MODULAR FORMS 2019: LATTICES

ZEÉV RUDNICK

1. The space of lattices

Definition. *A lattice in $\mathbb{R}^d$ is a discrete subgroup $L \subset \mathbb{R}^d$ which spans $\mathbb{R}^d$.*

The canonical example is the integer lattice $\mathbb{Z}^d$.

"Discrete" means that any element $\ell \in L$ is isolated from the rest, that is there is some $\epsilon(\ell) > 0$ so that $\mathrm{dist}(\ell, \ell') = |\ell - \ell'| \geq \epsilon(\ell)$ for all $\ell' \neq \ell$ in L. Since L is a subgroup of $\mathbb{R}$, we may in fact take ϵ uniform, by translation invariance of the distance: if $\delta = \inf |\ell| = \mathrm{dist}(\ell, 0)$ then $\mathrm{dist}(\ell, \ell') = |\ell' - \ell| = \mathrm{dist}(\ell - \ell', 0) \geq \delta$.

Discreteness also implies there L has no accumulation points, because if $\{\ell_n\}$ is a sequence of distinct points with $\ell_n \to x$, then we may, by throwing out some points, and relabeling we may assume that $|\ell_1 - x| \geq |\ell_2 - x| \geq \cdots \searrow 0$. But then $0 < |\ell_{n+1} - \ell_n| \leq |\ell_{n+1} - x| + |x - \ell_n| \to 0$ contradicting discreteness.

Therefore any subset of L admits a shortest vector (not necessarily unique).

Theorem 1.1. *Any lattice $L \subset \mathbb{R}^d$ has a basis: There is a basis $w_1, \ldots, w_d$ of $\mathbb{R}^d$ such that $L = \mathbb{Z}w_1 + \cdots + \mathbb{Z}w_d$.*

Exercise 1. *Conversely, a set of the form $\mathbb{Z}w_1 + \cdots + \mathbb{Z}w_d$ with w_i linearly independent is a lattice.*

We begin with the one-dimensional case ($d = 1$).

Lemma 1.2. *A lattice in $\mathbb{R}$ is of the form $L = \mathbb{Z}w$ where $w \neq 0$ is a shortest nonzero vector: $|\ell| \geq |w|$ for all $0 \neq \ell \in L$.*

Proof. Let $\delta := \mathrm{dist}(0, L\backslash\{0\}) = \inf(\mathrm{dist}(\ell, 0) : \ell \neq 0) > 0$. By symmetry $\ell \mapsto -\ell$, we can find a sequence of positive elements of L so that $\ell_n \to \delta$. Since L has no accumulation points, that sequence has to stabilize: $\ell_n = \ell_N$ for all $n \geq N$, so that $w = \ell_N = \delta$ is a shortest vector.

Date: March 27, 2019.

Now we show that $L = \mathbb{Z}w$: By replacing w by $-w$, we can assume that $w > 0$. Clearly $\mathbb{Z}w \subset L$, and if there is some vector $\ell \in L\backslash\mathbb{Z}w$ then there is some integer n so that $nw < \ell < (n+1)w$, and then $\ell' := \ell - nw$ is a nonzero positive element of L which is shorter than w:

$$0 < \ell' = \ell - nw < (n+1)w - nw = w,$$

a contradiction. □

Now let's do the case $d = 2$ (and then stop).

Lemma 1.3. *A lattice in $\mathbb{R}^2$ is of the form $\mathbb{Z}w_1 + \mathbb{Z}w_2$ with w_1, w_2 linearly independent (over $\mathbb{R}$). Moreover, we may take w_1 a shortest nonzero vector, and w_2 a shortest vector linearly independent from w_1.*

Proof. Let $0 \neq w_1 \in L$ be a shortest vector. Then $L_1 := L \cap \mathbb{R}w_1$ is a lattice in $\mathbb{R}w_1$, and w_1 is a shortest vector in L_1, and so by the 1-dim case, $L_1 = L \cap \mathbb{R}w_1 = \mathbb{Z}w_1$.

