Recall that if $\dim \mathbb{Q}$, the Fermat–Pell equation.

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

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

$$2\langle x, y \rangle = \langle x + y, x + y \rangle - \langle x, x \rangle - \langle y, y \rangle = Q(x + y) - Q(x) - Q(y) \quad (1)$$

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 $\langle x, y \rangle \in \mathbb{Z}$ for all $x, y \in L$ then $\langle x, x \rangle \in \mathbb{Z}$ for all $x \in L$, 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 $L = \mathbb{Z}^2$ and $\langle x, y \rangle = \frac{1}{2}x^t \begin{pmatrix} -2 & -1 \\ 1 & -2 \end{pmatrix} y$, for which $Q(x) = x_1^2 - x_1x_2 + x_2^2 \in \mathbb{Z}$ for all $x = (x_1, x_2) \in \mathbb{Z}^2$, but $\langle (1, 0), (0, 1) \rangle = -1/2$.

It also follows from (1) that if $(L, \langle \cdot, \cdot \rangle)$ is integral then $Q(x + y) \equiv Q(x) + Q(y) \mod 2$ for all $x, y \in L$; that is, the map $L \to \mathbb{Z}$, $x \mapsto Q(x)$ descends to a homomorphism $L \to \mathbb{Z}/2\mathbb{Z}$. The lattice is said to be even if this homomorphism is trivial, i.e. if $\langle x, x \rangle \in 2\mathbb{Z}$ for all $x \in L$. Note that conversely if a lattice has $\langle x, x \rangle \in 2\mathbb{Z}$ for all $x$ 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 $V = L \otimes \mathbb{R}$. The pairing $\langle \cdot, \cdot \rangle$ extends linearly to a symmetric bilinear form $V \times V \to \mathbb{R}$, 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 $\langle x, y \rangle = \sum_{j=1}^n c_j x_j y_j$ for some $c_j \in \mathbb{R}$, 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. $x \in V_0$ if and only if $\langle x_0, x \rangle = 0$ for all $x \in V$. 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 $\dim V_+ = n_+$ and $\dim V_- = n_-$.
\( n_- = 0 \) (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 \((n_+, n_-)\).

**Warnings:** i) We cannot use the definition “\( x \neq 0 \Rightarrow \langle x, x \rangle > 0 \)” to characterize positive-definite lattices \( L \) if \( x \) is allowed to range only over \( L \) (rather than \( L \otimes \mathbb{R} \)). A standard counterexample is \( L = \mathbb{Z}^2 \) and \( \langle x, y \rangle = (x_1 - tx_2)(y_1 - ty_2) \) for some irrational constant \( t \): the nonzero vector \( x = (t, 1) \in L \otimes \mathbb{R} \) satisfies \( \langle x, x \rangle = 0 \), but \( \langle x, x \rangle \) is positive for every nonzero lattice vector. It is true that the lattice is positive (negative) semidefinite if and only if \( \langle x, x \rangle \geq 0 \) (resp. \( \langle x, x \rangle \leq 0 \)) for every \( x \in L \); and we shall soon see that for a *rational* lattice the positivity of \( \langle x, x \rangle \) for all nonzero \( x \in L \) 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 \( x \in V \): either the Euclidean length \( \langle x, x \rangle^{1/2} \) of \( x \), or its square \( \langle x, x \rangle = Q(x) \). 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 \( V \equiv \mathbb{R}^n \) together with a bilinear pairing \( \langle \cdot, \cdot \rangle \), and define 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 \( (\mathbb{R}/\mathbb{Z})^n \)). As an abstract group \( L \) is thus isomorphic with the free abelian group \( \mathbb{Z}^n \) of rank \( n \). Therefore \( L \) is determined by the images, call them \( v_1, \ldots, v_n \), of the standard generators of \( \mathbb{Z}^n \) under a group isomorphism \( \mathbb{Z}^n \cong L \). We say the \( v_i \) *generate*, or are *generators* of \( L \): each vector in \( L \) can be written as \( \sum_{i=1}^n a_i v_i \) for some unique integers \( a_1, \ldots, a_n \). Vectors \( v_1, \ldots, v_n \in V \) generate a lattice if and only if they constitute an \( \mathbb{R} \)-linear basis for \( V \), and then \( L \) is the \( \mathbb{Z} \)-span of this basis. For instance, the \( \mathbb{Z} \)-span of the standard orthonormal basis \( e_1, \ldots, e_n \) of \( \mathbb{R}^n \) (with the standard Euclidean pairing \( \langle x, y \rangle = \sum_{j=1}^n x_j y_j \)) is the lattice \( \mathbb{Z}^n \). 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 \( \mathbb{R}^n \). 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 \( x = (x_1, \ldots, x_n)^T \) and \( y = (y_1, \ldots, y_n)^T \) we have

\[
\langle x, y \rangle = \sum_{i=1}^n \sum_{j=1}^n x_i y_j \langle e_i, e_j \rangle = x^T A y.
\] (2)

