Lecture 1

3/3/18

Modular Forms

used to -

* Study diophantine equations
* Quadratic Forms
* Models for mechanical systems which display "chaos"

Quadratic Form - $Q(x_1, \dots, x_d) = \sum_{i \le j} a_{ij} x_i x_j$ $\quad a_{ij} \in \mathbb{Z}$ $\quad$ (e.g. $Q(x_1, \dots, x_d) = x_1^2 + \dots + x_d^2$)

Which integers are represented by Q, that is, $n \stackrel{?}{=} Q(x_1, \dots, x_d)$ for $x = (x_1, \dots, x_d) \in \mathbb{Z}^d$.

$n = x^2 + y^2$?

$n = x^2 + y^2 + z^2$? $\quad r_Q(n) = \#\{x \in \mathbb{Z}^d \mid Q(x) = n\}$

$n = x^2 + y^2 + z^2 + w^2$?

Thm: (Fermat)

p prime, $p = x^2 + y^2 \iff p = 2$, $p \equiv 1 \bmod 4$

$n \ge 0$ integer, $n = x^2 + y^2 \iff$ factor $n = 2^a \cdot \prod_{p_i \equiv 1 (4)} p_i^{a_i} \cdot \prod_{q_j \equiv 3 (4)} q_j^{b_j}$, b_j - even

(Taught in basic NT course)

Moreover, when $Q = x^2 + y^2$, $r_Q(p) = \begin{cases} 4, & p = 2 \\ 0, & p \equiv 3 (4) \\ 8, & p \equiv 1 (4) \end{cases}$

$2 = (\pm 1)^2 + (\pm 1)^2$

$5 = (\pm 2)^2 + (\pm 1)^2$
$\quad\; = (\pm 1)^2 + (\pm 2)^2$

To study $r_Q(n)$, use a θ-function $\theta_Q(\tau) = \sum_{\vec{m} \in \mathbb{Z}^d} e^{\pi i \tau Q(\vec{m})} =$

$$= \sum_n r_Q(n) e^{2\pi i n \tau}$$

We have -

1) $\theta(\tau + 1) = \theta(\tau)$ $\quad$ (Trivial)

Will have extra symmetries.

Example: $Q(x) = x^2$, $\Theta_1(\tau) = \sum_{n=-\infty}^{\infty} e^{2\pi i n^2 \cdot \tau}$, $Im(\tau) > 0$, $\tau = x+iy$

$\tau \mapsto -1/\tau$ gives:

$$\Theta_1(-1/\tau) = \sum_{n=-\infty}^{\infty} e^{\frac{1}{\pi i} 2\pi i n^2 x} e^{-2\pi n^2 \cdot y/|\tau|}$$

is analytic in $\mathbb{H} = \{\tau = x+iy \mid y>0\}$ → space of lattices

$$\Theta(-1/\tau) = \sqrt{\tau}\,\Theta(\tau)$$

Example: $\Theta_2(\tau) = \sum_{(x,y)\in\mathbb{Z}^2} e^{2\pi i \tau (x^2+y^2)} = \Theta_1(\tau)^2$

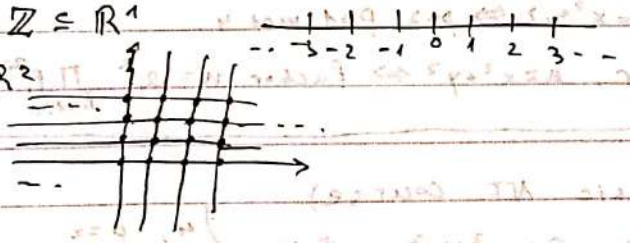
In some cases, the constraints of symmetry will give us uniqueness; and so if by other methods we can construct a function with these properties, we get it, in a way which is easier to calculate its coefficients.

The space of Lattices

Def: A *Lattice* in $\mathbb{R}^d$ is a discrete subgroup $L \subseteq \mathbb{R}^d$ which spans $\mathbb{R}^d$.

