IDEAL CLASSES AND SL_2

KEITH CONRAD

1. Introduction

A standard group action in complex analysis is the action of $\mathrm{GL}_2(\mathbf{C})$ on the Riemann sphere $\mathbf{C} \cup \{\infty\}$ by linear fractional transformations (Möbius transformations):

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} z = \frac{az+b}{cz+d}. \tag{1.1}$$

We need to allow the value ∞ since $cz+d$ might be 0. (If that happens, $az+b \neq 0$ since $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ is invertible.) When $z = \infty$, the value of (1.1) is $a/c \in \mathbf{C} \cup \{\infty\}$.

It is easy to see this action of $\mathrm{GL}_2(\mathbf{C})$ on the Riemann sphere is transitive (that is, there is one orbit): for every $a \in \mathbf{C}$,

$$\begin{pmatrix} a & a-1 \\ 1 & 1 \end{pmatrix} \infty = a, \tag{1.2}$$

so the orbit of ∞ passes through all points. In fact, since $\left(\begin{smallmatrix} a & a-1 \\ 1 & 1 \end{smallmatrix}\right)$ has determinant 1, the action of $\mathrm{SL}_2(\mathbf{C})$ on $\mathbf{C} \cup \{\infty\}$ is transitive.

However, the action of $\mathrm{SL}_2(\mathbf{R})$ on the Riemann sphere is not transitive. The reason is the formula for imaginary parts under a real linear fractional transformation:

$$\mathrm{Im}\left(\frac{az+b}{cz+d}\right) = \frac{(ad-bc)\,\mathrm{Im}(z)}{|cz+d|^2}$$

when $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbf{R})$. Thus the imaginary parts of z and $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)z$ have the same sign when $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ has determinant 1. The action of $\mathrm{SL}_2(\mathbf{R})$ on the Riemann sphere has three orbits: $\mathbf{R} \cup \{\infty\}$, the upper half-plane $\mathfrak{h} = \{x+iy : y > 0\}$, and the lower half-plane. To see that the action of $\mathrm{SL}_2(\mathbf{R})$ on $\mathfrak{h}$ is transitive, pick $x+iy$ with $y > 0$. Then

$$\begin{pmatrix} \sqrt{y} & x/\sqrt{y} \\ 0 & 1/\sqrt{y} \end{pmatrix} i = x+iy,$$

and the matrix here is in $\mathrm{SL}_2(\mathbf{R})$. (This action of $\mathrm{SL}_2(\mathbf{R})$ on the upper half-plane is essentially one of the models for the isometries of the hyperbolic plane.)

The action (1.1) makes sense with $\mathbf{C}$ replaced by any field K, and gives a transitive group action of $\mathrm{GL}_2(K)$ on the set $K \cup \{\infty\}$. Just as over the complex numbers, the formula (1.2) shows the action of $\mathrm{SL}_2(K)$ on $K \cup \{\infty\}$ is transitive.

Now take K to be a number field, and replace the group $\mathrm{SL}_2(K)$ with its subgroup $\mathrm{SL}_2(\mathcal{O}_K)$. The point ∞ and all of $\mathcal{O}_K$ are in the same $\mathrm{SL}_2(\mathcal{O}_K)$-orbit on $K \cup \{\infty\}$ (take $a \in \mathcal{O}_K$ in (1.2)), but there could be more than one $\mathrm{SL}_2(\mathcal{O}_K)$-orbit.

Theorem 1.1. *For a number field K, the number of orbits for $\mathrm{SL}_2(\mathcal{O}_K)$ on $K \cup \{\infty\}$ is the class number of K.*

There are finitely many orbits since the class number of K is finite, and this finiteness is a non-trivial statement!

In Section 2, we will prove $\mathrm{SL}_2(\mathcal{O}_K)$ acts transitively on $K \cup \{\infty\}$ if and only if K has class number 1. This is the simplest case of Theorem 1.1. As preparation for the general case, in Section 3 we will change our language from $K \cup \{\infty\}$ to the projective line over K, whose relevance (among other things) is that it removes the peculiar status of ∞. (It seems useful to treat the special case of class number 1 without mentioning the projective line, if only to underscore what it is one is gaining by using the projective line in the general case.) In Section 4 we prove Theorem 1.1 in general. This theorem is particularly important for totally real K (in the context of Hilbert modular forms [1, pp. 36–38], [2, pp. 7–8]), but it holds for any number field K.

