17/3/19 $\boxed{\text{הרצאה } 3}$

<u>תבניות ריבועיות בינאריות</u>

$a,b,c\in\mathbb{Z}$, נסמן $f=[a,b,c]=ax^2+bxy+cy^2$ מוגדרת חיובית $\iff$ $disc(f)<0$ וגם $a>0$.

נאמר ש- $f\sim g$ (שקולות <u>במובן הצר</u>) אם - $g(x,y)=f(\alpha x+\beta y,\gamma x+\delta y)$ כאשר $\begin{pmatrix}\alpha&\beta\\ \gamma&\delta\end{pmatrix}\in SL_2(\mathbb{Z})$.

הבחנו ש- $f\sim g \Rightarrow disc(f)=disc(g)$. ההיפך לאו דווקא נכון.

הבחנו שאם $D=disc f$, אזי $D\equiv 0,1 \pmod 4$, ולהפך. לכל D כזה יש תבנית כנ״ל.

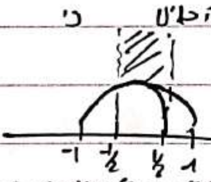
הבחנו שמתקיים -

<u>משפט</u>: ① יש מספר סופי $h(D)$ של מחלקות שקילות של תבניות עם $disc(f)=D$.

② כל תבנית שקולה לתבנית מצומצמת, $-a<b\le a<c$ או $0\le b\le a=c$.

נתמקד רק בתבניות פרימיטיביות - $gcd(a,b,c)=1$. דיברנו על נקודת הייגנר - $f=[a,b,c]\mapsto\tau_f=\frac{-b+\sqrt{D}}{2a}\in\mathbb{H}$, τ_f הוא היחיד τ כך ש- $f(\tau,1)=0$ וגם $\tau\in\mathbb{H}$. הבחנו כי $f\sim g\iff\tau_f\sim\tau_g$ תחת הפעולה מכיוון ב- $SL_2(\mathbb{Z})$.

דיברנו על התחום היסודי -



$\boxed{\text{סוף התזכורת}}$

<u>הקשר לאריתמטיקה של הרחבות ריבועיות דמיוניות של $\mathbb{Q}$</u>

יהי $d<0$ שלם וחסר ריבועים. ניקח -

$$K:=\mathbb{Q}(\sqrt{d})=span_{\mathbb{Q}}\{1,\sqrt{d}\}$$

זה שדה, תת שדה של $\mathbb{C}$, <u>שאינו</u> מוכל ב- $\mathbb{R}$ (כי $d<0$). יודעים ש- $[K:\mathbb{Q}]=2$.

למשל, עבור $d=-1$, מקבלים את שדה "המספרים של גאוס" $\mathbb{Q}(i)$, $i=+\sqrt{-1}$.

חוג <u>השלמים</u> של K, $\mathcal{O}_K:=\{\alpha\in K \mid \alpha \text{ שורש של } f,\ f\in\mathbb{Z}[x] \text{ מתוקן}\}$. עובדה - זהו חוג (כלומר, $\mathcal{O}_K$ סגור תחת חיבור וכפל).

<u>עובדה</u>: במקרה של הרחבה ריבועית $K=\mathbb{Q}(\sqrt{d})$, d חסר ריבועים,

$$\mathcal{O}_K=\mathbb{Z}[\omega_K]=\mathbb{Z}+\omega_K\mathbb{Z}$$

כאשר -

$$\omega_K=\begin{cases}\sqrt{d}, & d\not\equiv 1 \pmod 4\\ \frac{1+\sqrt{d}}{2}, & d\equiv 1 \pmod 4\end{cases} \text{ - שורש של - } \begin{cases}x^2+x+\frac{1-D}{4}, & D=d\equiv 1(4)\\ x^2-\frac{D}{4}, & D=4d, d\not\equiv 1(4)\end{cases}$$

למשל, $d=-1 \Rightarrow \mathcal{O}_{\mathbb{Q}[\sqrt{-1}]}=\mathbb{Z}[i]$, $d=-3$ אז $\mathcal{O}_{\mathbb{Q}[\sqrt{-3}]}=\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]=\mathbb{Z}[\underbrace{-\frac{1+\sqrt{-3}}{2}}_{\rho}]$ –
חוג השלמים של אייזנשטיין.

