31/3/19

הרצאה 5

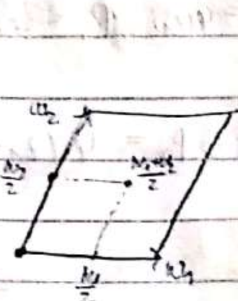
"חצאי מחזורים"

$L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$

$G_k(L) = \sum_{\omega \in L} \frac{1}{\omega^k}, \quad k \geq 3$

$g_2(L) = 60\, G_4(L)$

$g_3(L) = 140\, G_6(L)$



נסמן $\omega_3 := \omega_1 + \omega_2$.

חצאי מחזורים := נקודה $z \in \mathbb{C}/L$ כך ש- $2z \equiv 0 \pmod L$ וגם $z \not\equiv 0 \pmod L$. שימו לב: הם יכולים להיות $\frac{\omega_1}{2}, \frac{\omega_2}{2}, \frac{\omega_3}{2}$.

נגדיר $e_j = \wp(\omega_j/2)$.

טענה: e_1, e_2, e_3 שונים [illegible].

(הוכחה בהמשך)

מוטיבציה: המשוואה הדיפרנציאלית שהוכחנו בשיעור שעבר,

$$(\wp')^2 = 4\wp^3 - g_2\wp - g_3$$

הראנו ש- $\wp'$ אי-זוגית, ונובע ש- $\wp'(\frac{\omega_j}{2}) = 0$. (ראינו בשיעור שעבר)

מכאן, e_1, e_2, e_3 הם שורשים של הפולינום $4x^3 - g_2x - g_3$. אם נדע שהשורשים האלו שונים, נקבל 3 שורשים שונים של הפולינום, ולכן –

$$4x^3 - g_2x - g_3 = 4(x-e_1)(x-e_2)(x-e_3)$$

אז נגדיר את הדיסקרימיננטה המודולרית:

$$\Delta(L) = \prod_{1 \leq i < j \leq 3} (e_i - e_j)^2 = \frac{1}{4^2} \cdot \mathrm{disc}(4x^3 - g_2x - g_3)$$

? אין צורך בהגדרה

הגדרה: בהינתן פולינום $f(x) = a_dx^d + \dots + a_1x + a_0$, $a_d \neq 0$, ניתן לכתוב $f(x) = a_d \prod_{j=1}^{d} (x - e_j)$ כאשר $\{e_j\}$ שורשי הפולינום. נגדיר –

$$\mathrm{disc}(f) := a_d^{2(d-1)} \prod_{1 \leq i < j \leq d} (e_i - e_j)^2$$

בפרט,

$\mathrm{disc} f \neq 0 \iff$ השורשים שונים

משפט: $\mathrm{disc}(f)$ פולינום במקדמים $a_d, \dots, a_0$.

נסמן –

$$V = \begin{pmatrix} 1 & \cdots & 1 \\ e_1 & \cdots & e_d \\ \vdots & & \vdots \\ e_1^{d-1} & \cdots & e_d^{d-1} \end{pmatrix}$$

– מטריצת ונדרמונדה.

הדטרמיננטה שלה היא –

$$\det V = \prod_{j > i} (e_j - e_i)$$

וכן,

$$\det VV^T = \prod_{j > i} (e_j - e_i)^2$$

אצלנו במקרה $n=3$,

$$V\cdot V^T=\begin{pmatrix}1&1&1\\e_1&e_2&e_3\\e_1^2&e_2^2&e_3^2\end{pmatrix}\begin{pmatrix}1&e_1&e_1^2\\1&e_2&e_2^2\\1&e_3&e_3^2\end{pmatrix}=\begin{pmatrix}\overset{3}{\cancel{1}}&\sum e_j&\sum e_j^2\\\sum e_j&\sum e_j^2&\sum e_j^3\\\sum e_j^2&\sum e_j^3&\sum e_j^4\end{pmatrix}=$$

$$=\begin{pmatrix}3&s_1&s_2\\s_1&s_2&s_3\\s_2&s_3&s_4\end{pmatrix}\qquad s_k=\sum e_j^k$$

