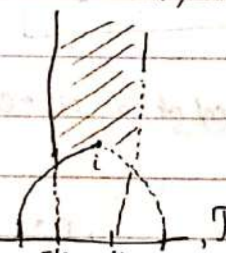
10/3/17 הרצאה 2

פעם קודמת – דיברנו על מרחב השריגים ב- $\mathbb{R}^2 \cong \mathbb{C}$. (שריג) $L \subseteq \mathbb{R}^2$ – תת חבורה דיסקרטית שפורשת את $\mathbb{R}^2$ ($L=\mathbb{Z}\omega_1+\mathbb{Z}\omega_2 \Leftarrow$) הגדרנו יחס שקילות של הומותטיה – $L \sim \lambda L$, $\lambda\in\mathbb{C}$. (כיווץ/מתיחה + סיבוב)



הראינו ש- $\frac{H}{SL_2(\mathbb{Z})} \cong \frac{\text{שריגים}}{\text{הומותטיה}}$.

הבאנו משפט – בהינתן התחום היסודי, $F=\left\{\tau\in H \,\middle|\, \begin{matrix}|\tau|>1,\ -\frac{1}{2}<Re\,\tau<\frac{1}{2} \\ \text{or } |\tau|=1,\ -\frac{1}{2}\le Re\,\tau\le 0\end{matrix}\right\}$,

1) לכל $\tau\in H$ יש $g\in SL_2(\mathbb{Z})$ כך ש- $g\tau\in F$
2) אין שני נקודות ב- F ששקולות זו לזו
3) $(ST)\rho=\rho$, $S=\begin{pmatrix}0&1\\-1&0\end{pmatrix}$, $i=Si$, ואין שקילויות נוספות אחרות
4) $SL_2(\mathbb{Z})=\langle S,T\rangle$, $T=\begin{pmatrix}1&1\\0&1\end{pmatrix}$.

תבניות ריבועיות בינאריות

בהינתן תבנית $f(x,y)=ax^2+bxy+cy^2$, $a,b,c\in\mathbb{Z}$, (נשאל) לאיזה מספרים "מיוצגים" ע"י f, כלומר, $n=f(x,y)$? [עבור $(x,y)\in\mathbb{Z}^2$]

או לחלופין (נרצה) "ייצוג" כך ש- $n=f(r,s)$, $r,s\in\mathbb{Z}^2$ עם $gcd(r,s)=1$. ("פרימ'") כמו נקרא ייצוג נאות.

למשל, 3 לא סכום ריבועים רציונליים, אבל אם כן היה, אז הם היו צריכים להיות שלמים.

שקילות תבניות ריבועיות

בהינתן תבנית $f(x,y)$ נגדיר תבנית חדשה.

$$g(x,y)=f(\alpha x+\beta y,\ \gamma x+\delta y), \quad \alpha,\beta,\gamma,\delta\in\mathbb{Z}$$

אם $\begin{pmatrix}\alpha&\beta\\\gamma&\delta\end{pmatrix}\in GL_2(\mathbb{Z})$ (כלומר, $\det\begin{pmatrix}\alpha&\beta\\\gamma&\delta\end{pmatrix}=\pm1$) נאמר ש- f,g שקולות. נאמר שהן שקולות במובן הצר אם $\det\begin{pmatrix}\alpha&\beta\\\gamma&\delta\end{pmatrix}=1$.

לכל תבנית $f=[a,b,c]$ נתאים מטריצה, $M_f=\begin{pmatrix}a&b/2\\b/2&c\end{pmatrix}$, כך ש-

$$f(x,y)=(x\ \ y)\begin{pmatrix}a&b/2\\b/2&c\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}$$

שאלה: כמה תבניות ריבועיות הן שקולות? (דומה, כי יש פעולה מוגדרת ב- $SL_2(\mathbb{Z})$) האם לשני מטריצות שקולות יש דרך לקבוע האם הן שקולות או לא?

שאלה קשה כי תבניות שקולות מייצגות אותם ערכים. יש אינווריאנטים גם שאומר אם המטריצות שקולות או לא מעל המרוכבים –

הגדרה: הדיסקרימיננטה של $f=[a,b,c]$ היא $D_f=b^2-4ac$, או $D_f=-4\det(M_f)$.