<u>הגדרה</u>: ה<u>דיסקרימיננטה</u> של הרחבה ריבועית $K=\mathbb{Q}[\sqrt{d}]$ היא –

$$D_K=\begin{cases}4d, & d\not\equiv 1 \pmod 4\\ d, & d\equiv 1 \pmod 4\end{cases}$$

<u>הגדרה</u>: <u>דיסקרימיננטה יסודית</u> (fundamental discriminant) היא דיסקרימיננטה של הרחבה ריבועית:

$$D=\begin{cases}4d, & d\not\equiv 1 \pmod 4\\ d, & d\equiv 1 \pmod 4\end{cases}$$

עבור d חסר ריבועים.

ב-$\mathcal{O}_K$ – שהוא חוג – יש אידיאלים, $I\triangleleft\mathcal{O}_K$. אם $I\neq 0$ אז $I\subseteq\mathcal{O}_K\subseteq\mathbb{C}$ הוא <u>סריג</u>, כלומר, ישנם $\alpha,\beta\in I$, בת"ל מעל $\mathbb{R}$, כך ש-$I=\mathbb{Z}\alpha+\mathbb{Z}\beta$.
אם $\mathcal{O}_K\triangleright I\neq 0$ אזי $\#\mathcal{O}_K/I<\infty$. נגדיר $N(I)=\#\mathcal{O}_K/I$.
<u>דוגמה</u>: אם ראשי, כלומר $I=\mathcal{O}_K\cdot\alpha$, עבור $0\neq\alpha\in\mathcal{O}_K$, מקבלים –

$$N(I)=Norm_{K/\mathbb{Q}}(\alpha)=\alpha\cdot\bar{\alpha}=|\alpha|^2$$

למשל ב-$K=\mathbb{Q}[i]$, $\mathcal{O}_K=\mathbb{Z}[i]$, ועבור $\alpha=m+ni$ מקבלים: $N(\alpha\mathcal{O}_K)=m^2+n^2$.

<u>הגדרה</u>: בסיס <u>חיובי</u> של אידיאל I הוא בסיס סדור, $I=\langle\alpha,\beta\rangle=\mathbb{Z}\alpha+\mathbb{Z}\beta$, כך ש- $\frac{\alpha\bar{\beta}-\bar{\alpha}\beta}{\sqrt{D}}>0$.

<u>הערה</u>: אם α,β בסיס חיובי אזי β,α בסיס שלילי.

בהינתן $I=\langle\alpha,\beta\rangle$ בסיס חיובי, נתאים תבנית ריבועית, פרימיטיבית,

$$Q_{\langle\alpha,\beta\rangle}(x,y)=\frac{N(x\alpha+y\beta)}{N(I)}$$

<u>טענה</u>: $Q_{\langle\alpha,\beta\rangle}$ תבנית ריבועית <u>שלמה</u> עם דיסקרימיננטה D_K.

<u>משפט</u>: ① החלפת בסיס (חיובי) נותנת ~~[illegible]~~ תבנית שקולה (במובן הזה)
② וכן, כל אידיאלים מתאימים מחלקת שקילות של תבניות (שקילות זהה) של תבניות עם דיסקרימיננטה D_K.

<u>הגדרה</u>: אידיאלים שקולים – $I\sim J$, אם $0\neq I,J\triangleleft\mathcal{O}_K$, הם נקראים שקולים כאשר $I\cdot(\alpha)=J\cdot(\beta)$, עבור $0\neq\alpha,\beta\in\mathcal{O}_K$.

ולמשל, $\alpha\sim(1)=\mathcal{O}_K$.

מסקנה: אידיאלים שאינם שקולים נותנים תבניות לא שקולות, ולהיפך.