כלומר עכשיו נשאר רק לחשב את s_k במונחי של הפולינומים הסימטריים המתאימים בשרשרת! למשל, אם c_i הפולינום הסימטרי האלמנטרי ה-i, אז

$$s_1^2=s_2+2c_2,\ s_1=c_1$$

בדרך זו מקבלים: ולכן,

$$4x^3-g_2x-g_3=4\left(x^3-\frac{g_2}{4}x-\frac{g_3}{4}\right)\Rightarrow disc(4x^3-g_2x-g_3)=4^2disc\left(x^3-\frac{g_2}{4}x-\frac{g_3}{4}\right)=$$
$$=4^2\left(4\left(\frac{g_2}{4}\right)^3-27\left(\frac{g_3}{4}\right)^2\right)$$

כי $disc(x^3-px-q)=4p^3-27q^2$. לכן,

$$\Delta(L)=g_2^3-27g_3^2$$

דוגמאות לפונקציות על מרחב הסריגים -

Δ "תבנית חוד" spitzenform || cusp form

G_k "תבנית מודולרית" $G_k(\lambda L)=\lambda^{-k}G_k(L)$

טענה: $e_i=\wp(\frac{\omega_i}{2})$ שונים זה מזה $\Leftrightarrow \Delta(L)\neq 0$

הוכחה: נזכור ש-$\wp$ מסדר 2 - מקבל כל ערך ב-$\bar{\mathbb{C}}$, כולל ∞, בדיוק פעמיים (עם ריבוי).

כמו כן, $\wp'$ - פונקציה אי-זוגית - $f(z)=\wp(z)-e_1=\wp(z)-\wp(\frac{\omega_1}{2})$ היא אליפטית, מסדר 2. שמתאפסת ב-$z=\frac{\omega_1}{2}$, $\wp'(\frac{\omega_1}{2})=0$ אז זה אפס כפול.

ולכן אין לה עוד אפסים. בפרט, $\wp(\frac{\omega_2}{2})\neq\wp(\frac{\omega_1}{2})$ ובדומה לאחרים.

המשוואה -

$$(\wp')^2=4\wp^3-g_2\wp-g_3$$

מאפשרת להגדיר העתקה: $\varphi:\mathbb{C}/L\to E_L$ כאשר -

$$E_L=\{(x,y)\in\mathbb{C}^2\mid y^2-4x^3+g_2x+g_3=0\}$$

ע״י -

$$z \longmapsto (\wp(z), \wp'(z))$$

כאשר $\varphi(0)=\infty$.

משפט: φ היא 1-1 ועל.

לכן, ניתן בעזרת φ להעביר את חוק החבורה על $\mathbb{C}/L$ אל E_L, ע״י -

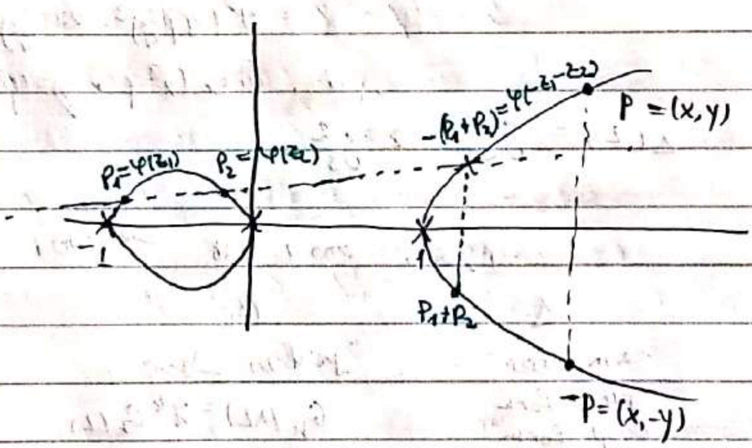
$$P_1, P_2 \in E_L, \quad P_1 \oplus P_2 := \varphi(z_1) \oplus \varphi(z_2) =: \varphi(z_1+z_2)$$

האיבר הניטרלי הוא $\varphi(0)=\infty$.

צ״ל: נניח ש- $\infty \neq \varphi(z)=(x,y) \Leftarrow$ $-\varphi(z) \overset{?}{=} (x,-y)$

$$\varphi(-z) = (\wp(z), \wp'(-z)) = (\wp(z), -\wp'(z)) = (x,-y)$$

למשל, עבור נקח את העקום $y^2 = 4(x^3-x)$.



הערה: מסדר 2, $2P_1=(0)$, כמו $-1,0,1$.

משפט: אם $z_1,z_2\neq 0 \pmod L$, $z_1 \neq \pm z_2 \pmod L$, אז $\varphi(z_1)$, $\varphi(z_2)$ ו- $\varphi(-(z_1+z_2))$ נמצאים על ישר אחד.

