УНИВЕРЗИТЕТ У БЕОГРАДУ

МАТЕМАТИЧКИ ФАКУЛТЕТ

Анета Козина

МОДУЛАРНА ГРУПА $\mathbf{SL_2(Z)}$

- Мастер рад -

Беорад, 2023.

Ментор:

др Горан Ђанковић, ванредни професор

Математички факултет, Универзитет у Београду

Чланови комисије:

др Зоран Петровић, редовни професор

Математички факултет, Универзитет у Београду

др Марко Радовановић, ванредни професор

Математички факултет, Универзитет у Београду

Садржај

Глава 1

Увод

Једна од најважнијих врста функција у линеарној алгебри су линеарне трансформације. Ове функције се могу задати помоћу матрица. Поред овога, матрице се користе за описивање различитих проблема у разним научним дисциплинама, посебно у математици, физици, економији и у рачунарству.

Матрице се у зависности од векторског простора над којим трансформација делује, јављају у различитим димензијама. На пример, линеарна трансформација у равни описује се матрицама димензија 2×2. Како прилазимо специфичним применама матрица могу се уочити и посебне врсте матрица.

У овом раду ће бити описане матрице димензија 2×2, чији су елементи цели бројеви, чија је детерминанта једнака 1, а које генеришу групу коју обележавамо са $SL_2(\boldsymbol{Z})$.

У поглављу 2 ће бити дат историјат настанка модуларне групе $SL_2(\boldsymbol{Z})$.

У поглављу 3 ће бити дат теоријски оквир овог рада и биће наведени основни појмови и теореме из теорије група релевантне за тему овог рада.

У поглављу 4 ће бити описана група матрица $SL_2(\boldsymbol{Z})$, као и начини генерисања ове групе матрица, уз пригодну визуелизацију и уз неколико примера.

У поглављу 5 ће бити описане конгруентне подгрупе од $SL_2(\boldsymbol{Z})$.

У поглављу 6 ће бити наведени примери у којима се користи ова модуларна група, док ћемо кроз поглавље 7 добити више информација о будућим истраживањима када је примена ове групе у питању.

Глава 2

Историјат

Прва детаљна истраживања о модуларној групи датирају из седамдесетих година деветнаестог века захваљујући Рихарду Дедекинду и Феликсу Клајну. Своја истраживања предочили су у оквиру програма Ерланген и објавили су их 1872. године.

Програм Ерланген је метода заснивања геометрија на теорији група и пројективној геометрији. Име је добио по Универзитету Ерланген-Нурнберг, где је Клајн радио. До 1872. године појавиле су се нееуклидске геометрије, али без начина да се одреди њихова хијерархија и односи. Клајнов метод је био фундаментално иновативан на три начина:

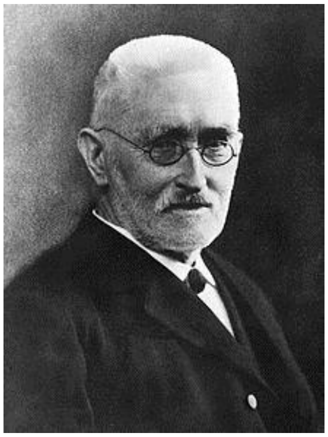
- Пројективна геометрија је била истакнута као универзални оквир који обухвата и усваја све остале разматране геометрије.

- Клајн је предложио да се употреба теорије група искористи као најефикаснији начин структурирања геометријског знања.

- Изразио је концептуалну идеју да сваки геометријски језик поседује своје специфичне концепте који се препознају кроз везе између подгрупа модуларне групе. Ово су били рани почеци примене подгрупа модуларне групе.

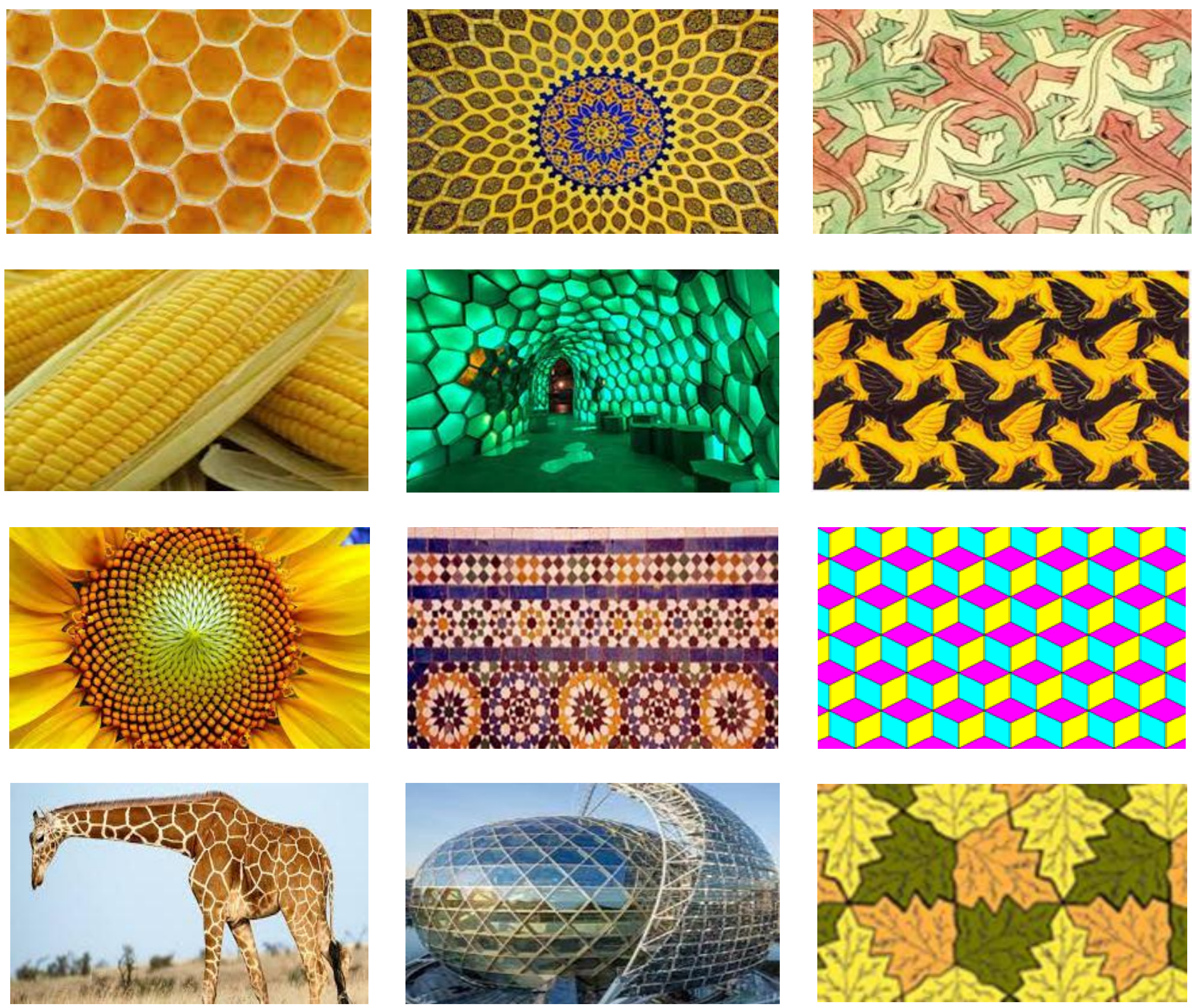
2.1. Рихард Дедекинд

Рихард Дедекинд (1831 — 1916) је био немачки математичар. Рођен је у Брауншвајгу, где је живео већи део свог живота и где је умро. На почетку свог школовања интересовао се за физику и хемију, док се након преласка на колегијум није окренуо теорији бројева, алгебри и аналитичкој геометрији. Дедекинд је докторирао 1852. године, са тезом под називом „О теорији Ојлерових интеграла”. Иако ова теза није дала пуне домете овог математичара, временом је показао таленат који поседује и постао је један од првих људи који су схватили важност појма група за алгебру и аритметику. Његове идеје настављају да утичу и на савремену математику.



2.1.1. Дедекиндове теселације

Теселација или поплочавање равни је поступак постављања геометријских облика у равни, без преклапања и празнина. Може се говорити и о теселацији делова равни или других површи, а могућа су и уопштења на више димензија. Могу се посматрати у еуклидској, хиперболичкој равни или на сфери. Заступљене су свуда око нас: у биљном и животињском свету (структура листа, структура кошнице, оклоп корњаче, различите шаре на кожи змија и гуштера) - *Слика 1 а)*, у архитектури и грађевинарству (поплочани тргови, зграде необичног дизајна) - *Слика 1 б)*, у уметности (шаре и орнаменти) - *Слика 1 ц)*, у компјутерској графици, оптици, кристалографији, друштвеним и рачунарским играма.

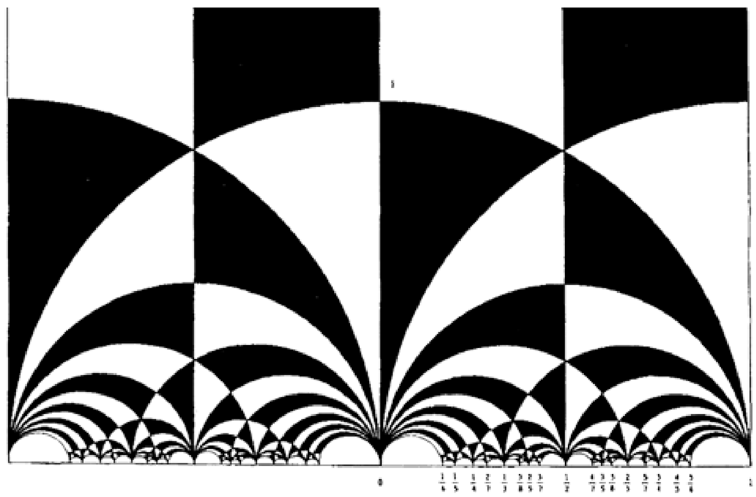


а) у биљном и животињском свету *б) у архитектури и грађевинарству* *ц) у уметности*

Слика 1 - Теселације

Разни математичари су се бавили теселацијама, почев од Архимеда, који је проучавањем слагања полигона без шупљина и преклапања, поставио основе за развијање идеја и принципа теселација.