Now take a shortest vector w_2 in $L\backslash L \cap \mathbb{R}w_1 = L\backslash\mathbb{Z}w_1$ (it exists because by discreteness, and subset of L admits a shortest vector). Note that $L \cap \mathbb{R}w_2 = \mathbb{Z}w_2$ again by the 1-dim case.

Because $w_2 \notin \mathbb{R}w_1$, we must have that w_1, w_2 span $\mathbb{R}^2$.

We claim that $L = \mathbb{Z}w_1 + \mathbb{Z}w_2$. Otherwise, take a vector $v \in L\backslash\mathbb{Z}w_1 + \mathbb{Z}w_2$. Write $v = x_1w_1 + x_2w_2$ with $x_i \in \mathbb{R}$. If one of x_i is integer, then we can replace v by $v' = v - x_iw_i$ to get a vector of the form $x_jw_j \in \mathbb{R}w_j \cap L = \mathbb{Z}w_j$, and so also the second coordinate is integer, contradicting $v \notin \mathbb{Z}w_1 + \mathbb{Z}w_2$. So we must have both $x_i \notin \mathbb{Z}$.

Take integers n_i so that $0 < |x_i - n_i| \leq 1/2$, and replace v by $v' = v - (n_1w_1 + n_2w_2) = y_1w_1 + y_2w_2$, to get a vector $v' = \in L\backslash(\mathbb{Z}w_1 + \mathbb{Z}w_2)$ which is small: Since y_1w_1, y_2w_2 are linearly independent, then by the refined triangle inequality,

$$|y_1w_1 + y_2w_2| <_{\neq} |y_1w_1| + |y_2w_2|$$

Recall $|w_1| \leq |w_2|$ and $|y_i| \leq 1/2$ to get

$$|v'| < |y_1w_1| + |y_2w_2| \leq \frac{1}{2}|w_1| + \frac{1}{2}|w_2| \leq \frac{1}{2}|w_2| + \frac{1}{2}|w_2| = |w_2|$$

and so $v' \in L\backslash\mathbb{R}w_1$ is a vector in L, linearly independent of w_1, which is shorter than w_2, contradicting the choice of w_2.

Hence $L = \mathbb{Z}w_1 + \mathbb{Z}w_2$. □

Remark: Let $L \subset \mathbb{R}^d$ be a discrete subgroup. The following are equivalent

(1) L spans $\mathbb{R}^d$
(2) $L = \mathbb{Z}w_1 + \cdots + \mathbb{Z}w_d$ for a basis of $\mathbb{R}^d$

(3) $\mathbb{R}^d/L$ is compact,
(4) $\mathrm{vol}(\mathbb{R}^d/L) < \infty$, that is there is a "fundamental domain" for L with finite volume.

1.1. **Change of basis and** $\mathrm{GL}(2,\mathbb{Z})$**.** Suppose $L = \mathbb{Z}w_1 + \mathbb{Z}w_2 = \mathbb{Z}w_1' + \mathbb{Z}w_2'$. This happens if and only if there is an invertible integer matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}(2,\mathbb{Z})$ such that

$$w_1' = aw_1 + w_2, \quad w_2 = cw_1 + dw_2$$

Note that for $A \in M(2,\mathbb{Z})$ to be invertible over $\mathbb{Z}$ it is necessary and sufficient that $\det A = \pm 1$ is invertible in $\mathbb{Z}$.

1.2. **Homothety classes.** Now identify $\mathbb{R}^2$ with $\mathbb{C}$. We say two lattices $L, L' \subset \mathbb{C}$ are homothetic if $L' = \lambda L$ for some scalar $\lambda \in \mathbb{C}^*$. Equivalently, L' is obtained from L by some dilation with a positive number $r > 0$ and a rotation. This is clearly an equivalence relation.