טענת עזר: אם f פונקציה אליפטית, z_j - האפסים השונים מודולו L (עם ריבוי), p_i - הקטבים (עם ריבוי). אזי,

$$\sum p_i - \sum z_j \in L$$

(**הוכחה:** $\sum z_i - \sum p_j = \frac{1}{2\pi i}\oint z\frac{f'}{f}$)

הוכחת **המשפט:** $z_1 \neq \pm z_2 \pmod L$, $z_i \notin L$ $\Leftarrow$ נסמן $P_1=\varphi(z_1)$, $P_2=\varphi(z_2)$ עבור
יש ישר אחד, מהצורה $y=Ax+B$:

כי $P_1=(x_1,y_1)$, $P_2=(x_2,y_2)$, מתכונות הנקודה נסתכל בפונקציה האליפטית:

$$f(z)=\wp'(z)-A\wp(z)-B$$

כן הפונקציה אליפטית עם קוטב מסדר 3 נקודות (אפסים), כאשר כך $z=0$-ב מודולו L.

לכן, $\gamma(f)=3$, ולכן לכל $a\in\mathbb{C}$ שיש 3 פתרונות בפרט יש 3 אפסים $f(z)$ - $z=z_1,z_2$ (נתונים) וכן z_3. נראה כי $z_3=-z_1-z_2$. ע"פ משפט הסכום,

$$z_1+z_2+z_3=(0+0+0)\in L$$

$$\Rightarrow z_1+z_2=-z_3 \pmod L$$

□

הכפלה ב-2:

סעיף: $P+P=2P$ היא הנקודה הנגדית של חיתוך המשיק ל-E ב-P עם העקומה.

נוסחאות מפורשות לחוק החיבור

כדי מה שהוכחנו - ברור שיש וכן יוצא:

$$P_1=(x_1,y_1),\quad P_2=(x_2,y_2)$$

$$P_1\oplus P_2=(x_3,-y_3)$$

מכאן: ברור מהגאומטריה

$$-y_3=y_1+\frac{y_1-y_2}{x_1-x_2}(x_3-x_1)$$

$$x_3=-x_1-x_2+\frac{1}{4}\left(\frac{y_1-y_2}{x_1-x_2}\right)^2$$

מהנ"ל: יהיו $P_1=(x_1,y_1)$, $P_2=(x_2,y_2)$, $P_1\oplus P_2=(x_3,-y_3)$ - נקודות על העקום $y^2=4x^3-g_2x-g_3$ בישר $y=Ax+B$.

$$(Ax+B)^2=4x^3-g_2x-g_3$$

$$A^2x^2+2ABx+B^2$$

נקבל משוואה ממעלה 3,

$$4(x-x_1)(x-x_2)(x-x_3)=4x^3-A^2x^2-(g_2+2AB)x-(g_3+B^2)=0$$

ע"פ נוסחאות וייטה -

$$\frac{A^2}{4}=x_1+x_2+x_3$$

הכפלה ב-2: אם $(x_3,-y_3)=2P\neq P=(x_1,y_1)$

$$x_3=-2x_1+\frac{1}{4}\left(\frac{f'(x_1)}{2y_1}\right)^2 \qquad (y^2=f(x)=4x^3-g_2x-g_3)$$

$$y_3=y_1+\frac{f'(x_1)}{2y_1}(x_3-x_1)$$

הערה: $2(x_1,0)=\infty=(0)$

מסקנה: אם $K \subseteq \mathbb{C}$ תת שדה, למשל $K=\mathbb{Q}$, כך ש- $g_2, g_3 \in K$ ואם $\Delta \neq 0$ אז

$$E(K) = \{(x,y) \in K^2 \mid y^2 = 4x^3 - g_2 x - g_3\}$$

$\cup\{\infty\}$ סגור תחת הפעולה - הנו תת-חבורה.

משפט: (Mordell - 1922) - החבורה של הנקודות הרציונליות $E(\mathbb{Q})$ נוצרת סופית.

הכללה: (A. Weil, 1928) כנ"ל עבור K - שדה מספרים כלשהו.

דוגמה - Bachet (1621)

פתרון של משוואה $c \in \mathbb{Z}$ נתון, $y^2 - x^3 = c$, $x,y \in \mathbb{Q}$.