Рихард Дедекинд је 1877. године открио једну од најпознатијих слика у математици: црно-белу теселацију горње полуравни у хиперболичким троугловима - *Слика 2*.



Слика 2 - „Дедекиндова теселација”

Иако је позната под називом „Дедекиндова теселација”, не постоје слике те теселације у његовом раду из 1877. године. Такође, недостатак аргумената у његовом представљању ове теселације, као и коришћење чињеница које је раније користио Гаус, доводе до недоумица чија је заправо ово теселација.

2.2. Феликс Клајн

Феликс Клајн (1849 - 1925) је био немачки математичар, познат по своме раду на теорији група, теорији функција, нееуклидској геометрији и на повезивању геометрије са теоријом група. Његов „Ерланген програм”, којим је извршио класификацију геометрија на основу основних симетрија, има велики утицај и на данашњу математику и физику.

Клајн је 1879. године истраживао дејство $PSL(2,7)$, које је користио за даље експлицитно представљање Риманове површи.

У раду Феликса Клајна под називом „О трансформацији елиптичких функција и решењу једначина петог степена” из

1878. године појављује се прва слика „Дедекиндове теселације” - *Слика 3*. Додатно, Клајн укључује и појам оријентације као додатне вредности, које пружају јасно објашњење зашто се црни троуглови оријентишу у супротном смеру од казаљке на сату, док се бели троуглови оријентишу у смеру казаљке на сату. У свом представљању рада потврђује да је Дедекинд имао на уму ову слику када је писао рад 1877. године, али прву слику и адекватна објашњења добијамо захваљујући Феликсу Клајну.

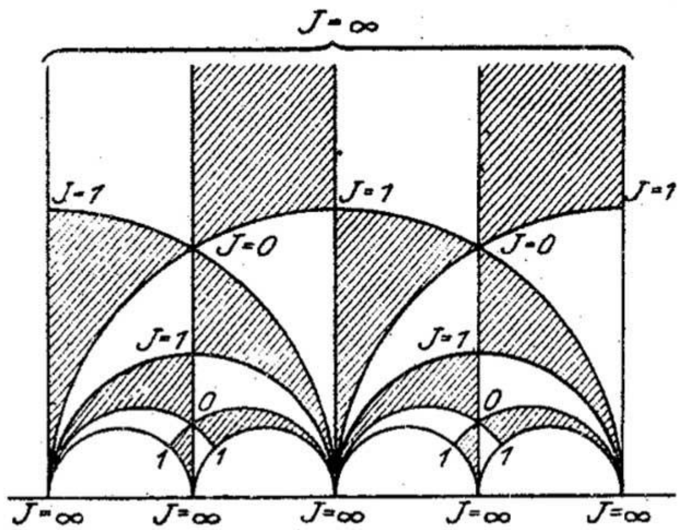


Fig. 7.

Слика 3 - Прва слика „Дедекиндове теселације”

У случају хиперболичке равни, теселације се могу конструисати коришћењем групе $SL_2(\boldsymbol{Z})$, која је математичка група са којом ћемо се упознати у наставку рада.

Група $SL_2(\boldsymbol{Z})$ има особине које омогућавају манипулацију хиперболичком равни и проучавање њених симетрија. Елементи ове групе имају одређене математичке особине које пружају методе за извођење трансформација равни, као што су ротација, рефлексија или транслација. Када се примене ове трансформације на одређену тачку или облик у равни, добијају се нове тачке које припадају истој орбити под дејством групе $SL_2(\boldsymbol{Z})$.

Теселација хиперболичке равни се формира тако што се плочице теселације поставе на такав начин да одговарају орбитама тачака под дејством групе $SL_2(\boldsymbol{Z})$. Ове орбите често имају симетричне облике који се понављају у теселацији. Конкретни елементи у групи $SL_2(\boldsymbol{Z})$ могу бити повезани са одређеним симетричним облицима или трансформацијама у теселацији.

Група $SL_2(\boldsymbol{Z})$ пружа алгебарску структуру и математички оквир за проучавање симетрија теселација хиперболичке равни. Кроз анализу елемената групе и њихових дејстава на тачке у равни, могуће је боље разумети симетрије и карактеристике теселација хиперболичке равни.

Глава 3

Теоријски оквир

3.1. Дефиниција групе

Нека је G непразан скуп и нека је $\cdot: G \cdot G \rightarrow G$ бинарна операција на њему. Тада алгебарску структуру $(G,\cdot)$ зовемо групоид. Групоиди могу имати одређена додатна својства која су од интереса за посебно проучавање, на пример:

(i) Групоид $(G,\cdot)$ је асоцијативан уколико за све $a, b, c \in G$ важи

$$(a \cdot b) \cdot c = a \cdot (b \cdot c).$$

Асоцијативни групоиди се још зову и полугрупе.

(ii) Групоид $(G,\cdot)$ има јединицу ако постоји елемент $1 \in G$ (који је, као што се лако види, нужно јединствен) тако да

$$1 \cdot a = a \cdot 1 = a,$$

важи за све $a \in G$. Полугрупе са јединицом се називају моноиди.

(iii) Нека је $(G,\cdot)$ групоид са јединицом 1. За елемент $a \in G$ кажемо да је инвертибилан ако постоји $b \in G$ тако да је

$$b \cdot a = a \cdot b = 1.$$

За елемент b кажемо да је инверз елемента a. Веома се лако показује да је инверз елемента a, ако постоји, јединствен, па има смисла да се тај инверз означи са a^{-1} (будући да је он једнозначно одређен елементом a).

Дефиниција 3.1.1. Група је моноид у којем је сваки елемент инвертибилан.

За дату групу G и $a \in G$ може се догодити да је неки степен елемента a једнак јединици, $a^n = 1$. Уколико постоји, најмањи позитиван цео број n са овом особином зовемо ред елемента a у G. У супротном, ако такво n не постоји, кажемо да је елемент a бесконачног реда.

Ред групе је кардинал $|G|$. Према томе, разликујемо коначне и бесконачне групе. Групе које задовољавају $ab = ba$ за све $a, b \in G$ зовемо Абелове групе.

3.2. Групе матрица

Нека је α линеарна трансформација, тј. ендоморфизам векторског простора V коначне димензије n над пољем $\boldsymbol{F}$. Претпоставимо да смо фиксирали једну базу $e_1, \dots, e_n$ векторског простора V. Посматрајмо слике ових базних елемената у односу на α; тада постоје коефицијенти $a_{ij} \in \boldsymbol{F}$, $1 \leq i, j \leq n$, тако да важи

$$\alpha(e_j) = \sum_{i=1}^{n} a_{ij} e_i.$$

Тада, ако узмемо произвољан вектор $x = x_1 e_1 + \cdots + x_n e_n$, добијамо

$$\alpha(x) = \sum_{j=1}^{n} x_j \alpha(e_j) = \sum_{j=1}^{n} x_j \sum_{i=1}^{n} a_{ij} e_i = \sum_{i=1}^{n} \left(\sum_{j=1}^{n} a_{ij} x_j\right) e_i,$$

што значи да ако сваки елемент x горњег облика идентификујемо са вектор-колоном $(x_1, \dots, x_n)^T$, тада α поприма облик

$$\alpha(x) = \mathrm{A}x,$$

где је матрица $\mathrm{A} = (a_{ij})$. При томе, ако ендоморфизму β одговара матрица B, тада је

$$\alpha(\beta(x)) = \mathrm{A}Bx,$$

одакле следи да је $End(V)$, моноид ендоморфизама од векторског простора V, изоморфан са пуним матричним моноидом $M_n(\boldsymbol{F})$ свих матрица димензија $n \times n$ над пољем $\boldsymbol{F}$. У том изоморфизму, група инвертибилних елемената $End(V)^X = Aut(V)$ (тј. група аутоморфизама од V) одговара колекцији свих матрица над $\boldsymbol{F}$ чија је детерминанта инвертибилни елемент у $\boldsymbol{F}$ (у случају поља, било који ненула елемент). Дакле, ради се о групи свих регуларних (инвертибилних) $n \times n$ матрица, коју зовемо општа линеарна група и означавамо са $GL_n(\boldsymbol{F})$. Ако се ограничимо само на матрице чија је детерминанта једнака 1, добијамо подгрупу од $GL_n(\boldsymbol{F})$ коју зовемо специјална линеарна група, у ознаци $SL_n(\boldsymbol{F})$.

3.3. Изоморфизми и аутоморфизми

Нека су $(G_1,\cdot)$ и $(G_2,*)$ групе. За G_1 и G_2 кажемо да су изоморфне, у ознаци $G_1 \cong G_2$, ако постоји бијекција $\varphi : G_1 \to G_2$ таква да за све $a, b \in G_1$ важи

$$\varphi(a \cdot b) = \varphi(a) * \varphi(b).$$

3.4. Дефиниција подгрупе

Пропозиција 3.4.1. Нека је G група и H њен непразан подскуп. Тада је H подгрупа од G ако и само ако важе услови:

(1) за све $a, b \in H$ важи $ab \in H$;

(2) $1 \in H$;

(3) за све $a \in H$ важи $a^{-1} \in H$.

3.5. Генераторни скупови

Пропозиција 3.5.1. Нека је $\{H_i : i \in I\}$ произвољна непразна фамилија подгрупа групе G. Тада је и

$$H = \bigcap_{i \in I} H_i$$

такође подгрупа од G. За сваки подскуп $\mathrm{A} \subseteq G$ постоји најмања подгрупа од G (у смислу скуповне инклузије) која садржи A; наиме, то је

$$\bigcap_{A \subseteq H \leq G} H.$$

За ову подгрупу кажемо да је подгрупа генерисана скупом A, и означавамо је са ⟨A⟩.

Пропозиција 3.5.2. Нека је G група и $\mathrm{A} \subseteq G$. Ако је A празан скуп, онда са E означимо $\langle \emptyset \rangle = E$. У случају да је A непразан скуп , тада је:

$$\langle A\rangle = \{a_1^{\varepsilon_1} \dots a_n^{\varepsilon_n} : n \geq 1, a_i \in A, \varepsilon_i \in \{-1,1\} \text{ за све } 1 \leq i \leq n\}.$$

Уколико је $\langle A\rangle = G$ кажемо да је A генераторни скуп групе G. Група је коначно генерисана ако има коначан генераторни скуп.