Example: 1) $L = \mathbb{Z} \subseteq \mathbb{R}^1$

2) $L = \mathbb{Z}^2 \subseteq \mathbb{R}^2$



Def: A discrete set $S \subseteq \mathbb{R}^d$ is a set without accumulation points, or a set in which every point is isolated:

$$\forall s \in S.\ \exists \varepsilon(s) > 0.\ |s'-s| \geq \varepsilon(s),\ \forall s' \neq s$$

Comments: Because L is a subgroup we can take $\varepsilon(l) = \varepsilon_0 > 0$ independent of l.

$\varepsilon_0 = \inf \{|0-l'| \mid 0 \neq l' \in L\}$ = length of a shortest non zero vector.

Note that $\{(n,0) \mid n \in \mathbb{Z}\} \subseteq \mathbb{R}^2$ is a discrete subgroup of $\mathbb{R}^2$ but doesn't span $\mathbb{R}^2$, so it's not a lattice.

Thm: Every lattice has a basis $L \subseteq \mathbb{R}^d$, so, $\exists w_1, \dots, w_d \in \mathbb{R}^d$ linearly independent and span $\mathbb{R}^d$, and $L = \mathbb{Z}w_1 + \dots + \mathbb{Z}w_d$.

(Why, if we have this result, to take the abstract definition? Just because the abstract way is the way we encounter lattices "in nature" - say an elliptic function is a function with 2 linearly ind. periods; then the space of periods turns out to be a lattice)

Comment: Every subset of L has a shortest, non zero, vector. → o/w since $0 \in L$, we have that 0 is an accumulation point

Proof of the thm: (Only for $d \leq 2$ - higher d is a exercise)

$d=1$ - Want $L \subseteq \mathbb{R}^1 \Rightarrow L = \mathbb{Z}w_1$, $w_1 \neq 0$

Take $0 \neq w_1$ a shortest vector. If need replace $w_1 \to -w_1$ to have $w_1 > 0$. Want $L = \mathbb{Z}w_1$. O/w, $\mathbb{Z}w_1 \subsetneq L$. Assume $\exists l \in L - \mathbb{Z}w_1$.

So, $\exists n \in \mathbb{Z}$ s.t $nw_1 < l < (n+1)w_1$

$\Rightarrow 0 < l - nw_1 < w_1$, $l - nw_1 \in L$

contradicting the minimality of w_1.

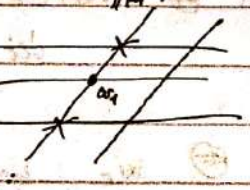
$d=2$ Will show $L = \mathbb{Z}w_1 + \mathbb{Z}w_2$, where w_1 is a shortest non zero vector, w_2 is a shortest vector linearly ind. of w_1.

Claim: This choice of w_1, w_2 gives $L = \mathbb{Z}w_1 + \mathbb{Z}w_2$.

clearly, "$\supseteq$" holds. Look at $L \cap \mathbb{R}w_1 \subseteq \mathbb{R}w_1$, a one-dim Lattice. (Obviously a subgroup, and discrete)

By dim 1 case, $L \cap \mathbb{R}w_1 = \mathbb{Z}w_1$. Want $L = \mathbb{Z}w_1 + \mathbb{Z}w_2$.

Assume $l \in L$. Write $l = x_1w_1 + x_2w_2$, $x_i \in \mathbb{R}$.



Firstly note $n_2 x_2 \in \mathbb{Z} \Rightarrow x_2 \in \mathbb{Z}$, since then, $l - n_2w_2 \in L \cap \mathbb{R}w_1$, so $l - n_2w_2 \in \mathbb{Z}w_2$, and $x_1 \in \mathbb{Z}$ as well.

Likewise, $L \cap \mathbb{R}w_2 = \mathbb{Z}w_2$ so we'll get $x_1 \in \mathbb{Z} \Rightarrow x_2 \in \mathbb{Z}$. So we can assume $x_1, x_2 \notin \mathbb{Z}$.

