_k\sigma|_k\gamma$, so we need to understand the effect of $f \rightsquigarrow f|_k\gamma$, $\gamma = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ $(\mathrm{Stab}_{PSL_2(\mathbb{Z})}(i\infty) = \langle\gamma\rangle)$ on the q-expansion at $i\infty$. (where f is modular of wt k relative to Γ)

$(f|_k\gamma)(\tau) = f(\tau+1)$. Write $f(\tau) = \sum_n a_n(f)\left(q^{\frac{1}{a}}\right)^n$

$$f(\tau+1) = \sum_n a_n(f)\left(e^{\frac{2\pi i(\tau+1)}{a}}\right)^n$$

So $f(\tau+1) = \sum_n a_n(f) \left(e^{\frac{2\pi i}{a}}\right)^n q^{\frac{1}{a}}$, write $\zeta_a := e^{\frac{2\pi i}{a}}$.

Then $f(\tau+1) = \sum_n (a_n(f) \cdot \zeta_a^n)\, q^{\frac{1}{a}}$, so the q-expansion of f at a cusp depend on the choice of σ up to roots of unity.

Def: Let f be a very weak modular form relative to Γ.

- f is called a <u>weak modular form</u> if $N_\sigma = \inf_n \{ a_{n,\sigma}(f) \neq 0 \} > -\infty$ for all cusps c of Γ (finitely-many conditions, as $\Gamma \backslash \mathbb{P}^1(\mathbb{Q})$ is finite).
- f is called a <u>modular form</u> if $N_\sigma \geq 0$ $\forall$ cusps.
- f is called a <u>cusp form</u> if $N_\sigma > 0$ $\forall$ cusps.

Theorem: Let n be an integer, $n \equiv 0 \pmod 8$. Let $L \subseteq \mathbb{R}^n$ be an even unimodular lattice (e.g. E_8, $E_8 \oplus E_8$, D_{16}^+, Λ_{24}, ...)

Then $\Theta_L(q) = \sum_{\lambda \in \Lambda} q^{\lambda \cdot \lambda / 2}$, $q = e^{2\pi i z}$ is a modular form for $\Gamma = SL_2(\mathbb{Z})$, of weight $\frac{n}{2}$.

Pf/ Since $SL_2(\mathbb{Z})$ is generated by $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, it suffices to show that the functional equations for S and T hold.

$f|_k T = f$ is clear from $e^{2\pi i \tau \frac{\lambda \cdot \lambda}{2}}$ ← integer, which is invariant under $\tau \mapsto \tau+1$.

We have proven, for L unimodular, that $\Theta_L(z) = \left(\frac{i}{z}\right)^{n/2} \Theta_L\left(\frac{-1}{z}\right)$

$(\Theta_L|_{n/2} S)(\tau) = j(S,\tau)^{-n/2}\, \Theta_L\left(\frac{-1}{\tau}\right)$. But $j(S,\tau) = \tau$, so we get the result using that $i^{-n/2}$ because $8 \mid n$.

A more general theorem (See Iwaniec, §10).

<u>Theorem</u>: Let n be an <u>even integer</u>. Let L be an even integral lattice in $\mathbb{R}^n$, with Gramm matrix A.
Let N be the minimal positive integer such that NA^{-1} is also even integral. (the "level")

Then Θ_L is a modular form of wt $\frac{n}{2}$, ~~level~~ $\Gamma_0(N)$ and character ε.

That is, Θ_L is a modular form of wt $\frac{n}{2}$ for the group $\Gamma_1(N)$, and $\varepsilon : \Gamma_0(N)/\Gamma_1(N) \longrightarrow \{\pm 1\}$ is a character on $(\mathbb{Z}/N\mathbb{Z})^\times$

s.t. $\Theta_L\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\tau\right) = (c\tau + d)^{n/2}\,\varepsilon(d)\,\Theta_L(\tau)$

ε is defined as follows: $\begin{cases} \varepsilon(-1) = (-1)^{n/2} \\ \varepsilon(d) = \left(\frac{D}{d}\right) \text{ (Jacobi symbol) for } d > 0. \end{cases}$

where $D = (-1)^{n/2}\det(A)$

if $D = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, then $\left(\frac{D}{d}\right) = \prod_i \left(\frac{p_i}{d}\right)^{\alpha_i}$, where $\left(\frac{p_i}{d}\right) = \begin{cases} 0 & p_i \mid d \\ +1 & D = \square \bmod p_i \\ -1 & \text{else} \end{cases}$

<u>Remark</u>: if f is mod. form of weight k, for some $\Gamma \ni -I_2$, then
$f(\tau) = (-1)^k f(\tau) \Rightarrow$ no nonzero mod. forms for k odd (if $-I_2 \in \Gamma$)

So there are no nonzero modular forms of odd weight for $SL_2(\mathbb{Z})$, $\Gamma_0(N)$, or more generally, for any $\varepsilon : \frac{\Gamma_0(N)}{\Gamma_1(N)} \to \mathbb{C}^\times$, no nonzero odd-weight modular forms on $(\Gamma_0(N), \varepsilon)$.

Modular Forms of even weight.

Let f be a modular form of wt 2 for some $\Gamma \subseteq SL_2(\mathbb{Z})$. (finite index).

Consider the differential $\omega(\tau) = f(\tau)\,d\tau$ on $\mathcal{H}$.

Given γ, consider $\gamma : \mathcal{H} \to \mathcal{H}$.

The pullback $(\gamma^*\omega)(\tau) = f(\gamma\tau)\,d(\gamma\tau) = j(\gamma,\tau)^2 f(\tau)\, d(\gamma\tau) = (c\tau+d)^2 f(\tau)\, d(\gamma\tau)$

$$d(\gamma\tau) = d\left(\frac{a\tau+b}{c\tau+d}\right) = \frac{a(c\tau+d) - c(a\tau+b)}{(c\tau+d)^2}\, d\tau = (c\tau+d)^{-2}\, d\tau$$

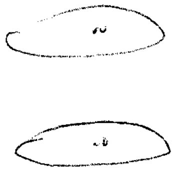
So $\gamma^*\omega = \omega$.

Therefore, $\omega = \omega_f$ is a meromorphic differential on $Y(\Gamma) = {}_{\Gamma}\backslash^{\mathcal{H}}$.

Example. $x \longmapsto -x$ is an automorphism of the disk $B(0,1)$.

The differential $x\,dx$ is invariant under this auto.

Consider the map



x
$\downarrow$
x^2 ← Fixe coordinate y. So $y = x^2$.

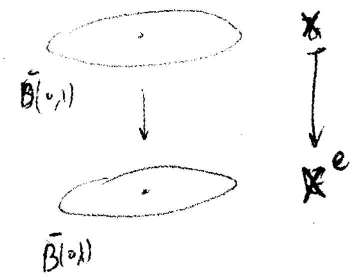
Then $\pi^*\left(\frac{1}{2}dy\right) = \frac{1}{2}dx^2 = x\,dx$.

So a vanishing differential $(x\,dx)$ descends to a non-vanishing $\left(\frac{1}{2}dy\right)$ differential.

In our situation, let $\Gamma' \subseteq \Gamma$ with no elliptic elements ~~points~~. Then the projection $\mathcal{H} \to {}_{\Gamma}\backslash^{\mathcal{H}}$ factors through ${}_{\Gamma'}\backslash^{\mathcal{H}}$.

The map $\mathcal{H} \to {}_{\Gamma'}\backslash^{\mathcal{H}}$ is unramified, so it's a local iso, and ω_f descends to a differential on ${}_{\Gamma'}\backslash^{\mathcal{H}}$. But the map ${}_{\Gamma'}\backslash^{\mathcal{H}} \to {}_{\Gamma}\backslash^{\mathcal{H}}$ can be ramified!

In general, we can always pass to a disk model:



where e = ramification index. ~~…~~

The differential ω_f is locally $f(x)\,dx$, $f(x)$ holo. on $\bar{B}(0,1)$, and descends to some $g(y)\,dy$ where g is holomorphic except possibly at 0.

$$\pi^*(g(y)\,dy) = f(x)\,dx$$

$$\| $$

$$g(x^e)\,d(x^e) = e x^{e-1} g(x^e)\,dx$$

$\Rightarrow$ order of vanishing ~~at~~: $e \operatorname{ord}_y g(y) + (e-1) = \operatorname{ord}_x f(x) \Rightarrow$

$$\Rightarrow \operatorname{ord}_y g(y) = \frac{1}{e}\operatorname{ord}_x f(x) - \frac{e-1}{e}$$

More generally, if f is a modular form of weight $2k$, then:

$f(\tau)(d\tau)^k$ is an invariant k-differential on $\mathcal{H}$.
(kth tensor power of $\Omega^1_{\mathcal{H}}$)

So $\overset{\omega_f}{f(\tau)(d\tau)^k}$ descends to a meromorphic k-differential on $Y(\Gamma) = {}_{\Gamma}\backslash^{\mathcal{H}}$.

Let $x \in \mathcal{H}$ be an elliptic point of order $\underset{\uparrow\, 2 \text{ or } 3}{e}$ $\left(e = \#\operatorname{Stab}_{\bar{\Gamma}}(x)\right)$.

Then $\operatorname{ord}_{\bar{x}}(\omega_f) = \frac{1}{e}\operatorname{ord}_x(f) - k\,\frac{e-1}{e}$

(see Miyake's book for further explanations).
(§2.3)

• The situation at the cusps.

Let $f(\tau)$ have weight $2k$, and level Γ. Suppose f is holomorphic.
Let a = width of $i\infty$ for Γ. Let $q_a = e^{\frac{2\pi i \tau}{a}}$

$$f(\tau) = \sum_{n=0}^{\infty} a_n q_a^n . \qquad dq_a = \frac{2\pi i}{a} q_a \, d\tau \Rightarrow d\tau = \frac{a}{2\pi i} \frac{dq_a}{q_a}$$

So locally $f(\tau)(d\tau)^k = * \, q_a^{-k} \sum_{n=0}^{\infty} a_n q_a^n \cdot (dq_a)^k$.

So $f(\tau)(d\tau)^k$ is holomorphic at $i\infty \iff f$ vanishes at ∞ to order at least k.

Example. $k=1$ $f(\tau)d\tau$ is holomorphic at $\infty \iff f$ vanishes at $i\infty$.

More generally, $\omega_f = f(\tau)(d\tau)^k$ is holomorphic on $X(\Gamma)$ ← compactified
if and only if, for every cusp c, $N_c \geqslant k$ $\Big(N_c = \inf\limits_n \{ a_{n,c}(f) \neq 0 \}$ where $\sigma(i\infty) = c$ $\Big)$

(for $k=1$, ω_f is hol. diff on $X(\Gamma) \iff f$ is a cusp form).

Note: This whole discussion can be reversed: k-differentials with poles of order at most k at every cusp of $X(\Gamma)$ produce holomorphic modular forms of weight $2k$ relative to Γ.

$$\left(\text{via} \quad \omega \longmapsto \frac{\pi^* \omega}{(d\tau)^k} \quad , \quad \pi : \mathcal{H} \to \Gamma\backslash\mathcal{H} \right).$$

Let $\Omega^k_{X(\Gamma)}$ = sheaf of k-differentials on $X(\Gamma)$.

Let $M_{2k}(\Gamma) = \{$hol. weight-$2k$ modular forms on $X(\Gamma)\}$ ($\mathbb{C}$-vectorspace)

$S_{2k}(\Gamma) = \{$cusp forms of weight-$2k$ on $X(\Gamma)\}$ ($\mathbb{C}$-vectorspace)

We have, from the previous discussion, ~~if Γ has no elliptic elements~~,

$$\mathcal{M}_{2k}(\Gamma) = H^0\left(X(\Gamma), \Omega^k_{X(\Gamma)}(k\cdot P_\Gamma)\right)$$ allow pole of order at most k at the cusps

$$S_{2k}(\Gamma) = H^0\left(X(\Gamma), \Omega^k_{X(\Gamma)}((k-1)P_\Gamma)\right)$$ (holomorphic otherwise)

where • P_Γ = divisor of cusps on $X(\Gamma)$ (if $c_1\Gamma, \dots, c_h\Gamma = \mathbb{P}^1(\mathbb{Q})/\Gamma$,

then $P_\Gamma = [c_1] + \dots + [c_h]$)

~~[illegible]~~

• The Riemann-Roch Theorem.

Let X be a compact Riemann surface.

Let $\mathcal{O}$ be the sheaf of ~~regular~~ holomorphic functions on X.

$\mathcal{O}(U) = \{f: U \to \mathbb{C} \mid f \text{ analytic}\}$.

In general: $\mathcal{F}(Y) =: H^0(Y, \mathcal{F})$ for any sheaf $\mathcal{F}$ on Y.

$H^0(X, \mathcal{O}) = \mathcal{O}(X) = \mathbb{C}$. X is compact.

A divisor D on X is an element of the free abelian group on the $\{P : P \in X\}$.

So $D = \sum_{P\in X} a_P [P]$, $a_P \in \mathbb{Z}$, $a_P = 0$ except for finitely-many P.

The degree of D is $\deg D := \sum_{P \in X} a_P$ ← finite sum.

$D \geq 0$ if each $a_P \geq 0$ $(\forall P)$.

$D_1 \geq D_2$ if $D_1 - D_2 \geq 0$.

Given $U \subseteq X$, $D|_U := \sum_{P\in U} a_P [P]$ (just take the part supported on U)

Define, for each divisor D, $\mathcal{O}(D)$ a sheaf:

$$\mathcal{O}(D)(U) := \{ f : U \to \mathbb{P}^1 \text{ meromorphic} : \operatorname{div}(f) \geq -D|_U \} \cup \{0\}$$

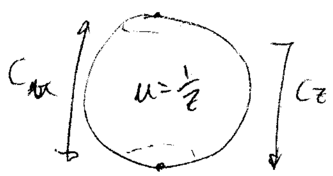
where $\operatorname{div}(f) = \sum_{p \in U} \operatorname{ord}_p(f) \cdot [p]$ $\quad \operatorname{ord}_p(f)$ is the order of $f = \sum_n^{\infty} s_n z^n$ if z is a local chart around p.

Rk: If f is meromorphic on X, then $\deg(\operatorname{div}(f)) = 0$.

Example: If $\deg D < 0$, then $\deg(-D) > 0$.

Then $H^0(X, \mathcal{O}(D)) = \{0\}$: if $f \neq 0$ and $f \in \mathcal{O}(D)(X)$, then $\operatorname{div}(f) \geq -D \Rightarrow 0 = \deg(\operatorname{div} f) \geq \deg(-D) > 0 \Rightarrow !!$

Example: $X = \mathbb{P}^1_{\mathbb{C}}$



Glued via $u = \frac{1}{z}$

$D = r \cdot [\infty]$.

$$H^0(X, \mathcal{O}(D)) = \begin{cases} 0 & \text{if } r < 0 \\ \mathbb{C} & \text{if } r = 0 \\ \mathbb{C} \oplus \mathbb{C}z \oplus \cdots \oplus \mathbb{C}z^r & \text{if } r > 0 \end{cases}$$

rat'l functions with divisor $\geq -r[\infty]$

dim $= r+1$

Example: $y^2 = f(x) = x^3 + ax + b$, $a, b \in \mathbb{C}$, f separable (distinct roots)

Gives an elliptic curve in $\mathbb{P}^2_{(x:y:z)}$, $y^2 z = x^3 + axz^2 + bz^3$.

If $z = 0$, get $0 = x^3 \Rightarrow x = 0$. So one point at ∞: $[0:1:0]$, which is added to the affine curve.

One checks that this is a nonsingular algebraic curve, so gives a compact Riemann Surface.

(cont example)

There is a map

$$\begin{array}{ccc} X & \ni & (x,y) \\ \pi \downarrow & & \downarrow \\ \mathbb{P}^1_x & & x \end{array}$$

(extends to infinity by sending $[0:1:0] \mapsto \infty \in \mathbb{P}^1$).