3.6. Косети и индекс подгрупе

Нека је $H \leq G$ и $g \in G$. Скуп облика $H\{g\}$ (који краће пишемо Hg) зовемо десни косет подгрупе H. Аналогно дефинишемо и леви косет gH подгрупе H у G.

3.7. Нормалне подгрупе

За подгрупу H групе G кажемо да је нормална, у ознаци $H \trianglelefteq G$, ако за све $g \in G$ важи

$$gH = Hg,$$

тј. ако се сваки леви косет од H поклапа са одговарајућим десним косетом. Група је проста ако не садржи нетривијалне нормалне подгрупе (различите од E и G, које су увек нормалне).

3.8. Дејство групе на скуп

Дејство групе G на непразан скуп X је пресликавање $\theta : X \times G \to X$ (при чему, ради прегледности, $\theta(x,g)$ понекад краће пишемо као x^g) које задовољава услове

$$(x^g)^h = x^{gh} \qquad \text{и} \qquad x^1 = x,$$

за све $x \in X$, $g, h \in G$.

Нека је G група и θ њено дејство на скуп X. На скупу X дефинишемо релацију $\sim$ на следећи начин:

$$x \sim y \Leftrightarrow y = x^g \text{ за неко } g \in G.$$

Лако се показује да је $\sim$ релација еквиваленције на X. Класу еквиваленције елемента $x \in X$ зовемо орбита од x и означавамо са x^G. Дакле,

$$x^G = \{x^g : g \in G\}.$$

За $x \in X$, скуп

$$G_x = \{g \in G : x^g = x\}$$

називамо стабилизатор елемента x.

3.9. Композициони низови и теорема Жордан-Хелдера

Нека је G произвољна група. Низ подгрупа од G који задовољава

$$E = H_n \lhd H_{n-1} \lhd \cdots \lhd H_0 = G$$

се назива нормални низ групе G (дужине n). При томе, нотација $H_{i+1} \lhd H_i$ означава да је $H_{i+1} \trianglelefteq H_i$ и $H_{i+1} \neq H_i$. Приметимо да се при томе од подгрупа H_k (осим, наравно, H_1) не тражи да буду нормалне у G, већ само у претходном члану низа, H_{k-1}. Групе $H_i \,/\, H_{i+1}$, $0 \le i \le n-1$, се називају фактори посматраног нормалног низа. Ако је за све $0 \le i \le n-1$, H_{i+1} максимална нормална подгрупа од H_i, другим речима, ако су сви фактори просте групе, тада нормални низ $E = H_n \lhd H_{n-1} \lhd \cdots \lhd H_0 = G$ зовемо композициони низ групе G.

За нормалне низове

$$E = H_n \lhd H_{n-1} \lhd \cdots \lhd H_0 = G$$

и

$$E = K_m \lhd K_{m-1} \lhd \cdots \lhd K_0 = G$$

кажемо да су еквивалентни ако је $n = m$ и при томе постоји пермутација π скупа $\{0,1,\dots,n-1\}$ тако да је $H_i \,/\, H_{i+1} \cong K_{\pi(i)} \,/\, K_{\pi(i)+1}$ за све $0 \le i \le n-1$.

Теорема 3.9.1. (Теорема Жордан-Хелдера) Свака два композициона низа групе G су еквивалентна.

Глава 4

Група матрица $SL_2(Z)$

Група $SL_2(\boldsymbol{Z})$ се састоји од свих матрица 2×2 чији су коефицијенти цели бројеви, а детерминанта једнака 1. Другим речима, то је група са основним скупом:

$$\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \boldsymbol{Z}, ad - bc = 1\right\}.$$

Група $SL_2(\boldsymbol{Z})$ лежи дискретно у $SL_2(\boldsymbol{R})$ и има улогу донекле сличну оној коју има $\boldsymbol{Z}$ унутар $\boldsymbol{R}$. Она је основни пример дискретне неабелове групе. Два посебна примера елемената у $SL_2(\boldsymbol{Z})$ су:

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

Матрица S има ред 4 ($S^2 = -I_2$), док T има бесконачан ред $\left(T^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}\right)$ и $ST = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$ има ред 6 ($(ST)^3 = -I_2$).

Теорема 4.1. Матрице S и T генеришу $SL_2(\boldsymbol{Z})$.

Након доказивања ове теореме проћи ћемо неколико последица и разматраћемо подгрупе коначног индекса у $SL_2(\boldsymbol{Z})$.

Доказ:

Нека је $G = \langle S, T\rangle$ подгрупа од $SL_2(\boldsymbol{Z})$ која је генерисана са S и T. Даћемо два доказа да је $G = SL_2(\boldsymbol{Z})$, један алгебарски, а други геометријски.

Алгебарски доказ почињемо тако што ћемо записати ефекат S и T^n на уопштену матрицу множењем са леве стране:

$$S\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} -c & -d \\ a & b \end{pmatrix}, \; T^n\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a + nc & b + nd \\ c & d \end{pmatrix}. \tag{4.1}$$

G је подгрупа од $SL_2(\boldsymbol{Z})$. Доказујемо да је $SL_2(\boldsymbol{Z})$ подгрупа од G. Нека је $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ произвољни елемент из $SL_2(\boldsymbol{Z})$. Претпоставимо да је $c \neq 0$. Ако је $|a| \geq |c|$, дељењем a са c добија се: $a = cq + r$, где је $0 \leq r < |c|$. Према (4.1), $T^{-q}\gamma$ има горњи леви елемент $a - qc = r$, који је мањи од доњег левог елемента c у $T^{-q}\gamma$. Применом S мењају се елементи a са c, b са d, горњи елементи супротног знака, па затим применимо алгоритам дељења у $\boldsymbol{Z}$ ако је доњи леви елемент различит од нуле у циљу тражења степена од T множењем са леве стране тако да доњи леви елемент има мању апсолутну вредност него раније. Множењем γ довољним бројем пута са S и степеном T добија се матрица из $SL_2(\boldsymbol{Z})$ која има доњи леви елемент нулу. Таква матрица, пошто има детерминанту 1 је облика $\begin{pmatrix} \pm 1 & m \\ 0 & \pm 1 \end{pmatrix}$ где је m неки цео број и где су јединице на главној дијагонали истог знака. Ова матрица је T^m или $-T^{-m}$, тако да постоји неко $g \in G$ такво да је $g\gamma = \pm T^n$ за неко $n \in \boldsymbol{Z}$. Одатле следи да је $SL_2(\boldsymbol{Z})$ подгрупа од G, па је $SL_2(\boldsymbol{Z}) = G$.

У овом алгебарском доказу G дејствује на $SL_2(\boldsymbol{Z})$ са операцијом множења са леве стране.

За <u>геометријски доказ</u> узећемо групу $GL_2^+(\boldsymbol{R})$ (група инвертибилних 2×2 матрица са реалним коефицијентима и позитивном детерминантом) која дејствује на горњу комплексну полураван $\mathfrak{h} = \{x + iy : y > 0\}$ билинеарним транформацијама. За $\tau \in \mathfrak{h}$ дефинишимо:

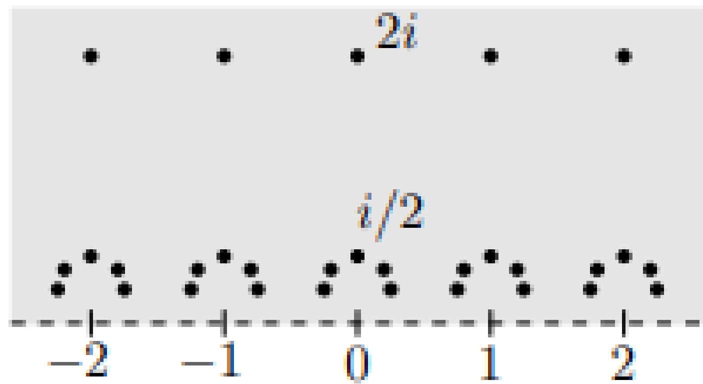
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \tau = \frac{a\tau + b}{c\tau + d}.$$

Мотив за ово је то што се у $\mathfrak{h}$ имагинарни део може изразити као:

$$Im\left(\frac{a\tau + b}{c\tau + d}\right) = \frac{(ad - bc)\, Im(\tau)}{|c\tau + d|^2}, \tag{4.2}$$

при чему је $\tau \in \mathbf{C} - \left\{-\frac{d}{c}\right\}$ и a, b, c, d су реални бројеви. Ако $\tau \in \mathfrak{h}$ и $ad - bc > 0$ тада $\frac{a\tau+b}{c\tau+d} \in \mathfrak{h}$. Да би визуелно приказали како група $GL_2^+(\boldsymbol{R})$ дејствује на $\mathfrak{h}$, треба показати да је $I_2\tau = \tau$ и $A(B\tau) = (AB)\tau$ за све A и B из $GL_2^+(\boldsymbol{R})$. Овакво дејство не прави разлику између матрица различитог знака (γ и $-\gamma$ дејствују на $\mathfrak{h}$ на исти начин), али ово неће бити проблем за примену овог дејства за доказивање $G = SL_2(\boldsymbol{Z})$ јер је $-I_2 = S^2 \in G$.

Кључна идеја геометријског доказа је то да када $SL_2(\boldsymbol{Z})$ дејствује на тачку у $\mathfrak{h}$, доводи до тога да се њена орбита приближава x-оси. Ово је илустровано на *Слици 4*, која приказује тачке у $SL_2(\boldsymbol{Z})$ које су орбите од $2i$ (укључујући $S(2i) = -\frac{1}{2i} = \frac{i}{2}$).



Слика 4: Илустрација скупа тачака у $SL_2(\mathbf{Z})$ које представљају орбиту од 2i

На основу слике, нека је γ произвољан елемент из $SL_2(\mathbf{Z})$ и узмимо да је $\tau := \gamma(2i)$.