Let $\mathcal{R}$ be the set of lattices in $\mathbb{C}$, and $X(1) := \mathcal{R}/\mathbb{C}^*$ the set of homothety classes. We want to give a geometric description of $X(1)$.

Let

$$\mathcal{M} = \{(w_1, w_1) \in \mathbb{C}^2 : \mathrm{Im}(w_1/w_2) > 0\}$$

To any pair $(w_1, w_2) \in \mathcal{M}$ we associate the lattice $L = \mathbb{Z}w_1 + \mathbb{Z}w_2 \in \mathcal{R}$. Conversely, to any lattice $L \subset \mathbb{C}$ we have a basis w_1, w_2 so in particular w_1, w_2 are linearly independent over $\mathbb{R}$, so that $\mathrm{Im}(w_1/w_2) \neq 0$. Since

$$\mathrm{Im}\,\frac{1}{\tau} = -\,\mathrm{Im}(\tau)/|\tau|^2$$

we can change the role of w_1 and w_2 and obtain that the set of bases of L is split into two "oriented" equivalence classes, say the "positive" bases are those with $\mathrm{Im}(w_1/w_2) > 0$. Thus there is a surjective map

$$\mathcal{M} \to \mathcal{R}, \quad (w_1, w_2) \mapsto \mathbb{Z}w_1 + \mathbb{Z}w_2$$

Any two (ordered) bases $\langle w_1, w_2\rangle$ and $\langle w_1', w_2'\rangle$ differ by an element of $\mathrm{GL}(2,\mathbb{Z})$, and two belong to the same oriented equivalence class iff they differ by an element in $\mathrm{SL}(2,\mathbb{Z})$, since

$$\mathrm{Im}\,\frac{aw_1 + bw_2}{cw_1 + dw_2} = \mathrm{Im}\,\frac{a\frac{w_1}{w_2} + b}{c\frac{w_1}{w_2} + d} = \frac{ad - bc}{|c\frac{w_1}{w_2} + d|^2}\,\mathrm{Im}(w_1/w_2)$$

Thus we obtain a bijection

$$\mathcal{M}/\,\mathrm{SL}(2,\mathbb{Z}) \simeq \mathcal{R}$$

This bijection descends to a bijection with the space $X(1)$ of homothety classes of lattices

$$\mathbb{C}^*\backslash\mathcal{M}/\operatorname{SL}(2,\mathbb{Z}) \simeq \mathcal{R}/\mathbb{C}^* =: X(1)$$

$$(w_1, w_2) \mapsto \mathbb{Z}1 + \mathbb{Z}\tau, \quad \tau := \frac{w_1}{w_2} \in \mathbb{H}$$

The number $\tau := \frac{w_1}{w_2}$ is an element of the upper half-plane $\mathbb{H}$, so the space $X(1)$ of homothety classes of lattices is identified with the quotient space $\mathbb{H}/\operatorname{SL}(2,\mathbb{Z})$.

1.3. **The fundamental domain.** To any homothety class of lattices, we can find, by scaling appropriately, a basis $(1, \tau)$ where 1 is a shortest vector, and $\tau = x + iy$ is linearly independent and $|\tau| \geq 1$ (since 1 is a shortest vector); and if necessary replacing it by $-\tau$, we can assume that $y = \operatorname{Im}(\tau) > 0$, so that $(1, \tau) \in \mathcal{M}$. We can also take τ to be a shortest vector linearly independent from 1. This forces $x = \operatorname{Re}(\tau) \in [-1/2, 1/2]$. Indeed, if we replace $\tau = w_2$ by $\tau' = \tau - n = w_2 - nw_1$, then we still get a basis element, with $\operatorname{Im}(\tau') = \operatorname{Im}(\tau) = y$, and

$$|\tau'|^2 = (x-n)^2 + y^2$$

so that we get a minimal value when $|x - n| \leq 1/2$. Thus each homothety class in $X(1)$ gives us an number in the (closure of the) region (see Figure 1)

$$\mathcal{F} = \{\tau \in \mathbb{H} : \operatorname{Re}(\tau) \in [-\frac{1}{2}, \frac{1}{2}), \quad |\tau| > 1 \text{ or } |\tau| = 1 \text{ and } \operatorname{Re}\tau \leq 0\}$$