The map is ramified at $\{x : \exists! y \text{ with } y^2 = f(x)\} = \{\underset{\text{root of } f}{\alpha, \beta, \gamma}\} \cup \{\infty\}$.

Q: Why is it ramified at ∞?

A: The Hurwitz's formula gives:

$$\underbrace{2g(X) - 2}_{\text{even}} = \underbrace{\deg(\pi) \cdot (2g(\mathbb{P}^1) - 2)}_{\text{even}} + \sum_{P \in X} (e_P - 1)$$

$\Rightarrow \sum (e_P - 1)$ is even.

Have 3 ramification points on the affine piece, ~~all~~ with $e_P = 2$, which contributes 3 in $\sum (e_P - 1)$. So ∞ must also be a ramif. point.

~~And~~

So $\sum (e_P - 1) = 4 \Rightarrow g(X) = 1$ (as $\deg(\pi) = 2$).

$$\mathrm{ord}_P(\pi^* x) = \begin{cases} \mathrm{ord}_{\pi(P)}(x) & \text{if } P \text{ is unramified} \\ 2\,\mathrm{ord}_{\pi(P)}(x) & \text{if } P \text{ is ramified} \end{cases}$$

So $\mathrm{div}(x) = [(0, \overbrace{\sqrt{-\alpha\beta\gamma}}^{\sqrt{f(0)}})] + [(0, -\overbrace{\sqrt{-\alpha\beta\gamma}}^{\sqrt{f(0)}})] - 2[\infty]$ (true even if 0 is a root of f).

Similarly,

$$\mathrm{div}(y) = [(\alpha, 0)] + [(\beta, 0)] + [(\gamma, 0)] - 3[\infty]$$

(vanishes at the root to order 1, b/c $\sqrt{(x-\alpha)(x-\beta)(x-\beta)}$ is a local parameter)

Note that $\mathcal{O} = \mathcal{O}(0)$ ← divisor 0, and

$1 \in H^0(X, \mathcal{O}) = \mathbb{C}$

$x \in H^0(X, \mathcal{O}(2 \cdot [\infty]))$

$y \in H^0(X, \mathcal{O}(3 \cdot [\infty]))$

(Rk: $H^0(X, \mathcal{O}([\infty])) = \mathbb{C}$. For else we get $f: X \to \mathbb{P}^1$ of degree $1 \Rightarrow$

$\Rightarrow f$ is an isomorphism $\Rightarrow$!! (different genus!)).

A sheaf $\mathcal{F}$ on a R.S. X is called <u>invertible</u> if $\mathcal{F}$ is locally isomorphic to $\mathcal{O}_X$.

<u>Example</u>: $f: X \to \mathbb{P}^1$, meromorphic, and let $D = \mathrm{div}(f)$.

$$\mathcal{O}(D)(U) \equiv \{ f: U \to \mathbb{P}^1 : \mathrm{div}(f)|_U \geq -D \}.$$

Then $\mathcal{O}(D) \simeq \mathcal{O}_X$ (globally) b/c $\mathrm{div}\, g = \mathrm{div}\, g + \mathrm{div}\, f \geq -D + D = 0$

$$g \longmapsto g \cdot f.$$

In fact for any D, $\mathcal{O}(D) \simeq \mathcal{O}$ locally, b/c locally any divisor D is the divisor of a function:

given D, $\exists\ X = \bigcup U_i$, $f_i : X \to \mathbb{P}^1$ s.t. $\mathrm{div}(f_i)|_{U_i} = D|_{U_i}$.

Then we get local isos $\mathcal{O}(D)|_{U_i} \simeq \mathcal{O}|_{U_i}$

$$g \mapsto g \cdot f_i$$

Moreover, any invertible sheaf is isomorphic to $\mathcal{O}(D)$ for some divisor D.

Let Ω_X = sheaf of regular (i.e. holomorphic) differentials on X.

- Ω_X exists ($\forall U$, $\Omega_X(U)$ is a $\mathcal{O}_X(U)$-module).
- admits the following local description:

given x and a local chart U with coordinate z, then $\Omega_X|_U \simeq \{ f(z)\,dz : f \text{ hol on } B(0,1) \}$

If there is another chart around x with $w = h(z)$ the change of variables, then $f(h(z))\, h'(z)\, dz = f(w)\, dw$.

If $\mathcal{F}$ is an invertible sheaf can define $\mathcal{F}^{\otimes k}$,

$$\mathcal{F}^{\otimes k}(U) := \mathcal{F}(U) \underset{\mathcal{O}(U)}{\otimes} \cdots \underset{\mathcal{O}(U)}{\otimes} \mathcal{F}(U) \quad (k \text{ times}).$$

The restriction maps $\mathcal{F}(U) \to \mathcal{F}(V)$ extend to maps $\mathcal{F}^{\otimes k}(U) \to \mathcal{F}^{\otimes k}(V)$

Since $\mathcal{F}$ is invertible, locally $\mathcal{F} \simeq \mathcal{O}$ and so $\mathcal{F}^{\otimes k} \simeq \mathcal{O}^{\otimes k} \simeq \mathcal{O}$

So $\mathcal{F}^{\otimes k}$ is still invertible.

<u>Example</u>: $\mathcal{O}(D)^{\otimes k} \simeq \mathcal{O}(k \cdot D)$.

<u>Example</u>: $\Omega_X^{\otimes k} = \{ f(z)(dz)^k : f(z) \text{ hol on } B(0,1) \}$

to recall how things are glued together:

in this case, $f(w)(dw)^k = f(h(z))\, h'(z)^k (dz)^k$.

We can also talk about meromorphic differentials. (it's not an invertible sheaf anymore).

Locally, $\{ f(z)\, dz : f(z) \text{ is meromorphic} \}$.

<u>Example</u>: dz on $\mathbb{P}^1 \supseteq \mathbb{A}^1_z$.

dz is holomorphic on $\mathbb{A}^1_z$. Let u be a local parameter at ∞ (say $u = \frac{1}{z}$).

Then $z = \frac{1}{u}$, $dz = \frac{-1}{u^2} du$. So dz has a pole of order 2 at $u = 0$ (ie at ∞).

Note that we can consider the divisor of a differential:

Can say if $\omega = f(z)\, dz$ (locally), then $\mathrm{div}(\omega)$ at x is $\mathrm{ord}_0(f) \cdot [x]$.

Then if $\omega = f(h(z))\, h'(z)\, dz$, as h is biholomorphic and $h(0) = 0$, $h(z) = \lambda z + \text{h.o.t.}$, $\lambda \neq 0$

So $\mathrm{ord}_0(f(h(z)) \cdot h'(z)) = \mathrm{ord}_0(f(z))$, so well-defined!.

In the example we are considering, get $\operatorname{div}(dz) = -2\cdot[\infty]$.

One can always find a global meromorphic differential

(e.g pick $X \to \mathbb{P}^1$, and take the pullback of dz).

Let $K =$ canonical divisor $= \operatorname{div}(\omega)$, where ω is any meromorphic differential.
(depends on the choice of ω).

Then $\mathcal{O}(K) \cong \Omega_X$

If ω_1 ~~is another~~ is a holomorphic differential (say, on U), then

$\frac{\omega_1}{\omega}$ is a meromorphic function ~~of~~ on U, and $\operatorname{div}\left(\frac{\omega_1}{\omega}\right) = \operatorname{div}(\omega_1) - \operatorname{div}(\omega) \geq$

$\geq -\operatorname{div}(\omega) = -K \quad \Rightarrow \quad \frac{\omega_1}{\omega} \in \mathcal{O}(K)(U)$.

This gives the map $\Omega_X(U) \to \mathcal{O}(K)(U)$.

It's not hard to see that this is an isomorphism.

Also, if $K = \operatorname{div}(\omega)$, $K' = \operatorname{div}(\omega')$, then $\frac{\omega}{\omega'}$ is a meromorphic function

that gives an iso $\mathcal{O}(K) \to \mathcal{O}(K')$.

$$f \longmapsto f\cdot\frac{\omega}{\omega'}$$

Also, $K' = K + \operatorname{div}\underbrace{(\omega/\omega')}_{\text{function}} \Rightarrow \deg K' = \deg K$.

Exercise: find all holomorphic differentials on $Y^2 = X^{2g+1} + \dots + a_1 X + a_0$.

Example: $\frac{dx}{Y}$ is a holo. differential on $Y^2 = X^3 + a_2X^2 + a_1X + a_0$
assume it has distinct roots

Theorem (Riemann-Roch). Let D be a divisor on X, $g(X)=g$.

$$\dim H^0(X,\mathcal{O}(D)) = \dim H^0(X,\mathcal{O}(K-D)) + \deg(D) + 1 - g.$$

- Let D be 0. Then $\mathcal{O}(D)=\mathcal{O}_X$, $H^0(X,\mathcal{O}(D)) \simeq \mathbb{C}$.

  So (RR⇒) $\dim H^0(X,\mathcal{O}(K)) = g$.

  As $\mathcal{O}(K) \simeq \Omega_X$, we get that $g = \dim_{\mathbb{C}}$ (v.sp. of holomorphic differentials).

- Let $D=K$.

  Then RR ⇒ $\deg(K) = 2g-2$.

- If $\deg D < 0$,

  $\dim H^0(X,\mathcal{O}(D)) = 0$

Example: X genus 1 curve. (eg $y^2=x^3+ax^2+bx+c$)

Take $D>0$. Then RR ⇒ $\dim H^0(\mathcal{O}(D)) = \dim H^0(\mathcal{O}(K-D)) + \deg D$.

Can take $K=0$ $\left(=\operatorname{div}\left(\frac{dx}{y}\right)\right)$. So $H^0(\mathcal{O}(K-D)) = H^0(\mathcal{O}(-D)) = \{0\}$.

So we get $\dim H^0(\mathcal{O}(D)) = \deg D$ (for genus 1, and effective divisors!)

Pick a point on X, and call it ∞. Note that $H^0(\mathcal{O}(r\infty)) \subseteq H^0(\mathcal{O}((r+1)\infty))$

r	0	1	2	3	4	5	6
$\dim H^0(\mathcal{O}(r\cdot\infty))$	1	1	2	3	4	5	6
new function	1	-	x	y	x^2	xy	x^3 or y^2

⇒ $\{1,x,y,x^2,xy,x^3,y^2\} \in H^0(\mathcal{O}(6\infty))$ ⇒ linearly dependent (and coeffs of x^3, y^2 are non zero).

In general, get some equation of the form:

$$Y^2 + a_1 XY + a_3 Y = X^3 + a_2 X^2 + a_4 X + a_6$$

(we can replace Y by λY, $\lambda \in \mathbb{C}^\times$).

<u>Conclusion</u>: there exists a map (rational map): $X \dashrightarrow \mathbb{A}^2 \subseteq \mathbb{P}^2$

$t \longmapsto (x(t), y(t)) \in \underset{\text{zero locus}}{Z}(Y^2 Z + a_1 XYZ + a_3 YZ^2 \dots)$

<u>Theorem</u>: This map is an iso $X \to Z(Y^2 Z + a_1 XYZ + a_3 YZ^2 = \dots + a_6 Z^3)$

(See Silverman or Hartshorne)

<u>Recall</u>: $\Gamma \subseteq SL_2(\mathbb{Z})$, with no elliptic elements (eg $\Gamma \subseteq \Gamma_1(N)$, $N \geq 3$, $\Gamma \subseteq \Gamma(3)$)

$X = {}_\Gamma\backslash\mathcal{H}^*$.

$\mathcal{M}_{2k}(\Gamma) \cong H^0(X(\Gamma), \overbrace{\Omega^{\otimes k}(k \cdot P_\Gamma)}^{\text{meromorphic differentials with poles at worst } kP_\Gamma})$ $\left(P_\Gamma = \sum_{c \text{ cusp of } X(\Gamma)} [c] \right)$.

$S_{2k}(\Gamma) \cong H^0(X(\Gamma), \Omega^{\otimes k}((k-1)P_\Gamma))$.

<u>Theorem</u>: Let $\varepsilon_\infty := \# P_\Gamma = \deg P_\Gamma$.

Then
$$\dim \mathcal{M}_{2k}(\Gamma) = \begin{cases} (2k-1)(g-1) + k \cdot \varepsilon_\infty & \text{if } k \geq 1 \\ 1 & \text{if } k = 0 \\ 0 & \text{if } k < 0 \end{cases}$$

$$\dim S_{2k}(\Gamma) = \begin{cases} (2k-1)(g-1) + (k-1)\varepsilon_\infty & \text{if } k \geq 2 \\ g & \text{if } k = 1 \\ 0 & \text{if } k \leq 0 \end{cases}$$

<u>Conclusion</u>: The space of modular forms for any $\Gamma' \subseteq SL_2(\mathbb{Z})$ and any weight r is finite-dimensional.

Pf/ If $\Gamma \subseteq \Gamma'$, then $\mathcal{M}_{2k}(\Gamma') \subseteq \mathcal{M}_{2k}(\Gamma)$. Choose $\Gamma := \Gamma' \cap \Gamma(3)$ and use thm. //

Note that if r is odd and $M_r(\Gamma') \neq \{0\}$, let $f \neq 0$, $f \in M_r(\Gamma')$.

Then
$$\begin{aligned} M_r(\Gamma') &\hookrightarrow M_{2r}(\Gamma') \\ g &\longmapsto g\cdot f \end{aligned}$$
and $\dim M_{2r}(\Gamma') < \infty \Rightarrow \checkmark$.

Pf (of Thm):

$\Omega^{\otimes k}(\ell \cdot P_\Gamma) \cong \mathcal{O}(kK + \ell P_\Gamma)$.

Assume first $k \geq 1$.

R.R $\Rightarrow \dim H^0(\Omega^{\otimes k}(\ell P_\Gamma)) = \dim H^0(\mathcal{O}(K - (kK + \ell P_\Gamma))) + \deg(kK + \ell P_\Gamma) + 1 - g =$

$= \dim H^0(\mathcal{O}((1-k)K - \ell P_\Gamma)) + k(2g-2) + \ell \varepsilon_\infty + 1 - g$

Assume $g \geq 1$.

For $k > 1$ and $\ell = k$ or $\ell = k-1$; or for $k = 1$ and $\ell = k$,

$-(k-1)K - \ell P_\Gamma$ has negative degree.

So the first term of RHS is 0 and we get $\dim H^0(\Omega^{\otimes k}(\ell P_\Gamma)) = (2k-1)(g-1) + \ell \varepsilon_\infty$

It remains the case $k = 1$, $\ell = k - 1 = 0$.

$\dim H^0(\Omega) = g$, as we computed before.

If $g = 0$:

$$\dim H^0(\mathbb{P}^1, \mathcal{O}(D)) = \begin{cases} 0 & \text{if } \deg D < 0 \\ 1 + \deg D & \text{if } \deg D \geq 0 \end{cases} \quad (\text{because } D \sim (\deg D)\cdot[\infty])$$

For $D = kK + \ell P_\Gamma$, as ~~$\deg D = -(k-1)(2g-2) - \ell \varepsilon_\infty = 2(k-1) - \ell \varepsilon_\infty$~~

$$\deg D = k\cdot(-2) + \ell \varepsilon_\infty = \begin{cases} k(\varepsilon_\infty - 2) & \ell = k \\ -2k + (k-1)\varepsilon_\infty & \ell = k-1 \end{cases}$$

(cont'd)

To get formulas for $K \geq 2$, need the degrees of D to be ≥ 0.