За $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ из G, при чему је $ad - bc = 1$, а на основу (4.2), добија се:

$$Im\,(g\tau) = \frac{Im\,(\tau)}{|c\tau + d|^2}. \tag{4.3}$$

Уведимо да је $\tau = x + iy$. Тада именилац из (4.3) постаје:

$$|c\tau + d|^2 = (cx + d)^2 + (cy)^2,$$

а пошто је $y \neq 0$, онда постоји само коначно много целих бројева c и d за које важи да је $|c\tau + d|$ мањи од задате границе. Овде се узима τ да је фиксно, а c и d се могу мењати. Због тога, $Im\,(g\tau)$ има максималну вредност када g узима вредности из G (за фиксно τ) на основу чега се може претпоставити да постоји неко $g_0 \in G$ такво да:

$$Im\,(g\tau) \leq Im\,(g_0\tau),$$

за све $g \in G$.

Пошто је $Sg_0 \in G$, а по особини максималног елемента следи да је $Im\left((Sg_0)\tau\right) \leq Im\,(g_0\tau)$ и са $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = S$ добија се:

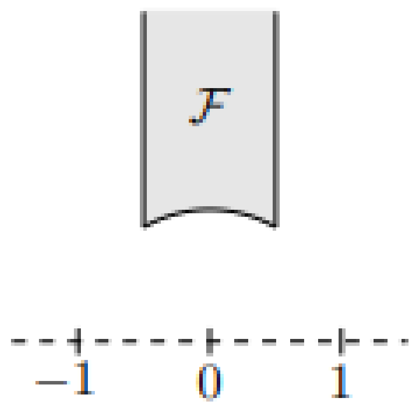
$$Im\left((Sg_0)\tau\right) = \frac{Im\,(g_0\tau)}{|g_0\tau|^2} \leq Im\,(g_0\tau).$$

Одавде је $|g_0\tau|^2 \geq 1$ па је и $|g_0\tau| \geq 1$. Пошто је $Im\,(T^n g_0\tau) = Im\,(g_0\tau)$ и $T^n g_0 \in G$, заменом $g_0\tau$ са $T^n g_0\tau$ и сређивањем као са матрицом S, може се показати да је $|T^n g_0\tau| \geq 1$ за све $n \in \mathbf{Z}$.

Примена T (или T^{-1}) на $g_0\tau$ промениће његов реални део за 1 (или за -1) без да утиче на његов имагинарни део. За неко n, $T^n g_0\tau$ има реални део између $\frac{1}{2}$ и $-\frac{1}{2}$. Применом тог степена од T може се показати да G–орбита од $\tau = \gamma(2i)$ има елементе у скупу:

$$F = \left\{\tau \in \mathfrak{h}: |Re(\tau)| \le \frac{1}{2}, |\tau| \ge 1\right\}. \tag{4.4}$$

Види *Слику 5*. Напомињемо да је $Im(\tau) \ge \frac{\sqrt{3}}{2} > \frac{1}{2}$ за све $\tau \in F$.



Слика 5: Илустрација фундаменталног домена

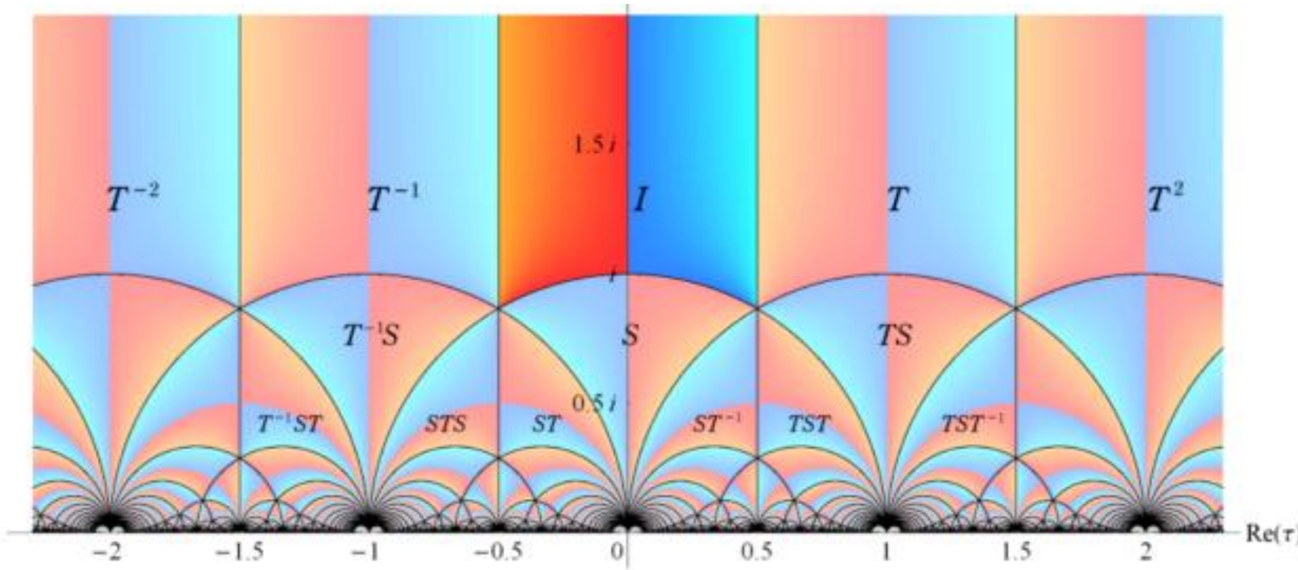
За γ из $SL_2(\boldsymbol{Z})$ показано је да постоји $g \in G$ такво да је $g(\gamma(2i)) = g\gamma(2i)$ из F. Из овога следи да је:

$$g\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\boldsymbol{Z}) \Rightarrow Im((g\gamma)(2i)) = \frac{2}{4c^2 + d^2} \ge \frac{\sqrt{3}}{2},$$

па је $c = 0$ $\left(\text{јер је } \frac{2}{4} = \frac{1}{2} < \frac{\sqrt{3}}{2}\right)$. Тада је $ad = 1$, па је $a = d = \pm 1$ и $(g\gamma)(2i) = \frac{a(2i)+b}{d} = 2\mathrm{i} \pm b$. Да би $Re((g\gamma)(2i)) \in \left[-\frac{1}{2}, \frac{1}{2}\right]$ морамо узети $b = 0$, па је $g\gamma = \pm I_2$. Одавде је $\gamma = \pm g^{-1}$, а пошто је $-I_2 = S^2 \in G$, добија се $\gamma \in G$. ∎

Област F на *Слици 5* назива се фундаментални домен за дејство $SL_2(\boldsymbol{Z})$ на $\mathfrak{h}$. То је аналогно интервалу [0,1] који је фундаментални домен за дејство транслације $\boldsymbol{Z}$ на $\boldsymbol{R}$: свака тачка у простору $\mathfrak{h}$ или $\boldsymbol{R}$ има тачку своје орбите (од $SL_2(\boldsymbol{Z})$ или $\boldsymbol{Z}$) у фундаменталном домену (F или [0,1]) и све тачке фундаменталног домена које припадају истој орбити леже на граници.

На *Слици 6* је дата декомпозиција $\mathfrak{h}$ на транслације $\gamma(F)$ када γ пролази кроз $SL_2(\boldsymbol{Z})$, са $\gamma = I_2$ која одговара F.



Слика 6: Транслације којима је покривен простор $\mathfrak{h}$ *(теселација хиперболичке равни)*

Различите транслације преклапају се само преко ивичних кривих, и како се приближавамо x-оси, $\mathfrak{h}$ се попуњава са бесконачно много ових транслација. Фундаментални домен и слике његових транслација се називају идеални троуглови зато што су ограничени са 3 ивице и имају 2 темена који су у $\mathfrak{h}$ и једно које није у $\mathfrak{h}$ – оно је или рационалан број на x-оси или је $i\infty$.

Пример 4.1. Помоћу алгебарског доказа теореме 4.1. изразимо матрицу $A = \begin{pmatrix} 17 & 29 \\ 7 & 12 \end{pmatrix}$ помоћу матрица S и T.

Пошто је $17 = 7 \cdot 2 + 3$, од 17 морамо одузети $7 \cdot 2$. Други елемент у првом реду постаје $29 - 2 \cdot 12 = 5$:

$$T^{-2}A = \begin{pmatrix} 3 & 5 \\ 7 & 12 \end{pmatrix}.$$

Затим треба заменити елементе 3 и 7 множењем са S:

$$ST^{-2}A = \begin{pmatrix} -7 & -12 \\ 3 & 5 \end{pmatrix}.$$

Дељењем -7 са 3, имамо $-7 = 3 \cdot (-3) + 2$, значи на -7 треба додати $3 \cdot 3$, то се постиже множењем са T^3:

$$T^3ST^{-2}A = \begin{pmatrix} 2 & 3 \\ 3 & 5 \end{pmatrix}.$$

Поново множимо са S да би заменили елементе прве колоне:

$$ST^3ST^{-2}A = \begin{pmatrix} -3 & -5 \\ 2 & 3 \end{pmatrix}.$$

Пошто је $-3 = 2 \cdot (-2) + 1$:

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

Множењем са S:

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

Пошто је $-2 = 1 \cdot (-2) + 0$, множењем са $T^{\,2}$:

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

Множењем са S:

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

Изражавање A:

$$ST^{\,2}ST^2ST^3ST^{-2}A = S^2T,$$

$$\begin{pmatrix} 17 & 29 \\ 7 & 12 \end{pmatrix} = A = (ST^{\,2}ST^2ST^3ST^{-2})^{-1}S^2T,$$

$$\mathrm{A} = (ST^{\,2}ST^2ST^3ST^{-2})^{-1}S^2T = T^2S^{-1}T^{-3}S^{-1}T^{-2}S^{-1}T^{-2}S^{-1}S^2T = T^2ST^{-3}ST^{-2}ST^{-2}ST,$$

јер је $S^{-1} = S$.