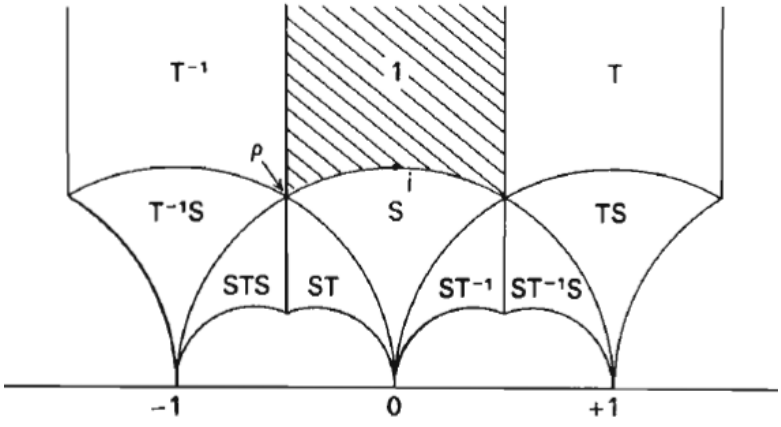

FIGURE 1. The fundamental domain $\mathcal{F}$ (shaded) and it's translates.

We will show that two elements of the interior of $\mathcal{F}$ represent different classes of $X(1)$, and that the only equivalences are of i with itself and of $\rho = e^{2\pi i/3}$ with itself.

From now on, we denote

$$\Gamma = \mathrm{SL}(2,\mathbb{Z})/\{\pm I\}$$

First, we define two important transformations $S, T \in \Gamma$

$$S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} : \tau \mapsto -\frac{1}{\tau} \qquad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} : \tau \mapsto \tau + 1$$

Theorem 1.4. *a) For every $\tau \in \mathbb{H}$, there is some $g \in \Gamma$ so that $g\tau \in \mathcal{F}$.*

b) If two distinct points $\tau, \tau' \in \overline{\mathcal{F}}$ are Γ-equivalent, then they lie on the boundary of $\mathcal{F}$, and either $\mathrm{Re}(\tau) = \pm 1/2$ and $\tau' = T^{\pm 1}\tau = \tau \pm 1$, or $|\tau| = 1$ and $\tau' = S\tau = -1/\tau$,

c) Let $I(\tau) = \mathrm{Stab}_\Gamma(\tau)$. Then $I(\tau) = \{\pm I\}$ except if τ is Γ-equivalent to

- *i, in which case $I(i) = \{\pm I, \pm S\}$*
- *$\rho := e^{2\pi i/3}$, in which case $I(\rho) = \{\pm I, \pm ST, \pm (ST)^2\}$ is generated by ST*
- *$-\overline{\rho} = e^{\pi i/3}$, when $I(-\overline{\rho}) = \{\pm I, \pm TS, \pm (TS)^2\}$ is generated by TS.*

d) Γ (in fact $\mathrm{SL}(2,\mathbb{Z})$) is generated by S and T.