טענה: לתבניות שקולות יש אותה דיסקרימיננטה.

הוכחה: אם $g=f\circ A$, כאשר $A=\begin{pmatrix}\alpha&\beta\\ \gamma&\delta\end{pmatrix}\in GL_2(\mathbb{Z})/SL_2(\mathbb{Z})$, אזי - $M_g=A^T M_f A$ ∴

מכאן, $\det M_g=\det A^2\cdot\det M_f$. אם $\det A^2=1$ אז $\det M_g=\det M_f$ ובפרט לדיסקרימיננטות.

הגדרה: תבנית ריבועית היא מוגדרת חיובית אם $f(x,y)>0$ לכל $(0,0)\neq(x,y)\in\mathbb{R}^2$.

נשים לב, כי אם $f(x,y)=ax^2+bxy+cy^2$ אזי -

$$(*)\quad 4af(x,y)=(2ax+by)^2-D_f\cdot y^2$$

אכן,

$$RHS=4a^2x+4abxy+b^2y^2-D_fy^2=4a^2+4abxy+4acy^2$$

$$b^2-D_f=4ac$$

מסקנה: f מוגדרת חיובית $\iff$ $D_f<0$, $a>0$. f מוגדרת (חיובית/שלילית) $\iff$ $D_f<0$.

הוכחה: ברור מהזהות (*). □

שקילות משמרת מוגדרות חיובית. אכן הדטרמיננטה נשמרת וגם סימן המקדם הראשי.

שאלה: בהינתן f,g מוגדרות חיובית עם אותה דיסקרימיננטה $D<0$, להכריע האם $f\sim g$?

הגדרה: נסמן מספר המחלקה -

$$h(D)=\#\{\text{proper equivalence classes of positive def forms, with } disc(f)=D\}$$

נשים לב שמאחר ש- $D=b^2-4ac<0$, נובע $D\equiv 0,1 \pmod 4$.

הערה: אם $D\equiv 0,1 \pmod 4$, $D<0$, אזי $h(D)\geq 1$, ויש שני מחלקות ראשיות -

* אם $D\equiv 0 \pmod 4$, $x^2-\frac{D}{4}y^2$
* אם $D\equiv 1 \pmod 4$, $x^2+xy+\frac{1-D}{4}\cdot y^2$

משפט: אם $D<0$, $D\equiv 0,1 \pmod 4$ אזי $h(D)<\infty$.

הוכחה בהמשך.

נקודת השרש

בהינתן תבנית $f=[a,b,c]$ מוגדרת חיובית עם דיסקרימיננטה $D=b^2-4ac$, נתאים $\mathbb{H}\ni\tau_f\leftarrow f$ הפתרון היחיד ב-$\mathbb{H}$ ל- $f(\tau,1)=0$: במפורש,

$$(a>0)\quad a\tau^2+b\tau+c=0\Rightarrow \tau=\frac{-b+\sqrt{D}}{2a}=\frac{-b+i\sqrt{|D|}}{2a}\in\mathbb{H}$$

למה: $f=[a,b,c]$, $g=[a',b',c']$, כך ש- $D_f=D_g=D$. אזי:

1) $f=g \iff \tau_f=\tau_g$

2) $f\sim_{SL_2(\mathbb{Z})}g \iff \tau_f\sim_{SL_2(\mathbb{Z})}\tau_g$

הערה:

① נניח $D_f=D_g$. אז, גם $\tau_f=\tau_g$, נכתוב-

$$\tau_f=\frac{-b+i\sqrt{|D|}}{2a}, \quad \tau_g=\frac{-b'+i\sqrt{|D|}}{2a'}$$

ולכן- $a=a' \Leftarrow \frac{\sqrt{|D|}}{2a}=\frac{\sqrt{|D|}}{2a'}$

וגם $-\frac{b}{2a}=-\frac{b'}{2a'}$ ולכן גם $b=b'$.