As a further illustration of the link between SL_2 and classical number theory, we show in an appendix that the Euclidean algorithm on $\mathbf{Z}$ is more or less equivalent to the group $\mathrm{SL}_2(\mathbf{Z})$ being generated by the matrices $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$.

The prerequisites we need about number fields are: in any number field all fractional ideals are invertible, and any fractional ideal has two generators. That only two generators are needed for fractional ideals in a number field appears as an exercise in several introductory algebraic number theory books, but it may seem like an isolated fact in such books (I thought so when I first saw it!). Its use in the proof of Theorem 1.1 shows it is not.

2. Transitivity and Class Number One

As an example of class number one, take $K = \mathbf{Q}$. We will show every rational number is in the $\mathrm{SL}_2(\mathbf{Z})$-orbit of ∞. Pick a rational number r, and write it in reduced form as $r = a/c$, so a and c are relatively prime integers. (If $r = 0$, use $a = 0$ and $c = 1$.) Since $(a, c) = 1$, we can solve the equation $ad - bc = 1$ in integers b and d, which means we get a matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ in $\mathrm{SL}_2(\mathbf{Z})$ whose first column is $\binom{a}{c}$. This matrix sends ∞ to $a/c = r$.

Conversely, if we know by some independent means that the $\mathrm{SL}_2(\mathbf{Z})$-action on $\mathbf{Q} \cup \{\infty\}$ is transitive, then for any rational number r we can find a matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbf{Z})$ sending ∞ to r, so $r = a/c$. Since $ad - bc = 1$, a and c have no common factors, so we can write r as a ratio of relatively prime integers. Thus, the fact that the $\mathrm{SL}_2(\mathbf{Z})$-action on $\mathbf{Q} \cup \{\infty\}$ is transitive is equivalent to the ability to write rational numbers in reduced form over $\mathbf{Z}$.

A similar argument shows the action of $\mathrm{SL}_2(\mathcal{O}_K)$ on $K \cup \{\infty\}$ is transitive if and only if every element of K can be written in 'reduced form,' *i.e.*, as a ratio of relatively prime algebraic integers from $\mathcal{O}_K$.

Theorem 2.1. *Every element of $K^\times$ has the form α/β where $(\alpha, \beta) = (1)$ in $\mathcal{O}_K$ if and only if K has class number 1.*

Proof. If K has class number 1 then $\mathcal{O}_K$ is a PID, so a UFD, so any ratio of nonzero elements of $\mathcal{O}_K$ can be put in a reduced form.

Conversely, suppose each ratio of nonzero elements of $\mathcal{O}_K$ can be put in reduced form. To show every ideal is principal, pick an ideal $\mathfrak{a}$. We may suppose $\mathfrak{a} \neq (0)$, so $\mathfrak{a} = (x, y)$ where x and y are in $\mathcal{O}_K$ and neither is 0. By hypothesis we can write $x/y = \alpha/\beta$ where $(\alpha, \beta) = (1)$. Then $x\beta = y\alpha$, so $(x)(\beta) = (y)(\alpha)$. The ideals (α) and (β) are relatively prime, so $(\alpha) \mid (x)$. Thus $\alpha \mid x$, so $x = \alpha\gamma$ for some $\gamma \in \mathcal{O}_K$. Then $\alpha\gamma\beta = y\alpha$, so $y = \beta\gamma$. It follows that $\mathfrak{a} = (x, y) = (\alpha\gamma, \beta\gamma) = (\alpha, \beta)(\gamma) = (1)(\gamma) = (\gamma)$ is principal. $\square$

Thus, the number of orbits for $\mathrm{SL}_2(\mathcal{O}_K)$ on $K \cup \{\infty\}$ is 1 if and only if K has class number 1.