למשל $c=-2$. פתרון נתון -

$y^2 - x^3 = -2$ הפתרון הוא למשל - $x=3, y=5$

ע"י זה נקבל, עם חוק החיבור של העקום האליפטי הנ"ל,

$$\left(y/2 = Y,\ y^2 = 4x^3 - 4c,\ X = x \right)$$

$$2P_1 = P_2 \Rightarrow X_2 = \frac{129}{100},\ Y_2 = -\frac{383}{1000}$$

$$2P_2 = P_4 \Rightarrow X_4 = \frac{2340922881}{7660^2},\ Y_4 = (\dots)$$

בעיה לפתרון - מהו המספר שמסמן מהו הגודל? באופן כללי, מה יש סביב שלמים, האם הם ... בעיה לא פתורה. לא ניתן לתת אלגוריתם באופן כללי.

תרגיל: למצוא 3 פתרונות רציונליים, (x,y), $y \neq 0$, למשוואה $y^2 - x^3 = -1$.

"אומרים" ש- $E(\mathbb{Q})$ נ"ס אם E "מוגדר מעל $\mathbb{Q}$".

$$\Leftarrow E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus F$$

F סופי - קל לחשב

$r = r(E)$ - ה"דרגה" של העקום E - מסתורי

השערת Birch, Swinnerton-Dyer

שאלה פתוחה: האם E יכול להיות בעל r גדול כרצוננו?

דוגמאות לעקום: מדרגה אפס - פרמה, $x^3+y^3=1$.

מדרגה אחד - $x^3+y^2=24$.

שאלה פתוחה - האם $r(E)$ לא חסום?

תבניות מודולריות

הגדרה: פונקציית סריגים ממשקל k היא פונקציה של סריגים, F, ש- $F(\lambda L)=\lambda^{-k}F(L)$ לכל L סריג, $\lambda\in\mathbb{C}^*$.

למשל, $G_k(L)=\sum'_{\omega\in L}\omega^{-k}$ - טור אייזנשטיין, $k>2$ (משקל k), וגם $\Delta=g_2^3-27g_3^2$ ממשקל 12 כאשר $g_2=60G_4,\ g_3=140G_6$.

לפונקציה F כנ"ל, נגדיר $f:\mathbb{H}\to\mathbb{C}$, $\mathbb{H}=\{\tau=x+iy \mid y>0\}$, ע"י:

$$f(\tau)=F(\mathbb{Z}\tau+\mathbb{Z}\cdot 1)$$

טענה: לכל $\begin{pmatrix}a&b\\c&d\end{pmatrix}\in SL_2(\mathbb{Z})$,

$$f\left(\frac{a\tau+b}{c\tau+d}\right)=(c\tau+d)^k f(\tau)$$

הוכחה: נסמן,

$$f\left(\frac{a\tau+b}{c\tau+d}\right):=F\left(\left\langle\frac{a\tau+b}{c\tau+d},1\right\rangle\right)$$

אם $\begin{pmatrix}a&b\\c&d\end{pmatrix}\in SL_2(\mathbb{Z})$, אזי -

$$L=\langle\tau,1\rangle=\langle a\tau+b,c\tau+d\rangle=(c\tau+d)\left\langle\frac{a\tau+b}{c\tau+d},1\right\rangle -$$

$$L'=\left\langle\frac{a\tau+b}{c\tau+d}\right\rangle=(c\tau+d)^{-1}\langle\tau,1\rangle=(c\tau+d)^{-1}L$$

ולכן

$$f\left(\frac{a\tau+b}{c\tau+d}\right)=f(L')=\frac{1}{(c\tau+d)^k}f(L) \quad \square$$

הגדרה: תבנית מודולרית חלשה ממשקל k היא פונקציה מרומורפית $f:\mathbb{H}\to\mathbb{C}$ שמקיימת את משוואת הטרנספורמציה,

$$f\left(\frac{a\tau+b}{c\tau+d}\right)=(c\tau+d)^k f(\tau),\quad \forall\begin{pmatrix}a&b\\c&d\end{pmatrix}\in SL_2(\mathbb{Z})$$

דוגמה: $G_k(\tau)=\sum_{0\neq(m,n)\in\mathbb{Z}^2}\frac{1}{(m\tau+n)^k}$, $k>2$ ו- Δ.

