Math 272y: Rational Lattices and their Theta Functions

9 September 2019: Lattice basics

This first chapter is mainly for fixing definitions and notations. The mathematical content is mostly what one might expect from adapting to $\mathbf{Z}^n$ the familiar structure of symmetric pairings on $\mathbf{R}^n$. Still there are a few novel features, such as the notion of an even lattice and the connection with the Fermat–Pell equation.

By a *lattice* we mean a finitely-generated free abelian group L together with a symmetric bilinear pairing $L \times L \to \mathbf{R}$. The *rank* of the lattice is the rank of L, which is the integer $n \geq 0$ such that $L \cong \mathbf{Z}^n$. The bilinear form is often denoted $\langle \cdot, \cdot \rangle$. The lattice is said to be *rational* if $\langle \cdot, \cdot \rangle$ takes values in $\mathbf{Q}$, and *integral* if $\langle \cdot, \cdot \rangle$ takes values in $\mathbf{Z}$.

The associated quadratic form $Q : L \to \mathbf{R}$ is defined by $Q(x) = \langle \mathbf{x}, \mathbf{x} \rangle$; the well-known "polarization" identity

$$2\langle \mathbf{x}, \mathbf{y} \rangle = \langle \mathbf{x}+\mathbf{y}, \mathbf{x}+\mathbf{y} \rangle - \langle \mathbf{x}, \mathbf{x} \rangle - \langle \mathbf{y}, \mathbf{y} \rangle = Q(\mathbf{x}+\mathbf{y}) - Q(\mathbf{x}) - Q(\mathbf{y}) \tag{1}$$

lets us recover $\langle \cdot, \cdot \rangle$ from Q. It follows from (1) that the lattice is rational if and only if Q takes rational values. Note that it is *not* true that the lattice is integral if and only if Q takes integral values: certainly if $\langle \mathbf{x}, \mathbf{y} \rangle \in \mathbf{Z}$ for all $\mathbf{x}, \mathbf{y} \in L$ then $\langle \mathbf{x}, \mathbf{x} \rangle \in \mathbf{Z}$ for all $\mathbf{x} \in L$, but in the reverse direction we can only conclude that $\langle \cdot, \cdot \rangle$ takes half-integral values because of the factor of 2 in (1). We have already seen the example of $L = \mathbf{Z}^2$ and $\langle \mathbf{x}, \mathbf{y} \rangle = \frac{1}{2}\, \mathbf{x}^{\mathsf{T}} \left(\begin{smallmatrix} 2 & -1 \\ -1 & 2 \end{smallmatrix}\right) \mathbf{y}$, for which $Q(\mathbf{x}) = x_1^2 - x_1 x_2 + x_2^2 \in \mathbf{Z}$ for all $\mathbf{x} = (x_1, x_2) \in \mathbf{Z}^2$, but $\langle (1,0), (0,1) \rangle = -1/2$.

It also follows from (1) that if $(L, \langle \cdot, \cdot \rangle)$ is integral then $Q(\mathbf{x}+\mathbf{y}) \equiv Q(\mathbf{x}) + Q(\mathbf{y}) \bmod 2$ for all $\mathbf{x}, \mathbf{y} \in L$; that is, the map $L \to \mathbf{Z},\ \mathbf{x} \mapsto Q(\mathbf{x})$ descends to a homomorphism $L \to \mathbf{Z}/2\mathbf{Z}$. The lattice is said to be *even* if this homomorphism is trivial, i.e. if $\langle \mathbf{x}, \mathbf{x} \rangle \in 2\mathbf{Z}$ for all $\mathbf{x} \in L$. Note that conversely if a lattice has $\langle \mathbf{x}, \mathbf{x} \rangle \in 2\mathbf{Z}$ for all $\mathbf{x}$ then the lattice is automatically integral, again by (1). An integral lattice that is not even is said to be *odd*. "Most" integral lattices are odd, but even lattices arise naturally in several contexts and will be of particular interest to us.