~~It's enough~~ to show that $\mathcal{E}_\infty \geq 3$. We first

$$g(X(\Gamma)) = 1 + \frac{d}{12} - \frac{1}{2}\mathcal{E}_\infty \qquad (\mathcal{E}_2 = \mathcal{E}_3 = 0 \text{ b/c no elliptic elements}). \qquad d = [PSL_2(\mathbb{Z}) : \bar{\Gamma}].$$

$$g = 0 \Rightarrow \mathcal{E}_\infty = 2 + \frac{d}{6} > 2 \Rightarrow \mathcal{E}_\infty \geq 3 \quad (\text{it's an integer}).$$

$$\deg(k\text{-}D) = 2(k-1) - l\,\mathcal{E}_\infty \overset{\mathcal{E}_\infty \geq 3}{\leq} 2(k-1) - 3l.$$

If $l = k$, this is always negative.

If $l = k-1$, this is negative unless $k=1$.

But if $k=1$, go back to the original question: $\dim H^0(\Omega) = g$ ✓.

· Remaining the case ($k=0$):

$$\dim \begin{cases} M_{2k} \\ S_{2k} \end{cases} = \dim H^0(X(\Gamma), \underbrace{\Omega^k(lP_\Gamma)}_{\substack{\text{if } k=0 \\ \mathcal{O}(lP_\Gamma)}}) \qquad (l = k, k-1).$$

So $M_{2k} \simeq H^0(X(\Gamma), \mathcal{O})$ ← has dim 1 $(\simeq \mathbb{C})$

$S_{2k} \simeq H^0(X(\Gamma), \mathcal{O}(-P_\Gamma))$ ← dim'n of global functions with zeros at P_Γ ← dim 0

If $k < 0$, there are no modular forms of weight k (except 0).

$f \neq 0$ hol. mod form of level Γ, of weight k. Want a contradiction.

f^2 is hol of level Γ, weight $2k$ (⇒ can assume f is hol of weight $2k$ for Γ)

Replace Γ by $\Gamma' \subseteq \Gamma$ (large) so that $g(X(\Gamma')) \gg 0$ so that $\exists\, h \neq 0$, cusp form of weight $-2k$ (>0) ← By the solved cases of the theorem.

Then $f^2 \cdot g$ is hol mod. form of level Γ', weight 0 which vanishes at the cusps

$\Rightarrow f^2 g = 0 \underset{g \neq 0}{\overset{?}{\Rightarrow}} f = 0 \Rightarrow$!!

For the theorem, we assumed that $\tilde{\Gamma}$ has no elliptic elements.

A slight strengthening allows to assume that $\bar{\Gamma}$ has no elliptic elements (even weight)

There is, however, a general case theorem: (Diamond-Shurman, Miyake).

$$\dim M_k = \begin{cases} (k-1)(g-1) + \left\lfloor \frac{k}{4} \right\rfloor \varepsilon_2 + \left\lfloor \frac{k}{3} \right\rfloor \varepsilon_3 + \frac{k}{2} \varepsilon_\infty & \text{if } k \text{ even } k \geq 2 \\ 1 & \text{if } k = 0 \\ 0 & \text{if } k < 0 \end{cases}$$

$$\dim S_k = \begin{cases} (k-1)(g-1) + \left\lfloor \frac{k}{4} \right\rfloor \varepsilon_2 + \left\lfloor \frac{k}{3} \right\rfloor \varepsilon_3 + \left(\frac{k}{2} - 1\right) \varepsilon_\infty & \text{if } k \text{ even } k \geq 2 \\ g & \text{if } k = 2 \\ 0 & \text{if } k \leq 0 \end{cases}$$

There are also general formulas for <u>odd</u> weight, except for $k=1$ $\leftarrow$ open!

Putting together previous discussions, we get:

<u>Conclusion</u>: Let f be a modular form of weight $2k$ and level Γ.

$$\operatorname{div}(\omega_f) = \sum_{x \in \frac{\mathcal{H}}{\Gamma}} \left(\frac{\operatorname{ord}_x(f)}{e_x} - k \frac{e_x - 1}{e_x} \right)[x] + \sum_{x \in \Gamma_p} \left(\operatorname{ord}_x(f) - k \right)[x]$$

As ω_f is a global meromorphic section of $\Omega^k \simeq \mathcal{O}(k.K)$, we get:

$$\deg(\operatorname{div}(\omega_f)) = \sum_{x \in \frac{\mathcal{H}}{\Gamma}} \left(\frac{\operatorname{ord}_x f}{e_x} - k \frac{e_x - 1}{e_x} \right) + \sum_{x \in \Gamma_p} \left(\operatorname{ord}_x(f) - k \right) = k(2g-2).$$

<u>Example</u>: Take $\Gamma = PSL_2(\mathbb{Z})$. Then:

$$-2k = \sum_{x \neq i, \rho} \operatorname{ord}_x(f) + \frac{1}{2} \operatorname{ord}_i(f) - \frac{k}{2} + \frac{1}{3} \operatorname{ord}_\rho(f) - \frac{2}{3} k + \left(\operatorname{ord}_\infty(f) - k \right)$$

Rearranging, we get:

Prop: if f is a modular form of weight $2K$ on $PSL_2(\mathbb{Z})$,

then $$\mathrm{ord}_\infty(f) + \mathrm{ord}_i(f) + \frac{1}{3}\mathrm{ord}_\rho(f) + \sum_{x \neq i,\rho,\infty} \mathrm{ord}_x(f) = \frac{K}{6}$$

Also, understanding the correspondence wt $2K \leftrightarrow K$-diff'ls, we get:

Corollary: Let L be an even unimodular lattice in $\mathbb{R}^n$.

Then $n \equiv 0 \pmod 8$.

Pf (Serre, "A course in arithmetic")

also even unimodular

Suppose not. Replace L by $L \oplus L$ or $L \oplus L \oplus L \oplus L$, we may assume that $n \equiv 4 \pmod 8$.

general thm using $L^\vee = L$

We have $\Theta_L\left(\frac{-1}{z}\right) = \left(\frac{z}{i}\right)^{\frac{n}{2}} \Theta_L(z) = (-1)^{\frac{n}{4}} z^{n/2}\Theta_L(z) = -z^{n/2}\Theta_L(z)$.

Let $\omega(z) = \Theta_L(z)(dz)^{n/4}$ (a holomorphic $n/4$-diff. on $\mathcal{H}$).

If $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, then $S^*\omega(z) = \omega(S\cdot z) = \Theta_L\left(\frac{-1}{z}\right) d\left(\frac{-1}{z}\right)^{n/4} =$

$\ldots = -\omega(z)$.

On the other hand, $T^*\omega(z) = \omega(Tz) = \omega(z+1) = \Theta_L(z+1)\, d(z+1)^{n/4} \overset{L \text{ even}}{=}$

$= \Theta_L(z)(dz)^{n/4} = \omega(z)$.

So $(ST)^*\omega(z) = T^*S^*\omega(z) = -\omega(z)$ $(*)$

But $(ST)^3 = Id_{PSL_2(\mathbb{Z})} \Rightarrow (ST^3)^*\omega(z) = \omega(z)$. But from $(*)$, we get $-\omega(z)$. So $\omega(z) = 0 \Rightarrow$!!

- Eisenstein series:

Let $N \geq 1$, $k \geq 3$ be integers.

Let $c, d \in \mathbb{Z}$.

omit $(m,n)=(0,0)$ if necessary

Consider $G_k(\tau; c,d; N) := \sum'_{(m,n)\equiv(c,d) \bmod N} (m\tau+n)^{-k}$

Theorem: $G_k(\tau; c,d; N)$ is a holomorphic modular form of weight k for the modular group $\Gamma(N) = \{ \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod N \}$.

It depends only on $(c,d) \bmod N$.

It has a q-expansion at the cusp $i\infty$, $q = e^{\frac{2\pi i \tau}{N}}$

$$a_0 + \frac{(-2\pi i)^k}{N^k (k-1)!} \sum_{n=1}^{\infty} a_n \cdot q^n$$

with:
$$a_0 = \begin{cases} 0 & \text{if } c \not\equiv 0 \pmod N \\ \sum'_{n\equiv d \pmod N} n^{-k} & \text{if } c \equiv 0 \pmod N \end{cases}$$

$$a_n = \sum_{\substack{m,\nu \\ m\nu = n \\ m \equiv c \pmod N}} (\operatorname{sgn} \nu) \cdot \nu^{k-1} \left(e^{2\pi i \frac{d}{N}}\right)^{\nu}$$

Consider the case $N=1$. (ie level $SL_2(\mathbb{Z})$), k even (otherwise would get 0!)

Take (WLOG, as $N=1$) $c=d=0$.

$$G_k(\tau) = \sum'_{m,n} (m\tau+n)^{-k} = 2\zeta(k) + \frac{(2\pi i)^k}{(k-1)!} 2 \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n$$

where $\sigma_{k-1}(n) = \sum_{\substack{d \mid n \\ d \geq 1}} d^{k-1}$, $q = e^{2\pi i \tau}$

If k is positive and even,

$$\zeta(k) = \frac{2^{k-1}}{k!} B_{k/2}\, \pi^k \quad \text{where} \quad \frac{x}{e^x - 1} = 1 - \frac{x}{2} + \sum_{k=1}^{\infty} (-1)^{k+1} B_k \frac{x^{2k}}{(2k)!}$$

k	1	2	3	4	5	6
B_k	$\frac{1}{6}$	$\frac{1}{30}$	$\frac{1}{42}$	$\frac{1}{30}$	$\frac{5}{66}$	$\frac{691}{2730}$

Let E_k be the Eisenstein series $\frac{1}{2\zeta(k)} G_k = 1 + (-1)^{k/2} \frac{2k}{B_{k/2}} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n$

(k even, as for k odd it is $\equiv 0$)

<u>Examples:</u>

$$E_4 = 1 + 240 \sum_{n \geq 1} \sigma_3(n) q^n$$

$$E_6 = 1 - 504 \sum_{n \geq 1} \sigma_5(n) q^n$$

$$E_8 = 1 + 480 \sum_{n \geq 1} \sigma_7(n) q^n$$

$$E_{12} = 1 + \frac{65520}{691} \sum_{n \geq 1} \sigma_{11}(n) q^n$$

<u>Theorem:</u> The graded ring of modular forms of level $SL_2(\mathbb{Z})$ is the free polynomial ring $\mathbb{C}[E_4, E_6]$ with weights $w(E_4) = 4$, $w(E_6) = 6$.

(i.e. $\exists$ iso of graded rings:

$$\mathbb{C}[x,y] \xrightarrow{\sim} \bigoplus M_{2k}(SL_2(\mathbb{Z})) \quad \text{where } wt(x) = 4,\ wt(y) = 6$$

$$x \longmapsto E_4$$
$$y \longmapsto E_6$$
$$1 \longmapsto 1$$

Corollary 1 $M_4 = \mathbb{C}\cdot E_4$, $M_6 = \mathbb{C}\cdot E_6$, $M_8 = \mathbb{C}\, E_4^2$, $M_{10} = \mathbb{C}\, E_4 E_6$,

and so the first weight for which there is a cusp form is 12.

Let $\Delta = \left(\frac{E_4^3 - E_6^2}{1728}\right)$. Then $\Delta = q + \text{h.o.t.}$ is a cusp form, and $M_{12} = \mathbb{C}E_{12} \oplus \mathbb{C}\Delta$ (or $\mathbb{C}\, E_4^3 \oplus \mathbb{C}\Delta$).

Δ has a simple zero at the cusp (∞).

Corollary 2 Let L ("E_8") be the E_8-lattice (not E_8 as Eisenstein series!).

Then $\Theta_L = E_4$ because $\Theta_L = 1 + \text{h.o.t}$, and $wt(\Theta_L) = 4$.

In particular, L has kissing number 240, and the number of vectors $\lambda \in L$ of $\frac{|\lambda|^2}{2} = n$ is $240\,\sigma_3(n)$.

Corollary 3: Let Λ_{24} be the Leech lattice and Θ its theta-function.

Then $\Theta = E_{12} - \frac{65520}{691}\Delta$.

(b/c Θ is a modular form for $SL_2(\mathbb{Z})$ s.t. $\Theta = 1 + 0\, q^2 + \text{h.o.t}$

(Λ_{24} has no vectors λ of norm $\sqrt{2}$).

This expression actually gives a formula for the kissing number.

Corollary 4: The even unimodular lattices of dimension 16 all have the same theta function.

(Rk: up to iso, there are two lattices, $E_8 \oplus E_8$, D_{16}^+).

(b/c $M_8 = \mathbb{C}\cdot E_8$ and the Θ considered begin with $1 + \cdots$).

Proof (of thm):

First, note that there are no modular forms on $SL_2(\mathbb{Z})$ of either odd or negative weight.

Recall that, for $f \in M_{2k}$,

$$\frac{k}{6} = v_\infty(f) + \frac{1}{2} v_i(f) + \frac{1}{3} v_\rho(f) + \sum_{\substack{x \neq i, \rho, \infty \\ x \in \mathcal{H}^* / SL_2(\mathbb{Z})}} v_x(f) \qquad \left(\text{where } v_x(f) = \mathrm{ord}_x(f)\right)$$

Small k:

$k=0$: f is a constant $\Rightarrow M_0 = \mathbb{C} \cdot 1$.

$k=1$: $\frac{1}{6} = \square + \frac{1}{2}\square + \frac{1}{3}\square + \sum \square$ where $\square \in \mathbb{Z}_{\geq 0}$

$\Rightarrow$ no solutions ! $\Rightarrow M_2 = \{0\}$.

$k=2$: solutions only if f vanishes only at ρ, and does so to order 1.

Let f_1, f_2 be two such modular forms (of weight 4).

So $g := \frac{f_1}{f_2}$ is a holomorphic function $\Rightarrow g$ is a constant. So $\dim M_4 \leq 1$.

But $\mathbb{C} \cdot E_4 \subseteq M_4 \Rightarrow M_4 = \mathbb{C} E_4$.

$k=3$: Get $M_6 = \mathbb{C} \cdot E_6$, in the same way.

$k=4$: Get M_8 has dim ≤ 1. So $\mathbb{C} E_8 = \mathbb{C} E_4^2 = M_8$

$\Rightarrow E_4^2 = E_8$

$k=5$: Get M_{10} has dim $= 1$, so $\mathbb{C} E_{10} = \mathbb{C} E_4 E_6$.

Recall now $\Delta = \frac{1}{1728}\left(E_4^3 - E_6^2\right) = q + \text{h.o.t.}$

Claim: For ~~all~~ $k \geq 12$, even, let $E \in M_k$ be any non-cusp form.

(e.g. $E = E_k$).

Then $M_k = \mathbb{C}E \oplus \Delta \cdot M_{k-12}$

Proof: We can write $M_k = \mathbb{C}E \oplus S_k$

$$f \mapsto \frac{a_0(f)}{a_0(E)}E + \left(f - \frac{a_0(f)}{a_0(E)}E\right)$$

Define also $M_{k-12} \to S_k$ by $f \mapsto \Delta f$.

This is linear, injective $(\Delta(f_1 - f_2) = 0 \Rightarrow f_1 = f_2)$.

Finally, it is also surjective:

. Sp $h \in S_k$, $\frac{h}{\Delta}$ is a (possibly meromorphic) mod. form of weight $k-12$. The poles of $\frac{h}{\Delta}$ could only be at ∞, but

$v_\infty\left(\frac{h}{\Delta}\right) = v_\infty(h) - v_\infty(\Delta) = v_\infty(h) - 1 \underset{h \text{ is a cusp form}}{\geq 0}$.

Hence $\frac{h}{\Delta}$ is holomorphic, $\frac{h}{\Delta} \in M_{k-12}$.

Taking $E = E_4^a E_6^b$, note that any even integer $k \geq 12$ is $4a + 6b$ for some $a, b \geq 0$.

It follows that the map $\mathbb{C}[x,y] \to \bigoplus_{k=0}^{\infty} M_{2k}$ is graded and surjective.

The kernel of this map is a graded ideal $\Rightarrow$ generated by homogeneous polynomials.

(cont pf).

Such a homogeneous element gives a function on $\mathcal{H}$:

$$\sum_{\substack{i,j \\ 4i+6j=2k}} a_{ij} E_4^i E_6^j \equiv 0$$

$\in$ some k.