במילים אחרות, קיבלנו התאמה חח״ע ועל -

$$\left\{\begin{array}{c}\text{מחלקות שקילות של תבניות}\\ [a,b,c]\text{, עם דיסקרימיננטה}\\ D_K \text{ נתונה}\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\text{מחלקות שקילות}\\ \text{של אידיאלים}\\ K\text{-ב}\end{array}\right\}$$

תבניות פרימיטיביות

בפרט,

מסקנה: $h(D_K)=1 \iff$ כל אידיאל ב-$\mathcal{O}_K$ הוא ראשי.

למשל $D=-4$, $h(-4)=1 \Rightarrow$ החוג $\mathbb{Z}[i]$ ראשי.

בנוסף: $\mathcal{O}_K = I = \langle 1,\omega_K\rangle$;

$$Q_{\langle 1,\omega_K\rangle}(x,y) = \frac{N(x\cdot 1 + y\cdot\omega_K)}{N(\mathcal{O}_K)} = \frac{(x+y\omega)(x+y\bar\omega)}{1} =$$

$$= x^2 + (\omega+\bar\omega)xy + \omega\bar\omega y^2 =$$

$$= x^2 + tr(\omega)xy + Norm(\omega)y^2$$

① $D=4d$, $\omega_K=\sqrt{d}$, $\bar\omega=-\sqrt{d}$.

$$tr_{K/\mathbb{Q}}(\omega)=0$$

$$N_{K/\mathbb{Q}}(\omega)=\omega\cdot\bar\omega = -d = -D/4$$

$$Q_{\langle 1,\omega\rangle}(x,y)=x^2-\frac{D}{4}\cdot y^2$$

② $D=d\equiv 1 \pmod 4$, $\omega=\frac{1-\sqrt{D}}{2}$.

$$tr_{K/\mathbb{Q}}(\omega)=1$$

$$N_{K/\mathbb{Q}}(\omega)=\frac{1+\sqrt{D}}{2}\cdot\frac{1-\sqrt{D}}{2}=\frac{1-D}{4}$$

$$Q_{\langle 1,\omega\rangle}=x^2+xy+\frac{1-D}{4}y^2$$

כמו כן, קיבלנו את התבניות המצומצמות עם דיסקרימיננטה D_K.

תרגיל: חשבו את התבניות שמתאימות לבסיס נתון של אידיאל ראשי $\alpha\mathcal{O}_K$.

עובדה: $\mathcal{O}_K$ הוא חוג ראשי $\iff$ יש יחידות פירוק לראשוניים ב-$\mathcal{O}_K$.

דוגמה: כאן אין יחידות פירוק -

$$K=\mathbb{Q}(\sqrt{-6}),\quad \mathcal{O}_K=\mathbb{Z}[\sqrt{-6}]$$

פירוק מסכן - $\alpha=\beta\cdot\gamma$ כאשר β,γ לא הפיכים ב-$\mathcal{O}_K$. ואכן נוכל לכתוב -

$$-6=(\sqrt{-6})^2=-2\cdot 3$$

תישות שאין ש- $(\mathbb{Z}[\sqrt{-6}])^\times=\{\pm1\}$. אכן α הפיך $\Leftrightarrow$ $Norm(\alpha)=1$ ואם $\alpha=m+n\sqrt{-6}$, ואם הוא הפיך אז $1=Norm(\alpha)=m^2+6n^2 \Rightarrow n=0,\ m=\pm1$.
כמו כן, $2,3,\sqrt{-6}$ אי פריקים ב-$\mathcal{O}_K$ והם לא נבדלים בהפיך (כי ההפיכים ב-$\mathcal{O}_K$ הם ±1) לכן אין יחידות פירוק. והאם הם אי פריקים -
נניח - $2=\alpha\cdot\beta$ עבור $\alpha,\beta\in\mathcal{O}_K$, לא הפיכים $\Leftarrow$ וגם $N(\alpha),N(\beta)\neq1$. נקבל:

$$4=N(2)=N(\alpha)N(\beta)$$

$\Leftarrow N(\alpha),N(\beta)=2$. לכן אם נכתוב $\alpha=m+n\sqrt{-6}$ $\Leftarrow$ $m^2+6n^2=2$ וזה לא פתיר מעל $\mathbb{Z}$.
וכך $3,\sqrt{-6}$ עושים באותו אופן.
$\Leftarrow$ בספרה יש אידיאל לא ראשי. וניתן לחשב ש- $h(-24)=2$,
והתבניות המצומצמות הן - $[1,0,6]=x^2+6y^2$
והן - $[2,0,3]=2x^2+3y^2$ לא שקולות
כאן $[1,0,6]$ מתאים לאידיאל הראשי. נראה מה מתאים לקלס של $[2,0,3]$ - של האידיאלים השקולים.

