**Math 272y: Rational Lattices and their Theta Functions**

11 September 2019: Lattice basics II

**Lattice duality.** Suppose first that $V$ is a finite-dimensional real vector space without any further structure, and let $V^*$ be its dual vector space, $V^* = \mathrm{Hom}(V, \mathbf{R})$. We may still define a lattice $L \subset V$ as a discrete co-compact subgroup, or concretely (but not canonically) as the $\mathbf{Z}$-span of an $\mathbf{R}$-basis $e_1, \dots, e_n$. The *dual lattice* is then

$$L^* := \{\mathbf{x}^* \in V^* : \forall \mathbf{y} \in L,\ \mathbf{x}^*(\mathbf{y}) \in \mathbf{Z}\}.$$

This is indeed a lattice: we readily see that if $e_1, \dots, e_n$ is a $\mathbf{Z}$-basis for $L$ then the dual basis[1] $e_1^*, \dots, e_n^*$ is a $\mathbf{Z}$-basis for $L^*$. It soon follows that $L^* = \mathrm{Hom}(L, \mathbf{Z})$ (that is, every homomorphism $L \to \mathbf{Z}$ is realized by a unique $\mathbf{x}^* \in L^*$), and — as suggested by the "dual" terminology — the canonical identification of the double dual $(V^*)^*$ with $V$ takes the dual basis of $e_1^*, \dots, e_n^*$ back to $e_1, \dots, e_n$, and thus takes the dual of $L^*$ back to $L$. Once we have chosen some basis for $V$, and thus an identification $V \cong \mathbf{R}^n$, we can write any basis as the columns of some invertible matrix $M$, and then that basis generates the lattice $M\mathbf{Z}^n$; the dual basis then consists of the row vectors of $M^{-1}$, so the dual lattice is $\mathbf{Z}^n M^{-1}$ (in coordinates that make $e_1^*, \dots, e_n^*$ unit vectors).

We shall soon use Fourier analysis on $V$ and on its quotient torus $V/L$. In this context, $V^*$ is the Pontrjagin dual of $V$: any $\mathbf{x}^* \in V^*$ gives a continuous homomorphism $\mathbf{y} \mapsto \exp(2\pi i\, \mathbf{x}^*(\mathbf{y}))$ from $V$ to the unit circle. This identifies $L^*$ with the annihilator of $L$, and thus with the Pontrjagin dual of $V/L$.

Now restore our usual setting where $L$ is equipped with a symmetric bilinear pairing $\langle \cdot, \cdot \rangle$. Assume that the pairing is *nondegenerate*. Then its linear extension to $V = L \otimes \mathbf{R}$ identifies $V$ with $V^*$, so we may and do regard $L^*$ as a lattice *in the same space* $L \otimes \mathbf{R}$, and this can give rise to a much richer structure; notably, when $L$ is integral, $L^*$ contains $L$ with finite index, and the index is $|\mathrm{disc}\, L|$. Before pursuing this further, we give a few general formulas and relations that do not even assume that $L$ is rational, and then some general constructions of new lattices from old and their effect on the dual.

Fix a $\mathbf{Z}$-basis for $L$ (and thus a choice of coordinates for $L$ and $V$), let $A$ be the Gram matrix, and recall that $\langle \mathbf{x}, \mathbf{y} \rangle = \mathbf{x}^{\mathsf{T}} A \mathbf{y}$ for all $\mathbf{x}, \mathbf{y} \in V$. If $\mathbf{x} \in L^*$ then $\mathbf{x}^{\mathsf{T}} A \mathbf{y} \in \mathbf{Z}$ for all integer vectors $\mathbf{y}$; but this is equivalent to $\mathbf{x}^{\mathsf{T}} A$ having integer coordinates. Since $\mathbf{x}^{\mathsf{T}} A = (A^{\mathsf{T}} \mathbf{x})^{\mathsf{T}}$, this means that the dual

[1] Recall that the dual basis consists of the functionals determined by

$$e_i^*(e_j) = \delta_{ij} = \begin{cases} 1, & \text{if } i = j; \\ 0, & \text{if } i \neq j. \end{cases}$$

basis for $L^*$ consists of the columns of $(A^\mathsf{T})^{-1}$. It follows that the Gram matrix for $L^*$ relative to this basis is $A^{-1}A\,(A^\mathsf{T})^{-1} = (A^\mathsf{T})^{-1}$. In particular,

$$\operatorname{disc} L^* = \det(A^\mathsf{T})^{-1} = (\det A)^{-1} = (\operatorname{disc} L)^{-1}. \tag{1}$$