To connect our definition of a lattice with our geometrical intuition for lattices, we often think of L as a subgroup of the real vector space $V = L \otimes \mathbf{R}$. The pairing $\langle \cdot, \cdot \rangle$ extends linearly to a symmetric bilinear form $V \times V \to \mathbf{R}$, which we again denote by $\langle \cdot, \cdot \rangle$. The lattice is said to be *degenerate* or *nondegenerate* according as the symmetric bilinear form on V is degenerate or nondegenerate respectively; likewise *positive (semi)definite*, *negative (semi)definite*, or *indefinite*. Recall that if $\dim V = n$ then for any symmetric bilinear form $\langle \cdot, \cdot \rangle$ on V there are orthogonal bases, i.e. a choice of coordinates such that $\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{j=1}^{n} c_j x_j y_j$ for some $c_j \in \mathbf{R}$, and the numbers of positive, negative, and zero coefficients c_j are invariants of the pairing, independent of the choice of orthogonal basis; these invariants constitute the *signature* (n_+, n_-, n_0) of the pairing $\langle \cdot, \cdot \rangle$, with $n = n_+ + n_- + n_0$.[1] We call this also the signature of the lattice. In particular, the lattice is nondegenerate if and only if $n_0 = 0$; it is positive (negative) semidefinite if and only if

[1] This is "Sylvester's law of inertia"; a proof sketch follows. Let V_0 be the kernel of the pairing, i.e. $\mathbf{x}_0 \in V_0$ if and only if $\langle \mathbf{x}_0, \mathbf{x} \rangle = 0$ for all $\mathbf{x} \in V$. Then $\langle \cdot, \cdot \rangle$ descends to a nondegenerate pairing on $V' := V/V_0$. By Gram-Schmidt there is an orthogonal basis for V'. Lift this basis arbitrarily to V, and extend by any basis of V_0 to obtain an orthogonal basis for V. Now $n_0 = \dim V_0$ is certainly invariant, and we've written $V' = V_+ \oplus V_-$ where $\dim V_\pm = n_\pm$ and

$n_- = 0$ (resp. $n_+ = 0$); and it is positive (negative) definite if and only if it is positive (negative) semidefinite and nondegenerate, i.e. if and only if it has signature $(n, 0, 0)$ (resp. $(0, n, 0)$). For a nondegenerate pairing or lattice we often omit n_0 and write the signature as (n_+, n_-).[2]

Warnings: i) We cannot use the definition "$\mathbf{x} \neq 0 \Rightarrow \langle \mathbf{x}, \mathbf{x} \rangle > 0$" to characterize positive-definite lattices L if $\mathbf{x}$ is allowed to range only over L (rather than $L \otimes \mathbf{R}$). A standard counterexample is $L = \mathbf{Z}^2$ and $\langle \mathbf{x}, \mathbf{y} \rangle = (x_1 - tx_2)(y_1 - ty_2)$ for some irrational constant t: the nonzero vector $\mathbf{x} = (t, 1) \in L \otimes \mathbf{R}$ satisfies $\langle \mathbf{x}, \mathbf{x} \rangle = 0$, but $\langle \mathbf{x}, \mathbf{x} \rangle$ is positive for every nonzero lattice vector. It *is* true that the lattice is positive (negative) *semi*definite if and only if $\langle \mathbf{x}, \mathbf{x} \rangle \geq 0$ (resp. $\langle \mathbf{x}, \mathbf{x} \rangle \leq 0$) for every $\mathbf{x} \in L$; and we shall soon see that for a *rational* lattice the positivity of $\langle \mathbf{x}, \mathbf{x} \rangle$ for all nonzero $\mathbf{x} \in L$ does guarantee that L is positive-definite.
ii) When $\langle \cdot, \cdot \rangle$ is positive-definite, one sees two definitions of the "norm" of a vector $\mathbf{x} \in V$: either the Euclidean length $\langle \mathbf{x}, \mathbf{x} \rangle^{1/2}$ of $\mathbf{x}$, or its square $\langle \mathbf{x}, \mathbf{x} \rangle = Q(\mathbf{x})$. We shall always use "norm" to mean Q, not $Q^{1/2}$; not only is this the more natural choice in the context of number theory, but also it is the choice that still makes sense for pairings for which Q can take negative values.