התאמה: תבניות $\to$ אידיאלים:
$f=[a,b,c]$, $b^2-4ac=D_K$ תבנית, מתאים לה אידיאל עם בסיס סדור $\langle a,\frac{b-\sqrt{D_K}}{2}\rangle$. תישוב - זה אידיאל. וכן ניתן לחשב -

$$Q_{\langle a,\frac{b-\sqrt{D_K}}{2}\rangle}(x,y)=[a,b,c]$$

תרגיל: לבדוק את מה שצריך לבדוק.

ולכן $[2,0,3]$ לפי מתאים לאידיאל $2\mathbb{Z}+\sqrt{-6}\mathbb{Z}$. זה לא אידיאל ראשי: כי האינדקס שלו 2; ונניח הוא ראשי היה מספר שנורמתו 2, ורצינו שאין כזה.
יש בספר ... משפט על הרחבות ריבועיות ממשיות (כמו $\mathbb{Q}(\sqrt{2})$) עם מבנה קצת שונה. להרחבות לא ריבועיות - אין כזו תאוריה.

הערה: (גאוס)
יש רק 9 הרחבות ריבועיות דמיוניות עם יחידות פירוק לאי פריקים
$$\mathbb{Q}(\sqrt{d}),\quad d=\overbrace{-1,-2,-3,-7,-11}^{\text{אוקלידיות}},\overbrace{\dots,-163}^{\text{לא אוקלידיות}}$$
(הוכחה בשנות ה-60)

השערה: (פתוחה, קשה)

יש אינסוף הרחבות ריבועיות ממשיות ($\mathbb{Q}(\sqrt{d})$, כלומר), עם יחידות פירוק.

(בקורס נוכיח לאינסוף ערכים של d)

פרק 3 - פונקציות אליפטיות

הגדרה: פונקציה אליפטית היא פונקציה מרומורפית $f(z)$ עם שני מחזורים בת"ל מעל $\mathbb{R}$

ω מחזור - $f(z+\omega)=f(z)$ לכל z.

הערה: מכירים פונקציות עם מחזור אחד, למשל $\sin(z)$ (עם מחזורים $2\pi k$). אינן אליפטיות. גם: קבועים. לא.

הערה: נגדיר L_f, אוסף המחזורים של f פונקציה מרומורפית לא קבועה. מהווה תת חבורה דיסקרטית של $\mathbb{C}$. (תרגיל בבית)

דוגמה - $L_f=\{0\}$, $L_{\sin}=\{2\pi\mathbb{Z}\}$. על סמך המין שלו לא יהיה דיסקרטי. של $\mathbb{R}^n$ האפשרות הנוספת היא $L_f=\mathbb{Z}^2$.

מסקנה: L_f היא דיסקרטית אם f מרומורפית לא קבועה.

הוכחה: לפונקציה מרומורפית האפסים מבודדים, ולכן גם ... - $\{\omega : f(\omega)-f(0)\} \supseteq L_f$.
אז LHS דיסקרטית. ולכן גם L_f. ∎

פונקציית $\wp(z;L)$ של ויירשטראס

יהי $L\subseteq\mathbb{C}$ סריג. נגדיר -

$$\wp(z,L):=\frac{1}{z^2}+\sum_{0\neq\omega\in L}\left(\frac{1}{(z-\omega)^2}-\frac{1}{\omega^2}\right)$$

משפט: הפונקציה $\wp$ היא אליפטית, ו- $L_\wp=L$.