למה: f מודולרית חלשה ממשקל k $\iff$ $f(\tau+1)=f(\tau),\ f\left(\frac{-1}{\tau}\right)=\tau^k f(\tau)$ ($f:\mathbb{H}\to\mathbb{C}$ מרומ')

הוכחה: כי ש- $SL_2(\mathbb{Z})=\langle S,T\rangle$. $\square$

הבחנה: $f(\tau+1)=f(\tau)$ משמעותה ש- f פונקציה של $q=e^{2\pi i\tau}$.

$$\mathbb{H}\twoheadrightarrow\mathbb{D}^*=\{q: 0<|q|<1\}$$
$$\tau\mapsto e^{2\pi i\tau}$$

לכן,

לכל $y>0$, $\tau = x+iy$, $|q| = |e^{2\pi i \tau}| = e^{-2\pi y}$

$f(\tau)$ מרומורפית $\Leftarrow$ $f(\tau)=\tilde{f}(q)$ כאשר $\tilde{f}$ מרומורפית ב-$0<|q|<1$.

הגדרה: תבנית מודולרית ממשקל k היא פונקציה הולומורפית $f: \mathbb{H} \to \mathbb{C}$, שמקיימת
(1) f נשמרת הטרנספורמציה, וכן ש-$\tilde{f}(q)$ ניתנת להמשכה הולומורפית ל-$q=0$.

תזכורת: (משפט רימן על סינגולריות סליקה)
תהא $D \subseteq \mathbb{C}$, $p \in D$, f הולומורפית ב-$D \setminus \{p\}$. אזי f ניתנת להמשכה הולומורפית ל-p $\Leftrightarrow$ f חסומה בסביבת p.

∴ לבדוק ש-f תבנית מודולרית $\Leftrightarrow$ לבדוק ש-$\tilde{f}(q)$ חסומה כאשר $q \to 0$, או $f(\tau)$ חסומה כאשר $\operatorname{Im}(\tau) \to \infty$.

טענה: $G_k(\tau)$ תבנית מודולרית ממשקל k, $k>2$, k זוגי.

הוכחה: נותר להראות:

$$G_k(i\infty) := \lim_{\operatorname{Im}\tau \to \infty} G_k(\tau)$$

$$= \lim_{\operatorname{Im}\tau \to \infty} \sum_{(0,0)\neq(m,n)\in\mathbb{Z}^2} \frac{1}{(m\tau+n)^k} = \sum_{(0,0)\neq(m,n)\in\mathbb{Z}^2} \lim_{\tau\to\infty} \frac{1}{(m\tau+n)^k} = \begin{cases} 0, & m\neq 0 \\ 1/n^k, & m=0 \end{cases}$$

$$\Rightarrow \lim_{\operatorname{Im}\tau \to \infty} G_k(\tau) = \sum_{(0,n)\neq(0,0)} \frac{1}{n^k} = 2\sum_{n=1}^{\infty} \frac{1}{n^k} = 2\zeta(k) \quad \square$$

מסקנה: Δ תבנית מודולרית ממשקל 12.

סימון - $M_k = M_k(SL_2(\mathbb{Z})) =$ מרחב התבניות המודולריות ממשקל k.

הגדרה: תבנית חוד (cusp form) ממשקל k היא $f \in M_k$
כך ש- $f(i\infty)=0$. נסמן ב-S_k.

טענה: לכל $k>2$ זוגי, $M_k = \mathbb{C}G_k + S_k$

הוכחה: כי $f(i\infty)$ קיים, f היא פונקציונל לינארי על M_k עם
גרעין S_k, ויש תבנית שאינה חוד (G_k) $\Rightarrow f - \frac{f(i\infty)}{2\zeta(k)} G_k \in S_k$ $\square$

הוכחה: $M_k=0$ אם k אי-זוגי. ניקח $I=\begin{pmatrix}-1 & \\ & -1\end{pmatrix}\in SL_2(\mathbb{Z})$,

$$f(\tau)=f\left(\frac{-1\cdot\tau+0}{0\cdot\tau-1}\right)=(0\cdot\tau-1)^k f(\tau)=(-1)^k f(\tau)=-f(\tau)$$

$\Leftarrow$ $f=0$.

משפט: $\Delta\in S_{12}$ היא תבנית חוד.

$$\Delta(i\infty)=g_2(i\infty)^3-27g_3^2(i\infty)=[60G_4(i\infty)]^3-27\cdot[140G_6(i\infty)]^2=$$
$$=(120\,\zeta(4))^3-27\,(280\,\zeta(6))^2$$

משפט: (euler)

מתקיים $\zeta(2)=\pi^2/6$, וכן -

$$\zeta(4)=\frac{\pi^4}{90},\quad \zeta(6)=\frac{\pi^6}{945}$$