Alternatively, we could start from a finite-dimensional real vector space $V \cong \mathbf{R}^n$ together with a bilinear pairing $\langle \cdot, \cdot \rangle$, and define a A *lattice in* V to be a discrete co-compact subgroup $L \subset V$, that is, a discrete subgroup such that the quotient V/L is compact (and thus necessarily homeomorphic with the n-torus $(\mathbf{R}/\mathbf{Z})^n$). As an abstract group L is thus isomorphic with the free abelian group $\mathbf{Z}^n$ of rank n. Therefore L is determined by the images, call them $\mathbf{v}_1, \ldots, \mathbf{v}_n$, of the standard generators of $\mathbf{Z}^n$ under a group isomorphism $\mathbf{Z}^n \xrightarrow{\sim} L$. We say the $\mathbf{v}_i$ *generate*, or are *generators* of, L: each vector in L can be written as $\sum_{i=1}^n a_i \mathbf{v}_i$ for some *unique* integers $a_1, \ldots, a_n$. Vectors $\mathbf{v}_1, \ldots, \mathbf{v}_n \in V$ generate a lattice if and only if they constitute an $\mathbf{R}$-linear basis for V, and then L is the $\mathbf{Z}$-span of this basis. For instance, the $\mathbf{Z}$-span of the standard orthonormal basis $e_1, \ldots, e_n$ of $\mathbf{R}^n$ (with the standard Euclidean pairing $\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{j=1}^n x_j y_j$) is the lattice $\mathbf{Z}^n$. This more concrete definition is better suited for explicit computation, but less canonical because most lattices have no canonical choice of generators even up to isometries of V.

Choose a basis $e_1, \ldots, e_n$ of V, and thus an isomorphism of V with $\mathbf{R}^n$. Recall that the *Gram matrix* of a bilinear pairing $\langle \cdot, \cdot \rangle$ on V is the $n \times n$ matrix, call it A, whose (i, j) entry is $\langle e_i, e_j \rangle$. This matrix is symmetric if and only if the pairing is symmetric. Then for any vectors $\mathbf{x} = (x_1, \ldots, x_n)^\mathsf{T}$ and $\mathbf{y} = (y_1, \ldots, y_n)^\mathsf{T}$ we have

$$\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{i=1}^n \sum_{j=1}^n x_i y_j \langle e_i, e_j \rangle = \mathbf{x}^\mathsf{T} A \mathbf{y}. \tag{2}$$

Note that $\mathbf{x}, \mathbf{y}$ are regarded as *column* vectors (so that matrices can act on vectors from the left), and $\mathbf{x}^\mathsf{T}$ is the transpose of $\mathbf{x}$ (same entries $x_1, \ldots, x_n$ forming a row vector). Thus (2) gives the formula for the pairing $\langle \cdot, \cdot \rangle$ on the lattice $\mathbf{Z}^n \subset V$. For a general lattice L, choose generators, and let $M \in \mathrm{GL}_n(\mathbf{R})$ be the matrix whose columns are the generators' coordinates; then $L = M\mathbf{Z}^n$, so $M^\mathsf{T} A M$ is the symmetric matrix whose (i, j) entry is the pairing of the i-th and j-th generators, i.e., the Gram matrix of L with respect to our chosen generators.

$\langle \cdot, \cdot \rangle$ is positive-definite on V_+ and negative-definite on V_-. Then n_+ is the maximal dimension of *any* positive-definite subspace of V', because a subspace of higher dimension must have nonzero intersection with V_-. Therefore n_+ is an invariant of the pairing, and the invariance of n_- is proved in much the same way.

[2] Many sources use "signature" for the difference $n_+ - n_-$; for nondegenerate pairings this number, together with the rank, contains the same information as (n_+, n_-).

The lattice is rational if and only if it has a Gram matrix with all entries rational; it is integral if and only if it has a Gram matrix with all entries integral; and it is even if and only if it has a Gram matrix with all entries integral and all diagonal entries even.

In particular, $M\mathbf{Z}^n = \mathbf{Z}^n$ if and only if $M \in \mathrm{GL}_n(\mathbf{Z})$. Note that for a commutative ring R the group $\mathrm{GL}_n(R)$ consists of $n \times n$ matrices M with an inverse M^{-1} such that both M and M^{-1} have entries in R; equivalently,[3] $\mathrm{GL}_n(R)$ consists of $M \in \mathrm{Mat}_{n\times n}(R)$ such that $\det M$ is a unit in R. For $R = \mathbf{Z}$ this means that $\mathrm{GL}_n(\mathbf{Z})$ consists of the $n \times n$ integer matrices of determinant ± 1. For us, this means that lattices L, L' with Gram matrices A, A' are isomorphic if and only if $A' = M^\intercal A M$ for some $M \in \mathrm{GL}_n(\mathbf{Z})$, Note that this equivalence relation on symmetric matrices preserves the rationality and integrality criteria; necessariy it is also true that if $A \in \mathrm{Mat}_{n\times n}(\mathbf{Z})$ has all diagonal entries in $2\mathbf{Z}$ then the same is true of $M^\intercal A M$, though this is not so immediately visible from the formulas for matrix multiplication.

