Different realizations of the upper half plane $\mathbb{H}$ and the reduction of quadratic forms

Urs Fuchs fuchsu@student.ethz.ch

In this talk I describe how the upper half plane $\mathbb{H}$ can be realized as a quotient group of $SL(2,\mathbb{Z})$ and as the symmetric positive definit 2×2-matrices with determinant 1.
The second realization can be used to reduce quadratic forms onto a normal form, which is induced by the fundamental domain of $\mathbb{H}$ under $SL(2,\mathbb{Z})$.
I provide an example of this reduction and an other example on the decomposition of any matrix in $SL(2,\mathbb{Z})$ into a word in the matrices S and T, which generate $SL(2,\mathbb{Z})$.

1 Realizations of the upper half plane $\mathbb{H}$

1.1 Realization of $\mathbb{H}$ as a quotient of $SL(2,\mathbb{R})$

Lemma 1 $SL(2,\mathbb{R})$ operates transitively on $\mathbb{H}$ and $\mathrm{Stab}(i) = SO(2)$

Proof: $\tau \in \mathbb{H}$

1. $M\tau \in \mathbb{H}$ because $\mathrm{Im}(M\tau) = \mathrm{Im}\left(\frac{a\tau+b}{c\tau+d}\right) = \frac{\mathrm{Im}((a\tau+b)(c\tau+d))}{|c\tau+d|^2} = \frac{\mathrm{Im}(\tau)}{|c\tau+d|^2} > 0$
2. $(MN)\tau = M(N(\tau))$ is well known from Moebius-Transformations
3. Transitivity:
   $\tau = x + iy \quad y > 0$
   Define $M := \begin{pmatrix} y^{-\frac{1}{2}} & xy^{-\frac{1}{2}} \\ 0 & y^{\frac{1}{2}} \end{pmatrix} \in SL(2,\mathbb{R})$
   $\Rightarrow M\tau = \frac{1}{y}(x+iy) - \frac{x}{y} = i \Rightarrow \forall \tau \in \mathbb{H}\, \exists M \in SL(2,\mathbb{R})\, M\tau = i$
   $\Rightarrow \tau, \tau' \in \mathbb{H} \Rightarrow M, M' \in SL(2,\mathbb{R})$ such that
   $\Rightarrow M\tau = M'\tau' = i \Rightarrow \underbrace{M'^{-1}M}_{\in SL(2,\mathbb{R})}\tau = \tau'$
4. $\mathrm{Stab}(i) = SO(2)$:
   $M \in SL(2,\mathbb{R}) \quad M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$
   $i \in \mathrm{Fix}(M) \Leftrightarrow \frac{ai+b}{ci+d} = i \Leftrightarrow ai + b = -c + di \Leftrightarrow a = d \quad b = -c$
   $\Leftrightarrow M = \left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right) \in SO(2)$ □

$SO(2)$ is not normal in $SL(2,\mathbb{R}) \Rightarrow SL(2,\mathbb{R})/SO(2,\mathbb{R})$ is not a group, but it is a set with an acting of $SL(2,\mathbb{R})$ by translation:
$t : SL(2,\mathbb{R}) \times SL(2,\mathbb{R})/SO(2) \to SL(2,\mathbb{R})/SO(2)$
$(N, MSO(2)) \to (NM)SO(2)$
that is the identity matrix acts trivial and $N(N'(MSO(2))) = (NN')MSO(2)$

Proposition 1 The map $\varphi : SL(2\mathbb{R})/SO(2) \to \mathbb{H} \quad MSO(2) \to Mi$
is a bijection which is compatible with the action of $SL(2,\mathbb{R})$, i.e.

$$\begin{array}{ccc} SL(2,\mathbb{R})/SO(2) & \xrightarrow[\varphi]{} & \mathbb{H} \\ {\scriptstyle t_M}\downarrow & & \downarrow{\scriptstyle M} \\ SL(2,\mathbb{R})/SO(2) & \xrightarrow[\varphi]{} & \mathbb{H} \end{array} \quad \text{commutes } \forall M \in SL(2,\mathbb{R})$$

Proof: φ is welldefined because SO(2) is the stabilisator of i.
That φ is bijective is a general fact of algebra: If a group G acts on a set $S \ni x$, then there is a bijection between $G/\mathrm{Stab}(x)$ and the orbit of x under G. The commutativity of the diagram follows by the definition of the maps, t_M denotes the translation by M. □