Напомена 4.1. Рад са верижним разломцима је уско повезан са множењем матрицама S и T. Да бисмо показали како добити матрицу изражену преко S и T, посматрајмо однос елемената у првој колони $\frac{17}{7}$ из примера 4.1.:

$$\frac{17}{7} = 3 - \frac{4}{7} = 3 - \frac{1}{\frac{7}{4}} = 3 - \frac{1}{2 - \frac{1}{4}}.$$

Коришћењем бројева 3, 2 и 4 као експоненте T, добија се матрица:

$$T^3ST^2ST^4S = \begin{pmatrix} 17 & -5 \\ 7 & -2 \end{pmatrix},$$

чија је прва колона иста као у почетној. Да бисмо добили другу колону, рачунамо:

$\begin{pmatrix} 17 & 29 \\ 7 & 12 \end{pmatrix} = \begin{pmatrix} 17 & -5 \\ 7 & -2 \end{pmatrix} M$, за $M = \begin{pmatrix} 17 & -5 \\ 7 & -2 \end{pmatrix}^{-1} \cdot \begin{pmatrix} 17 & 29 \\ 7 & 12 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} = T^2$, тако да:

$$\begin{pmatrix} 17 & 29 \\ 7 & 12 \end{pmatrix} = \begin{pmatrix} 17 & -5 \\ 7 & -2 \end{pmatrix} T^2 = T^3ST^2ST^4ST^2.$$

Ово је другачији израз за $\begin{pmatrix} 17 & 29 \\ 7 & 12 \end{pmatrix}$ него што смо раније добили.

Последица 4.1. Група $SL_2(\boldsymbol{Z})$ је генерисана двема матрицама коначног реда.

Доказ:

Имамо да је $SL_2(\boldsymbol{Z}) = \langle S, T \rangle = \langle S, ST \rangle$, где $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ има ред 4 и $ST = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$ има ред 6. ■

Последица 4.2. Сваки хомоморфизам $SL_2(\boldsymbol{Z}) \to \boldsymbol{C}^x$ има слику у 12. корену јединице.

Доказ:

По претходној последици $SL_2(\boldsymbol{Z})$ је генерисана матрицом S реда 4 и матрицом ST чији је ред 6. Међутим, хомоморфизам $SL_2(\boldsymbol{Z}) \to \mathbf{C}^x$ има слику у подгрупи генерисаној са μ_4 и μ_6, што је подгрупа генерисана са μ_{12}.

У овом контексту, симбол μ представља групу комплексних јединичних бројева. Група комплексних јединичних бројева обухвата све комплексне бројеве чија је апсолутна вредност једнака 1, тј. све бројеве који леже на јединичној кружници у комплексној равни.

На пример, μ_{12} представља групу у којој је сваки елемент 12. корен јединице. ■

Пример 4.2. Као илустрацију последице 4.2., наводимо пример хомоморфизма $\chi: SL_2(\boldsymbol{Z}) \rightarrow \boldsymbol{C}^x$ чије су све слике у 12. корену јединице:

$$\chi\begin{pmatrix} a & b \\ c & d \end{pmatrix} = e^{\frac{2\pi i}{12}\left((1-c^2)(bd+3(c-1)d+c+3)+c(a+d-3)\right)}.$$

На пример, $\chi(S) = -i$, $\chi(T) = e^{\frac{2\pi i}{12}} = -i\left(\frac{-1+\sqrt{3}i}{2}\right)$.

За $\tau \in \mathfrak{h}$ функција $\Delta(\tau) = e^{2\pi i\tau}\prod_{n\geq 1}\left(1-e^{2\pi in\tau}\right)^{24}$ задовољава $\Delta(\gamma\tau) = (c\tau+d)^{12}\Delta(\tau)$ за све $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ из $SL_2(\boldsymbol{Z})$ и њен 12. корен $f(\tau) = e^{\frac{2\pi i\tau}{12}}\prod_{n\geq 1}\left(1-e^{2\pi in\tau}\right)^2$ задовољава $f(\gamma\tau) = \chi(\gamma)(c\tau+d)f(\tau)$ за све $\gamma \in SL_2(\boldsymbol{Z})$.

Последица 4.3. Група $SL_2(\boldsymbol{Z})$ је генерисана матрицама $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ и $U = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$.

<u>Доказ:</u>

Обе матрице T и U су из $SL_2(\boldsymbol{Z})$, тако да $\langle T, U\rangle \subset SL_2(\boldsymbol{Z})$. Обрнуто, пошто је $S = T^{-1}UT^{-1}$, $\langle T, U\rangle \supset \langle S, T\rangle = SL_2(\boldsymbol{Z})$. ■

Теорема 4.2. Елементи коначног реда из $SL_2(\boldsymbol{Z})$ имају ред 1, 2, 3, 4 или 6.

<u>Доказ:</u>

Следећи примери потврђују постојање елемената наведених редова: I_2 има ред 1, $-I_2$ има ред 2, S има ред 4, ST има ред 6, $(ST)^2$ има ред 3.

Претпоставимо да $A \in SL_2(\boldsymbol{Z})$ има коначан ред n, тако да је $A^n - I_2 = O$. Треба да покажемо да n може бити 1, 2, 3, 4 или 6. Пошто је A матрица 2×2 са детерминантом 1, њен карактеристични полином је: $X^2 - tX + 1$, где је t траг матрице A. Кејли–Хамилтонова теорема тврди да је $A^2 - tA + I_2 = O$. Пошто A задовољава обе једначине $X^n - 1$ и $X^2 - tX + 1$, мора да задовољава и њихов највећи заједнички делилац НЗД ($X^n - 1$, $X^2 - tX + 1$). Тај НЗД има ограничен број могућности јер је t коначно: t је сума карактеристичних вредности матрице A који су корени из 1, а пошто је A коначног реда, тада је $|t| \leq 2$.

Случај 1: ($t = 2$). Пошто $X^n - 1$ има различите корене и $X^2 - 2X + 1 = (X-1)^2$, имамо да је НЗД $(X^n - 1, X^2 - 2X + 1) = X - 1$. Одавде је $A - I_2 = O$, па је $A = I_2$, чији је ред 1.

Случај 2: ($t = -2$). Пошто $X^n - 1$ има различите корене и $X^2 + 2X + 1 = (X+1)^2$, имамо да је НЗД $(X^n - 1, X^2 + 2X + 1) = X + 1$ ако је n парно и НЗД $(X^n - 1, X^2 + 2X + 1) = 1$, ако је n непарно. С обзиром на особине матрице A и њеног карактеристичног полинома (објашњено на почетку доказа), остаје да НЗД мора бити $X + 1$. Одавде је $A + I_2 = O$, па је $A = -I_2$, чији је ред 2.

Случај 3: ($t = 1$). Пошто је $X^2 - X + 1$ фактор од $X^3 + 1 = (X+1)(X^2 - X + 1)$, имамо да је $A^3 = -I_2$, па је $A^6 = I_2$. Пошто је $A^2 - A + I_2 = O$, не може бити $A^2 = I_2$, па је ред 6.

Случај 4: ($t = -1$). Пошто је $X^2 + X + 1$ фактор од $X^3 - 1 = (X-1)(X^2 + X + 1)$, имамо да је $A^3 = I_2$. Пошто је $A^2 + A + I_2 = O$, не може бити $A = I_2$, па је ред 3.

Случај 5: ($t = 0$). У овом случају $A^2 = -I_2$, па је $A^4 = I_2$, те A има ред 4. ■

Напомена 4.2. Очигледно је I_2 једина матрица у $SL_2(\boldsymbol{Z})$ реда 1. Доказ теореме 4.2. показује да је $-I_2$ једина матрица у $SL_2(\boldsymbol{Z})$ реда 2. У ствари, $-I_2$ је једина матрица у $SL_2(\boldsymbol{R})$ реда 2. Што се тиче конјугација у $SL_2(\boldsymbol{Z})$: матрице реда 3 су конјуговане са $\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$ или са $\begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$, матрице реда 4 су конјуговане са $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ или $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, а матрице реда 6 су конјуговане са $\begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$ или са $\begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}$.

Глава 5

Конгруентне подгрупе $SL_2(Z)$

Група $SL_2(\boldsymbol{Z})$ има неколико специфичних подгрупа које су важне у теорији група и математичкој физици. У теорији група, посебно у контексту групе $SL_2(\boldsymbol{Z})$, од изузетне важности су конгруентне подгрупе, које су дефинисане својством да садрже елементе који су конгруентни по модулу одређеном целом броју.

Основни начин проналажења подгрупа од $SL_2(\boldsymbol{Z})$ са коначним индексом је преко коначних група $SL_2(\boldsymbol{Z}/(N))$, где је N цео број.

За сваки цео број $N > 1$ природно пресликавање $SL_2(\boldsymbol{Z}) \to SL_2(\boldsymbol{Z}/(N))$ је хомоморфизам са језгром:

$$\Gamma(N) = ker\,(SL_2(\boldsymbol{Z}) \ \to \ SL_2(\boldsymbol{Z}/(N))) = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} mod\ N\right\}.$$

Наравно, ова подгрупа је дефинисана и за $N = 1$, $\Gamma(1) = SL_2(\boldsymbol{Z})$. Свако $\Gamma(N)$ има коначан индекс у $SL_2(\boldsymbol{Z})$, пошто се $SL_2(\boldsymbol{Z})/\Gamma(N)$ пројектује у $SL_2(\boldsymbol{Z}/(N))$, па свака подгрупа од $SL_2(\boldsymbol{Z})$, која садржи неко $\Gamma(N)$ има коначан индекс.

Подгрупа из $SL_2(\boldsymbol{Z})$ која садржи неко $\Gamma(N)$ назива се **конгруентна подгрупа**. Мотив за овакав назив је то да се таква подгрупа може описати коначним скупом конгруентних услова.

Теорема 5.1. Група $\Gamma(2) = \left\{A \in SL_2(\boldsymbol{Z}) : A \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod 2\right\}$ је генерисана матрицама $-I_2$, T^2 и U^2 где је:

$$T^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix},\ U^2 = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}.$$

Доказ:

Све наведене матрице $-I_2$, T^2 и U^2 су из $\Gamma(2)$, па $\langle -I_2, T^2, U^2\rangle \subset \Gamma(2)$. Да бисмо доказали обрнути смер, прилагодићемо алгебарски доказ да $SL_2(\boldsymbol{Z}) = \langle S, T\rangle$, тако што ћемо уместо обичне теореме о дељењу у $\boldsymbol{Z}$, користити модификовану теорему о дељењу у $\boldsymbol{Z}$ која гласи: ако је $a, b \in \boldsymbol{Z}$ са $b \neq 0$, тада је $a = bq + r$ где је $|r| \leq \frac{1}{2}|b|$.