It also follows that

$$\det A' = (\det M)^2 \det A = (\pm 1)^2 \det A = \det A.$$

Thus, even though there are many choices for A (once $n > 1$), the determinant of the Gram matrix is an invariant of the lattice, which we shall call its *discriminant* $\operatorname{disc} L$. Clearly if L is rational then so is $\operatorname{disc} L$. Likewise, if L is integral then so is $\operatorname{disc} L$; note that it is not enough for Q to take integral values: the lattice associate to the quadratic form $x_1^2 - x_1x_2 + x_2^2$ has discriminant $\det \frac{1}{2}\left(\begin{smallmatrix} 2 & -1 \\ -1 & 2 \end{smallmatrix}\right) = 3/4 \notin \mathbf{Z}$. It is still true that for such a lattice $\operatorname{disc} L \in 2^{-n}\mathbf{Z}$.

The discriminant vanishes if and only if L is degenerate; otherwise the discriminant has sign $(-1)^{n_-}$. In particular, a positive-definite lattice has positive discriminant. (Small warning: a *negative*-definite lattice does not always have negative discriminant; as we just saw, in this case $\operatorname{disc} L > 0$ or $\operatorname{disc} L < 0$ according as the rank of L is even or odd.) In the positive-definite case, the discriminant has a nice geometric interpretation: $(\operatorname{disc} L)^{1/2}$ is the volume of the quotient torus $\mathbf{R}^n/L$, and thus also the "sparsity" (inverse density) of L in $\mathbf{R}^n$, using the volume form on $\mathbf{R}^n$ consistent with the inner product. To see this, fix orthonormal coordinates on $\mathbf{R}^n$, and let M be a generator matrix for L; then $\operatorname{disc} L = \det M^\intercal M = (\det M)^2$, and it is well-known that $|\det M|$ is the volume of the parallelepiped spanned by the columns of M, which is a fundamental domain for the action of L on $\mathbf{R}^n$ by translation.

We can now prove that a rational lattice is positive-definite if and only if $\langle \mathbf{x}, \mathbf{x} \rangle > 0$ for all nonzero $\mathbf{x} \in L$: here A has rational entries, so if $\det A = 0$ then $\ker A$ contains a nonzero vector in $\mathbf{Q}^n$, and thus (multiplying by a common denominator) some nonzero $\mathbf{x} \in \mathbf{Z}^n$ with $\langle \mathbf{x}, \mathbf{x} \rangle = \mathbf{x}^\intercal A \mathbf{x} = 0$.

Once we have chosen generators of a rank-n lattice L, its *automorphisms* are identified with matrices $M \in \mathrm{GL}_n(\mathbf{Z})$ such that $M^\intercal A M = A$. When the lattice is positive-definite (or negative-definite), the automorphism group must be finite, because it is a discrete subgroup of the orthogonal group

$$O_Q = \{M \in \mathrm{GL}_n(\mathbf{R}) : \forall \mathbf{x} \in \mathbf{R}^n,\ Q(M\mathbf{x}) = Q(\mathbf{x})\},$$

and O_Q is compact when Q is definite. On the other hand, indefinite lattices can have an infinite automorphism group. For example, every transformation of the form $(x_1, x_2) \mapsto (x_1, x_2 + kx_1)$

[3] This condition is necessary because the determinant is multiplicative, and sufficient because $M \operatorname{adj} M = (\operatorname{adj} M)M = \det M \cdot I_n$. The familiar criterion $\det M \neq 0$ works only over a field.

($k \in \mathbf{Z}$) is an automorphism of the degenerate pairing $\langle \mathbf{x}, \mathbf{y} \rangle = x_1 y_1$ on $\mathbf{Z}^2$ (and even "worse": the full group $\mathrm{GL}_2(\mathbf{Z})$ is the automorphism group of the zero pairing). More interestingly, for each even integer k, the matrix $\begin{pmatrix} F_{k-1} & F_k \\ F_k & F_{k+1} \end{pmatrix}$ gives an automorphism of the indefinite (but nondegenerate) even lattice with Gram matrix $\left(\begin{smallmatrix} 2 & 1 \\ 1 & -2 \end{smallmatrix}\right)$; here F_k is the k-th Fibonacci number, so for example $k = 0$ gives the identity matrix and $k = 8$ gives $\left(\begin{smallmatrix} 13 & 21 \\ 21 & 34 \end{smallmatrix}\right)$. In general, a rational lattice L of rank 2 and signature $(1, 1)$ has infinite automorphism group if and only if $(-\operatorname{disc} L)$ is not a square; this comes down to the unit theorem for real quadratic fields.