② אם $g=f\circ A$, אז, $\tau_g=A^{-1}(\tau_f)$ כאשר $A=\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}\in SL_2(\mathbb{Z})$. נחשב ישירות-

$$0=g(\tau_g,1)=f(\alpha\tau_g+\beta,\gamma\tau_g+\delta)=a(\alpha\tau_g+\beta)^2+b(\alpha\tau_g+\beta)(\gamma\tau_g+\delta)+c(\gamma\tau_g+\delta)^2=$$

$$=(\gamma\tau_g+\delta)^2\left[a\left(\frac{\alpha\tau_g+\beta}{\gamma\tau_g+\delta}\right)^2+b\left(\frac{\alpha\tau_g+\beta}{\gamma\tau_g+\delta}\right)+c\right]=(\gamma\tau_g+\delta)^2 f(A\tau_g,1)$$

אבל $Im(\tau_g)>0$ ולכן $f(A\tau_g,1)=0 \Leftarrow (\gamma\tau_g+\delta)^2\neq 0$. וכן, שכן $A\tau_g\in\mathbb{H}$

אז, נקבל $\tau_g=A^{-1}(\tau_f) \Leftarrow A\tau_g=\tau_f$. הכיוון ההפוך - אותו חישוב. □

תורת הצמצום (Reduction Theory) - לגראנז'

הגדרה: תהי $f=[a,b,c]$ תבנית מוגדרת חיובית, עם $disc(f)=D<0$. נאמר ש-f מצומצמת
אם- $0\le b\le a=c$ או $-a<b\le a<c$

טענה: f מצומצמת $\Leftrightarrow \tau_f\in\mathcal{F}'$.

הוכחה: נחשב את $|\tau_f|^2=\left(\frac{-b}{2a}\right)^2+\left(\frac{\sqrt{|D|}}{2a}\right)^2=\frac{b^2-D}{4a^2}=\frac{c}{a}$. צריך $c\ge a$
וגם $Re\,\tau_f=\frac{-b}{2a}\in[-\frac{1}{2},\frac{1}{2})$. כל פשוט תשובה. □

משפט: כל תבנית מוגדרת חיובית $f=[a,b,c]$ היא שקולה (במובן הצר) לתבנית מצומצמת יחידה.

דוגמה, נחשב את $h(-4)=1$. צריך $D=-4$. יש מייד את התבנית הראשית- x^2+y^2. נראה שהיא מיצה. צריך למצוא את כל התבניות המצומצמות $[a,b,c]$ עם דיסקרימיננטה $b^2-4ac=-4$. אם $f=[a,b,c]$ מצומצמת אז בפרט $a\le c$.

$$4a^2\underset{a\le c}{\le}4ac=b^2+4$$

וכן $1\le a\le\frac{\sqrt{|D|}}{\sqrt{3}} \Leftarrow \frac{\sqrt{|D|}}{2a}=Im(\tau_f)\ge\frac{\sqrt{3}}{2} \Leftarrow \tau_f\in\mathcal{F}$. אך אם $|D|=4$

אז $a=1 \Leftarrow 1\le a\le\frac{\sqrt{4}}{\sqrt{3}}=1.(\dots)$.

עכשיו, $b=0,1 \Leftarrow -1<b\le 1$

(כמו ל-(דטרמיננטה) $b\equiv D \pmod 2 \Leftarrow b^2=D+4ac\equiv D \pmod 2$. אז b זוגי, ובפרט $b=0$. עכשיו,
a,b,D קבועים אז $c=\frac{b^2-D}{4a}=\frac{4}{4}=1$, ולכן התבנית היא $[1,0,1]$.

מסקנה: $f=[a,b,c]$ מצומצמת ⟸ $1\le a\le\sqrt{\frac{|D|}{3}}$, וכן $|b|\le a\le\sqrt{\frac{|D|}{3}}$. ⟸ עבור ס' a,b,D

ולכן, $h(D)\ll|D|<\infty$. הוכחנו גם משהו יותר טוב - $h(D)\ll\sqrt{|D|}\cdot\log|D|$.