If $E_4^{\frac{k}{2}}$ doesn't appear, then all monomials have E_6, so after dividing by E_6, we get a relation of smaller weight. Same for $E_6^{k/3}$.

So the relation can be assumed to be:

$$\alpha E_4^{k/2} + \beta E_6^{k/3} + \sum_{\substack{i>0 \\ j>0}} a_{ij} E_4^i E_6^j = 0.$$

But at i, $E_6(i)=0$ and $E_4(i) \neq 0 \Rightarrow \alpha = 0 \Rightarrow$ contradiction.

Therefore, the map is an iso of graded rings, as wanted.

Remark/exercise: One can strengthen the result. We can consider the image of $\bigoplus_{k=0}^{\infty} M_{2k} \longrightarrow$ holomorphic functions on $\mathcal{H}$.

One can prove that this map is injective:

if $f_1, \dots, f_r$ are hol. ~~factors~~ functions of weight $k_1 < k_2 < \dots < k_r$,

~~and~~ $f_1 + \dots + f_r \equiv 0$ as a function on $\mathcal{H}$,

then $f_i \equiv 0$ $\forall i$.

Exercise: Find the structure of the graded ring of modular forms for $X(2)$.

$$\begin{array}{c} X(2) \\ \downarrow \quad \text{Galois} \cong \Gamma(1)/\Gamma(2) \cong SL_2(\mathbb{Z}/2\mathbb{Z}) = S_3. \\ X(1) \end{array}$$

Back to Eisenstein series:

Write $G_k(\tau) = G_k(\tau, c, d, N) = \sum\limits_{(m,n) \equiv (c,d) \bmod N}' (m\tau + n)^{-k}$ $\quad k \geq 3$, $\cancel{\tau \in} \mathcal{H}$.

Lemma: $G_k(\tau)$ is absolutely convergent.

Pf/ Can assume (just makes it more difficult in any case) $N = 1$.

Consider the set $\{m\tau + n : m, n \in \mathbb{Z}\}$ as a lattice in $\mathbb{C} \simeq \mathbb{R}^2$.

So suffices to show: if $\Gamma \subseteq \mathbb{C} \simeq \mathbb{R}^2$ is a lattice, then for $\sigma > 2$,

$$\sum_{\gamma \in \Gamma}' \frac{1}{|\gamma|^\sigma} < \infty.$$

Under $\mathbb{C} \simeq \mathbb{R}^2$, $|\cdot|$ corresponds to $\|\cdot\|$.

Γ corresponds to a lattice Γ' with a Gram matrix A,

So $\sum' \frac{1}{|\gamma|^\sigma} = \sum\limits_{\lambda \in \Gamma'}' \frac{1}{|\lambda|^\sigma} = \sum\limits_{a \in \mathbb{Z}^2}' \frac{1}{\|a\|_A^\sigma}$ where $\|a\|_A = {}^t a A a$.

$\|\cdot\|_A$ is a norm, so $\exists\, C$ s.t. $\|a\|_A \geq C \cdot \|a\|$ $\forall a \in \mathbb{Z}^2$.

So then $\sum' \frac{1}{|\gamma|^\sigma} \leq C \sum\limits_{(x,y) \in \mathbb{Z}^2}' \frac{1}{(x^2+y^2)^{\sigma/2}}$

Now $\frac{1}{(x^2+y^2)^{\sigma/2}} \leq \int_{x-1}^{x} \int_{y-1}^{y} \frac{1}{(x^2+y^2)^{\sigma/2}}\, dx\,dy$ if $x \geq 1, y \geq 1$.

So it's enough to show that $\iint_{\mathbb{R}^2 \setminus B^-(0,1)} \frac{dx\,dy}{(x^2+y^2)^{\sigma/2}} < \infty$.

$(x,y) = r(\cos\theta, \sin\theta) \rightsquigarrow \int_{r=1}^{\infty} \int_{\theta=0}^{2\pi} \frac{r\,dr\,d\theta}{r^\sigma} = 2\pi \int_1^\infty \frac{dr}{r^{\sigma-1}} = \frac{2\pi}{\sigma} < \infty.$

To calculate the q-expansion of G_K, we use:

$$\sin(\pi\tau) = \pi\tau\prod_{n=1}^{\infty}\left(1-\frac{\tau^2}{n^2}\right) \qquad (\text{Ahlfors ch 4, §2.3})$$

By taking the logarithmic derivative, find:

$$\pi\cot\pi\tau = \sum_{m\in\mathbb{Z}}(m+\tau)^{-1} := \lim_{N\to\infty}\left(\frac{1}{\tau}+\sum_{m=1}^{N}\left(\frac{1}{m+\tau}+\frac{1}{-m+\tau}\right)\right)$$

By differentiating this term by term,

$$\frac{\pi^2}{\sin^2\pi\tau} = \sum_{m\in\mathbb{Z}}(m+\tau)^{-2}$$

Now, $e^{\pi i\tau} - e^{-\pi i\tau} = 2i\sin(\pi\tau)$, write $q = e^{2\pi i\tau}$

and so $\frac{(1-q)^2}{q} = \left(\frac{1-e^{2\pi i\tau}}{e^{\pi i\tau}}\right)^2 = -4\sin^2(\pi\tau)$.

$$\frac{1}{(1-q)^2} = (1+q+q^2+\cdots)^2$$

$$\sum_{m\in\mathbb{Z}}(m+\tau)^{-2} = \frac{\pi^2}{\sin^2(\pi\tau)} = \frac{-4\pi^2 q}{(1-q)^2} = (2\pi i)^2\sum_{n=1}^{\infty} n q^n$$

Taking derivatives $k-2$ times, we get (w.r.t. τ)

$$\boxed{\sum_{m\in\mathbb{Z}}(m+\tau)^{-k} = \frac{(-2\pi i)^k}{(k-1)!}\sum_{n=1}^{\infty} n^{k-1}q^n}$$

Recall: $G_K(\tau; c,d,N) = \sum_{(m,n)\equiv(c,d)(N)}{}' (m\tau+n)^{-k}$

If a_0 is the constant term, then $a_0 = \sum_{\substack{n\in\mathbb{Z}\\ n\equiv d \bmod N}}{}' n^{-k}$

Consider now $G_k - a_0 = \sum_{\substack{m \equiv c \bmod N \\ m \neq 0}} \sum_{n \in \mathbb{Z}} (m\tau + Nn + d)^{-k} = \sum_{\substack{m \equiv c\ (N) \\ m \neq 0}} \sum_{n \in \mathbb{Z}} \left(n + \frac{d+m\tau}{N}\right)^{-k} N^{-k}$

$$= \sum_{\substack{m \equiv c\ (N) \\ m \neq 0}} N^{-k} \cdot \left(\sum_{n \in \mathbb{Z}} \left(n + \frac{d+m\tau}{N}\right)^{-k} \right) = \qquad (\Gamma(k) = (k-1)!)$$

* have a formula for this

$$= \frac{(-2\pi i)^k}{N^k \Gamma(k)} \sum_{\substack{m \equiv c \\ m > 0}} \sum_{\nu=1}^{\infty} \nu^{k-1} \left(e^{2\pi i \left(\frac{d+m\tau}{N}\right)\nu} + (-1)^k e^{2\pi i \left(\frac{m\tau - d}{N}\right)\nu} \right).$$

$$= \frac{(-2\pi i)^k}{N^k \Gamma(k)} \sum_{\substack{m \equiv c \\ m > 0}} \sum_{\nu=1}^{\infty} \nu^{k-1} q^{m\nu} \left(e^{2\pi i d\nu/N} + (-1)^k e^{-2\pi i d\nu/N} \right)$$

with $q = e^{2\pi i \tau/N}$

$$= \frac{(-2\pi i)^k}{N^k \Gamma(k)} \sum_{\lambda=1}^{\infty} a_\lambda q^\lambda \quad \text{where } a_\lambda = \sum_{\substack{m \equiv c \\ m > 0 \\ m\nu = \lambda}} \nu^{k-1} \left(e^{2\pi i d/N}\right)^\nu + \sum_{\substack{m \equiv c \\ m < 0 \\ m\nu = \lambda}} (-1)^k \nu^{k-1} \left(e^{\frac{2\pi i d}{N}}\right)^\nu$$

So $a_\lambda = \sum_{\substack{m \equiv c \\ m\nu = \lambda}} \mathrm{Sign}(\nu)\, \nu^{k-1} \left(e^{\frac{2\pi i d}{N}}\right)^\nu$ as wanted.

Clearly, $G_k(\tau, c, d, N)$ depends only on the congruence class of $(c,d) \bmod N$.

Lemma: Let $M \in SL_2(\mathbb{Z})$. Then $G_k(\tau, (c,d); N)|_k M = G_k(\tau, (c,d)M; N)$

Pf

$$G_k(\tau, (c,d), N)\Big|_k \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \sum_{(m,n) \equiv (c,d)(N)}{}' \left(m \cdot \frac{\alpha\tau + \beta}{\gamma\tau + \delta} + n \right)^{-k} \cdot (\gamma\tau + \delta)^{-k} =$$

$$= \sum{}' \big((m\alpha + n\gamma)\tau + (m\beta + n\delta)\big)^{-k} = \sum \left((m,n) \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} \tau \\ 1 \end{pmatrix} \right)^{-k} = \sum_{(m',n') \equiv (c,d)M \ (\mathrm{mod}\ N)} \left((m'\ n') \begin{pmatrix} \tau \\ 1 \end{pmatrix} \right)^{-k} //$$

As a corollary to the lemma, if $M \in \Gamma(N)$, then

$$G_k(\tau, (c,d); N)\big|_k M = G_k(\tau, (c,d); N)$$, i.e. it is a modular form for $\Gamma(N)$, perhaps meromorphic at the cusps.

But, since every $G_k(c,d)$ is holomorphic at $i\infty$ and since the q-expansion of $G_k(c,d)$ at another cusp is via the q-expansion of $G_k(c,d)|_k M$ for some $M \in SL_2(\mathbb{Z})$, we conclude that $G_k(c,d)$ is holo. at __every__ cusp. (and note that we __know__ the q-expansion at those cusps!)

(Thm).

__Remark__: This can be used to create modular forms for subgroups

$SL_2(\mathbb{Z}) \supseteq \Gamma \supseteq \Gamma(N)$ (called congruence subgroups).

(not every finite index sgp of $SL_2(\mathbb{Z})$ is a congruence sgp!).

If $\Gamma \supseteq \Gamma(N)$, consider:

$$\sum_{\substack{\gamma \text{ reps for} \\ \Gamma/\Gamma(N)}} G_k(\tau, (c,d), N)\big|_k \gamma \;=\; \text{holomorphic modular form of weight } k \text{ for } \Gamma$$

(possible 0!)

$$\parallel$$

$$\sum G_k(\tau, (c,d)\gamma; N) \overset{\text{can be done, easily.}}{=} \sum_{\lambda=0}^{\infty} a_\lambda q^\lambda$$

$\sum$

Elliptic Curves ~~over~~ $\mathbb{C}$ (Silverman, VI)

§ Elliptic Functions.

Let $\Lambda \subseteq \mathbb{C}$ be a lattice. A meromorphic function $f : \mathbb{C} \to \mathbb{P}^1$ is called Λ-elliptic if $f(z+\lambda) = f(z)$ $\forall \lambda \in \Lambda$, $\forall z \in \mathbb{C}$

(if $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$, then f is Λ-elliptic $\iff$ $f(z+\omega_1) = f(z+\omega_2) = f(z)$ $\forall z \in \mathbb{C}$)

(f Λ-elliptic $\iff$ $f : \mathbb{C}/\Lambda \to \mathbb{P}^1$ is meromorphic on $\mathbb{C}/\Lambda$ (a cx torus)).

Prop: An elliptic function with no zeros (or no poles) is constant.

Pf/ Let $D = [0,1]\omega_1 + [0,1)\omega_2$

just consider $\frac{1}{f}$.

Then $\mathbb{C} = \bigcup_{\lambda \in \Lambda} (\bar{D} + \lambda)$.

If f has no poles, then $|f|$ a finite maximum on $\bar{D}$, and so $|f|$ has a maximum on $\mathbb{C}$. By Liouville, f is constant.

Rk: also using more machinery: if $f : T = \mathbb{C}/\Lambda \to \mathbb{C}$ (f has no poles), then T is a cpct R.S. $\Rightarrow$ f is constant.

Thm: Let f be a Λ-elliptic function. Then:

1) $\displaystyle\sum_{x \in D} \mathrm{res}_x(f) = 0$

2) $\displaystyle\sum_{x \in D} \mathrm{ord}_x(f) = 0$

3) $\displaystyle\sum_{x \in D} \mathrm{ord}_x(f) \cdot x \equiv 0 \pmod{\Lambda}$

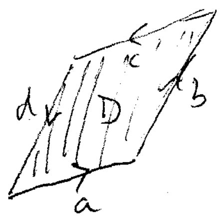
Proof:

Assume (if necessary, shift D) that f has no zeros or poles at ∂D.

$f(z)\,dz$ is meromorphic differential on $T = \mathbb{C}/\Lambda$. Residue Thm gives the result (1).

For (2), $\deg(\operatorname{div} f) = \sum \operatorname{ord}_x f = 0$.

We will, however, proof (1) and (2) using more elementary techniques.



The residue thm (on $\mathbb{C}$) says $\displaystyle\sum_{x \in D} \operatorname{res}_x(f) = \frac{1}{2\pi i}\int_{\partial D} f(z)\,dz$.

Now, by periodicity of f, $\displaystyle\int_{\partial D} f = 0$ ✓.

For (2), consider f', which is also Λ-elliptic. So $\frac{f'}{f}$ is Λ-elliptic.

$$\therefore \quad 0 = \sum_{x \in D} \operatorname{Res}_x\left(\frac{f'}{f}\right) = \sum_{x \in D} \operatorname{ord}_x(f)$$

This is because if q is a local parameter at x,

$f = a_0 + a_1 q + \cdots$, $a_0 \neq 0$, $\frac{f'}{f} = b_0 + b_1 q + \cdots$ ($b_0 = 0$ can happen).

if $a_0 \neq 0$, $f = q^n(a_0 + a_1 q + \cdots)$, $a_0 \neq 0$, $n \neq 0$.

Then $\frac{f'}{f} = n q^{-1} +$ hol' function of q.

For (3), we apply the residue thm for $z \cdot \frac{f'(z)}{f(z)}$.

$$\frac{1}{2\pi i}\int_{\partial D} \frac{z f'(z)}{f(z)}\,dz = \sum_{x \in D} \operatorname{res}_x\left((z-x)\frac{f'(z)}{f(z)} + x\frac{f'(z)}{f(z)}\right) = \sum_{x \in D} x \cdot \operatorname{ord}_x(f)$$

On the other hand, computing the integral along the path gives that it belongs to Λ. //

Def: A Λ-elliptic function f is of order n if it has exactly n poles (equivalently, n zeroes) in D, counted with multiplicities.

Remark: If $T = \mathbb{C}/\Lambda$, the order of f is the degree of $f : T \to \mathbb{P}^1$.

A corollary of part 1 of Thm, is that there are no elliptic functions of order 1: this would mean a unique simple pole in D. But then the residue there will not be 0, so contradicting part (1').

But we already knew this: $f : T \to \mathbb{P}^1$ of degree 1 is an iso $\Rightarrow$ iso!

(or, by R-R, $\dim H^0(\mathcal{O}_T(x)) = 1 \Rightarrow H^0(\mathcal{O}_T(x)) = \mathbb{C}$)

§ The Weierstrass-$\wp$-function and uniformization.