3. The Projective Line

In this section, K is any field.

The set of numbers $K \cup \{\infty\}$ can be thought of as the possible slopes of different lines through the origin in K^2. Rather than determine such lines by their slopes, we can determine such lines by naming a representative point (x, y) on the line, excluding $(0, 0)$ (which lies on all such lines). But we face the issue: when do two non-zero points (x, y) and (x', y') lie on the same line through the origin? Since a line through the origin is the set of scalar multiples of any non-zero point on that line, (x, y) and (x', y') lie on the same line through the origin when $(x', y') = \lambda(x, y)$ for some $\lambda \in K^\times$.

Definition 3.1. The *projective line* over K is the set of points in $K^2 - \{(0, 0)\}$ modulo scaling by $K^\times$. That is, we set $(x, y) \sim (x', y')$ if and only if there is some $\lambda \in K^\times$ such that $x' = \lambda x$ and $y' = \lambda y$. The equivalence classes for $\sim$ form the projective line over K.

We denote the projective line over K by $\mathbf{P}^1(K)$. (Strictly speaking, the projective line over K is a richer geometric object than merely the set of equivalence classes $\mathbf{P}^1(K)$, but our definition will be adequate for our purposes.) The equivalence class of (x, y) in $\mathbf{P}^1(K)$ is denoted $[x, y]$ and is called a point of $\mathbf{P}^1(K)$. For instance, in $\mathbf{P}^1(\mathbf{R})$, $[2, 3] = [4, 8] = [1, 3/2]$. Provided $x \neq 0$, we have $[x, y] = [1, y/x]$, and $[1, a] = [1, b]$ if and only if $a = b$. We have $[0, y] = [x', y']$ if and only if $x' = 0$, and in this case $[0, y] = [0, 1]$. Thus, every point of $\mathbf{P}^1(K)$ equals $[1, y]$ for a unique $y \in K$ or is the point $[0, 1]$. By an analogous argument, every point of $\mathbf{P}^1(K)$ is $[x, 1]$ for a unique $x \in K$ or is the point $[1, 0]$. For the points $[x, y]$ with neither x nor y equal to 0, we can write them either as $[1, y/x]$ or $[x/y, 1]$. (To change between the two coordinates amounts to $t \leftrightarrow 1/t$ on $K^\times$.)

The passage from $[x, y]$ to the ratio y/x, with the exceptional case $x = 0$, corresponds to the idea of recovering a line's slope as a number in $K \cup \{\infty\}$. In other words, the correspondence between $\mathbf{P}^1(K)$ and $K \cup \{\infty\}$ comes about from

$$[x, y] \mapsto \begin{cases} y/x, & \text{if } x \neq 0, \\ \infty, & \text{if } x = 0. \end{cases}$$

Since $[x, y] = [x', y']$ if and only if (x, y) and (x', y') are non-zero scalar multiples, the ratio y/x (provided $x \neq 0$) is a well-defined number in terms of the point $[x, y]$ even though the coordinates x and y themselves are not uniquely determined from $[x, y]$.

We get another correspondence between $\mathbf{P}^1(K)$ and $K \cup \{\infty\}$ by associating $[x, y]$ to x/y or ∞:

$$[x, y] \mapsto \begin{cases} x/y, & \text{if } y \neq 0, \\ \infty, & \text{if } y = 0. \end{cases} \tag{3.1}$$

Now we describe an action of $\mathrm{GL}_2(K)$ on $\mathbf{P}^1(K)$ that corresponds to (1.1). For an invertible matrix $A \in \mathrm{GL}_2(K)$, and a non-zero vector $v \in K^2$, the product Av is non-zero and

$$A(\lambda v) = \lambda A v$$

for any $\lambda \in K$. Therefore A sends all points on one line through the origin in K^2 to all points on another line through the origin in K^2. (No such line collapses under A since A is invertible.) This means the usual action of $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ on column vectors in K^2 lets us define A as a transformation of $\mathbf{P}^1(K)$:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax+by \\ cx+dy \end{pmatrix} \rightsquigarrow \begin{pmatrix} a & b \\ c & d \end{pmatrix}[x,y] := [ax+by, cx+dy]. \tag{3.2}$$