Note that \( x, y \) are regarded as *column* vectors (so that matrices can act on vectors from the left), and \( x^T \) is the transpose of \( x \) (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 \( \mathbb{Z}^n \subset V \). For a general lattice \( L \), choose generators, and let \( M \in \text{GL}_n(\mathbb{R}) \) be the matrix whose columns are the generators’ coordinates; then \( L = M \mathbb{Z}^n \), so \( M^T A M \) 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, $MZ^n = Z^n$ if and only if $M \in \text{GL}_n(\mathbb{Z})$. Note that for a commutative ring $R$ the group $\text{GL}_n(R)$ consists of $n \times n$ matrices $M$ with an inverse $M^{-1}$ such that both $M$ and $M^{-1}$ have entries in $R$; equivalently, $\text{GL}_n(R)$ consists of $M \in \text{Mat}_{n \times n}(R)$ such that $\det M$ is a unit in $R$. For $R = \mathbb{Z}$ this means that $\text{GL}_n(\mathbb{Z})$ consists of the $n \times n$ integer matrices of determinant $\pm 1$. For us, this means that lattices $L, L'$ with Gram matrices $A, A'$ are isomorphic if and only if $A' = M^T A M$ for some $M \in \text{GL}_n(\mathbb{Z})$. Note that this equivalence relation on symmetric matrices preserves the rationality and integrality criteria; necessarily it is also true that if $A \in \text{Mat}_{n \times n}(\mathbb{Z})$ has all diagonal entries in $2\mathbb{Z}$ then the same is true of $M^T A M$, 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 $\text{disc} L$. Clearly if $L$ is rational then so is $\text{disc} L$. Likewise, if $L$ is integral then so is $\text{disc} L$; note that it is not enough for $Q$ to take integral values: the lattice associate to the quadratic form $x_1^2 - x_1 x_2 + x_2^2$ has discriminant $\det \frac{1}{2} \begin{pmatrix} 2 & 1 \\ -1 & 2 \end{pmatrix} = 3/4 \notin \mathbb{Z}$. It is still true that for such a lattice $\text{disc} L \in 2^{-n} \mathbb{Z}$.

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 $\text{disc} L > 0$ or $\text{disc} L < 0$ according as the rank of $L$ is even or odd.) In the positive-definite case, the discriminant has a nice geometric interpretation: $(\text{disc} L)^{1/2}$ is the volume of the quotient torus $\mathbb{R}^n/L$, and thus also the “sparsity” (inverse density) of $L$ in $\mathbb{R}^n$, using the volume form on $\mathbb{R}^n$ consistent with the inner product. To see this, fix orthonormal coordinates on $\mathbb{R}^n$, and let $M$ be a generator matrix for $L$; then $\text{disc} L = \det M^T M = (\det M)^2$, 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 $\mathbb{R}^n$ by translation.

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

Once we have chosen generators of a rank-$n$ lattice $L$, its automorphisms are identified with matrices $M \in \text{GL}_n(\mathbb{Z})$ such that $M^T A M = A$. 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

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

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 $(x_1, x_2) \mapsto (x_1, x_2 + k x_1)$

---

3This condition is necessary because the determinant is multiplicative, and sufficient because $M \text{adj} M = (\text{adj} M) M = \det M \cdot I_n$. The familiar criterion $\det M \neq 0$ works only over a field.
(k ∈ ℤ) is an automorphism of the degenerate pairing ⟨x, y⟩ = x₁y₁ on ℤ² (and even “worse”: the full group GL₂(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 \( \begin{pmatrix} 2 & 1 \\ 1 & -2 \end{pmatrix} \); here \( F_k \) is the \( k \)-th Fibonacci number, so for example \( k = 0 \) gives the identity matrix and \( k = 8 \) gives \( \begin{pmatrix} 13 & 21 \\ 21 & 34 \end{pmatrix} \). In general, a rational lattice \( L \) of rank 2 and signature \((1, 1)\) has infinite automorphism group if and only if \((- \text{disc } L)\) is not a square; this comes down to the unit theorem for real quadratic fields.