Define $\wp(z,\Lambda) := \frac{1}{z^2} + \sum_{\substack{\omega\in\Lambda \\ \omega\neq 0}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right)$, and the Eisenstein series:

$$G_{2k}(\Lambda) := \sum_{\substack{\omega\in\Lambda \\ \omega\neq 0}} \frac{1}{\omega^{2k}}.$$

Remark: If $\Lambda = \mathbb{Z}\tau \oplus \mathbb{Z}$, $\tau \in \mathcal{H}$, then $G_{2k}(\Lambda) = \sum'_{(m,n)\in\mathbb{Z}^2} (m\tau + n)^{-2k} = G_{2k}(\tau, (0,0), 1)$

(we defined them before, weight $2k$ and level 1).

In particular, it is a well-defined complex number.

For general Λ, write $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ s.t $\frac{\omega_1}{\omega_2} \in \mathcal{H}$. Then

$\Lambda = \omega_2 \cdot \tilde{\Lambda}$, $\tilde{\Lambda} = \mathbb{Z}\frac{\omega_1}{\omega_2} \oplus \mathbb{Z}$, and $G_{2k}(\Lambda) = \omega_2^{-2k} G_{2k}(\tilde{\Lambda})$,

so it is well-defined as well.

Note: in general, $G_{2k}(c\cdot\Lambda) = c^{-2k} G_{2k}(\Lambda)$ (homog. of weight $-2k$).

Theorem: The series defining $\wp(z)$ ~~do~~ converges absolutely and uniformly on any compact set in $\mathbb{C}\setminus\Lambda$.

It defines a meromorphic Λ-elliptic function, which is even, and has a pole of order 2.

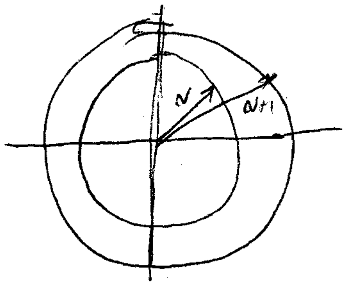
The Laurent expansion of $\wp(z)$ around 0 is:

$$\wp(z) = \frac{1}{z^2} + \sum_{k=1}^{\infty} (2k+1)\, G_{2k+2}(\Lambda)\, z^{2k}$$

Pf

Lemma: For some constant C, for any $N \geq 1$, $\# S(N) = \#\{\omega\in\Lambda : N \leq |\omega| < N+1\} < C\cdot N$.

Pf Let $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$.



Associate to each $\omega\in S(N)$, the "tile" $\omega + D$.

where $D = [0,1)\omega_1 + [0,1)\omega_2$.

The tile $\omega + D$ is contained in $S(N,r) = \{x : N - r \leq |x| \leq N+1+r\}$,

where $r = |\omega_1| + |\omega_2|$.

Because the tiles are disjoint, $\# S(N)\cdot \mathrm{vol}(D) \leq \mathrm{vol}(S(N,r)) \Rightarrow$

$$\# S(N) \leq \frac{\mathrm{vol}(S(N,r))}{\mathrm{vol}(D)} = \frac{1}{\mathrm{vol}(D)}\,\pi\left((N+1+r)^2 - (N-r)^2\right) = \frac{\pi}{\mathrm{vol}(D)}\left((4r+2)N + 2r+1\right) < C\cdot N$$

//

Now: if $|\omega| \geq 2|z|$ (and this happens except for finitely many points) ($z \in \text{Compact} \subseteq \mathbb{C}\setminus\Lambda$)

then
$$\left|\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right| = \left|\frac{z(2\omega - z)}{\omega^2(z-\omega)^2}\right| = \left|\frac{z}{\omega^3}\right| \left|\frac{2 - z/\omega}{(z/\omega - 1)^2}\right| \leq \left|\frac{z}{\omega^3}\right| \frac{2 + |z/\omega|}{\left(\frac{1}{2}\right)^2} \leq 10\,\frac{|z|}{|\omega|^3}.$$

When z is restricted to a cpct set, we get $\left|\frac{1}{(z-\omega)^2}-\frac{1}{\omega^2}\right| \leq C\cdot\frac{1}{|\omega|^3}$.

This estimate, together with the lemma, gives absolute convergence:

it is dominated by $\tilde{C}\cdot\sum_{n=1}^{\infty}\frac{1}{n^2}$ ✓.

It is also clear, from the definition, that there is a point of order 2 at each lattice point

$\mathcal{P}(z)$ is even: $\mathcal{P}(-z) = \frac{1}{(-z)^2}+\sum{}'\left(\frac{1}{(-z-\omega)^2}-\frac{1}{(-\omega)^2}\right) \overset{\Lambda \text{ stable under } \omega\mapsto\omega^{-1}}{=} \mathcal{P}(z)$

Since $\mathcal{P}(z)$ is unif. abs. conv., can compute (term by term)

$$\mathcal{P}'(z) = -2z^{-3}+\sum_{\Lambda}{}'\frac{-2}{(z-\omega)^3} = -2\sum_{\Lambda}\frac{1}{(z-\omega)^3}$$

So $\mathcal{P}'(z)$ has a pole of order 3 at any point of $\Lambda \Rightarrow \mathcal{P}(z)$ has a pole of order 2 at each point of Λ.

Moreover, $\mathcal{P}'(z)$ is Λ-elliptic of order 3.

Fix $\omega\in\Lambda$. The function $f(z) := \mathcal{P}(z+\omega)$ has derivative $\mathcal{P}'(z+\omega) \overset{\text{at } z}{=} \mathcal{P}'(z)$.

That is, $z\mapsto \mathcal{P}(z+\omega)-\mathcal{P}(z)$ is constant. For $z=-\frac{\omega}{2}$, as $\mathcal{P}$ is even, we get that the constant is 0, hence $\mathcal{P}(z)$ is elliptic for Λ.

Remains the Laurent expansion around 0: Spse $|z|<|\omega|$ $(\forall\omega\in\Lambda\setminus\{0\})$.

$$(z-\omega)^{-2}-\omega^{-2} = \omega^{-2}\left(\left(1-\frac{z}{\omega}\right)^{-2}-1\right) = \omega^{-2}\left(\sum_{n=1}^{\infty}(n+1)\left(\frac{z}{\omega}\right)^n\right) = \sum_{n=1}^{\infty}(n+1)z^n\omega^{-n+2}$$

Therefore, around 0,

$$\mathcal{P}(z) = \frac{1}{z^2}+\sum_{\Lambda}{}'\sum_{n=1}^{\infty}(n+1)z^n\omega^{-n+2} = \frac{1}{z^2}+\sum_{n=1}^{\infty}(n+1)\underbrace{\left(\sum_{\Lambda}{}'\omega^{-n+2}\right)}_{0 \text{ for } n \text{ odd}}z^n =$$

$$= \frac{1}{z^2}+\sum_{n=1}^{\infty}(2n+1)z^{2n}G_{2n+2}(\Lambda).$$

<u>Theorem</u>: Let $g_2 = g_2(\Lambda) = 60\, G_4(\Lambda)$ (for a fixed Λ).
$g_3 = g_3(\Lambda) = 140\, G_6(\Lambda)$.

1) $\wp'(z)^2 = 4\wp(z)^3 - g_2 \wp(z) - g_3$

2) The polynomial $4X^3 - g_2 X - g_3$ is separable; its discriminant is
$\Delta(\Lambda) = 16(g_2^3 - 27 g_3^2)$, and it doesn't vanish.

3) Let $E/\mathbb{C}$ be the elliptic curve with affine model $Y^2 = 4X^3 - g_2 X - g_3$.
Then the map $\phi : \mathbb{C}/\Lambda \to E(\mathbb{C}) \subseteq \mathbb{P}^2$ given by:

$\phi(z) = (\wp(z) : \wp'(z) : 1)$ (away from 0, and extend by $0 \mapsto (0:1:0)$)

is a complex-analytic isomorphism.

<u>Proof</u>: (1) $\wp(z) = z^{-2} + 3G_4 z^2 + 5G_6 z^4 + \cdots$
$\wp'(z) = -2z^{-3} + 6G_4 z + 20 G_6 z^3 + \cdots$

$\Rightarrow \wp(z)^3 = z^{-6} + 9G_4 z^{-2} + 15 G_6 + \text{h.o.t.}$

and $\wp'(z)^2 = 4z^{-6} - 24 G_4 z^{-2} - 80 G_6 + \text{h.o.t.}$

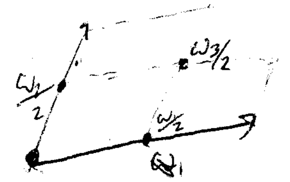
$\Rightarrow \wp'(z)^2 - 4\wp(z)^3 + 60 G_4 \wp(z) + 140 G_6$ = holomorphic at $z=0$, with a zero at $z=0$.

However, LHS is then a Λ-elliptic function without poles $\Rightarrow$ identically 0. ✓.

(2) One could check (by hand) the formula for the discriminant. Write then
$\Lambda = \omega_2 \hat{\Lambda}$. Then $\Delta(\Lambda) = c(\omega_2)\overset{\neq 0}{} \Delta(\tau)$ ($\Delta(\tau)$ = the modular form $\Delta(\tau)$ cusp form of weight 12).
(use the formula $\Delta(\tau) = E_4^3 - E_6^2$) and we know that $\Delta(\tau) \neq 0$

Alternative:

Consider the values of $\wp'$ at $\frac{\omega_1}{2}, \frac{\omega_2}{2}, \frac{\omega_3}{2}$, where $\omega_3 = \omega_1 + \omega_2$.



At any point x, $\wp'(-x) = -\wp'(x)$ ($\wp'$ odd) (because $\wp$ is even)

Also, $\wp'$ is periodic, so $\wp'\left(\frac{\omega_i}{2}\right) = -\wp'\left(\frac{-\omega_i}{2}\right) = -\wp'\left(\frac{\omega_i}{2}\right) \Rightarrow \wp'\left(\frac{\omega_i}{2}\right) = 0$.

It follows that the polynomial $f(x) = 4x^3 - g_2 x - g_3$ vanishes at the points $x = \wp\left(\frac{\omega_i}{2}\right)$, $i = 1, 2, 3$.

The function $\wp(z) - \wp\left(\frac{\omega_i}{2}\right)$ is an elliptic function of order 2. It vanishes at $z = \frac{\omega_i}{2}$, hence it vanishes there to order 2 (b/c $\wp'\left(\frac{\omega_i}{2}\right) = 0$).

$\Rightarrow \wp(z) - \wp\left(\frac{\omega_i}{2}\right)$ has no other zeros in D.

In particular, $\wp\left(\frac{\omega_j}{2}\right) - \wp\left(\frac{\omega_i}{2}\right) \neq 0$ for $j \neq i$ $\Rightarrow \wp\left(\frac{\omega_1}{2}\right), \wp\left(\frac{\omega_2}{2}\right), \wp\left(\frac{\omega_3}{2}\right)$ are all distinct, and also are all the roots of f $\Rightarrow f$ is separable.

i) Want to show that

$$\begin{aligned} \phi : \mathbb{C}/\Lambda &\to E(\mathbb{C}) \quad \text{is an iso.} \\ z &\mapsto (\wp(z) : \wp'(z) : 1). \end{aligned}$$

Injective: Given $(x, y) \in E(\mathbb{C})$. $\left.\begin{array}{l} \wp(z) = x_0 \\ \wp'(z) = y_0 \end{array}\right\}$

There exists 2 values of z, $\{z_0, -z_0\}$ s.t. $\wp(z_0) = x_0 = \wp(-z_0)$

But $\wp'(z_0) = -\wp'(z_0) \Rightarrow$ exactly one solution if $y_0 \neq 0$.

If $y_0 = 0$, then $z_0 = -z_0$ (by previous part), so fine.

Surjective: Same argument, backwards.

Note that $\mathbb{C}/\Lambda$ is also a group. How does this structure carry over to $E(\mathbb{C})$?

Given $z_1, z_2 \in \mathbb{C}/\Lambda$, they correspond to (x_1,y_1), (x_2,y_2) in $E(\mathbb{C})$.

Also, z_1+z_2 corresponds to $(x_3,y_3) = (\wp(z_1+z_2), \wp'(z_1+z_2))$

Recall: if f is a Λ-elliptic function, then

- $\sum_{P \in \mathbb{C}/\Lambda} \mathrm{ord}_P(f) = 0$

- $\sum_{P \in \mathbb{C}/\Lambda} \mathrm{ord}_P(f) \cdot [P] \in \Lambda$

Conversely, if these two conditions are satisfied, ~~the~~

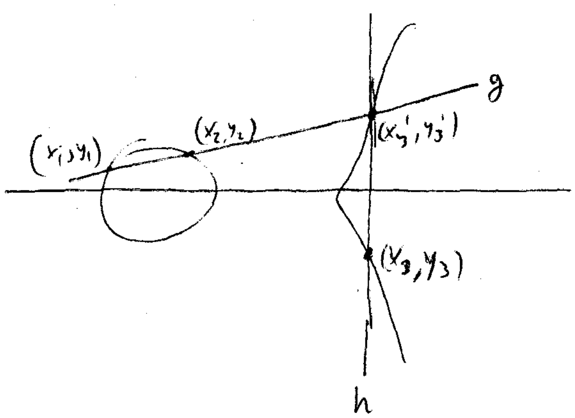
(i.e. $\sum n_P [P] \in \Lambda$ and $\sum n_P = 0 \Rightarrow \exists f$ s.t. $(f) = \sum n_P [P]$).

(we will prove this later, maybe).

So $\exists f_{z_1,z_2}$ having zeros at z_1 and z_2, and poles at 0 and z_1+z_2 (all simple).

(if they are equal, then simple becomes double).

This is a same to say that $\exists f$ on $E(\mathbb{C})$ having simple zeros at (x_1,y_1) and (x_2,y_2), and poles at (x_3,y_3) and $\infty = (0:1:0)$.



$\mathrm{div}(g) = (x_1,y_1) + (x_2,y_2) + (x_3,y_3) - 3\cdot(0:1:0)$.

$\mathrm{div}(h) = (x_3',y_3') + (x_3,y_3) - 2(0:1:0)$.

$\therefore \mathrm{div}\left(\frac{g}{h}\right) = (x_1,y_1) + (x_2,y_2) - (x_3,y_3) - (0:1:0)$

So $f = \frac{g}{h}$ has the correct divisor.

Now, let $m := \frac{y_2 - y_1}{x_2 - x_1}$ be the slope of the line $g=0$

So $y = mx + c$ is the line $g=0$

From the equation $y^2 = x^3 + aX + b$ $\Big\} \Rightarrow x^3 - m^2x^2 + \dots + \dots = 0$

Know that x_1, x_2 are roots, so $x_1 + x_2 + x_3' = m^2$.

As $x_3' = x_3$, get:

$$\boxed{x_3 = m^2 - x_1 - x_2}$$

Then, $y_3 = -(mx_3 + c)$

We want to prove a claim that we used:

Prop: Given $a_1, \dots, a_k, b_1, \dots, b_k \in \mathbb{C}$ s.t. $\sum a_i = \sum b_i \mod \Lambda$, then $\exists f$ Λ-periodic s.t. $(f) = \sum [a_i] - \sum [b_i]$

- Riemann theta function:

Let $\Theta(z, \tau) := \sum_{n \in \mathbb{Z}} \exp(\pi i n^2 \tau + 2\pi i n z)$, $\tau \in \mathcal{H}$, $z \in \mathbb{C}$.

Note that $\Theta(0, \tau) =$ theta function of the lattice $\mathbb{Z}$.

The series $\Theta(z, \tau)$ converges uniformly and absolutely on compact sets in $\mathbb{C} \times \mathcal{H}$. In fact, if $|\mathrm{Im}(z)| < C$ & $\mathrm{Im}(\tau) > \varepsilon$, then $\left|e^{\pi i n^2 \tau + 2\pi i n z}\right| < \left|e^{-\pi |n| \varepsilon} e^{2\pi C}\right|^{|n|}$

So choose $n_0 \gg 0$ s.t $e^{-\pi n_0 \varepsilon} e^{2\pi C} < 1$, to find:

$$\left| e^{\pi i n^2 \tau + 2\pi i n z} \right| < \left(e^{-\pi \varepsilon} \right)^{|n|^2 - |n| \cdot n_0} \qquad \text{for } |n| \geq n_0$$

This gives uniform absolute convergence on our set.