When $y \neq 0$, let $z = x/y$. Then the element of $K \cup \{\infty\}$ corresponding by (3.1) to $[ax+by, cx+dy]$ is

$$\frac{ax+by}{cx+dy} = \frac{az+b}{cz+d},$$

interpreted as ∞ when the denominator is 0. Writing $[x,y]$ as $[z,1]$, we see that the action of $\mathrm{GL}_2(K)$ on $K \cup \{\infty\}$ given by (1.1), with the peculiar role of ∞, is the same as the action of $\mathrm{GL}_2(K)$ on $\mathbf{P}^1(K)$ given by the right side of (3.2). And now, in $\mathbf{P}^1(K)$, there is no more mysterious ∞. Everything is homogeneous.

4. Orbits and Ideal Classes

For $x, y \in K$, not both zero, we write $[x,y]$ for a point in $\mathbf{P}^1(K)$ and $(x,y) = x\mathcal{O}_K + y\mathcal{O}_K$ for a fractional ideal. Since every fractional ideal has two generators, (x,y) is a completely general fractional ideal as x and y vary (avoiding $x = y = 0$).

Now we are ready to prove Theorem 1.1 in general.

Proof. Step 1: If $[x,y]$ and $[x',y']$ are in the same $\mathrm{SL}_2(\mathcal{O}_K)$-orbit, then the fractional ideals (x,y) and (x',y') are in the same ideal class.

Being in the same orbit means

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \lambda x' \\ \lambda y' \end{pmatrix} \tag{4.1}$$

for some $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathcal{O}_K)$ and $\lambda \in K^\times$. Thus

$$\begin{aligned} ax+by &= \lambda x', \\ cx+dy &= \lambda y', \end{aligned}$$

so $(\lambda x', \lambda y') \subset (x,y)$. Multiplying both sides of (4.1) by the inverse $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)^{-1} \in \mathrm{SL}_2(\mathcal{O}_K)$ gives the reverse containment, so $(x,y) = (\lambda x', \lambda y') = \lambda(x',y')$.

As far as Step 1 is concerned, $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ could have been in $\mathrm{GL}_2(\mathcal{O}_K)$ rather than $\mathrm{SL}_2(\mathcal{O}_K)$.

Step 2: If (x,y) and (x',y') are in the same ideal class, then the points $[x,y]$ and $[x',y']$ in $\mathbf{P}^1(K)$ are in the same $\mathrm{SL}_2(\mathcal{O}_K)$-orbit.

We can write $(x,y) = \lambda(x',y') = (\lambda x', \lambda y')$ for some $\lambda \in K^\times$ and we want to show $[x,y]$ and $[x',y'] = [\lambda x', \lambda y']$ are in the same orbit of $\mathrm{SL}_2(\mathcal{O}_K)$. Since $(x,y) = (\lambda x', \lambda y')$, we seek a relation between pairs of generators for the *same* fractional ideal.

Let $\mathfrak{a} = (x,y)$. The inverse ideal $\mathfrak{a}^{-1}$ has two generators, say $\mathfrak{a}^{-1} = (r,s)$. From the equation $(1) = (x,y)(r,s) = (xr, xs, yr, ys)$, there are $\alpha, \beta, \gamma, \delta \in \mathcal{O}_K$ such that

$$\begin{aligned} 1 &= \alpha xr + \beta xs + \gamma yr + \delta ys \\ &= (\alpha r + \beta s)x + (\gamma r + \delta s)y. \end{aligned}$$

Note $\alpha r + \beta s$ and $\gamma r + \delta s$ are in $\mathfrak{a}^{-1}$. Setting $\mu = -(\gamma r + \delta s)$ and $\nu = \alpha r + \beta s$, the matrix $M = \left(\begin{smallmatrix} x & \mu \\ y & \nu \end{smallmatrix}\right)$ in $\mathrm{M}_2(K)$ has determinant 1 and its second column has entries in $\mathfrak{a}^{-1}$.