Choose integers $n_1, n_2 \in \mathbb{Z}$ s.t $0 < |x_1 - n_1| \leq 1/2$
$0 < |x_2 - n_2| \leq 1/2$

Look at: $l' = l - (n_1 w_1 + n_2 w_2) \in L$
$= (x_1 - n_1)w_1 + (x_2 - n_2)w_2$

First attempt: I want to show $|l'| < |w_2|$ and is lin. ind. of w_1 => contradiction.

$$|l'| \overset{\otimes}{\leq} |x_1 - n_1||w_1| + |x_2 - n_2||w_2| \leq \tfrac{1}{2}|w_1| + \tfrac{1}{2}|w_2| \leq$$
$$\downarrow |w_1| \leq |w_2|$$
$$\leq |w_2| \text{ - fails...}$$

We can fix - in $\otimes$ there's a strict inequality since (as $x_1 - n_1, x_2 - n_2 \neq 0, 0$) we have lin. ind.

General argument - the same idea. □

Changes of Basis

Say $L = \mathbb{Z}w_1 + \mathbb{Z}w_2 = \mathbb{Z}w_1' + \mathbb{Z}w_2'$

we have - $w_1' = aw_1 + bw_2$
$w_2' = cw_1 + dw_2$ $\quad a,b,c,d \in \mathbb{Z}$
$w_1 = a'w_1 + b'w_2'$ $\quad a',b',c',d' \in \mathbb{Z}$
$w_2 = c'w_1 + d'w_2'$

Here, $\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$ are integral with integral matrices

So are in $GL_2(\mathbb{Z})$.

Lemma: Let $A \in Mat_2(\mathbb{Z})$. Then $A^{-1} \in Mat_2(\mathbb{Z}) \Leftrightarrow \det A$ is an invertible integer $\Leftrightarrow \det A = \pm 1$.

Proof: $\Rightarrow$ Write $A \cdot B = I$, $A, B \in Mat_2(\mathbb{Z})$, then
$\det(A) \cdot \det(B) = 1$, and $\det(A), \det(B) \in \mathbb{Z}$ since A, B has entries in $\mathbb{Z}$

$\Leftarrow$ We have (Kramer's thm) -

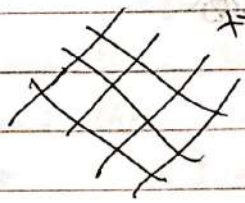
$$A^{-1} = \frac{1}{\det A}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

□

The space of 2-dim lattices

Homothety Classes: If $\lambda \in \mathbb{C}^\times$, $L \subseteq \mathbb{R}^2 = \mathbb{C}$ a lattice, we can get another lattice, $\lambda L \subseteq \mathbb{C}$.

$\mathbb{Z}^2, (2\mathbb{Z})^2$



$\lambda = \rho e^{i\pi/4}$, $\lambda\mathbb{Z}^2$

Def: $L, \lambda L$ are Homothetic.

Let $\mathcal{R} = \{$all latices in $\mathbb{C}\}$

$\mathcal{R}/\mathbb{C}^\times = \{$Homothety classes$\}$

Goal: Geometric picture of $\mathcal{R}/\mathbb{C}^\times$ –

→ non zero since are linearly ind.

Let $\mathcal{M} = \{(\omega_1, \omega_2) \in \mathbb{C}^2 \mid \mathrm{Im}(\omega_1/\omega_2) > 0\}$.

We have a map, surjective,

$$\mathcal{M} \twoheadrightarrow \mathcal{R}$$

$$(\omega_1, \omega_2) \mapsto L(\omega) = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 \qquad (\tau = x+iy)$$

(Surjective – $L = \mathbb{Z}\omega + \mathbb{Z}\omega' = \mathbb{Z}\omega' + \mathbb{Z}\omega$, $\tau = \omega/\omega' \notin \mathbb{R}$; $\mathrm{Im}(\omega'/\omega) = \mathrm{Im}(1/\tau)$,

So if is <0, we can switch – $\tau \cdot \bar{\tau} = |\tau|^2 > 0$, $\frac{1}{\tau} = \frac{\bar{\tau}}{|\tau|^2}$, $\mathrm{Im}(\frac{1}{\tau}) = -\frac{\gamma}{|\tau|^2}$)