**Scaling, direct sums, and sublattices.** If $L$ is a lattice then for every $c \in \mathbf{R}$ we obtain a pairing on $L$, call it temporarily $\langle\cdot,\cdot\rangle_c$, by defining $\langle \mathbf{x}, \mathbf{y}\rangle_c = c\langle \mathbf{x}, \mathbf{y}\rangle$. We denote the resulting lattice by $L\langle c\rangle$. This scaled lattice is nondegenerate if and only if $L$ is nondegenerate and $c \neq 0$; it has the same signature as $L$ if $c > 0$, and the opposite signature $(n_-, n_+, n_0)$ if $c < 0$; and if $L$ has Gram matrix $A$ then $L\langle c\rangle$ has Gram matrix $cA$ relative to the same basis. The discriminant and dual are thus given by

$$\operatorname{disc}(L\langle c\rangle) = c^n \operatorname{disc} L, \quad (L\langle c\rangle)^* = c^{-1}L^*$$

where $n$ is the rank of $L$.

The (orthogonal) direct sum $L_1 \oplus L_2$ of lattices $L_1$ and $L_2$ is the group $L_1 \times L_2$, with

$$\langle (\mathbf{x}_1, \mathbf{x}_2), (\mathbf{y}_1, \mathbf{y}_2)\rangle_{L_1 \oplus L_2} = \langle \mathbf{x}_1, \mathbf{y}_1\rangle_{L_1} + \langle \mathbf{x}_2, \mathbf{y}_2\rangle_{L_2}.$$

It is nondegenerate if and only if both $L_1$ and $L_2$ are nondegenerate; the signature of $L_1 \oplus L_2$ is the sum of the signatures of $L_1$ and $L_2$ (so for instance $L_1 \oplus L_2$ is positive-(semi)definite if and only if both $L_1$ and $L_2$ are); and if $L_1, L_2$ have Gram matrices $A_1, A_2$ then $L_1 \oplus L_2$ has Gram matrix $\left(\begin{smallmatrix} A_1 & 0 \\ 0 & A_2 \end{smallmatrix}\right)$ relative to the concatenation of the same bases. The discriminant and dual are given by

$$\operatorname{disc}(L_1 \oplus L_2) = \operatorname{disc} L_1 \cdot \operatorname{disc} L_2, \quad (L_1 \oplus L_2)^* = L_1^* \oplus L_2^*.$$

We often abbreviate $L \oplus L$ as $L^2$, and more generally write $L^k$ as the direct sum of $k$ copies of $L$ ($k \geq 0$); note that this is consistent with the use of $\mathbf{Z}^n$ for the integer lattice in $\mathbf{R}^n$ with the usual inner product. We also write $\oplus_{j=1}^k L_j$ for the orthogonal direct sum $L_1 \oplus \cdots \oplus L_k$.

If $(L, \langle\cdot,\cdot\rangle)$ is a lattice, and $L' \subset L$ is any subgroup, then $L'$ is a free abelian group, so the restriction of $\langle\cdot,\cdot\rangle$ to $L'$ makes $L'$ a lattice too. Then $L' \otimes \mathbf{R}$ is a subspace of $L \otimes \mathbf{R}$, and is the same as $L \otimes \mathbf{R}$ if and only if the index $[L : L']$ is finite. In this case $L'$ is also a lattice in $L \otimes \mathbf{R}$, so has the same signature as $L$. We claim that then

$$\operatorname{disc} L' = [L : L']^2 \operatorname{disc} L. \tag{2}$$

This is to be expected from the interpretation of $|\operatorname{disc} L|$ as $(\operatorname{Vol}(V/L))^2$ (together with the fact that $\operatorname{disc} L$ and $\operatorname{disc} L'$ have the same sign), because we can form a fundamental region for $V/L'$ from $[L : L']$ disjoint translates of a fundamental region for $V/L$. To prove (2), write $L' = ML$ for some

integer matrix $M$ (that is, choose generators for $L'$ and write each in terms of the generators of $L$). Then $[L : L'] = |\det M|$, and $L'$ has Gram matrix $M^\intercal A M$, whose determinant is $(\det M)^2 \det A$, confirming (2).

If $L'$ is a finite-index sublattice of $L$, then $(L')^* \supseteq L^*$, and $[(L')^* : L^*] = [L : L']$ by combining (1) with (2). In fact, the quotient groups $L/L'$ and $(L')^*/L^*$ are isomorphic; there is generally no canonical isomorphism, but there is a canonical perfect pairing

$$(\cdot, \cdot) : ((L')^*/L^*) \times (L/L') \to \mathbf{Q}/\mathbf{Z} \tag{3}$$