1.2 Realization of $\mathbb{H}$ as $SPos(2,\mathbb{R})$

$SPos(2,\mathbb{R})$ denotes the 2×2-matrices which are symmetric positive definit and have determinant 1.
It's well known $S = \begin{pmatrix} \alpha & \beta \\ \beta & \gamma \end{pmatrix} \in SPos(2,\mathbb{R}) \Leftrightarrow \alpha > 0 \quad \det(S) = 1$
Now define $F : \mathbb{H} \to SPos(2,\mathbb{R}) : \tau \to F_\tau := \frac{1}{y} \begin{pmatrix} 1 & -x \\ -x & x^2+y^2 \end{pmatrix}$ where $\tau = x + iy$
F is well-defined because $\det(F_\tau) = 1 \quad \forall \tau \in \mathbb{H}$ and $\alpha = \frac{1}{y} > 0$
Define further $w : SPos(2,\mathbb{R}) \to \mathbb{H} : S \to w(S) := \frac{1}{\alpha}(-\beta + i) \in \mathbb{H}$

Proposition 2

(*i*) $w(F_\tau) = \tau \quad \forall \tau \in \mathbb{H}$

(*ii*) $S = F_{w(S)} \quad \forall S \in SPos(2,\mathbb{R})$

Thus the map F is bijective with inverse w.

Proof:

(i) $w(F_\tau) = w\left(\frac{1}{y}\begin{pmatrix} 1 & -x \\ -x & x^2+y^2 \end{pmatrix}\right) = y(\frac{x}{y} + i) = x + iy = \tau$

(ii) $F_{w(S)} = F_{\frac{1}{\alpha}(-\beta+i)} = \alpha \begin{pmatrix} 1 & \frac{\beta}{\alpha} \\ \frac{\beta}{\alpha} & \frac{\beta^2+1}{\alpha^2} \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \beta & \frac{\beta^2+1}{\alpha} \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \beta & \gamma \end{pmatrix}$ because we have $\alpha\gamma - \beta^2 = 1$ since $S \in SPos(2,\mathbb{R})$ □

Lemma 2 $SL(2,\mathbb{R})$ operates on $SPos(2,\mathbb{R})$ by:
$SL(2,\mathbb{R}) \times SPos(2,\mathbb{R}) \to SPos(2,\mathbb{R}) : (M,S) \to M * S := M^{-1T} S M^{-1}$

Proof: $M*S \in SPos(2,\mathbb{R})$ because $\det(M^{-1T}SM^{-1}) = 1$. $M*S$ is symmetric since S is symmetric.
$M * S$ is positive definit: Write $\mathbb{R}^2 \ni \begin{pmatrix} u \\ v \end{pmatrix} = M \begin{pmatrix} x \\ y \end{pmatrix} \Rightarrow \begin{pmatrix} u \\ v \end{pmatrix}^T (M * S) \begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix}^T M^T M^{-1T} S M^{-1} M \begin{pmatrix} x \\ y \end{pmatrix} > 0$ for $(0,0) \neq (u,v)$
Moreover $(LM)*S = (LM)^{-1T}S(LM)^{-1} = L^{-1T}M^{-1T}SM^{-1}L^{-1} = L*(M*S)$ and the identity acts trivially. □

Proposition 3

(i) $w(M * S) = Mw(S)$

(ii) $F_{M\tau} = M * F_\tau$

Thus the operation of $SL(2,\mathbb{R})$ on $SPos(2,\mathbb{R})$ is compatible to the operation of $SL(2,\mathbb{R})$ on $\mathbb{H}$, i.e. the following diagram commutes for all $M \in SL(2,\mathbb{R})$:

$$\begin{array}{ccc} SPos(2,\mathbb{R})/SO(2) & \underset{F}{\overset{w}{\rightleftarrows}} & \mathbb{H} \\ \downarrow{\scriptstyle M*} & & \downarrow{\scriptstyle M} \\ SPos(2,\mathbb{R})/SO(2) & \underset{F}{\overset{w}{\rightleftarrows}} & \mathbb{H} \end{array}$$

Lemma 3 For $S \in SPos(2,\mathbb{R})$ is $w = w(S)$ the unique solution $w \in \mathbb{H}$ of the equation: $\begin{pmatrix} w \\ 1 \end{pmatrix}^T S \begin{pmatrix} w \\ 1 \end{pmatrix} = \alpha w^2 + 2\beta w + \gamma = 0$

Proof (Lemma 3): $\frac{-2\beta \pm \sqrt{4\beta^2 - 4\alpha\gamma}}{2\alpha} = -\frac{\beta}{\alpha} \pm \frac{1}{\alpha}\sqrt{\beta^2 - \alpha\gamma} = -\frac{\beta}{\alpha} \pm \frac{i}{\alpha}$
because $\beta^2 - \alpha\gamma = -\det(S) = -1$ □