Lemma:

1) $\Theta(z+1, \tau) = \Theta(z, \tau)$

2) $\Theta(z+\tau, \tau) = \exp(-\pi i \tau - 2\pi i z)\, \Theta(z, \tau)$

Pf (1) clear (term by term)

(2)

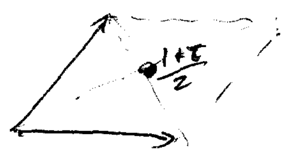
$$\Theta(z+\tau, \tau) = \sum \exp\left(\pi i n^2 \tau + 2\pi i n (z+\tau)\right) = \cancel{\sum \exp(\pi i (n+1)^2 \tau +}$$

$$= \sum_{n \in \mathbb{Z}} \exp\left(\pi i (n+1)^2 \tau + 2\pi i (n+1) z\right) \exp(-\pi i \tau - 2\pi i z) =$$

$$= \exp(-\pi i \tau - 2\pi i z)\, \Theta(z, \tau).$$

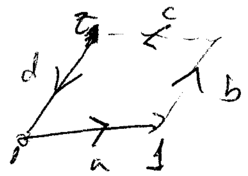
Note that the zeros of $\Theta(\cdot, \tau)$ are $\mathbb{Z}\tau + \mathbb{Z}$ - periodic.

Prop: Θ vanishes at a single point simple zero in the "standard" fundamental domain for $\Lambda = \mathbb{Z}\tau + \mathbb{Z}$. This is the point $\frac{1+\tau}{2}$.



Pf # zeros of Θ in D is $\frac{1}{2\pi i} \int_{\partial D} \frac{\Theta'}{\Theta}\, dz$ (shift the domain if needed).

Since $\Theta(z+1,\tau)=\Theta(z,\tau)$, the integrals over b and d cancel each other:



Let $\gamma = \exp(-\pi i \tau)$.

Then $\Theta(z+\tau,\tau) = \gamma \exp(-2\pi i z)\, \Theta(z,\tau)$

$\Rightarrow \Theta'(z+\tau,\tau) = \gamma \exp(-2\pi i z)\,\Theta'(z,\tau) - 2\pi i \gamma \exp(-2\pi i z)\,\Theta(z,\tau).$

So $\displaystyle\int_c \frac{\Theta'(z,\tau)}{\Theta(z,\tau)}\,dz = -\int_a \frac{\Theta'}{\Theta}\,dz + \int_a 2\pi i\, dz \Rightarrow \frac{1}{2\pi i}\int_{\partial D} \frac{\Theta'}{\Theta}\,dz = 1.$

Hence Θ has a single simple zero in D.

Define now the Riemann theta functions with characteristic $\begin{bmatrix} a \\ b \end{bmatrix}$ ($a, b \in \mathbb{R}$) by:

$$\Theta\begin{bmatrix} a \\ b \end{bmatrix}(z,\tau) := \sum_{n\in\mathbb{Z}} \exp\left(\pi i (n+a)^2 \tau + 2\pi i (n+a)(z+b)\right) =$$

$$= \exp\left(\pi i a^2 \tau + 2\pi i a(z+b)\right)\Theta(z+a\tau+b,\tau)$$

To finish the lemma, it is then enough to show that:

$\Theta\begin{bmatrix} 1/2 \\ 1/2 \end{bmatrix}(z,\tau)$ vanishes at $z=0$.

This will follow from checking that $\Theta\begin{bmatrix} 1/2 \\ 1/2 \end{bmatrix}(z,\tau)$ is an odd function in z:

$$\Theta\begin{bmatrix} 1/2 \\ 1/2 \end{bmatrix}(-z,\tau) = \sum_{n\in\mathbb{Z}} \exp\left(\pi i (n+\tfrac{1}{2})^2 \tau + 2\pi i (n+\tfrac{1}{2})(-z+\tfrac{1}{2})\right).$$

Let $m := -1-n$. Get $\displaystyle\sum_{m\in\mathbb{Z}} \exp\left(\pi i (-m-\tfrac{1}{2})^2 \tau\right) + 2\pi i\left((-m-\tfrac{1}{2})(-z+\tfrac{1}{2})\right) =$ ↓

Get $\Theta\begin{bmatrix}1/2\\1/2\end{bmatrix}(z,\tau) = \sum_{m\in\mathbb{Z}} \exp\left(\pi i(m+\tfrac{1}{2})^2\tau + 2\pi i(m+\tfrac{1}{2})(z+\tfrac{1}{2}) - 2\pi i(m+\tfrac{1}{2})\right)$

$= -1\cdot\Theta\begin{bmatrix}1/2\\1/2\end{bmatrix}(z,\tau)$ as wanted.

Prop: Let $a_1,\dots,a_k, b_1,\dots,b_k \in \mathbb{C}$ s.t. $\sum a_i = \sum b_i$ ← not mod Λ!

Then $f(z) := \prod_{1\le i\le k} \Theta(z-a_i,\tau) \Big/ \prod_{1\le i\le k}\Theta(z-b_i,\tau)$

is a $(\mathbb{Z}\tau+\mathbb{Z})$-periodic function, with divisor mod $\mathbb{Z}\tau+\mathbb{Z}$.

given by: zeroes $\{a_i+\frac{1+\tau}{2}\}$, poles $\{b_i+\frac{1+\tau}{2}\}$.

Pf

$f(z+1)=f(z)$ clearly.

$$f(z+\tau) = \prod_{i=1}^{k} \frac{\exp(-\pi i\tau - 2\pi i(z-a_i))\,\Theta(z-a_i,\tau)}{\exp(-\pi i\tau-2\pi i(z-b_i))\,\Theta(z-b_i,\tau)} = \exp\left(+2\pi i\left(\textstyle\sum a_i - \sum b_i\right)\right) f(z)$$

$\sum a_i = \sum b_i$

✓

Corollary (Thm).

Let $\Lambda\subseteq\mathbb{C}$ be a lattice, $z_1,z_2\in\mathbb{C}$. Then $\exists$ a Λ-elliptic function f such that $(f) = [z_1]+[z_2]-[0]-[z_1+z_2]$

Pf/ Immediate if $\Lambda=\mathbb{Z}\tau+\mathbb{Z}$, and deduce the general case by, if $\Lambda = \mathbb{Z}\omega_1\oplus\mathbb{Z}\omega_2$ with $\frac{\omega_1}{\omega_2}\in\mathcal{H}$, then multiply by $\frac{1}{\omega_2}$ get $\mathbb{Z}\tau+\mathbb{Z}$.

The next goal is to prove the following Theorem:

<u>Thm</u>: $\exists$ equivalence of categories btween

$$\left\{\begin{array}{l}\text{1-dim'l complex tori } \mathbb{C}/\Lambda \text{ up to } \cong, \\ \text{with morphisms:} \\ \mathrm{Hom}(\mathbb{C}/\Lambda_1, \mathbb{C}/\Lambda_2) = \{\lambda \in \mathbb{C} : \lambda \Lambda_1 \subseteq \Lambda_2\}\end{array}\right\} \longleftrightarrow \left\{\begin{array}{l}\text{complex elliptic curves up to iso} \\ \text{with morphisms:} \\ \mathrm{Hom}(E_1, E_2) = \left\{\begin{array}{l} f: E_1 \to E_2 \text{ s.t.} \\ f \text{ is a morphism of} \\ \text{alg. curves which} \\ \text{is a gp hom}\end{array}\right\}\end{array}\right\}$$

Recall that to $\mathbb{C}/\Lambda$ we associated the elliptic curve

$$y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda) \qquad \text{(using the Weierstraß } \wp\text{-function)}$$

Given $E/\mathbb{C}$, we've seen ("more or less") that E is given by

$$Ay^2 + Bxy + Cy = Dx^3 + Ex^2 + Fx + G, \quad AD \neq 0, \text{ nonsingular.}$$

By $y \rightsquigarrow \frac{y}{\sqrt{A}}$, $x \rightsquigarrow \frac{x}{\sqrt[3]{D}}\sqrt[3]{4}$, can assume that $A = 1$, $D = 4$.

Next, $y \rightsquigarrow y + \frac{B}{2}x$ gives that one can assume $B = 0$.

Then, $y \rightsquigarrow y + \frac{C}{2}$, ...

Get $y^2 = 4x^3 - g_2 x - g_3$, for some $g_2, g_3 \in \mathbb{C}$. $\leftarrow$ and nonsingular curve.

<u>Q</u>: Can we find Λ s.t. $g_2 = g_2(\Lambda)$, $g_3 = g_3(\Lambda)$

<u>Lemma</u>: Let $g_2, g_3 \in \mathbb{C}$ s.t. $g_2^3 - 27g_3^2 \neq 0$ ($\Leftrightarrow 4x^3 - g_2x - g_3$ is separable).

Then $\exists$ lattice $\Lambda \subseteq \mathbb{C}$ with $g_2 = g_2(\Lambda)$, $g_3 = g_3(\Lambda)$.

Pf/ Let $f: \dfrac{g_3(\tau)^2}{g_2(\tau)^3} = \text{const} \times \dfrac{E_6^2}{E_4^3}$. $f: \mathcal{H}^*/SL_2(\mathbb{Z}) \to \mathbb{P}^1$, non-constant.

The function $f : \mathcal{H}^*/_{SL_2(\mathbb{Z})} \to \mathbb{P}^1$ is nonconstant $\Rightarrow$ surjective.

$\Rightarrow \exists\, \tau$ s.t. $\dfrac{g_3(\tau)^2}{g_2(\tau)^3} = \dfrac{g_3^2}{g_2^3} \in \mathbb{C} \cup \{\infty\}$.

Assume first that $\underline{g_2(\tau) \neq 0}$. Then also $g_2 \neq 0$.

Since $g_2(a\Lambda) = a^{-4} g_2(\Lambda)$, we can find a s.t. $g_2(a(\mathbb{Z}\tau + \mathbb{Z})) = g_2$.

Then $g_3(a(\mathbb{Z}\tau+\mathbb{Z}))^2 = g_3^2$ ✓.

Hence $g_3(a(\mathbb{Z}\tau + \mathbb{Z})) = \pm g_3$. If we get $(-)$, replace a by $i \cdot a$. In that case, $g_3(ia(\mathbb{Z}\tau+\mathbb{Z})) = i^{-6} g_3(a(\mathbb{Z}\tau+\mathbb{Z})) = g_3$, and $i^{-4} = 1 \Rightarrow$ ✓.

$\underline{\text{If } g_2(\tau) = 0}$, then also $g_2 = 0$ (b/c E_4, E_6 have no common zeros)

Then $g_3 \neq 0$, and in this case can rescale the lattice so that

$g_3(a(\mathbb{Z}\tau+\mathbb{Z})) = g_3$, in the same way.

We just need to check that $g_3^2/g_2^3 = \frac{1}{27}$ is the exactly the case $\tau = \infty$.

<u>Conclusion</u>: Any $E/_{\mathbb{C}}$ is isomorphic to some $\mathbb{C}/_\Lambda$.

<u>Lemma</u>: Let Λ_1, Λ_2 be lattices in $\mathbb{C}$, and $f : \mathbb{C}/_{\Lambda_1} \to \mathbb{C}/_{\Lambda_2}$ an analytic map & gp homomorphism. Then $\exists!\, \lambda \in \mathbb{C}$ s.t.

$$\begin{tikzcd} \mathbb{C} \arrow[r, "\cdot\lambda"] \arrow[d, "\pi_1"'] & \mathbb{C} \arrow[d, "\pi_2"] \\ \mathbb{C}/_{\Lambda_1} \arrow[r, "f"] & \mathbb{C}/_{\Lambda_2} \end{tikzcd}$$

(In particular, $\lambda \Lambda_1 \subseteq \Lambda_2$, and if $f \neq 0$, $\operatorname{Ker} f = \frac{1}{\lambda}\Lambda_1 / \Lambda_2$)

Proof: If $f \neq 0$, then f is surjective and of finite degree.

(by theory of R.S.).

The fibers over any point in $\mathbb{C}/\Lambda_2$ have the same cardinality,

$\# \operatorname{Ker} f$ (b/c f is a gp hom).

In particular, f is unramified, and $\mathbb{C}/\Lambda_1 \xrightarrow{f} \mathbb{C}/\Lambda_2$ is a covering map.

(as topological spaces)

Then
$$\begin{tikzcd} \mathbb{C} \arrow[d] \arrow[dr] & \\ \mathbb{C}/\Lambda_1 \arrow[r] & \mathbb{C}/\Lambda_2 \end{tikzcd}$$
also a covering map

But can complete the picture with
$$\begin{tikzcd} \mathbb{C} \arrow[r, dashed, "\tilde{f}"] \arrow[d] \arrow[dr] & \mathbb{C} \arrow[d] \\ \mathbb{C}/\Lambda_1 \arrow[r, "f"'] & \mathbb{C}/\Lambda_2 \end{tikzcd}$$
univ. covering space of $\mathbb{C}/\Lambda_2$

B/c $\mathbb{C} \to \mathbb{C}/\Lambda_2$ is universal cover,

can lift the map $\mathbb{C} \to \mathbb{C}/\Lambda_1 \xrightarrow{f} \mathbb{C}/\Lambda_2$.

By the cx structure we have, $\hat{f}$ is analytic. In particular,

$\exists\, \varepsilon$ s.t.
$$\begin{tikzcd} B(0,\varepsilon) \arrow[r, "\hat{f}"] \arrow[d, "\cong"'] & V \arrow[d, "\cong"] \\ V_1 \arrow[r, "\cong", "f"'] & V_2 \end{tikzcd}$$
V, V_1, V_2 open sets

$\cong$ means bianalytic.

Choose n s.t. $\frac{1}{n} < \varepsilon$. Then $k\hat{f}\left(\frac{1}{kn}\right) \bmod \Lambda_2$ is $k \cdot f\left(\frac{1}{kn} \bmod \Lambda_1\right)$

$= k \cdot \frac{1}{k} f\left(\frac{1}{n} \bmod \Lambda_1\right) \implies k\hat{f}\left(\frac{1}{kn}\right) = \hat{f}\left(\frac{1}{n}\right) \quad \forall\, k \geq 1$ integer.

Define then $\lambda := \tilde{f}\left(\frac{1}{n}\right) / \frac{1}{n}$.

Then $\tilde{f}\left(\frac{1}{kn}\right) = \lambda \cdot \frac{1}{kn}$

So the two analytic maps $\tilde{f}$ and $\cdot\lambda$ agree on the set $\frac{1}{kn}$, $k=1,2,3,\ldots$

Because this set has an accumulation point (0), this implies that $\tilde{f} = \cdot\lambda$.

If we have

$$\begin{array}{ccc} E_1(\mathbb{C}) & \xrightarrow{f} & E_2(\mathbb{C}) \\ \wr\| & & \wr\| \\ \mathbb{C}/\Lambda_1 & \overset{\text{"}f\text{"}}{\dashrightarrow} & \mathbb{C}/\Lambda_2 \end{array}$$

, such f is multiplication by $\lambda(f) \in \mathbb{C}$.

We still need to show that any analytic map $E_1(\mathbb{C}) \to E_2(\mathbb{C})$ is in fact algebraic.

Write $E_i(\mathbb{C}) \simeq \mathbb{C}/\Lambda_i$.

$$\begin{array}{ccc} \mathbb{C} & \xrightarrow{\lambda} & \mathbb{C} \\ \downarrow & & \downarrow \\ E_1(\mathbb{C}) \simeq \mathbb{C}/\Lambda_1 & \xrightarrow{f} & \mathbb{C}/\Lambda_2 \simeq E_2(\mathbb{C}) \end{array}$$

To show: f comes from an alg. map $E_1 \to E_2$.