Similarly, using $\lambda x'$ and $\lambda y'$ in place of x and y, there is a matrix $N = \left(\begin{smallmatrix} \lambda x' & \mu' \\ \lambda y' & \nu' \end{smallmatrix}\right) \in \mathrm{M}_2(K)$ with determinant 1 and its second column has entries in $\mathfrak{a}^{-1}$.

Since $\mu, \nu, \mu', \nu' \in \mathfrak{a}^{-1}$, the product

$$MN^{-1} = \begin{pmatrix} x & \mu \\ y & \nu \end{pmatrix} \begin{pmatrix} \nu' & -\mu' \\ -\lambda y' & \lambda x' \end{pmatrix}$$

has determinant 1 and entries in $\mathcal{O}_K$. Therefore MN^{-1} is in $\mathrm{SL}_2(K) \cap \mathrm{M}_2(\mathcal{O}_K) = \mathrm{SL}_2(\mathcal{O}_K)$.

As $M\left[\begin{smallmatrix}1\\0\end{smallmatrix}\right] = \left[\begin{smallmatrix}x\\y\end{smallmatrix}\right]$ and $N\left[\begin{smallmatrix}1\\0\end{smallmatrix}\right] = \left[\begin{smallmatrix}\lambda x'\\\lambda y'\end{smallmatrix}\right]$, we have $MN^{-1}\left[\begin{smallmatrix}\lambda x'\\\lambda y'\end{smallmatrix}\right] = M\left[\begin{smallmatrix}1\\0\end{smallmatrix}\right] = \left[\begin{smallmatrix}x\\y\end{smallmatrix}\right]$, so $[x, y]$ and $[\lambda x', \lambda y'] = [x', y']$ are in the same $\mathrm{SL}_2(\mathcal{O}_K)$-orbit. $\square$

Our bijection between the $\mathrm{SL}_2(\mathcal{O}_K)$-orbits in $\mathbf{P}^1(K)$ and the ideal classes of K associates the identity ideal class $(x = 1, y = 0)$ with the orbit of $[1, 0] = \infty$ in $\mathbf{P}^1(K)$.

Remark 4.1. Different pairs of generators of the same fractional ideal usually correspond to different points in $\mathbf{P}^1(K)$. For example, $(2, 1) = (-2, 1) = \mathcal{O}_K$ as ideals, but $[2, 1] \neq [-2, 1]$ in $\mathbf{P}^1(K)$ (that is, $2 \neq -2$ in K).

Everything we have done here carries over to a general Dedekind domain, with identical proofs. We will just state the result.

Theorem 4.2. *Let R be a Dedekind domain and F be its fraction field. When $\mathrm{SL}_2(R)$ acts on $F \cup \{\infty\}$ by (1.1), its orbits are in bijection with the ideal class group of R. In particular, $\mathrm{SL}_2(R)$ acts transitively on $F \cup \{\infty\}$ if and only if R is a* PID*.*

Let's see what Theorem 1.1 says in an example.

Example 4.3. The ideal class group of $\mathbf{Q}(\sqrt{-5})$ has order 2, so $\mathrm{SL}_2(\mathbf{Z}[\sqrt{-5}])$ acting on $\mathbf{P}^1(\mathbf{Q}(\sqrt{-5}))$ has two orbits. The ideal classes are represented by (1) and $(2, 1+\sqrt{-5})$, so the $\mathrm{SL}_2(\mathbf{Z}[\sqrt{-5}])$-orbits in $\mathbf{P}^1(\mathbf{Q}(\sqrt{-5}))$ are represented by the points $[1, 0]$ and $[2, 1+\sqrt{-5}]$. Since all nonprincipal ideals in $\mathrm{SL}_2(\mathbf{Z}[\sqrt{-5}])$ are in the same ideal class, if ideals (x, y) and (x', y') in $\mathbf{Z}[\sqrt{-5}]$ are nonprincipal then the points $[x, y]$ and $[x', y']$ in $\mathbf{P}^1(\mathbf{Q}(\sqrt{-5}))$ are in the same $\mathrm{SL}_2(\mathbf{Z}[\sqrt{-5}])$-orbit: $[x, y] = A[x', y']$ for some $A \in \mathrm{SL}_2(\mathbf{Z}[\sqrt{-5}])$.