Proof (Proposition 3):

(i) $\tilde{w} := w(M*S)$, $w := w(S)$, $M*S =: \left(\begin{smallmatrix}\alpha & \beta \\ \beta & \gamma\end{smallmatrix}\right)$, $M = \left(\begin{smallmatrix}a & b \\ c & d\end{smallmatrix}\right)$ and $z := M^{-1}\tilde{w} \Rightarrow z \in \mathbb{H}$
By Lemma 2, $\tilde{w}$ is the unique solution in $\mathbb{H}$ of $0 = \left(\begin{smallmatrix}\tilde{w} \\ 1\end{smallmatrix}\right)^T M^{-1T} S M^{-1} \left(\begin{smallmatrix}\tilde{w} \\ 1\end{smallmatrix}\right) = \left(\begin{smallmatrix}z \\ 1\end{smallmatrix}\right)^T S \left(\begin{smallmatrix}z \\ 1\end{smallmatrix}\right) (-c\tilde{w}+a)^2$ where the second equality follows by $M^{-1}\left(\begin{smallmatrix}\tilde{w} \\ 1\end{smallmatrix}\right) = \left(\begin{smallmatrix}d\tilde{w}-b \\ -c\tilde{w}+a\end{smallmatrix}\right) = (-c\tilde{w}+a)\left(\begin{smallmatrix}\frac{d\tilde{w}-b}{-c\tilde{w}+a} \\ 1\end{smallmatrix}\right) = \underbrace{(-c\tilde{w}+a)}_{\neq 0}\left(\begin{smallmatrix}z \\ 1\end{smallmatrix}\right)$
Thus $\left(\begin{smallmatrix}z \\ 1\end{smallmatrix}\right)^T S \left(\begin{smallmatrix}z \\ 1\end{smallmatrix}\right) = 0 \overset{\text{Lemma 2}}{\Rightarrow} z = w \Rightarrow z = M^{-1}\tilde{w} = w$
$\Rightarrow Mw = \tilde{w} = w(M*S)$

(ii) $\tau := w(S) \Rightarrow S = F_\tau$
$F_{M\tau} = F_{Mw(S)} \overset{\text{Prop 3(i)}}{=} F_{w(M*S)} \overset{\text{Prop 2(ii)}}{=} M*S = M*F_\tau$ □

Define $\mathcal{F} := \{\tau \in \mathbb{H} \,|\, |\mathrm{Re}(\tau)| \leq \frac{1}{2}, |\tau| \geq 1\}$, the fundamental domain of $\mathbb{H}$ under the action of $SL(2,\mathbb{Z})$.

Recall the following Proposition about the fundamental domain:

Proposition 4

(*i*) $\forall \tau \in \mathbb{H}\, \exists M \in SL(2,\mathbb{Z})$ such that $M\tau \in \mathcal{F}$

(ii) If τ and $M\tau$ are in $\mathcal{F}^\circ \Rightarrow M = \pm E$

Now look at the image of $\mathcal{F}$ under $F : \tau \to F_\tau = \frac{1}{y}\left(\begin{smallmatrix}1 & -x \\ -x & x^2+y^2\end{smallmatrix}\right) \tau \in \mathcal{F}$:
Since $x + iy \in \mathcal{F}$ we have $|x| \leq \frac{1}{2}$
This implies $\frac{2|x|}{y} = 2|\beta| \leq \frac{1}{y} = \alpha \Rightarrow 2|\beta| \leq \alpha$.
Moreover $\alpha = \frac{1}{y} \leq \frac{x^2+y^2}{y} = \gamma$ since $x + iy \in \mathcal{F}$
$\Rightarrow 0 \leq 2|\beta| \leq \alpha \leq \gamma$ and these matrices are mapped back to $\mathcal{F}$ under w.
$\Rightarrow \mathcal{P} := \left\{\left(\begin{smallmatrix}\alpha & \beta \\ \beta & \gamma\end{smallmatrix}\right) \in SPos(2,\mathbb{R}) | 0 \leq 2|\beta| \leq \alpha \leq \gamma\right\}$

Corollary

(*i*) $\forall S \in SPos(2,\mathbb{R})\, \exists M \in SL(2,\mathbb{Z})$ such that $M^TSM \in \mathcal{P}$

(ii) If S and M^TSM are in $\mathcal{P}^\circ \Rightarrow M = \pm E$

2 Reduction of quadratic forms

Definition: A *quadratic form* (over $\mathbb{Z}$) is a polynomial in two variables $f(x,y) = ax^2 + bxy + cy^2$ with coefficients in $\mathbb{Z}$.
A quadratic form is called *reduced*, if $|b| \leq a \leq c$.
$\Delta = b^2 - 4ac$ is called the *discriminant* of the quadratic form.

