Lattices

Michel Waldschmidt

This file is available at the address
http://www.imj-prg.fr/~michel.waldschmidt/articles/pdf/Lattices.pdf

This file contains a draft version of the three courses,
the six exercises with their solutions and some references.

First course: 18/07/2025 13 : 00 − 13 : 50

Lattices already occurred in the course by Francesco Campagna when he spoke on elliptic curves over $\mathbb{C}$ (the complex representation of elliptic curves involves lattices in $\mathbb{C} \simeq \mathbb{R}^2$, as periods of elliptic functions) and in the course by Fabien Pazuki on algebraic number theory (when he discussed ideals of the ring of integers of a number field and the canonical embedding of a number field, of the ring of integers of a number field, of the units inside the hyperplane of elements of norm 1).

We will give three definitions of lattices. The fact that the same object can be defined in several ways is something very useful. Lattices involve both algebra and topology: they are finitely generated free $\mathbb{Z}$–modules, and they are discrete subspaces of an Euclidean vector space.

We recall the topology of $\mathbb{R}^n$; we use the Euclidean norm for $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{R}^n$:

$$\|\mathbf{x}\| = \sqrt{\sum_{i=1}^{n} x_i^2}.$$

The *sphere* of center $\mathbf{x}_0$ and radius r is

$$B(\mathbf{x}_0, r) := \{\mathbf{x} \in \mathbb{R}^n \ \mid \ \|\mathbf{x} - \mathbf{x}_0\| \leqslant r\}.$$

It is a closed and bounded subset of $\mathbb{R}^n$, which means a compact. For $n = 1$ this is a closed segment of length $2r$, for $n = 2$ it is a disc of radius r and area πr^2, for $n = 3$ is it a sphere in the usual space of dimension 3, the volume of which is $4\pi r^3/3$. A sphere of radius r in $\mathbb{R}^n$ has volume $c_n r^n$, where c_n is the volume of the unit sphere (radius 1) in $\mathbb{R}^n$: $c_1 = 2$, $c_2 = \pi$, $c_3 = 4\pi/3$,

$$c_n = \frac{\pi^{n/2}}{(n/2)!}$$

where

$$(n/2)! = \Gamma((n/2)+1) = \int_0^\infty u^{n/2} \mathrm{e}^{-u} du,$$

where Γ is *Euler Gamma function*

$$\Gamma(x) = \int_0^\infty t^{x-1} \mathrm{e}^{-t} dt.$$

For instance

$$\Gamma(1/2) = \sqrt{\pi}, \quad \Gamma(1) = 1, \quad \Gamma(x+1) = x\Gamma(x)$$

and $(1/2)! = \Gamma(3/2) = \frac{1}{2}\Gamma(\frac{1}{2}) = \sqrt{\pi}/2$, $((n/2)+1)! = (n/2)!(n/2)$.

Recall that a $\mathbb{Z}$–module is nothing else than an abelian group. Here are some examples of subgroups of $\mathbb{R}$:

$$\{0\},\ \mathbb{R},\ \mathbb{Z},\ \mathbb{Z}\alpha,\ \mathbb{Q},\ \mathbb{Z}+\mathbb{Z}\sqrt{2},\ \mathbb{Z}+\mathbb{Z}\alpha,\ \ldots$$

for $\alpha \in \mathbb{R}$, and also the additive groups of subfields of $\mathbb{R}$ (including real number fields).

Questions:
• Which ones are finitely generated (as $\mathbb{Z}$–modules)?
• Which ones are open, closed, discrete?
(recall the definition of discrete; as an example the set $\{1/n \mid n \geqslant 1\}$ is a discrete subgroup of $\mathbb{R}$).

In the above list there is no example of a subgroup of $\mathbb{R}$ which is at the same time dense and discrete.