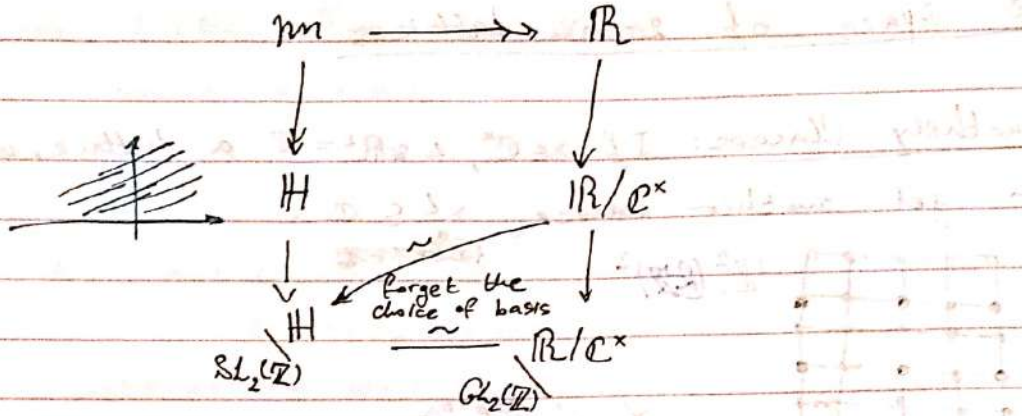
Note that by switching $(\omega_1, \omega_2) \rightsquigarrow (\lambda\omega_1, \lambda\omega_2)$ we get

$\mathrm{Im}(\omega_1/\omega_2) = \mathrm{Im}(\lambda\omega_1/\lambda\omega_2)$.

So we have a map,

$$\mathcal{M} \longrightarrow \mathbb{H} = \{\tau = x+iy,\ y>0\}$$

$$(\omega_1, \omega_2) \mapsto \tau = \omega_1/\omega_2$$



The claim is -

(1) Onto

(2) Homothety invariance

(3) Determinant = +1.

(3) - $w_1' = aw_1 + bw_2$

$w_2' = cw_1 + dw_2$

$\mathrm{Im}(w_1'/w_2') = \frac{ad-bc}{|c\frac{w_1}{w_2}+d|^2} \cdot \mathrm{Im}(\frac{w_1}{w_2})$ (So need $ad-bc > 0$ for $\mathrm{Im}(w_1'/w_2') > 0$)

Conclusion:

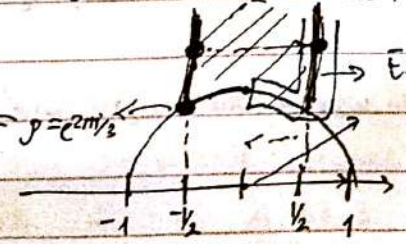
Homothety classes of lattices $\longleftrightarrow$ $SL_2(\mathbb{Z})\backslash\mathbb{H}$

$\mathbb{R}/\mathbb{C}^\times$

$\tau \sim \frac{a\tau+b}{c\tau+d}$, $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$

Define -

$\mathcal{F} = \{ \tau \in \mathbb{H}, |\tau| \geq 1$
$-1/2 \leq \mathrm{Re}(\tau) < 1/2$, if $|\tau| = 1$ then $\mathrm{Re}(\tau) \leq 0 \}$



Excluding these from the boundary

Thm:

a) $\forall \tau \in \mathbb{H}$, $\exists g \in SL_2(\mathbb{Z}) = \Gamma$ s.t. $g(\tau) \in \overline{F}$

b) If $\tau \neq \tau' \in \overline{F}$ are equivalent by Γ, then they lie on the boundary, and either $\mathrm{Re}(\tau) = -1/2$, $\tau' = \tau + 1 = \frac{1\cdot\tau+1}{0\cdot\tau+1}$ or $|\tau| = 1$, and $\tau' = -1/\tau$, $= \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}(\tau)$

c) Let $I(\tau) = \{g \in \Gamma \mid g\tau = \tau\}$. Then, $I(\tau) = \{\pm 1\}$ unless τ is Γ-equivalent to

a) i, and then $I(\tau) = \{\pm I, \pm S\}$, $S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$

b) ρ, and then $I(\tau) = \{\pm I, \pm S, \pm (ST)^2\}$, $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$

or ρ^2, $I(\tau) = \{\pm I, \pm TS, \pm (TS)^2\}$

d) $SL_2(\mathbb{Z}) = \langle S, T \rangle$

Proof: (only of (a), (b))