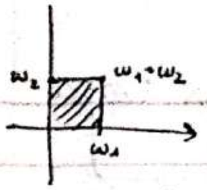
דוגמה יותר פשוטה - $k>2$, $f_k(z)=\sum_{\omega\in L}\frac{1}{(z-\omega)^k}$.

$$f_k(z+\omega_0)=\sum_{\omega\in L}\frac{1}{(z-\omega+\omega_0)^k}=\sum_{\omega'\in L}\frac{1}{(z-\omega')^k}=f_k(z)$$

תכונות כלליות של פונקציות אליפטיות

$L\subseteq\mathbb{C}$ סריג.

משפט: (Liouville) פונקציה אליפטית בלי קטבים היא קבועה.



<u>הוכחה:</u> ניקח D מקבילית יסודית של L, ונשים - $D = \{ t_1\omega_1 + t_2\omega_2 \mid 0 \le t_1, t_2 \le 1 \}$

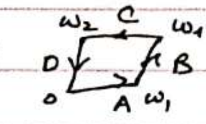
הערכים של f נקבעים ע"י ערכי f ב-D - קומפקטי, ולכן אם f אליפטית, f רציפה ב-D $\Leftarrow$ חסומה ב-D $\Leftarrow$ חסומה ב-$\mathbb{C}$. □

<u>טענה:</u> פונקציה אליפטית לא קבועה מקבלת כל ערך ב-$\mathbb{C}\cup\{\infty\}$.

<u>הוכחה:</u> אחרת, אם $f(z)\neq a$, אז $\frac{1}{f(z)-a}$ אליפטית, לא קבועה ולא מקבלת את ∞ $\Leftarrow$ חסומה - סתירה. □

<u>טענה:</u> f אליפטית לא קבועה, D מקבילית יסודית של f שאין קטבים של f על השפה ∂D. (תמיד אפשר לבחור כך ע"י הזזה) אזי,

$$\oint_{\partial D} f(z)\,dz = 0$$

<u>הוכחה:</u>  - פירוק

$$\oint_{\partial D} f(z)\,dz = \int_A + \int_B + \int_C + \int_D \quad , \quad C = A+\omega_2 ,\ D = B-\omega_1$$ עם כיוון אחרי

נראה:

$$\int_D = -\int_B \quad , \quad \int_C = -\int_A$$ ונסיים.

$$\int_A f(z) = \int_0^1 f(t\omega_1)\,d(t\omega_1)$$

$$\int_C f(z) = \int_0^1 f(\omega_1+\omega_2 - t\omega_1)(-d t\omega_1) = -\int_0^1 f((1-t)\omega_1)\,dt\omega_1 = -\int_0^1 f(s\omega_1)\,d(s\omega_1) \quad (s=1-t)$$

ובאופן דומה את השני. □

<u>טענה:</u> f אליפטית לא קבועה, D תחום יסודי ללא קטבים של f על ∂D. אזי -

$$0 = \frac{1}{2\pi i}\oint_{\partial D} f = \sum_{p_i \in D} \operatorname{res}_{p_i}(f)$$

<u>הוכחה:</u> נובע משפט קושי + הטענה הקודמת. □

<u>טענה:</u> f אליפטית לא קבועה, ללא קטבים/אפסים ב-∂D. אזי,

\# אפסים ב-D = \# קטבים ב-D (עם ריבוי)

<u>הוכחה:</u> אכן,

$$\#\text{אפסים ב-}D - \#\text{קטבים ב-}D = \frac{1}{2\pi i}\oint \frac{f'}{f}$$

אך f'/f - גם כן אליפטית. ולכן האינטגרל שם $=0$. □

הגדרה: הדרגה של של פונקציה אליפטית —

$\delta(f) =$ מספר הקטבים $=$ מספר האפסים $= \#\{z\in D \mid f(z)=a\}$ (ה.ם ס ריבוי)

אין כי $\gamma(f)\geq 1$ ולמעשה,

טענה: $\gamma(f)\geq 2$.

הוכחה: אם $\gamma(f)=1$, אז ל-f קוטב יחיד פשוט ב-D. אז $Res_p(f)\neq 0$ כי הקוטב... אבל סכום השאריות של הקטבים $=0$.

סתירה. $\square$