Нека је $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(2)$ тако да су a и d непарни, а b и c парни. Ако A има доњи леви елемент 0, тада је $A = \pm\begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}$ за неко $m \in \boldsymbol{Z}$. Пошто је A из $\Gamma(2)$, m мора бити парно. Пишемо:

$$m = 2k, \qquad A = \pm\begin{pmatrix} 1 & 2k \\ 0 & 1 \end{pmatrix} = \pm T^{2k} \in \langle -I_2, T^2\rangle.$$

Ако доњи леви елемент матрице A није 0, помножићемо A са одговарајућим степеном T^2 или U^2 са леве стране да бисмо смањили вредност $max(|a|, |c|)$. Пошто су a и c супротне парности и $a \neq \pm c$, онда је $|a| \neq |c|$ и тада је $max(|a|, |c|)$ или $|a|$ или $|c|$, али не обоје.

Ако је $|a| > |c|$ и $c \neq 0$, пишемо $a = (2c)q + r$, где је $|r| \leq \left(\frac{1}{2}\right)|2c| = |c|$. Тада је

$T^{-2q}A = \begin{pmatrix} 1 & -2q \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} r & b-2qd \\ c & d \end{pmatrix}$, са $max(|r|, |c|) = |c| < |a| = max(|a|, |c|)$.

Ако је $|a| < |c|$, тада (пошто знамо да је $a \neq 0$ и a је непарно) пишемо $c = (2a)q + r$ где је $|r| \leq \left(\frac{1}{2}\right)|2a| = |a|$. Сада је $U^{-2q}A = \begin{pmatrix} 1 & 0 \\ -2q & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ r & d-2bq \end{pmatrix}$, са $max(|a|, |r|) = |a| < |c| = max(|a|, |c|)$.

Наизменичном применом претходна два корака за неко $g \in \langle T^2, U^2\rangle$ доњи леви елемент од gA је 0, тако да на основу горњих тврђења $gA \in \langle -I_2, T^2\rangle$. Одатле следи да $A = g^{-1}gA \in \langle -I_2, T^2, U^2\rangle$. ■

Теорема 5.2. Природно пресликавање $SL_2(\boldsymbol{Z}) \rightarrow SL_2(\boldsymbol{Z}/(N))$ је „на”.

Доказ:

Нека је $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ произвољна матрица из $SL_2(\boldsymbol{Z}/(N))$. Применом Кинеске теореме о остацима, може се показати да постоји $b' \equiv b \bmod N$, такво да су a и b' узајамно прости. Тада, пошто је НЗД $(a, b') = 1$, постоје x и y такви да је $ax - b'y = 1$. Користећи ове x и y, ставимо да је:

$$c' = c + y\big(1 - (ad - b'c)\big), \qquad d' = d + x\big(1 - (ad - b'c)\big).$$

Матрица $\begin{pmatrix} a & b' \\ c' & d' \end{pmatrix}$ је из $SL_2(\boldsymbol{Z})$ што се види кроз директну проверу и конгруентна је са $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ из $SL_2(\boldsymbol{Z}/(N))$ по модулу N. ■

Пример 5.1. Нека је $A = \begin{pmatrix} 18 & 14 \\ 4 & 2 \end{pmatrix}$ и њена детерминанта је $det\mathrm{A} = -20 \equiv 1 \; mod\, 21$. Наћи матрицу из $SL_2(\boldsymbol{Z})$ која се пресликава на A из $SL_2(\boldsymbol{Z}/(21))$.

Горња два елемента нису узајамно прости бројеви, али ако уместо 14 ставимо $14 + 21 = 35$ добијамо узајамно просте бројеве. Решења једначине $18x - 35y = 1$ су $x = 2$ и $y = 1$, па се добија:

$$\begin{pmatrix} 18 & 14 \\ 4 & 2 \end{pmatrix} \equiv \begin{pmatrix} 18 & 35 \\ 109 & 212 \end{pmatrix} mod\, 21$$

и друга матрица је из $SL_2(\boldsymbol{Z})$.

Последица 5.1. За све природне бројеве $N > 1$, $SL_2(\boldsymbol{Z})$ / $\Gamma(N) \cong SL_2(\boldsymbol{Z}/(N))$.

Доказ:

У доказу се користи теорема о хомоморфизму:

Теорема о хомоморфизму: Нека је $\varphi\colon G \to H$ хомоморфизам група. Тада је

$$G/Ker\varphi \cong \mathrm{Im}\varphi.$$

Imφ је слика хомоморфизма.

Ако дефинишемо хомоморфизам φ: $SL_2(\boldsymbol{Z}) \to SL_2(\boldsymbol{Z}/(N))$, односно φ пресликава матрице из групе $SL_2(\boldsymbol{Z})$ у одговарајуће класе еквиваленције у групи $SL_2(\boldsymbol{Z}/(N))$, тада је $\Gamma(N)$ језгро $Ker\varphi$ тог хомоморфизма.

Како је φ сирјективни хомоморфизам (теорема 5.2.), теорема о хомоморфизму имплицира да је група $SL_2(\boldsymbol{Z})$ / $Ker\varphi$ изоморфна групи Imφ, односно групи $SL_2(\boldsymbol{Z}/(N))$.

Дакле, користећи теорему о хомоморфизму, можемо закључити да је група $SL_2(\boldsymbol{Z})$ / $\Gamma(N)$ изоморфна групи $SL_2(\boldsymbol{Z}/(N))$. ■

Последица 5.2. Коначна група $SL_2(\boldsymbol{Z}/(N))$ је генерисана са два елемента реда N.

Доказ:

Пошто је $SL_2(\boldsymbol{Z})$ генерисана са два елемента $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ и $U = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ (последица 4.3.) природним пресликавањем се показује да је $SL_2(\boldsymbol{Z}/(N))$ генерисана сликама T и U које су обе реда N. Да су матрице реда N можемо видети у наставку:

$$T^N = \begin{pmatrix} 1 & N \\ 0 & 1 \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \, mod \, N,$$

$$U^N = \begin{pmatrix} 1 & 0 \\ N & 1 \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \, mod \, N. \blacksquare$$

Последица 5.3. У $SL_2(\boldsymbol{Z})$ подгрупа $\langle S, T^2 \rangle$ има индекс 3.

Доказ:

Почнимо са показивањем да је $\Gamma(2) \subset \langle S, T^2 \rangle$. По теореми 5.1. довољно је да покажемо да су три генератора $-I_2$, T^2, U^2 од $\Gamma(2)$ у $\langle S, T^2 \rangle$: $-I_2 = S^2$, $T^2 = T^2$, $U^2 = ST^{-2}S^{-1}$.

Индекс од $\langle S, T^2 \rangle$ у $SL_2(\boldsymbol{Z})$ се одређује применом $\Gamma(2)$ и израчунавањем индекса подгрупе генерисане са S и T^2 у $SL_2(\boldsymbol{Z})$ / $\Gamma(2)$ $\cong$ $SL_2(\boldsymbol{Z}/(2))$. Пошто је $T^2 \in \Gamma(2)$, $S \notin \Gamma(2)$ и $-I_2 = S^2 \in \Gamma(2)$, група $\langle S, T^2 \rangle / \Gamma(2)$ има ред 2, па је њен индекс у $SL_2(\boldsymbol{Z}/(2)$ једнак $\frac{6}{2} = 3$. $\blacksquare$

Ако уместо $\langle S, T^2 \rangle$ ставимо $\langle S, T^m \rangle$, $m > 2$, нема аналогне последице са последицом 5.3.: група $\langle S, T^m \rangle$ нема коначан индекс у $SL_2(\boldsymbol{Z})$.

Пример 5.2. Доказ последице 5.3. показује да је $\langle S, T^2 \rangle$ конгруентна подгрупа пошто је $\Gamma(2) \subset \langle S, T^2 \rangle$. Слика од $\langle S, T^2 \rangle$ у $SL_2(\boldsymbol{Z})$ / $\Gamma(2) \cong SL_2(\boldsymbol{Z}/(2))$ је $\{\overline{I_2}, \ \bar{S}\}$, тако да $\langle S, T^2 \rangle$ можемо описати са конгруентним условима по модулу 2:

$$\langle S, T^2 \rangle = \left\{ A \in SL_2(\boldsymbol{Z}) \colon A \ \equiv \ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ или } \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \, mod \, 2 \right\}.$$

Теорема 5.3. Комутатор подгрупа $SL_2(\boldsymbol{Z})'$ је конгруентна подгрупа са индексом 12.

Доказ:

Пошто је $SL_2(\boldsymbol{Z})$ генерисана матрицом S реда 4 и матрицом ST реда 6, где је $S^2 = (ST)^3 = -I_2$, абелизација $SL_2(\boldsymbol{Z})$ / $SL_2(\boldsymbol{Z})'$ је генерисана са $g = \bar{S}$ и $h = \overline{ST}$, где је $g^4 = 1$, $h^6 = 1$, $g^2 = h^3$. Због комутативности сваки елемент од $SL_2(\boldsymbol{Z})$ / $SL_2(\boldsymbol{Z})'$ има облик $g^i h^j$ где је $0 \leq i \leq 3$ и $0 \leq j \leq 5$. Због $g^2 = h^3$ можемо сузити вредности за i: $0 \leq i \leq 1$. Број таквих различитих $g^i h^j$ је највише 12, тако да $[SL_2(\boldsymbol{Z}) : SL_2(\boldsymbol{Z})'] \leq 12.$ (5.1)

Следеће ћемо показати да $SL_2(\boldsymbol{Z})$ има цикличну фактор групу реда 12. То имплицира да је $[SL_2(\boldsymbol{Z}) : SL_2(\boldsymbol{Z})']$ најмање 12, па је због (5.1) индекс једнак 12. Из конструкције фактор-групе види се да је $\Gamma(2) \subset SL_2(\boldsymbol{Z})'$.

Према последици 5.1. природно пресликавање $SL_2(\boldsymbol{Z}) \rightarrow SL_2(\boldsymbol{Z}/(N))$ је сирјекција за све N. Према Кинеској теореми о остацима:

$$SL_2(\boldsymbol{Z}/(12)) \cong SL_2(\boldsymbol{Z}/(3)) \times SL_2(\boldsymbol{Z}/(4)),$$

и комбинујући ово са редукцијом по модулу 12, добија се:

$$SL_2(\boldsymbol{Z}) \twoheadrightarrow SL_2(\boldsymbol{Z}/(3)) \times SL_2(\boldsymbol{Z}/(4)) \tag{5.2}$$

са језгром $\Gamma(12)$.