If we are given two numbers z and z' in K, how can we determine if they are in the same $\mathrm{SL}_2(\mathcal{O}_K)$-orbit? The proof of Theorem 1.1 provides a method.

Step 1. Write z and z' as ratios from $\mathcal{O}_K$: $z = x/y$ and $z' = x'/y'$ for $x, y, x', y' \in \mathcal{O}_K$. Determine if the ideals (x, y) and (x', y') are in the same ideal class.[1] If they aren't, then z and z' aren't in the same orbit.

Step 2. If (x, y) and (x', y') are in the same ideal class, then there is $\lambda \in K^\times$ such that $(x, y) = \lambda(x', y') = (\lambda x', \lambda y')$. We seek $A \in \mathrm{SL}_2(\mathcal{O}_K)$ such that $Az' = z$: $A(x'/y') = x/y$.

Set $(x, y)^{-1} = (r, s)$ as fractional ideals and pick $\alpha, \beta, \gamma, \delta \in \mathcal{O}_K$ such that $1 = \alpha xr + \beta xs + \gamma ry + \delta ys$. Set $M = \left(\begin{smallmatrix} x & \mu \\ y & \nu \end{smallmatrix}\right)$ where $\mu = -(\gamma r + \delta s)$ and $\nu = \alpha r + \beta s$, so $M\infty = x/y = z$.

Since $(x, y) = (\lambda x', \lambda y')$, run through the previous paragraph with $\lambda x'$ in place of x and $\lambda y'$ in place of y (and use the same r and s) to get a 2×2 matrix $N = \left(\begin{smallmatrix} \lambda x' & \mu' \\ \lambda y' & \nu' \end{smallmatrix}\right)$, so $N\infty = (\lambda x'/\lambda y') = x'/y' = z'$. The matrix $A = MN^{-1}$ is in $\mathrm{SL}_2(\mathcal{O}_K)$ and $Az' = MN^{-1}z' = M\infty = z$.

Example 4.4. Consider the ideals

$$\mathfrak{p} = (2, 1+\sqrt{-5}) = (2, 1-\sqrt{-5}), \quad \mathfrak{q} = (3, 1+\sqrt{-5}), \quad \mathfrak{q}' = (3, 1-\sqrt{-5}).$$

[1] These ideals are $y(z, 1)$ and $y'(z', 1)$, so they are equivalent in the ideal class group to the fractional ideals $(z, 1)$ and $(z', 1)$.

These are all nonprincipal, so the numbers $2/(1+\sqrt{-5})$, $2/(1-\sqrt{-5})$, $3/(1+\sqrt{-5})$, and $3/(1-\sqrt{-5})$ are all in the same $\mathrm{SL}_2(\mathbf{Z}[\sqrt{-5}])$-orbit. It is easy to link the first and third numbers and second and fourth numbers with a matrix from $\mathrm{SL}_2(\mathbf{Z})$:

$$\begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix} \frac{2}{1+\sqrt{-5}} = \frac{2/(1+\sqrt{-5})-1}{2/(1+\sqrt{-5})} = \frac{1-\sqrt{-5}}{2} = \frac{3}{1+\sqrt{-5}}$$

and

$$\begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix} \frac{2}{1-\sqrt{-5}} = \frac{2/(1-\sqrt{-5})-1}{2/(1-\sqrt{-5})} = \frac{1+\sqrt{-5}}{2} = \frac{3}{1-\sqrt{-5}}.$$