(a) - Take $\tau \in \mathbb{H}$, let $\Gamma' = \langle S, T \rangle \subseteq SL_2(\mathbb{Z})$. Want - $\exists g \in \Gamma'$, s.t. $g\tau \in F$. Look at the set $\{c\tau + d \mid \begin{pmatrix} * & * \\ c & d \end{pmatrix} \in \Gamma'\} \subseteq \mathbb{Z}\tau + \mathbb{Z}\cdot 1 = L$

It has a shortest vector, $c_0\tau + d_0$, $g = \begin{pmatrix} * & * \\ c_0 & d_0 \end{pmatrix} \in \Gamma'$.

$\Leftrightarrow \mathrm{Im}(g_0\tau)$ is maximal among $\{\mathrm{Im}(g\tau) \mid g \in \Gamma'\}$

$\mathrm{Im}(g_0\tau) = \frac{\mathrm{Im}(\tau)}{|c_0\tau + d|^2}$, $\mathrm{Im}(g\tau) = \frac{\mathrm{Im}(\tau)}{|c\tau + d|^2}$

Claim: $|g_0\tau| \geq 1$. $\left(S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\right)$

O/w look at $(S \cdot g_0) \cdot \tau = \frac{-1}{g_0\tau}$ (Γ'). $\mathrm{Im}(Sg_0\tau) = \frac{\mathrm{Im}(g_0\tau)}{|g_0\tau|^2} > \mathrm{Im}(g_0\tau)$ - contradiction.

Next, Find $n \in \mathbb{Z}$ s.t. $-1/2 \leq \mathrm{Re}(g_0\tau) - n < 1/2$. So replace $g_0\tau$ by $T^{-n}g_0\tau$. $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} : \tau \mapsto \tau + 1$

with: 1) $-\frac{1}{2} \leq \mathrm{Re}(\tau') < \frac{1}{2}$

2) $\mathrm{Im}(\tau') = \mathrm{Im}(g_0\tau) \Rightarrow$ is still maximal! and so, τ' is outside of the unit circle.

Thus $\tau' \in \Gamma'\tau$, lies in $\overline{F}$.

(d) - $\Gamma' = \langle S, T \rangle = \Gamma = SL_2(\mathbb{Z})$.

$S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$

Example - $A = \begin{pmatrix} 4 & 9 \\ 3 & 7 \end{pmatrix} \in SL_2(\mathbb{Z})$

Note, $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \Rightarrow S \cdot A = \begin{pmatrix} -1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} c & d \\ -a & -b \end{pmatrix}$.

$T^4 A = \begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a+4c & b+4d \\ c & d \end{pmatrix}$

$A = \begin{pmatrix} 4 & 9 \\ 3 & 7 \end{pmatrix} \mapsto T^{-1}A = \begin{pmatrix} 1 & 2 \\ 3 & 7 \end{pmatrix} \to ST^{-1}A = \begin{pmatrix} 3 & 7 \\ -1 & -2 \end{pmatrix} \mapsto$

$T^3 S T^{-1} A = \begin{pmatrix} 0 & 1 \\ -1 & -2 \end{pmatrix}$

$ST^3ST^{-1}A = \begin{pmatrix} -1 & -2 \\ 0 & -1 \end{pmatrix} = -T^2 = S^2T^2$

$\Rightarrow A \in \langle S, T \rangle$

This is the euclidean algorithm - clearly it works, and $SL_2(\mathbb{Z}) = \langle S, T \rangle$.

Next time - using this fundamental domain discuss quadratic forms, moving the form to the fundamental domain.