Recall the notations for the *integral part* $\lfloor x \rfloor$ and the *fractional part* $\{x\}$ of a real number x:

$$x = \lfloor x \rfloor + \{x\}, \quad \lfloor x \rfloor \in \mathbb{Z}, \quad 0 \leqslant \{x\} < 1$$

which is the Euclidean division of x by 1. For x and y in $\mathbb{R}$ we have $\{x\} = \{y\}$ if and only if $x - y \in \mathbb{Z}$. Hence the map $x \mapsto \{x\}$ induces a bijective map $\mathbb{R}/\mathbb{Z} \to [0, 1)$.

The map $x \to \mathrm{e}^{2\mathrm{i}\pi x}$ is a surjective homomorphism from the additive group of $\mathbb{R}$ to the multiplicative group $\mathbb{C}^\times$. The image is the subgroup $\mathbb{U} := \{z \in \mathbb{C} \mid |z| = 1\}$ of $\mathbb{C}^\times$ and the kernel is $\mathbb{Z}$, hence we obtain an isomorphism between the additive group $\mathbb{R}/\mathbb{Z}$ and the multiplicative group $\mathbb{U}$.

Fact 1. *A subgroup of $\mathbb{R}$ is discrete if and only if it is of the form $\mathbb{Z}\alpha$, $\alpha \in \mathbb{R}$.*

Proof. Clearly for any $\alpha \in \mathbb{R}$ the subgroup $\mathbb{Z}\alpha$ is discrete in $\mathbb{R}$. Conversely, let G be a discrete subgroup of $\mathbb{R}$. If $G = \{0\}$ then $G = \mathbb{Z}\alpha$ with $\alpha = 0$. If $G \neq \{0\}$, there exists $\beta \in G$, $\beta \neq 0$. Let $\gamma = |\beta|$; hence $\gamma > 0$ and $\gamma = \pm\beta \in G$. Since 0 is not an accumulation point of G, there exists $\eta > 0$ such that $G \cap [-\eta, \eta] = \{0\}$. Hence the number

$$\alpha = \inf\{x \in G \mid x > 0\}$$

is well defined and belongs to G. Let $x \in G$. Use the Euclidean division:

$$x = m\alpha + r$$

with $m \in \mathbb{Z}$ and $0 \leqslant r \leqslant \alpha$, namely $m = \lfloor x/\alpha \rfloor$ and $r = \{x/\alpha\}$. From $r \in G$, $0 \leqslant r < \alpha$, we deduce $r = 0$, hence $G = \mathbb{Z}\alpha$. □

Fact 2. *A subgroup of $\mathbb{R}$ is dense if and only if it is not discrete.*

Proof. Clearly a dense subgroup of $\mathbb{R}$ is not discrete. Conversely, if G is a subgroup of $\mathbb{R}$ with is not discrete, then there exists $x_0 \in G$ which is an accumulation point : $x = \lim_{n\to\infty} x_n$ where x_n are pairwise distinct elements in G. Therefore $0 = \lim_{n\to\infty}(x - x_n)$ is an accumulation point. Let $y \in \mathbb{R}$ and let $\epsilon > 0$. Let $z \in G$ satisfy $0 < |z| \leqslant \epsilon$ and let $m = \lfloor y/|z| \rfloor$. Then $g := m|z| \in G$ and $|y - g| < \epsilon$. □

Exercice. A closed subgroup of $\mathbb{R}$ is either $\mathbb{R}$ or discrete.

Example. From these two facts one deduces a *theorem of Tchebychef*: let α be a real number; then the subgroup $\mathbb{Z}+\mathbb{Z}\alpha$ is discrete in $\mathbb{R}$ if and only if $\alpha \in \mathbb{Q}$. This subgroup is dense in $\mathbb{R}$ if and only if $\alpha \notin \mathbb{Q}$. As a consequence, if α is irrational, then for any $x \in \mathbb{R}$ and any $\epsilon > 0$ there exists $(a, b) \in \mathbb{Z}^2$ such that $|a + b\alpha - x| < \epsilon$. This is an example of a statement of *non homogeneous Diophantine approximation*.