<u>אלגוריתם הצמצום</u>

בהינתן $f=[a,b,c]$, $D=b^2-4ac<0$, $a>0$. יש לנו שני יוצרים ל-$SL_2(\mathbb{Z})$ -

$$S=\begin{pmatrix}0&1\\-1&0\end{pmatrix}: f=[a,b,c]\rightsquigarrow[c,-b,a],\quad \tau\mapsto -1/\tau$$

$$T=\begin{pmatrix}1&1\\0&1\end{pmatrix}: f=[a,b,c]\rightsquigarrow[a,b+2a,c'],\quad \tau\mapsto\tau+1$$

① $a>c$ - (נפעיל) S: נחליף את f ב-$[c,-b,a]$. אם $-c\le b<c$ <u>עצור</u>. אחרת רק נמשיך ל-②.

② אם $a\le c$, (נפעיל) T^n כדי לקבל $f\rightsquigarrow[a,b-2na,c']$, כך ש-$b-2na\in(-a,a]$. אם $c'>a$ - <u>עצור</u>. אם $c'<a$ רק ל-①. אם $c'=a$ - רק ל-③.

③ $a=c$, (נפעיל) את S ונקבל $f\to[a,-b,a]$. <u>עצור</u>.

<u>דוגמה</u>: ניקח $f=[6,7,6]$, $D=7^2-4\cdot6\cdot6=-95$. התבנית - $6x^2+7xy+6y^2$.

(נפעיל) את שלב ② כדי להעביר ל-$[6,-5,c']$. c' נמצא ע"י c,b,D - $D=-95=b'^2-4ac'=25-24c'$ ⟸ $120=24c'$ ⟸ $c'=5$. נקבל $[6,-5,5]$. (נפעיל) את שלב ① ונקבל $[5,5,6]$. <u>מצומצם</u>.

<u>דוגמה</u>: ניקח $f=[16,23,9]$, $D=-47$.

$$f\overset{①}{\rightsquigarrow}[9,-23,16]\underset{n=1}{\overset{②}{\rightsquigarrow}}[9,-5,c']=[9,-5,2]\overset{①}{\rightsquigarrow}$$

$$c'=2\Leftrightarrow -72=-36c'\Leftrightarrow -47=25-36\cdot c'$$

$$\overset{①}{\rightsquigarrow}[2,5,9]\underset{n=2}{\overset{②}{\rightsquigarrow}}[2,1,c']=[2,1,6]\ \text{- מצומצם}$$

$$c'=6\Leftrightarrow -47=1-8c'$$

בעיה <u>פתוחה</u>: חסם <u>תחתון</u> ל-$h(D)$. יודעים שעבור $D\equiv0,1 \pmod 4$, $D<0$,

$1<h(D)\ll|D|$, ואפשר ש-$h(D)\ll\sqrt{|D|}\log|D|$.

הייתה השערה של גאוס ש-$h(D)\underset{D\to-\infty}{\longrightarrow}\infty$.

<u>לנדאו</u>: (1918)

אם מניחים את השערת רימן יש חסם תחתון אפקטיבי, לא ברור בדיוק מה הקבועים $h(D)>100\cdot\frac{\sqrt{|D|}}{\log|D|}$.

<u>Heilbronn, Deuring, Mordell</u>: לא GRH ⟸ $h(D)\underset{-D\to\infty}{\longrightarrow}\infty$

⟸ ההשערה של גאוס נכונה. חישובים של גאוס:

D	-3	-4	-7	-8	-11	-12	-15	-16	-19	-20	-23	-24
$h(D)$	1	1	1	1	1	1	2	1	1	2	3	2

גאוס: $D=\underbrace{-3,-4,-7,-11,\dots,-163}_{13 \text{ דוגמאות}} \Rightarrow h(D)=1$

השערה: זה הכל, כלומר, $h(D)=1 \Rightarrow D \geq -163$.

ידוע: יש רק מספר סופי. (כי $h(D)\xrightarrow[D\to-\infty]{}\infty$).

היילברון - לינפוט: לכל היותר דוגמה אחת נוספת.

סיגל 1935: $h(D)>C(\varepsilon)|D|^{\frac{1}{2}-\varepsilon}$ לכל $\varepsilon>0$, קיים $C(\varepsilon)>0$.

$C(\varepsilon)$ לא אפקטיבי.

$h(D)=1 \longrightarrow D \geq -163$ - H. Stark, Baker

Ati Gross, Zagier - 1980 - חסם אפקטיבי, $h(D)>2019 \cdot \log(D)$.