In the affine part,

$$\left(\wp(z,\Lambda_1), \wp'(z,\Lambda_1)\right) \longmapsto \left(\wp(\lambda z,\Lambda_2), \wp'(\lambda z,\Lambda_2)\right)$$

This map is algebraic iff the maps $\left\{\begin{array}{l} z \bmod \Lambda_1 \mapsto \wp(\lambda z,\Lambda_2) \\ z \bmod \Lambda_1 \mapsto \wp'(\lambda z,\Lambda_2) \end{array}\right.$ are algebraic functions (on E).

There functions are Λ_1-elliptic. So it's enough to prove:

<u>Thm</u>: The field of Λ_1-elliptic functions is $\mathbb{C}\left(\wp(z,\Lambda), \wp'(z,\Lambda)\right)$

(therefore, on E_1, each of our functions is coming from some polynomial F in $\wp$, $\wp'$, i.e. it is $F(x,y)$.)

Pf/

Write $\Lambda = \Lambda_1$, $\wp(z) := \wp(z,\Lambda)$.

Let g be a Λ-elliptic function. $g(z) = \overbrace{\frac{g(z)+g(-z)}{2}}^{\text{even}} + \overbrace{\frac{g(z)-g(-z)}{2}}^{\text{odd}}$

So we can assume that g is either or odd.

If g is odd, then $g/\wp'$ is even, so enough to consider g <u>even</u>.

Then g defines a meromorphic analytic function on $E \simeq \mathbb{C}/\Lambda$.

The map $z \mapsto -z$ induces $(x,y) \mapsto (x,-y)$ on E

(as $\wp$ is even, $\wp'$ is odd).

So $\tilde{g}$ has the property that $\tilde{g}(x,y) = \tilde{g}(x,-y)$

$$\begin{tikzcd} E \arrow[d] & (x,y) \arrow[d, mapsto] \\ \mathbb{P}^1 & x \end{tikzcd}$$

See Silverman for more explanation.

$\tilde{g}(x,y) = \tilde{g}(x,-y) \Rightarrow \tilde{g}$ is a rational function coming from $\mathbb{P}^1$, i.e.

a rational function on X $\Rightarrow g$ = rat'l function on $\wp(z)$, as wanted.

//

- Some consequences of the uniformization theory.

- Let $m \neq 0$ be an integer. Let $[m] : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda$ be the multiplication-by-m map.

  This map corresponds to a mult. by m on an isomorphic elliptic curve (E_τ).

  The kernel of $[m]$ is $\frac{m^{-1}\Lambda}{\Lambda} \simeq (\mathbb{Z}/m\mathbb{Z})^2$.

  So on any elliptic curve, $E/\mathbb{C}$, $E[m] := \ker [m] \simeq (\mathbb{Z}/m\mathbb{Z})^2$.

- For any elliptic curve E, $\mathbb{Z} \subseteq \mathrm{End}(E) \leftarrow$ morphisms of curves + gp hom.

  $m \mapsto [m]$

- Thm: $\mathrm{End}(E) \cong \begin{cases} \mathbb{Z} \\ \mathcal{O} = \text{order in an quadratic imaginary field } K. \end{cases}$

  Rk: over other fields (eg $\overline{\mathbb{F}_p}$), there are more possibilities.

  End(E) could be a maximal order in a quaternion algebra over $\mathbb{Q}$.

  (in particular, of rank 4 over $\mathbb{Z}$) (ramified at p, ∞).

  Conversely, any such order arises.

Proof: $E/\mathbb{C}$ $E \simeq \mathbb{C}/\Lambda$, $\mathrm{End}(E) \simeq \{\lambda \in \mathbb{C} : \lambda\Lambda \subseteq \Lambda\}$, and so $\mathrm{End}(E)$ is a commutative ring with no zero divisors

$$\{\lambda \in \mathbb{C} : \lambda\Lambda \subseteq \Lambda\} \hookrightarrow \mathrm{End}(\Lambda \otimes \mathbb{Q}) \simeq \mathrm{End}(\mathbb{Q}^2) \simeq M_2(\mathbb{Q})$$

$$\lambda \longmapsto \lambda$$

Having no zero divisors, $\mathrm{End}(E) \otimes \mathbb{Q}$ is a field of degree 2 over $\mathbb{Q}$.

⋮

(continues proof).

Let wlog $\Lambda = \mathbb{Z} \oplus \mathbb{Z}\tau$, and let $\lambda \in \text{End}(E)$. Then $\lambda \cdot 1 = a + b\tau$ for some $a, b \in \mathbb{Z}$ $\Rightarrow$ $\lambda \in \mathbb{Q}(\tau)$.

So $\text{End}(E) \subseteq \text{End}(E) \otimes \mathbb{Q} \subseteq \mathbb{Q}(\tau)$.

So either $\text{End}(E) = \mathbb{Z}$ or $\text{End}(E)$ is a subring of $\mathbb{Q}(\tau)$.

<u>Rk</u>: $\lambda \cdot 1 = a + b\tau$

$\lambda \tau = c + d\tau = \lambda \cdot 1 \cdot \tau = (a + b\tau)\tau \Rightarrow b\tau^2 + (a-d)\tau - c = 0$

So τ is quadratic over $\mathbb{Q}$. Also, as $\text{Im}(\tau) > 1$, $\mathbb{Q}(\tau)$ is a <u>quadratic</u> imaginary field, and $\lambda \in \mathbb{Q}(\tau)$.

<u>Remains to show</u>: any element of $\text{End}(E)$ is integral $/\mathbb{Z}$ (so that $\text{End}(E)$ is an order of $\text{End}(E) \otimes \mathbb{Q} = \mathbb{Q}(\tau)$).

$\{\lambda \in \mathbb{C} : \lambda\Lambda \subseteq \Lambda\} \hookrightarrow \text{End}(\Lambda) \simeq M_2(\mathbb{Z})$

Use Cayley-Hamilton $\Rightarrow$ every $\lambda \in \text{End}(E)$ is integral.

Conversely, let $\mathcal{O} \subseteq K$ be an order. Fix an embedding $K \hookrightarrow \mathbb{C}$.

Then $\mathcal{O} \subseteq \mathbb{C}$, and $\mathcal{O}$ has $\mathbb{Z}$-rank 2.

Then $\mathcal{O}\mathbb{R} = K\mathbb{R} = \mathbb{C}$ $\Rightarrow$ $\mathcal{O}$ contains a basis for $\mathbb{C}/\mathbb{R}$ $\Rightarrow$ $\mathcal{O}$ is a lattice.

Let then $\mathbb{C}/\mathcal{O} =: E$, an elliptic curve. $\mathcal{O} \subseteq \text{End}(E)$ (if $\lambda \in \mathcal{O}$, $\lambda\mathcal{O} \subseteq \mathcal{O}$).

Equality: if $\lambda \in \text{End}(E)$, then $\lambda\mathcal{O} \subseteq \mathcal{O} \Rightarrow \lambda \cdot 1 \in \mathcal{O} \Rightarrow \lambda \in \mathcal{O}$.

///

<u>Exercise</u>: K quadratic imaginary, $\mathcal{C}\ell(K)$: fract ideals mod $\times\lambda$, $\lambda\in K^\times$.

Then show that $\mathcal{C}\ell(K) \overset{1:1}{\leftrightarrow}$ iso classes of $\mathbb{C}/\Lambda$ s.t. $\mathcal{O}_K = \mathrm{End}(\mathbb{C}/\Lambda)$.

You don't need to do the exercise, but:

$$\begin{array}{c} \mathcal{C}\ell(K) \hookrightarrow \text{primary binary quadratic forms with disc} = \text{disc } K \\ \updownarrow \\ \text{certain points } \tau \in \mathcal{H}/SL_2(\mathbb{Z}) \\ \updownarrow \\ \text{certain elliptic curves } \mathbb{C}/\Lambda_\tau,\ \Lambda_\tau = \mathbb{Z}\oplus\mathbb{Z}\tau \\ \updownarrow \\ \text{iso classes of ell curves } E \text{ with } \mathrm{End}(E) = \mathcal{O}_K. \end{array}$$

<u>Note</u>: (<u>Hint</u>) $\mathfrak{a} \subseteq K$ fract. ideal $\Leftrightarrow$ $\mathfrak{a}$ having rk 2 over $\mathbb{Z}$, $\mathcal{O}_K\cdot\mathfrak{a} \subseteq \mathfrak{a}$. $\rightsquigarrow \mathbb{C}/\mathfrak{a}$.

$\mathrm{End}(\mathbb{C}/\Lambda) = \mathcal{O}_K \overset{\text{wlog}}{\rightsquigarrow} 1 \in \Lambda$. ~~Show that $\mathcal{O}_K \subseteq \mathcal{O}_K\Lambda \subseteq K$~~.

and then show that $\mathcal{O}_K \subseteq \Lambda \subseteq K \Rightarrow \Lambda$ is a fractional ideal...

We now see that

$\{\text{iso classes of cx tori } \mathbb{C}/\Lambda\} \longleftrightarrow \{\text{lattices modulo homothety } (\Lambda \sim \lambda\Lambda,\ \lambda\in\mathbb{C}^\times)\}$.

Given Λ, choose a basis so that $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$, and $\frac{\omega_1}{\omega_2}\in\mathcal{H}$.

Let $\tau = \frac{\omega_1}{\omega_2}$. Then $\Lambda \sim \Lambda_\tau = \mathbb{Z}\tau + \mathbb{Z}$.

If we change basis to $a\omega_1 + b\omega_2$, $c\omega_1 + d\omega_2$, then $\begin{pmatrix} a & b \\ c & d\end{pmatrix} \in GL_2(\mathbb{Z})$

To have $\tau' = \frac{a\omega_1+b\omega_2}{c\omega_1+d\omega_2} \in \mathcal{H}$, must have $\det\begin{pmatrix} a & b \\ c & d\end{pmatrix} > 0$ (and also $\in \{\pm1\}$) $\Rightarrow$

$\Rightarrow \begin{pmatrix} a & b \\ c & d\end{pmatrix} \in SL_2(\mathbb{Z})$

Conversely, starting from $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$, get τ' ...

To Λ we associate the orbit $SL_2(\mathbb{Z})\tau$.

If $\Lambda_1 = \lambda\Lambda = \mathbb{Z}\lambda\omega_1 \oplus \mathbb{Z}\lambda\omega_2 \rightsquigarrow$ same orbit.

<u>Conclusion:</u>

$$\left\{ \begin{matrix} \text{iso classes of} \\ \text{complex elliptic curves} \end{matrix} \right\} \xleftrightarrow{\text{natural}} SL_2(\mathbb{Z}) \backslash \mathcal{H} = Y(1)$$

$$\mathbb{Z}\tau \oplus \mathbb{Z} = \Lambda_\tau \longleftarrow\!\!\shortmid \tau$$

Choosing any bijection $f : Y(1) \xrightarrow{\sim} \mathbb{C}$ ($Y(1)$ is iso to $\mathbb{C}$),

we have an invariant for elliptic curves:

Given E, $f(E) \in \mathbb{C}$, st $f(E) = f(\mathbb{C}/\Lambda_\tau) = f(\tau)$, and

$E_1 \cong E_2 \iff f(E_1) = f(E_2)$.

There is a "customary choice" for f, called the j-invariant:

$j : SL_2(\mathbb{Z}) \backslash \mathcal{H} \to \mathbb{C}$ given by $j(\tau) := 1728 \dfrac{g_2(\tau)^3}{g_2(\tau)^3 - 27 g_3(\tau)^2}$.

is a modular function (of weight 0).

One can show that it's an isomorphism.

If $E : y^2 = x^3 + ax + b$, by changing coordinates we can find:

$$j(E) = -1728 \frac{(4A)^3}{\Delta}, \text{ where } \Delta = -16(4A^3 + 27B^2).$$

• Modular Curves.

A full symplectic level structure:

$$\psi_\tau : (\mathbb{Z}/n\mathbb{Z})^2 \to E_\tau[n] = n^{-1}\Lambda_\tau / \Lambda_\tau = \langle \tfrac{1}{n}, \tfrac{\tau}{n} \rangle$$

Such that, say $(1,0) \mapsto \frac{1}{n}$, $(0,1) \mapsto \frac{\tau}{n}$.

(i.e. $\psi_\tau((x,y)) = \frac{1}{n}(1\ \ \tau)\begin{pmatrix} x \\ y \end{pmatrix}$.

$$\underset{\frac{1}{n}(1\ \tau')}{(\mathbb{Z}/n\mathbb{Z})^2 \xrightarrow{\sim}} E_{\tau'}[n] \xrightarrow{\cdot c\tau+d} E_\tau[n]$$

So $(x,y) \mapsto \frac{1}{n}(x+y\tau') \mapsto \frac{1}{n}\big(x(c\tau+d)+y(a\tau+b)\big) = \frac{1}{n}(xd+yb+xc\tau+ya\tau)$

$$= \frac{1}{n}(1\ \ \tau)\begin{pmatrix} d & b \\ c & a \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}$$

Hence instead of ψ_τ, we get $\psi_\tau \circ \overbrace{\begin{pmatrix} d & b \\ c & a \end{pmatrix}}^{\in \operatorname{Aut}((\mathbb{Z}/n\mathbb{Z})^2)}$.

So $\psi_{\tau'} = \psi_\tau \iff \begin{pmatrix} d & b \\ c & a \end{pmatrix} \in \Gamma(n) \iff \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(n)$.

Conclusion: if we associate to τ a pair (E_τ, ψ_τ), and

$$(E_\tau, \psi_\tau) \simeq (E_{\tau'}, \psi_{\tau'}) \iff \tau \underset{\Gamma(n)}{\sim} \tau'.$$

Q: Given $E/\mathbb{C}$ and an iso $\psi : (\mathbb{Z}/n\mathbb{Z})^2 \to E[n]$, is $(E,\psi) \simeq (E_\tau, \psi_\tau)$ for some $\tau \in \mathcal{H}$?

A: This is so if, and only if, ψ is "symplectic":

There is a pairing (the Weil pairing) $E[n] \times E[n] \to \mu_n \subseteq \mathbb{C}^\times$, which is bilinear, perfect and alternating.

On $(\mathbb{Z}/n\mathbb{Z})^2 \times (\mathbb{Z}/n\mathbb{Z})^2$ there's also a pairing $\langle \cdot, \cdot \rangle$:

it is given by sending $\langle (1,0), (0,1) \rangle := e^{\frac{2\pi i}{n}}$ (unique way of extending it, b/c declare it to be also bilinear, perfect and alternating.

Then ψ is symplectic if

$$\begin{tikzcd} E[n] \times E[n] \arrow[r, "\text{Weil}"] \arrow[d, "\psi \times \psi"'] \arrow[dr, phantom, "\circlearrowright"] & \mu_n \subseteq \mathbb{C}^\times \\ (\mathbb{Z}/n\mathbb{Z})^2 \times (\mathbb{Z}/n\mathbb{Z})^2 \arrow[ur, "\langle \cdot, \cdot \rangle"'] & \end{tikzcd}$$

Conclusion: $\mathcal{H}/\Gamma(n)$ parametrizes pairs (E, ψ), where ψ is a symplectic structure of level n.

For $\Gamma_1(n)$: Associate to τ a pair $(E_\tau, \frac{1}{n})$ a point of exact order n in E_τ.

For $\Gamma_0(n)$: Associate to τ a pair $(E_\tau, \langle \frac{1}{n} \rangle)$ a cyclic sgp of order n.

Using the previous calculation, we see that $(E_\tau, \frac{1}{n}) \simeq (E_{\tau'}, \frac{1}{n})$ if, and only if $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1(n)$.

Also, $(E_\tau, \langle \frac{1}{n} \rangle) \simeq (E_{\tau'}, \langle \frac{1}{n} \rangle) \iff \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(n)$.