that identifies each group with the other's dual. To define the pairing, lift elements $x^*, y$ of $(L')^*/L^*$ and $L/L'$ to some $\mathbf{x}^* \in (L')^*$ and $\mathbf{y} \in L$, and define $(x^*, y) = \mathbf{x}^*(\mathbf{y}) \bmod \mathbf{Z}$. It is routine to check that this pairing is well-defined (that is, depends on $x^*, y$ but not on the choice of lifts $\mathbf{x}^*, \mathbf{y}$). We next check that pairing is perfect. If there is some $x^*$ such that $(x^*, y) = 0$ for all $y \in (L/L')$ then $\mathbf{x}^*(\mathbf{y}) \in \mathbf{Z}$ for all $\mathbf{y} \in L$, so $\mathbf{x}^* \in L^*$ so $x = 0$ in $(L')^*/L^*$. Likewise, if there is some $y$ such that $(x^*, y) = 0$ for all $\mathbf{x}^* \in ((L')^*/L^*)$ then $\mathbf{y} \in ((L')^*)^* = L'$ so $y = 0$ in $(L/L')$.

**The discriminant group and form.** A lattice $L$ is integral if and only if $L \subseteq L^*$. In this case, the index $[L^* : L]$ is $(\operatorname{disc} L \,/\, \operatorname{disc} L^*)^{1/2} = |\operatorname{disc} L|$ by (2). In particular, $L$ is self-dual if and only if $L$ is integral and $\operatorname{disc} L = \pm 1$; lattices of discriminant $\pm 1$ are also called "unimodular".[2] For example, $\mathbf{Z}$ is self-dual, as is $\mathbf{Z}^n$ (positive-definite), and more generally $\mathbf{Z}^{n_+} \oplus (\mathbf{Z}\langle -1\rangle)^{n_-}$ (signature $(n_+, n_-)$) for any nonnegative integers $n, n_+, n_-$. Indeed $L\langle -1\rangle$ is self-dual if and only if $L$ is, and $L_1 \oplus L_2$ is self-dual if and only if $L_1$ and $L_2$ are. The culminating result of the first part (chapters I–V) of Serre's *A Course in Arithmetic* is the classification of indefinite self-dual lattices.

If $L$ is integral then $L^*/L$ is a finite abelian group of order $|\operatorname{disc} L|$, called the *discriminant group* of $L$. If $|\operatorname{disc} L|$ is not squarefree then the structure of this group can give a finer lattice invariant than just its size; for instance, the indefinite integral lattices $\mathbf{Z}^2 \oplus \mathbf{Z}\langle -9\rangle$ and $\mathbf{Z}^2\langle 3\rangle \oplus \mathbf{Z}\langle -1\rangle$ have the same signature and discriminant, but are not isomorphic because $\mathbf{Z}^2 \oplus \mathbf{Z}\langle -9\rangle$ has cyclic discriminant group but $\mathbf{Z}^2\langle 3\rangle \oplus \mathbf{Z}\langle -1\rangle$ does not.

An even finer invariant is the *discriminant form*, which is the symmetric bilinear pairing $(\cdot, \cdot) : (L^*/L) \times (L^*/L) \to \mathbf{Q}/\mathbf{Z}$ induced from $\langle \cdot, \cdot \rangle$: if $\mathbf{x}, \mathbf{x}', \mathbf{y}, \mathbf{y}' \in L^*$ with $\mathbf{x}' \equiv \mathbf{x}$ and $\mathbf{y}' \equiv \mathbf{y} \bmod L$ then $\langle \mathbf{x}', \mathbf{y}' \rangle \equiv \langle \mathbf{x}, \mathbf{y} \rangle \bmod \mathbf{Z}$, so we may define $([\mathbf{x}], [\mathbf{y}]) = \langle \mathbf{x}, \mathbf{y} \rangle \bmod \mathbf{Z}$. This is a perfect pairing: its kernel consists of the cosets mod $L$ of $\mathbf{x} \in L^*$ such that $\langle \mathbf{x}, \mathbf{y} \rangle \in \mathbf{Z}$ for all $\mathbf{y} \in L^*$; but such $\mathbf{x}$ are in the dual of $L^*$, which is $L$, so they map to the zero element of the discriminant group. (This is a special case of the pairing (3) and of the argument that that pairing is perfect.) For example, the indefinite integral lattices $\mathbf{Z}^{n-1} \oplus \mathbf{Z}\langle -3\rangle$ and $\mathbf{Z}^{n-2} \oplus \mathbf{Z}\langle -1\rangle \oplus \mathbf{Z}\langle 3\rangle$ (any $n \geq 2$) have the same signature $(n-1, 1)$ and isomorphic discriminant groups $\mathbf{Z}/3\mathbf{Z}$, but are not isomorphic because only $\mathbf{Z}^{n-1} \oplus \mathbf{Z}\langle -3\rangle$ has dual vectors of norm $-1/3 \bmod 1$. [Warning:

[2] One sometimes also encounters "bimodular" or "trimodular" for lattices of discriminant $\pm 2$ or $\pm 3$ respectively.

it *is* possible for an indefinite lattice to be isomorphic with more than one lattice of the form $\oplus_{j=1}^n \mathbf{Z}\langle c_j\rangle$, or equivalently for one quadratic form to be isomorphic with more than one "diagonal form" $\sum_{j=1}^n c_j x_j^2$; for example,[3] $x_1^2 - 5x_2^2 = -(2x_1+5x_2)^2 + 5(x_1+2x_2)^2$, with $\left(\begin{smallmatrix}2 & 5\\ 1 & 2\end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbf{Z})$ because $\det\left(\begin{smallmatrix}2 & 5\\ 1 & 2\end{smallmatrix}\right) = -1$ is a unit.]

*Special behavior at* 2*: the characteristic coset and shadow, etc.* Suppose now that $L$ is an integral lattice of odd discriminant. Then the homomorphism $L \to \mathbf{Z}/2\mathbf{Z}$, $\mathbf{x} \mapsto \langle \mathbf{x}, \mathbf{x}\rangle \bmod 2$ is represented by some coset $c \in L/2L$, called the *characteristic coset*; that is, $c$ consists of those $\mathbf{c} \in L$ such that $\langle \mathbf{x}, \mathbf{x}\rangle \equiv \langle \mathbf{x}, \mathbf{c}\rangle \bmod 2$ for all $\mathbf{x} \in L$. For example, the characteristic coset of $\mathbf{Z}^n$ consists of the vectors all of whose coordinates are odd integers; if $L_1, L_2$ are integral lattices of odd discriminant with characteristic cosets $c_1, c_2$, then the characteristic coset of $L_1 \oplus L_2$ is $(c_1, c_2)$; and the characteristic coset is $2L$ if and only if $L$ is even. All vectors in $c$ have the same norm mod 8, because

$$Q(\mathbf{c} + 2\mathbf{x}) = Q(\mathbf{c}) + 4(\langle \mathbf{c}, \mathbf{x}\rangle + \langle \mathbf{x}, \mathbf{x}\rangle) \tag{4}$$

and $\langle \mathbf{c}, \mathbf{x}\rangle$ and $\langle \mathbf{x}, \mathbf{x}\rangle$ have the same parity. This generalizes the fact that all odd squares are $1 \bmod 8$. This residue mod 8 is thus an invariant of any lattice of odd discriminant; this invariant additive under direct sums.[4] These results are sometimes stated for the "shadow" $\frac{1}{2}c$, which is a translate of $L$ by a half-lattice vector, and has all norms congruent mod 2 (note that in general these norms need not be integers, only quarter-integers); e.g. for $L = \mathbf{Z}^n$ the shadow norms are $n/4 \bmod 2$, and more generally if $L = \oplus_j \mathbf{Z}\langle c_j\rangle$ for some odd $c_j$ then the shadow norms are all $\frac{1}{4}\sum_j c_j \bmod 2$.

If $L$ is an *even* nondegenerate lattice then $Q$ descends to a well-defined quadratic form $q : L^*/L \to \mathbf{Q}/2\mathbf{Z}$, for a reason similar to (4): if $\mathbf{x}^* \in L^*$ and $\mathbf{y} \in L$ then

$$Q(\mathbf{x} + \mathbf{y}) = Q(\mathbf{x}) + 2\langle \mathbf{x}, \mathbf{y}\rangle + Q(\mathbf{y}),$$

and both $\langle \mathbf{x}, \mathbf{y}\rangle$ and $Q(\mathbf{y})$ are even integers. This quadratic form refines the pairing $(\cdot, \cdot)$, in the sense that

$$2(x, y) = q(x + y) - q(x) - q(y)$$

in $\mathbf{Q}/2\mathbf{Z}$, so from the values of $q$ we may recover any $(x, y)$ as an element of $\mathbf{Q}/\mathbf{Z}$.

[3] This example comes from the multiplication-by-$a$ map on the ring $\mathbf{Z}[\sqrt{5}]$, for the ring element $a = 2 + \sqrt{5}$ of algebraic norm $-1$. Note that the algebraic norm of $x_1 + x_2\sqrt{5}$ is $x_1^2 - 5x_2^2$, which is indeed a diagonal quadratic form; this is true more generally in any quadratic ring $\mathbf{Z}[\sqrt{\Delta}\,]$.

[4] Serre states this result only $\mathrm{disc}\, L = \pm 1$, but with essentially the same proof, which uses only that $\mathrm{disc}\, L$ is odd. We can generalize further to a rational lattice for which all the values of $\langle \cdot, \cdot\rangle$ have odd denominator and the discriminant also has odd numerator, i.e. a lattice that is 2-adically self-dual.