Linking $2/(1+\sqrt{-5})$ and $3/(1-\sqrt{-5})$ is not as simple: there is A in $\mathrm{SL}_2(\mathbf{Z}[\sqrt{-5}])$ such that $A\frac{3}{1-\sqrt{-5}} = \frac{2}{1+\sqrt{-5}}$, but there is no such A in $\mathrm{SL}_2(\mathbf{Z})$.[2] To find A we will follow Step 2 of the procedure above with $z = 2/(1+\sqrt{-5})$ and $z' = 3/(1-\sqrt{-5})$: set $x = 2$, $y = 1+\sqrt{-5}$, $x' = 3$, and $y' = 1-\sqrt{-5}$, so $\mathfrak{p} = (x,y)$ and $\mathfrak{q}' = (x', y')$. Since $\mathfrak{p}^2 = (2)$ and $\mathfrak{p}\mathfrak{q}' = (1-\sqrt{-5})$, we have $2\mathfrak{q}' = (1-\sqrt{-5})\mathfrak{p}$, so $\mathfrak{p} = \lambda\mathfrak{q}'$ for $\lambda = 2/(1-\sqrt{-5})$.

From $\mathfrak{p}^2 = (2)$, $\mathfrak{p}^{-1} = \frac{1}{2}\mathfrak{p} = (1, (1+\sqrt{-5})/2)$ as a fractional ideal. Then

$$(1) = \mathfrak{p}\mathfrak{p}^{-1} = (2, 1+\sqrt{-5})(1, (1+\sqrt{-5})/2) = (2, 1+\sqrt{-5}, 1+\sqrt{-5}, -2+\sqrt{-5}).$$

In Step 2, let $\alpha = -1$, $\beta = 1$, $\gamma = 0$, and $\delta = -1$, $\mu = (1+\sqrt{-5})/2$, and $\nu = (-1+\sqrt{-5})/2$, so $M = \left(\begin{smallmatrix} x & \mu \\ y & \nu \end{smallmatrix}\right) = \left(\begin{smallmatrix} 2 & (1+\sqrt{-5})/2 \\ 1+\sqrt{-5} & (-1+\sqrt{-5})/2 \end{smallmatrix}\right)$. In a similar way, with x and y replaced by $\lambda x' = 1+\sqrt{-5}$ and $\lambda y' = 2$, and using $\alpha = 1$, $\beta = -1$, $\gamma = -1$, $\delta = 0$, $\mu' = 1$, and $\nu' = (1-\sqrt{-5})/2$, we get the matrix $N = \left(\begin{smallmatrix} \lambda x' & \mu' \\ \lambda y' & \nu' \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1+\sqrt{-5} & 1 \\ 2 & (1-\sqrt{-5})/2 \end{smallmatrix}\right)$. Then

$$\begin{aligned} A = MN^{-1} &= \begin{pmatrix} 2 & (1+\sqrt{-5})/2 \\ 1+\sqrt{-5} & (-1+\sqrt{-5})/2 \end{pmatrix} \begin{pmatrix} (1-\sqrt{-5})/2 & -1 \\ -2 & 1+\sqrt{-5} \end{pmatrix} \\ &= \begin{pmatrix} -2\sqrt{-5} & -4+\sqrt{-5} \\ 4-\sqrt{-5} & -4-\sqrt{-5} \end{pmatrix}. \end{aligned}$$

Check $A \in \mathrm{SL}_2(\mathbf{Z}[\sqrt{-5}])$ and $Az' = z$, so $A(3/(1-\sqrt{-5})) = 2/(1+\sqrt{-5})$.

Appendix A. Generators for $\mathrm{SL}_2(\mathbf{Z})$

There are two important matrices in $\mathrm{SL}_2(\mathbf{Z})$:

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

It is left to the reader to check that $S^2 = -I_2$, so S has order 4, while $T^k = \left(\begin{smallmatrix} 1 & k \\ 0 & 1 \end{smallmatrix}\right)$ for any $k \in \mathbf{Z}$, so T has infinite order.

Theorem A.1. *The group* $\mathrm{SL}_2(\mathbf{Z})$ *is generated by* S *and* T.

Proof. As the proof will reveal, this theorem is the Euclidean algorithm in disguise.

First we check how S and any power of T change the entries in a matrix. Verify that

$$S\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} -c & -d \\ a & b \end{pmatrix},$$

and

$$T^k\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a+ck & b+dk \\ c & d \end{pmatrix}.$$

---

[2] We can link these numbers by an integral matrix with determinant -1: $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)\frac{3}{1-\sqrt{-5}} = \frac{1-\sqrt{-5}}{3} = \frac{2}{1+\sqrt{-5}}$.