Сада ћемо показати да $SL_2(\boldsymbol{Z}/(3))$ има фактор групу реда 3 (сигурно цикличну) и да $SL_2(\boldsymbol{Z}/(4))$ има фактор групу реда 4. Комбиновањем овога са (5.2) добија се:

$$SL_2(\boldsymbol{Z}) \twoheadrightarrow SL_2(\boldsymbol{Z}/(3)) \times SL_2(\boldsymbol{Z}/(4)) \twoheadrightarrow \boldsymbol{Z}/(3) \times \boldsymbol{Z}/(4)$$

са цикличном групом реда 12 и $\Gamma(12)$ садржаним у језгру.

Група $SL_2(\boldsymbol{Z}/(3))$ има ред 24 и експлицитним рачунањем има 8 елемената који су другог степена. Међутим, група има јединствену 2-Силову подгрупу која мора бити нормална и $SL_2(\boldsymbol{Z}/(3))$ / {2-Силова} има ред $\frac{24}{8} = 3$. (2-Силова подгрупа је изоморфна са Q_8 и $\langle\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\rangle$ је комплементарна подгрупа реда 3, тако да $SL_2(\boldsymbol{Z}/3) \cong Q_8 \times \boldsymbol{Z}/(3)$.)

Група $SL_2(\boldsymbol{Z}/(4))$ има ред 48. У овој групи нека је $x = \begin{pmatrix} 3 & 2 \\ 0 & 3 \end{pmatrix}$ и $y = \begin{pmatrix} 3 & 0 \\ 2 & 3 \end{pmatrix}$. Тада је $xy = yx = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$. Ове три матрице имају ред 2, тако да подгрупа $H = \langle x, y\rangle = \{I_2, x, y, xy\}$ има ред 4. Матрица $z = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$ из $SL_2(\boldsymbol{Z}/(4))$ има ред 3, и нормализује H пошто је $zxz^{-1} = y$, $zyz^{-1} = xy$, $zxyz^{-1} = x$. Према томе, $N = \langle x, y, z\rangle = \langle z, H\rangle = \{z^i h : i \in \boldsymbol{Z}, h \in H\}$ је подгрупа реда 12 и индекса 4.

Подгрупа N је нормална у $SL_2(\boldsymbol{Z}/(4))$. Да би доказали ово, довољно је показати да је $gNg^{-1} \subset N$, где за g треба узети $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ и $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, пошто ове две матрице генеришу $SL_2(\boldsymbol{Z}/(4))$ према доказу последице (3.2.). Ако је $g = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, тада је $gxg^{-1} = x,\ gyg^{-1} = xy$ и $gzg^{-1} = \begin{pmatrix} 3 & 3 \\ 1 & 0 \end{pmatrix} = z^2x$, а ако је $g = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ тада је $gxg^{-1} = xy, gyg^{-1} = y$ и $gzg^{-1} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} = z^2y$.

Фактор група $SL_2(\boldsymbol{Z}/(4))/N$ има ред $\frac{48}{12} = 4$. Прво ћемо показати да је фактор група циклична. Директним израчунавањем, свих 8 елемената групе $N\ /\ H$ су реда 3, тако да је H јединствена 2-Силова подгрупа од N. Подгрупа $\langle\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\rangle$ од $SL_2(\boldsymbol{Z}/(4))$ је циклична реда 4 и има тривијалан пресек са H, тако да има тривијалан пресек и са N. Одавде је $SL_2(\boldsymbol{Z}/(4))/N \cong \langle\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\rangle \cong \boldsymbol{Z}/(4)$. Има 5 група реда 12 које су изоморфне и само једна подгрупа која је реда 3, а то је A_4, тако да је $N \cong A_4$. Одавде је $SL_2(\boldsymbol{Z}/(4)) \cong A_4 \times \boldsymbol{Z}/(4)$. ∎

За $n \geq 2$ подгрупа од $SL_n(\boldsymbol{Z})$ се назива конгруентна подгрупа ако за неко $N \in \boldsymbol{Z}^+$ она садржи језгро природног пресликавања (које је „на”). У случају $n = 2$, све конгруентне подгрупе од $SL_n(\boldsymbol{Z})$ имају коначан индекс.

Међу подгрупама са коначним индексом у $SL_2(\boldsymbol{Z})$ посебно су важне конгруентне подгрупе у примени у теорији бројева због њихове улоге у модуларним формама.

Глава 6

Примена

Група $SL_2(\boldsymbol{Z})$ има значајну улогу у различитим математичким дисциплинама. Три примера су теорија бројева, теорија група и хиперболичка геометрија.

6.1. Теорија бројева

6.1.1. Теорија квадратних форми

Група $SL_2(\boldsymbol{Z})$ се користи у проучавању квадратних форми и њихових особина. Квадратне форме су изрази облика $ax^2 + bxy + cy^2$, где су a, b и c цели бројеви. Проучавање решења квадратних форми је важно у теорији бројева, посебно у контексту Диофантових једначина. Група $SL_2(\boldsymbol{Z})$ се користи за трансформацију квадратних форми и за проучавање еквивалентности међу њима.

6.1.2. Аутоморфне форме

Група $SL_2(\boldsymbol{Z})$ има блиску везу са аутоморфним формама, које представљају функције комплексне промењиве које трансформишу одређене равне облике под деловањем групе $SL_2(\boldsymbol{Z})$. Аутоморфне форме играју кључну улогу у теорији бројева, нарочито на разлагање бројева на просте факторе. Група $SL_2(\boldsymbol{Z})$ се користи за генерисање аутоморфних форми и за проучавање њихових особина.

6.1.3. Аритметика модуларних форми

Група $SL_2(\boldsymbol{Z})$ се такође користи и у проучавању аритметике модуларних форми. Модуларне форме су функције комплексне промењиве које испуњавају одређене особине модуларности. Оне имају дубоке везе са теоријом бројева, као и са другим областима математике попут алгебре и анализе. Група $SL_2(\boldsymbol{Z})$ се користи за генерисање и трансформацију модуларних форми, као и за проучавање њихових особина.

6.2. Теорија група

6.2.1. Теорија репрезентација

Група $SL_2(\boldsymbol{Z})$ је један од основних примера група које се проучавају у теорији репрезентација. Теорија репрезентација се бави проучавањем начина на које се математички објекти могу представити кроз линеарну трансформацију. Група $SL_2(\boldsymbol{Z})$ се користи као пример за проучавање репрезентација група и разумевање њихових особина.

6.2.2. Теорија квантних група

Група $SL_2(\boldsymbol{Z})$ се често користи као полазна тачка за разумевање и конструкцију квантних група. Теорија квантних група проучава алгебарске структуре које генерализују идеје група и омогућавају квантне аналогије у математици и физици. Ово је једна од актуелних математичких теорија која се тренутно изучава, посебно због примене у квантној физици.

6.3. Хиперболичка геометрија

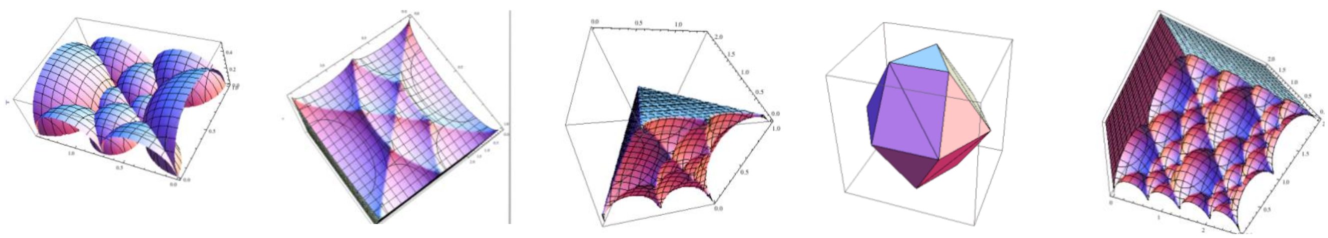
У хиперболичкој геометрији, група $SL_2(\boldsymbol{Z})$ има изузетну примену. Хиперболичка геометрија проучава геометрију равни са негативном закривљеношћу, познате као хиперболичке равни. Група $SL_2(\boldsymbol{Z})$ омогућава конструкцију и анализу теселација хиперболичке равни, што је један од кључних концепата у овој геометрији.

6.3.1. Теселације

Као што је било речи на почетку рада, у хиперболичкој геометрији теселације се могу конструисати помоћу групе $SL_2(\boldsymbol{Z})$. Свака плочица теселације одговара једној орбити тачака под дејством групе $SL_2(\boldsymbol{Z})$. Ове орбите тачака имају симетричне облике који се понављају у теселацији.

Теселације хиперболичке равни имају многе интересантне карактеристике, укључујући бесконачну симетрију. Могу се користити за проучавање различитих особина хиперболичке геометрије, као што су удаљености, углови, закривљеност и други концепти. Група $SL_2(\boldsymbol{Z})$ омогућава проучавање симетрија и трансформација у оквиру теселација, што је кључно за разумевање хиперболичке геометрије.

Такође, група $SL_2(\boldsymbol{Z})$ се користи у конструкцији хиперболичких модела и репрезентација хиперболичких објеката. Кроз математичке трансформације које се базирају на групи $SL_2(\boldsymbol{Z})$, могу се пружити репрезентације хиперболичких структура и облика, што омогућава боље разумевање њихових особина и својстава – *Слика 7*.



Идеалан фундаментални домен који произилази из $SL_2(\boldsymbol{Z}[\sqrt{-2}\,])$	*Изглед одоздо*	*Приближни идеални фундаментални домен који произилази из* $SL_2(\boldsymbol{Z}[\sqrt{-2}\,])$	*„Исправљена“ верзија идеалног фундаменталног домена која произилази из* $SL_2(\boldsymbol{Z}[\sqrt{-2}\,])$*- еуклидски пандан*	*Четири копије идеалног фундаменталног домена који произилазе из* $SL_2(\boldsymbol{Z}[\sqrt{-2}\,])$

Слика 7 - Шематска 3D слика полусфера које ограничавају полиедар

Укратко, група $SL_2(\boldsymbol{Z})$ има кључну улогу у проучавању хиперболичке геометрије. Кроз њену примену у конструкцији теселација, анализи симетрија и трансформација, као и у моделовању хиперболичких објеката, омогућено нам је да дубље истражимо и разумемо особине хиперболичке равни и простора.