In both cases, given a pair (E, data) either P or C (point of order n; cyclic of order n),

it is isomorphic $(E_\tau, \text{data}_\tau)$ (the problem of symplecticity doesn't appear here)

Conclusion:

$\Gamma_1(n) \backslash \mathcal{H}$ is the parameter space for pairs (E,P), $E/\mathbb{C}$ is a complex ell. curve and $P \in E(\mathbb{C})$ is a point of exact order n.

$\Gamma_0(n) \backslash \mathcal{H}$ is the parameter space for pairs (E,C), $E/\mathbb{C}$ is a complex ell. curve, and $C \subseteq E[n]$ is a cyclic sgp of order n.

Crash course on Hecke operators.

Fix $k \in \mathbb{Z}$. Let $\beta \in GL_2^+(\mathbb{Q})$, $f: \mathcal{H} \to \mathbb{C}$.

Define $(f|_k\beta)(\tau) := (\det \beta)^{k-1} j(\beta,\tau)^{-k} f(\beta\tau)$. $\quad \left(j(\beta,\tau) = c\tau + d \text{ if } \beta = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \right)$

Also, write $f|_k\beta = f[\beta]_k$ or $f[\beta]$.

This is a group action.

Let $\Gamma_1, \Gamma_2 \in SL_2(\mathbb{Z})$ be congruence subgroups $(\Gamma_i \supseteq \Gamma(n_i)$ for some $n_i \in \mathbb{Z})$.

Let $\alpha \in GL_2^+(\mathbb{Q})$.

The double coset $\Gamma_1 \alpha \Gamma_2 = \dot{\bigcup}_j \Gamma_1 \beta_j$ (finite union, b/c congruence sgps).

We define:

$$f[\Gamma_1 \alpha \Gamma_2]_k := \sum_j f[\beta_j]_k$$

Lemma (EZ): If $f \in M_k(\Gamma_1)$, then $f[\Gamma_1 \alpha \Gamma_2]_k$ is well-defined (it doesn't depend on the coset reps β_j).

and it is a modular form in $M_k(\Gamma_2)$.

If $f \in S_k(\Gamma_1)$, then $f[\Gamma_1 \alpha \Gamma_2]_k \in S_k(\Gamma_2)$.

Examples:

1) $\Gamma_1 \supset \Gamma_2$, $\alpha = Id$. Then $\Gamma_1 \alpha \Gamma_2 = \Gamma_1$, and $f[\Gamma_1 \alpha \Gamma_2] = f$.

This is viewing $f \in M_k(\Gamma_1)$ on a smaller group.

2) $\alpha^{-1}\Gamma_1 \alpha =: \Gamma_2$. Then $\Gamma_1 \alpha \Gamma_2 = \Gamma_1 \alpha$, so

$f[\Gamma_1 \alpha \Gamma_2] = f[\alpha]$.

In particular, if $\Gamma_1 \triangleleft \Gamma_0$, we get an action of Γ_0/Γ_1 on

$M_k(\Gamma_1)$, where $\bar{\alpha} \in \Gamma_0/\Gamma_1$ acts by $f[\alpha]$.

In particular, if $\Gamma_1 = \Gamma_1(N)$, $\Gamma_0 = \Gamma_0(N)$,

we get an action of $(\mathbb{Z}/N\mathbb{Z})^\times \simeq \Gamma_0(N)/\Gamma_1(N)$ on $M_k(\Gamma_1(N))$.

$$d \longleftarrow \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

fin. dim vectorspace

So we have a representation of $(\mathbb{Z}/N\mathbb{Z})^\times$ on $M_k(\Gamma_1(N))$

And hence we can decompose it:

$$M_k(\Gamma_1(N)) = \bigoplus_{\chi} M_k(\Gamma_1(N), \chi)$$

where the sum runs over all $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ characters.

Denote the action of $d \in (\mathbb{Z}/N\mathbb{Z})^\times$ by $\langle d \rangle$.

It's called the <u>diamond operator</u>:

$$f\langle d \rangle = f\begin{bmatrix} a & b \\ c & \tilde{d} \end{bmatrix}_k \quad \text{where} \quad \begin{pmatrix} a & b \\ c & \tilde{d} \end{pmatrix} \in \Gamma_0(N), \ d \equiv \tilde{d} \pmod N$$

We have then $f \in M_k(\Gamma_1(N), \chi) \Leftrightarrow f\langle d \rangle = \chi(d) \cdot f \ \ \forall d \in (\mathbb{Z}/N\mathbb{Z})^\times$.

Example: Let $\alpha = \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}$. The operator $\Gamma_1(N)\alpha\Gamma_1(N)$ is denoted T_p (the p^{th} Hecke operator).

$$f \cdot T_p = f\left[\Gamma_1(N)\begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}\Gamma_1(N)\right]_k.$$

Prop: $T_p f \; (= f \cdot T_p) = \begin{cases} \displaystyle\sum_{j=0}^{p-1} f\begin{bmatrix} 1 & j \\ 0 & p \end{bmatrix}_k & \text{if } p \mid N \\ \displaystyle\sum_{j=0}^{p-1} f\begin{bmatrix} 1 & j \\ 0 & p \end{bmatrix}_k + f\left[\underbrace{\begin{pmatrix} m & n \\ N & p \end{pmatrix}}_{\text{in } SL_2(\mathbb{Z}) \text{ (actually, in } \Gamma_0(N))}\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}\right]_k & p \nmid N \end{cases}$

Pf Requires work, but it's a matter of finding coset representatives. //

Prop: The action of the diamond and Hecke operators on q-expansions is as follows:

If $f \in M_k(\Gamma_1(N), \chi)$, $f = \sum a_n(f) q^n$.

$$a_n(f\langle d\rangle) = a_n(\chi(d) \cdot f) = \chi(d) \cdot a_n(f).$$

If $p \nmid N$,

$$a_n(T_p f) = a_{np}(f) + \chi(p)\, p^{k-1} \underbrace{a_{n/p}(f)}_{0 \text{ if } p \nmid n}$$

If $p \mid N$,

$$a_n(T_p f) = a_{np}(f)$$

Corollary: All the operators T_p (p a prime) and $\langle d \rangle$, $d \in (\mathbb{Z}/N\mathbb{Z})^\times$, commute with each other.

(just look at the q-expansions).

As all of them commute, one usually writes $T_p f$ or $\langle d \rangle f$ (on the left).

Proof (of Thm):

Just need to calculate from the expression of $f | T_p$:

$$f\left[\begin{smallmatrix}1 & j\\ 0 & p\end{smallmatrix}\right](\tau) = p^{k-1} p^{-k} f\left(\frac{\tau+j}{p}\right) = \frac{1}{p} f\left(\frac{\tau+j}{p}\right) = \frac{1}{p}\sum_{n=0}^{\infty} a_n(f)\, q^{\frac{n}{p}} \zeta^{jn}$$

(where $\zeta = e^{2\pi i/p}$)

The sum $\displaystyle\sum_{j=0}^{p-1} f\left[\begin{smallmatrix}1 & j\\ 0 & p\end{smallmatrix}\right] = \frac{1}{p}\sum_{n=0}^{\infty} a_n(f)\, q^{n/p} \sum_{j=0}^{p-1} (\zeta^n)^j$

If $p \nmid n$, $\zeta^n \neq 1$, and $\displaystyle\sum_{j=0}^{p-1}(\zeta^n)^j = 0$

If $p \mid n$, $\zeta^n = 1$, and $\displaystyle\sum_{j=0}^{p-1}(\zeta^n)^j = p$

Hence $\displaystyle\sum_{j=0}^{p-1} f\left[\begin{smallmatrix}1 & j\\ 0 & p\end{smallmatrix}\right] = \sum_{n=0}^{\infty} a_{np}(f)\, q^n$

This gives the formula for $p \mid N$. If $p \nmid N$, then need to add:

$$f\left[\begin{pmatrix}m & n\\ N & p\end{pmatrix}\begin{pmatrix}p & 0\\ 0 & 1\end{pmatrix}\right]_k = \left(f\left[\begin{smallmatrix}m & n\\ N & p\end{smallmatrix}\right]_k\right)\left[\begin{smallmatrix}p & 0\\ 0 & 1\end{smallmatrix}\right]_k = \left(\chi(p) f\right)\left[\begin{smallmatrix}p & 0\\ 0 & 1\end{smallmatrix}\right]_k$$

Now, $\displaystyle f\left[\begin{smallmatrix}p & 0\\ 0 & 1\end{smallmatrix}\right]_k(\tau) = p^{k-1} f(p\tau) = p^{k-1}\sum_{n=0}^{\infty} a_n(f)\, q^{np} = p^{k-1}\sum_{n\geq 0} a_{n/p}(f)\, p^n$

//

- Defining $\langle n \rangle$, T_n for all $n \geq 0$.

If $p \mid N$, define $\langle p \rangle = 0$.

If $n = \prod_i p_i^{a_i}$, define $\langle n \rangle = \prod_i \langle p_i \rangle^{a_i}$.

Let $T_1 =$ identity, and $T_{p^r} := T_p T_{p^{r-1}} - p^{k-1} \langle p \rangle T_{p^{r-2}}$ for $r \geq 2$.

Rk: if $p \mid N$, $T_{p^r} = (T_p)^r$.

Finally, define $T_n = \prod_i T_{p_i^{a_i}}$.

The operators $\{\langle n \rangle : n \geq 0\}$, $\{T_n : n \geq 0\}$ all commute.

One has the following identity (formally).

$$\sum_{n=1}^{\infty} T_n n^{-s} = \prod_p \left(1 - T_p p^{-s} + \langle p \rangle p^{k-1-2s}\right)^{-1}.$$

- The Petersson inner product.

Let $\Gamma \leq SL_2(\mathbb{Z})$ be a congruence subgroup (actually only need finite index).

Let D_Γ be its fundamental domain.

Define μ be the hyperbolic measure on $\mathcal{H}$, $d\mu(\tau) = \frac{dx\,dy}{y^2}$ if $\tau = x + iy$.

Rk: μ is $SL_2(\mathbb{R})$-invariant.

If $f, g \in S_k(\Gamma)$, let $\langle f, g \rangle_\Gamma := \frac{1}{\mathrm{vol}(D_\Gamma)} \int_{D_\Gamma} f(\tau) \overline{g(\tau)} \, \mathrm{Im}(\tau)^k \, d\mu(\tau)$

Rk: The factor $\frac{1}{vol(D_\Gamma)}$ is added so that if $f, g \in S_k(\Gamma')$, $\Gamma' \supset \Gamma$,

then $\langle f, g \rangle_{\Gamma'} = \langle f, g \rangle_\Gamma$.

Also, $vol(D_\Gamma) = [PSL_2(\mathbb{Z}) : \bar{\Gamma}] \cdot vol(D_{SL_2(\mathbb{Z})}) = [PSL_2(\mathbb{Z}) : \bar{\Gamma}] \cdot \pi/3$

Prop: $\langle \cdot, \cdot \rangle$ is an inner product on $S_k(\Gamma)$.

Pf/ Hermitian is clear, and linear + conj-linear is clear, too.

Positive-definite is also clear.

The only difficulty is showing that it is well-defined.

(use that f, g are cusp forms) //

Rk: one can take $\langle f g \rangle$ as long as one of them is a cusp form.

Theorem (Requires substantial work) (see Diamond & Shurman): The adjoint of the operators $\langle p \rangle$, T_p,

for $p \nmid N$ is:

$$\langle p \rangle^* = \langle p \rangle^{-1}$$

$$T_p^* = \langle p \rangle^{-1} T_p$$

In particular, $\langle p \rangle$ and T_p are normal operators (commute with their adjoint).

Corollary: On mod. forms for $\Gamma_0(N)$ $\left(= M_k(\Gamma_1(N), \mathbb{1})\right)^{\text{char}}$ ← trivial char:

T_p is self-adjoint.

<u>Corollary</u>: $S_k(\Gamma_1(N))$ has an orthonormal basis of simultaneous eigenforms for all $\langle p\rangle$, T_p. $(p \nmid N)$.

• <u>Old forms (and New forms)</u>

Let $d \mid N$. Then we have two maps $S_k(\Gamma_1(N/d)) \xrightarrow{\alpha_d} S_k(\Gamma_1(N))$

$$f(\tau) \longmapsto f(\tau)$$

and $S_k(\Gamma_1(N/d)) \xrightarrow{\beta_d} S_k(\Gamma_1(N))$

$$f(\tau) \longmapsto f(d\tau)$$

The space $S_k(\Gamma_1(N))^{old} := \sum_{1 \neq d \mid N} \left(\mathrm{Im}(\alpha_d) + \mathrm{Im}(\beta_d) \right)$ ← Subspace of $S_k(\Gamma_1(N))$ generated by this

We define also $S_k(\Gamma_1(N))^{new} := \left(S_k(\Gamma_1(N))^{old} \right)^{\perp}$ ← using the Petersson inner prod.

It's an easy check that:

$S_k(\Gamma_1(N))^{old}$ is preserved by all Hecke and diamond operators.

Hence, ~~So~~ is $S_k(\Gamma_1(N))^{new}$ (check it)

<u>Corollary</u>: $S_k(\Gamma_1(N))^{new}$ admits an orthonormal basis of eigenforms for all $\langle p\rangle$, T_p, $p \nmid N$.

<u>Theorem</u> (requires a lot of work): If $f \in S_k(\Gamma_1(N))^{new}$ is an eigenform for $\langle n\rangle$, T_n, $(n,N)=1$, then f is also an eigenform for all $\{\langle n\rangle, T_n\}$.

Furthermore, $a_1(f) \neq 0$. If $a_1(f) = 1$, (normalization), then f is called a <u>newform</u>.

Rk: a newform f is an element of $S_k(\Gamma_1(N))^{new}$ such that it is a normalized eigenform ~~st.~~ for all $\{\langle n\rangle, T_n\}$.

Thm': The set of newforms is an orthonormal basis for $S_k(\Gamma_1(N))^{new}$. Each newform lies in some eigenspace $S_k(\Gamma_1(N), \chi)$, and satisfies: $a_n(f)\cdot f = T_n f$.

Let $L(f,s) := \sum_{n=1}^{\infty} a_n(f) n^{-s}$. Then each newform has an Euler product expansion (if $f \in S_k(\Gamma_1(N), \chi)$)

$$L(f,s) = \prod_p \left(1 - a_p(f)p^{-s} + \chi(p)p^{k-1-2s}\right)^{-1}$$

There exists an interpretation for Hecke and diamond operators via a parameter-space picture.

Given $f \in S_k(\Gamma_1(N), \chi)$ a newform let $K(f)$ be the field obtained from ~~the~~ adjoining all the Fourier coeffs: $K(f) = \mathbb{Q}(a_1(f), a_2(f), a_3(f), \dots)$ ($a_1 = 1$)

It is known that $K(f)$ is a number field.

Let λ be a prime ideal of $K(f)$. (i.e of $\mathcal{O}_{K(f)}$).

Thm (Deligne): Assume $k \geq 2$. There is an irreducible representation of $G_{\mathbb{Q}} = Gal(\bar{\mathbb{Q}}/\mathbb{Q})$:

$$\rho = \rho_{f,\lambda} : G_{\mathbb{Q}} \to GL_2(K(f)_\lambda)$$

if $\lambda | \ell$, then $K(f)_\lambda$ is a finite ext of $\mathbb{Q}_\ell$.

(thm continues)

The representation ρ is unramified at all primes $p \nmid \ell N$.

For any $p \nmid \ell N$, the characteristic polynomial of

$$\rho(\mathrm{Frob}_p) \quad \text{is} \quad X^2 - a_p(f)X + \chi(p)\,p^{k-1}$$

This representation is <u>odd</u> $\left(\rho(\text{cx conj}) \text{ has } \det = -1\right)$

In particular, for $k=2$, $f \in \Gamma_0(N)$ (AP

the matrix of $\rho(\mathrm{Frob}_p)$ has trace $a_p(f)$ and determinant p.