Proposition 5 $f(x,y) = ax^2 + bxy + cy^2$ reduced, $\Delta < 0 \Rightarrow |b| \leq \sqrt{\frac{-\Delta}{3}}$

Proof: $4b^2 \leq 4ac = -\Delta + b^2 \Rightarrow 3b^2 \leq -\Delta$ □

Proposition 6 There is only a finite number of reduced quadratic forms for a fixed disciminant $\Delta < 0$

Proof: By Prop 5. $\exists$ only a finite number of b's to a fixed Δ and for each of these b's there is only finite number of factorisations of $b^2-\Delta$ in to the form $4ac$ $\Rightarrow \exists$ only a finite number of tripel (a,b,c) such that the associated f is reduced with a fixed $\Delta < 0$. $\square$

Why this $2|\beta|$ in the definition of $\mathcal{P}$ while we have $|b|$ in the definition of reduced? Because: $\begin{pmatrix} \alpha & \beta \\ \beta & \gamma \end{pmatrix} \leftrightarrow \alpha x^2 + 2\beta xy + \gamma y^2$

Observe that: Determinant of S doesn't change (under the action of $SL(2,\mathbb{Z})$) $\Leftrightarrow$ $\Delta = \frac{-\det(S)}{4}$ doesn't change.

The above Corollary shows, that every quadratic form in $SPos(2,\mathbb{R})$ is equivalent to a reduced quadratic form. How can this be done practically?

Example of a reduction of a quadratic form S, but more general $\det(S) \neq 1$

$$\left(\begin{smallmatrix} 2 & 3 \\ 3 & 5 \end{smallmatrix}\right) \sim f(x,y) := 2x^2+6xy+5y^2 \overset{\left(\begin{smallmatrix} 1 & -1 \\ 0 & 1 \end{smallmatrix}\right)}{\rightsquigarrow} 2(x-y)^2+6(x-y)y+5y^2 = 2x^2+2xy+y^2$$

$$\overset{\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)}{\rightsquigarrow} x^2-2xy+2y^2 \overset{\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)}{\rightsquigarrow} (x+y)^2-2(x+y)y+2y^2 = x^2+y^2$$

and this is a reduced form. The general strategy is to choose a matrix of the form $\left(\begin{smallmatrix} 1 & z \\ 0 & 1 \end{smallmatrix}\right) \in SL(2,\mathbb{Z})$ to reduce the absolute value of the second coefficient. Moreover if $|a| > |c|$ occurs, we have to interchange x and y by $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$.
Acting with the matrix M given is the same as replace $\left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right)$ by $M\left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right)$ in the polynomial $f(x,y)$.

Example **Representing a matrix in $SL(2,\mathbb{Z})$ by a word in S and T**

$S := \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ $\quad T := \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $A := \left(\begin{smallmatrix} 4 & 9 \\ 11 & 25 \end{smallmatrix}\right)$
$AT^n = \left(\begin{smallmatrix} 4 & 9 \\ 11 & 25 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 4 & 4n+9 \\ 11 & 11n+25 \end{smallmatrix}\right)$
Choose n such that $|a_{22}| = |11n+25| < 11 = |a_{21}|$, for example $n=-2$: $\Rightarrow AT^{-2} = \left(\begin{smallmatrix} 4 & 1 \\ 11 & 3 \end{smallmatrix}\right)$.
Now we want again to have $|a_{21}| < |a_{22}|$, so we interchange these two values by S:
$AT^{-2}S = \left(\begin{smallmatrix} 1 & -4 \\ 3 & -11 \end{smallmatrix}\right)$
Repeating this process we get:
$AT^{-2}ST^4 = \left(\begin{smallmatrix} 1 & 0 \\ 3 & 1 \end{smallmatrix}\right) \Rightarrow AT^{-2}ST^4S = \left(\begin{smallmatrix} 0 & 1 \\ 1 & -3 \end{smallmatrix}\right) \Rightarrow AT^{-2}ST^4ST^3 = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) = S$

Thus we can write A as a word in S and T:
$A = ST^{-3}S^3T^{-4}S^3T^2 = ST^{-3}ST^{-4}ST^2$ using $S^2 = -Id$