6.3.2. Поенкареов диск

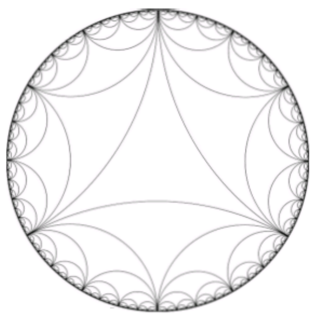
Поенкареов диск је геометријски објекат који се користи за моделирање хиперболичке равни. Поенкареов диск је један од начина да се представи хиперболичка раван на интуитиван начин. Он је конструисан као јединични диск на комплексној равни, где унутрашњост диска представља хиперболичку раван, а ивица диска представља бесконачност.

Један од кључних резултата у вези Поенкареовог диска и групе $SL_2(\boldsymbol{Z})$ је изоморфизам између ове две структуре. То значи да постоји бијекција између елемената Поенкареовог диска и елемената групе $SL_2(\boldsymbol{Z})$ која одржава операције. Овај изоморфизам омогућава корисну интерпретацију и разумевање хиперболичке геометрије кроз алгебарске концепте.

Поенкареов диск има неколико значајних особина које га чине корисним за проучавање хиперболичке геометрије и везе са групом $SL_2(\boldsymbol{Z})$.

- Хиперболичка метрика: У Поенкареовом диску се дефинише хиперболичка метрика која мери удаљеност између тачака на хиперболичкој равни. Ова метрика се разликује од еуклидске метрике и омогућава проучавање хиперболичке геометрије.

- Теселације Поенкареовог диска: Поенкареов диск може бити подељен на различите регионе помоћу теселација, које су геометријски облици који покривају целу површину диска. Ове теселације су повезане са групом $SL_2(\boldsymbol{Z})$ и њеним аутоморфизмима - *Слика 8*.



а) теселација у Поенкареовом диск моделу

б) примена у уметности и дизајну

Слика 8 - *Теселације Поенкареовог диска*

Изоморфизам између Поенкареовог диска и групе $SL_2(\boldsymbol{Z})$ омогућава нам да користимо алгебарске концепте групе $SL_2(\boldsymbol{Z})$ за проучавање хиперболичке геометрије на примеру Поенкареовог диска. Ово пружа дубље разумевање хиперболичке геометрије и омогућава нам да применимо алгебарске технике за проучавање математичких феномена на Поенкареовом диску.

6.3.3. Фрактали

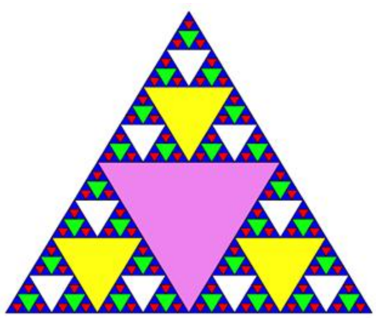
Група $SL_2(\boldsymbol{Z})$ има значајну примену у проучавању и конструкцији фрактала. Фрактали су комплексни математички објекти који показују самоподударност на различитим нивоима.

Они се могу генерисати кроз итеративне процесе који користе трансформације над тачкама или облицима.

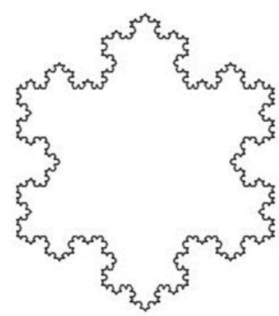
Група $SL_2(\boldsymbol{Z})$ се често користи у конструкцији фрактала кроз теорију динамичких система. Једна од познатих техника која се користи је позната као систем итериране функције (ИФС), где се комбинација афиних трансформација примењује на почетне тачке како би се генерисао фрактал. Афине трансформације у ИФС-у су обично представљене као матрице 2×2 са целобројним елементима из групе $SL_2(\boldsymbol{Z})$.

Кроз итеративно примењивање ових трансформација, тачке се премапирају на нове локације и стварају се детаљи и структуре које дефинишу фрактал. Самоподударност фрактала, односно њихова способност да покажу сличне облике на различитим скалама, често је повезана са својствима групе $SL_2(\boldsymbol{Z})$ и њеним деловањем на почетне тачке.

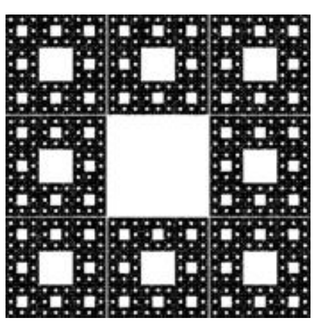
Фрактали генерисани групом $SL_2(\boldsymbol{Z})$ имају различите облике и карактеристике. На пример, популарни фрактал Сјерпински троугао може бити конструисан помоћу итерација афине трансформације која се може представити као елемент групе $SL_2(\boldsymbol{Z})$. Слично томе, фрактали попут Кохове криве, Барнслијевог тепиха и Манделбротовог скупа могу бити генерисани кроз примену итеративних трансформација изведених из групе $SL_2(\boldsymbol{Z})$ - *Слика 9*.



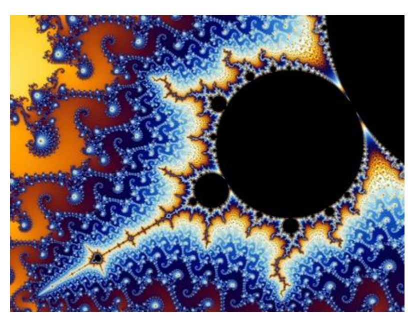
а) Сјерпински троугао



б) Кохова крива



в) Барнслијев тепих



г) Манделбротов скуп

Слика 9 - Фрактали

Ова веза између групе $SL_2(\boldsymbol{Z})$ и фрактала омогућава проучавање геометријских својстава фрактала кроз математичке трансформације и алгебарске операције које дефинише група. Такође, проучавање симетрија и инваријантности фрактала помоћу групе $SL_2(\boldsymbol{Z})$ омогућава дубље разумевање њихове структуре и карактеристика.

Укратко, група $SL_2(\boldsymbol{Z})$ игра важну улогу у примени код фрактала кроз конструкцију, генерисање и проучавање њихових геометријских својстава. Њено деловање и трансформације омогућавају стварање фрактала са самоподударним облицима и сложеним структурама које су карактеристичне за ове математичке објекте.

Глава 7

Закључак

Могућности примене групе $SL_2(\boldsymbol{Z})$ су изузетно велике. Важно је нагласити да постоје и друге потенцијалне примене групе $SL_2(\boldsymbol{Z})$ које нису споменуте у претходним одељцима. Ова група има богату структуру и својства која се могу искористити у разним математичким дисциплинама и истраживањима. Нека од подручја која се могу истраживати у будућности применом групе $SL_2(\boldsymbol{Z})$ су:

1. Криптографија: Група $SL_2(\boldsymbol{Z})$ може се користити у развоју криптографских алгоритама, посебно у вези са шифровањем и дешифровањем порука. Истраживање сигурносних аспеката и ефикасности примене групе $SL_2(\boldsymbol{Z})$ у криптографији могло би бити интересантно подручје за будућа истраживања.

2. Алгоритми и рачунарство: Група $SL_2(\boldsymbol{Z})$ може се применити у развоју ефикасних алгоритама за решавање одређених математичких проблема, попут решавања Диофантових једначина или генерисања теселација. Истраживање ефикасних алгоритама заснованих на групи $SL_2(\boldsymbol{Z})$ може имати значајан утицај на област рачунарства и примењене математике.

3. Физика и теоријска математика: Група $SL_2(\boldsymbol{Z})$ има везе са различитим аспектима физике, укључујући квантну механику, теорију струна и теорију квантних поља. Истраживање веза између групе $SL_2(\boldsymbol{Z})$ и ових физичких теорија може довести до нових увида и разумевања фундаменталних принципа природе.

У будућим истраживањима, ове су могућности само неки од путева који се могу испитати у вези са применом групе $SL_2(\boldsymbol{Z})$. Разумевање и истраживање њене улоге у различитим математичким дисциплинама може пружити нове перспективе и отворити врата за даља открића и развој математичких теорија.

Литература

[1] Conrad, K.: „SL2(Z)", University of Connecticut, Department of mathematics, New Haven.
[2] https://roywilliams.github.io/play/js/sl2z/
[3] https://www.youtube.com/watch?v=LolhzYwN1TQ
[4] Долинка, И.: „Предавања из теорије група", Универзитет Нови Сад, Департман за математику, Нови Сад, 2018.
[5] Harvey, W.J.: Introductory Lectures on SL(2, Z) and modular forms, King's College London, 2008.: http://www.ltcc.ac.uk/media/london-taught-course-centre/documents/Lecture-3-Notes.pdf
[6] https://www.math.mcgill.ca/darmon/courses/01-02/af/nicole.pdf
[7] Gangl, H.: Tessellations of Hyperbolic Space Notes for an Undergraduate Colloquium, 2013.: https://maths.dur.ac.uk/users/herbert.gangl/undergrad_colloq_2013.pdf
[8] http://rwoodley.org/?p=1322

Биографија

Анета Козина је рођена 04. јуна 1996. године у Зрењанину. У Конаку је завршила Основну школу „Вук Караџић“ 2011. године, а у Зрењанину „Зрењанинску гимназију“, природно - математички смер, 2015. године. По завршетку средње школе уписује основне академске студије математике на Природно-математичком факултету у Новом Саду. Дипломирала је у септембру 2020. године и стекла звање Дипломирани професор математике. Образовање је наставила на Математичком факултету у Београду, где у октобру 2020. године уписује мастер академске студије, модул Теоријска математика и примене. Закључно са јануаром 2022. године, положила је све испите на мастер студијама и тиме стекла услов за одбрану мастер рада.

Од фебруара до септембра 2021. године радила је као професор математике у Средњој школи „Вук Караџић“ у Сечњу. Од септембра 2021. године ради као професор математике у основној школи „Вук Караџић“ у Конаку.

Београд, 2023. *Анета Козина*