Thus, up to a sign change, multiplying by S on the left interchanges the rows. Multiplying by a power of T on the left adds a multiple of the second row to the first row and does not change the second row. Given a matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ in $\mathrm{SL}_2(\mathbf{Z})$, we can carry out the Euclidean algorithm on a and c by using left multiplication by S and powers of T. We use the power of T to carry out the division (if $a = cq + r$, use $k = -q$) and use S to interchange the roles of a and c to guarantee that the larger of the two numbers (in absolute value) is in the upper-left corner. (Multiplication by S will cause a sign change, but this has no serious effect on the algorithm.)

Since $ad - bc = 1$, a and c are relatively prime, so the last step of Euclid's algorithm will have a remainder of 1. This means, after suitable multiplication by S's and T's, we will have transformed the matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ into a matrix with first column $\left(\begin{smallmatrix} \pm 1 \\ 0 \end{smallmatrix}\right)$ or $\left(\begin{smallmatrix} 0 \\ \pm 1 \end{smallmatrix}\right)$. Left-multiplying by S interchanges the rows up to a sign, so we can suppose the first column is $\left(\begin{smallmatrix} \pm 1 \\ 0 \end{smallmatrix}\right)$. Any matrix of the form $\left(\begin{smallmatrix} 1 & x \\ 0 & y \end{smallmatrix}\right)$ in $\mathrm{SL}_2(\mathbf{Z})$ must have $y = 1$ (the determinant is 1), and then it is $\left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right) = T^x$. A matrix $\left(\begin{smallmatrix} -1 & x \\ 0 & y \end{smallmatrix}\right)$ in $\mathrm{SL}_2(\mathbf{Z})$ must have $y = -1$, so the matrix is $\left(\begin{smallmatrix} -1 & x \\ 0 & -1 \end{smallmatrix}\right) = (-I_2)T^{-x}$. Since $-I_2 = S^2$, we can finally unwind and express our original matrix in terms of S's and T's. □

Example A.2. Take $A = \left(\begin{smallmatrix} 26 & 7 \\ 11 & 3 \end{smallmatrix}\right)$. Since $26 = 11 \cdot 2 + 4$, we want to subtract $11 \cdot 2$ from 26:

$$T^{-2}A = \begin{pmatrix} 4 & 1 \\ 11 & 3 \end{pmatrix}.$$

Now we want to switch the roles of 4 and 11. Multiply by S:

$$ST^{-2}A = \begin{pmatrix} -11 & -3 \\ 4 & 1 \end{pmatrix}.$$

Dividing -11 by 4, we have $-11 = 4 \cdot (-3) + 1$, so we want to add $4 \cdot 3$ to -11. Multiply by T^3:

$$T^3ST^{-2}A = \begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix}.$$

Once again, multiply by S two switch the entries of the first column (up to sign):

$$ST^3ST^{-2}A = \begin{pmatrix} -4 & -1 \\ 1 & 0 \end{pmatrix}.$$

Our final division is: $-4 = 1(-4) + 0$. We want to add 4 to -4, so multiply by T^4:

$$T^4ST^3ST^{-2}A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = S.$$

Left-multiplying by the inverses of all the S's and T's on the left side, we obtain

$$A = T^2S^{-1}T^{-3}S^{-1}T^{-4}S.$$

Since $S^4 = I_2$, we can write S^{-1} as S^3 if we wish to use a positive exponent on S. However, a similar idea does not apply to the negative powers of T.

Remark A.3. Since $ST = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right)$ has order 6, we can write $\mathrm{SL}_2(\mathbf{Z}) = \langle S, ST \rangle$, which is a generating set of elements with finite order.

References

[1] E. B. Freitag, "Hilbert Modular Forms," Springer-Verlag, 1990.

[2] P. B. Garrett, "Holomorphic Hilbert Modular Forms," Wadsworth & Brooks/Cole, 1990.