Proof. a) Let $\Gamma' = \langle S, T\rangle \subseteq \Gamma$. For $\tau \in \mathbb{H}$, consider the Γ' orbit. Recall that

$$\mathrm{Im}\, g\tau = \frac{\mathrm{Im}\,\tau}{|c\tau + d|^2}, \quad g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Take a point $g\tau \in \Gamma'\tau$ with maximal imaginary part, which means that the vector $c\tau + d \in \mathbb{Z}1 + \mathbb{Z}\tau$ is shortest (in the orbit of Γ'). Necessarily $|g\tau| \geq 1$, otherwise $S(g\tau) \in \Gamma'\tau$ would have bigger imaginary part, because if $|g\tau| < 1$ then

$$\mathrm{Im}\, Sg\tau = \frac{\mathrm{Im}\, g\tau}{|g\tau|^2} > \mathrm{Im}\, g\tau$$

contradicting the maximality of $\mathrm{Im}\, g\tau$.

Now if $n - \frac{1}{2} \leq \mathrm{Re}\, g\tau < n + 1/2$, apply T^{-n} to $g\tau$ to obtain a point $\tau' = T^{-n}g\tau = g\tau - n \in \Gamma'\tau$ with real part in $[-1/2, 1/2)$, which has the same imaginary part as $g\tau$ and so lies in $\overline{\mathcal{F}}$.

We skip the proof of (b) and (c).

To prove (d), that $\Gamma = \langle S, T\rangle$. Given $g \in \Gamma$, pick $\tau_0 \in \mathrm{int}\mathcal{F}$ (e.g. $\tau_0 = 2i$) and consider the point $g\tau_0$. By part (a), there is some $g' \in \Gamma'$ such that $g'g\tau_0 \in \overline{\mathcal{F}}$. Then the points τ_0 and $g'g\tau_0$ lie in $\overline{\mathcal{F}}$, are equivalent

modulo Γ, and one of them is in the interior, hence by part (b) they must coincide: $\tau_0 = g'g\tau_0$. But by part (c), an interior point has only a trivial stabilizer, hence $g = \pm g'^{-1} \in \Gamma'$. Thus $\Gamma = \Gamma' = \langle S, T\rangle$. $\square$

1.4. **An algorithmic proof of generation of** $\mathrm{SL}(2,\mathbb{Z})$**.** Here is an alternative, algorithmic, proof that $\mathrm{SL}(2,\mathbb{Z})$ is generated by $S = \begin{pmatrix} & -1 \\ 1 & \end{pmatrix}$ and $T = \begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix}$: First observe the action of left multiplication of a matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ by S and T^n:

$$SA = \begin{pmatrix} & -1 \\ 1 & \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} -c & -d \\ a & b \end{pmatrix}$$

that is we switch the rows of A (and change the sign of the second row);

$$T^n A = \begin{pmatrix} 1 & n \\ & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a+nc & b+nd \\ c & d \end{pmatrix}$$

that is we add a multiple of the second row to the first, and do not change the second row.

So starting with A, if $|a| \geq |c|$ then we add a suitable multiple of the second row to the first (i.e. multiply A by T^n), to replace $a \mapsto a' = a + nc$ where now $|a'| < |c|$. Then we switch the first and second row (and change the sign of the old first row), to again be in the position that the new $a'' = -c$ is bigger in absolute value than the new $c'' = a'$. Now continue until we get to a point that the resulting matrix is upper triangular, and having determinant one with integer entries it must be of the form $\pm\begin{pmatrix} 1 & n \\ & 1 \end{pmatrix} = S^{\{0,2\}}T^n$. Hence we are done.

Example: $A = \begin{pmatrix} 4 & 9 \\ 3 & 7 \end{pmatrix}$. Then

$$A \mapsto T^{-1}A = \begin{pmatrix} 1 & -1 \\ & 1 \end{pmatrix}\begin{pmatrix} 4 & 9 \\ 3 & 7 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 3 & 7 \end{pmatrix} \mapsto ST^{-1}A = \begin{pmatrix} -3 & -7 \\ 1 & 2 \end{pmatrix}$$

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

Hence we find (recall that $S^{-1} = -S = S^3$)

$$A = TS^{-1}T^{-3}S^{-1}S^2T^2 = TS^{-1}T^{-3}ST^2 = -TST^{-3}ST^2$$