The situation that we described in dimension 1 does not extend to higher dimension. If G_1 and G_2 are subgroups of $\mathbb{R}$, then $G_1 \times G_2$ is a subgroup of $\mathbb{R}^2$ which may be neither discrete nor dense; an example is $\mathbb{R} \times \{0\}$.

We mention without proof that there is a theorem on the *structure of closed subgroups of* $\mathbb{R}^n$: after a change of variables, such a subgroup becomes $\mathbb{R}^m \times \{0\}^k \times \mathbb{Z}^{n-m-k}$. For a proof, see for instance [W1995].

There are several notions of rank. We introduce two of them: the rational rank (which we just call the rank) and the local rank.

Definition: The *rank* of a subgroup G of $\mathbb{R}^n$ is the dimension of the $\mathbb{Q}$–subspace of $\mathbb{R}^n$ spanned by G. Hence this is the maximal number of $\mathbb{Z}$–linearly independent elements in G.
Examples: the subgroups $\mathbb{Z}$ and $\mathbb{Q}$ of $\mathbb{R}$ have rank 1, $\mathbb{Z} + \mathbb{Z}\sqrt{2}$ has rank 2. The additive group of the real algebraic numbers and also $\mathbb{R}$ itself have infinite rank.

There are main differences between $\mathbb{Z}$–modules and $\mathbb{Q}$–vector spaces: a set of independent elements of a $\mathbb{Z}$–module is not always a subset of a basis, and a generating set of a $\mathbb{Z}$–module does not always contain a basis.

A finitely generated $\mathbb{Z}$–module has a finite rank; but $\mathbb{Q}$ has rank 1 and is not finitely generated.

Exercise. Let α_1 and α_2 be real numbers and G the subgroup

$$\mathbb{Z}^2 + \mathbb{Z}(\alpha_1, \alpha_2) = \{(a_1 + a_0\alpha_1, a_2 + a_0\alpha_2) \ \mid \ (a_0, a_1, a_2) \in \mathbb{Z}^3\}$$

of $\mathbb{R}^2$.
(a) Check that the following properties are equivalent:
(i) G has rank 2.
(ii) $(\alpha_1, \alpha_2) \in \mathbb{Q}^2$.
(iii) G is discrete in $\mathbb{R}^2$.
(b) Check that G is dense in $\mathbb{R}^2$ if and only if $1, \alpha_1, \alpha_2$ are $\mathbb{Q}$–linearly independent

Exercise. A discrete finitely subgroup of $\mathbb{R}^n$ has rank $\leqslant n$.

Let G be a subgroup of $\mathbb{R}^n$. The map

$$r \mapsto \dim_{\mathbb{R}} < G \cap B(0, r) >$$

from $\mathbb{R}_{>0}$ to $\mathbb{R}_{\geqslant 0}$ is an increasing function or r.

Definition: The *local rank* of a subgroup G of $\mathbb{R}^n$ is the limit for $r \to 0$ of the dimension of the $\mathbb{R}$–subspace spanned by $G \cap B(0, r)$.

Exercise. Check that a subgroup of $\mathbb{R}^n$ is discrete if and only if its local rank is 0.

Definition: An *Euclidean vector space* is a finite dimensional vector space E with a positive definite symmetric bilinear form

$$< \cdot, \cdot >: E \times E > \to \mathbb{R} :$$

- bilinear: $\mathbf{x} \mapsto < \mathbf{x}, \mathbf{y} >$ and $\mathbf{y} \mapsto < \mathbf{x}, \mathbf{y} >$ are linear forms $E \to \mathbb{R}$.
- symmetric,: $< \mathbf{x}, \mathbf{y} > = < \mathbf{y}, \mathbf{x} >$.
- positive definite: $< \mathbf{x}, \mathbf{x} > > 0$ for $\mathbf{x} \neq 0$.

Euclidean norm: $\|\mathbf{x}\| = \sqrt{< \mathbf{x}, \mathbf{x} >}$.

The main example is $\mathbb{R}^n$ with the standard inner product

$$< \mathbf{x}, \mathbf{y} > = \sum_{i=1}^{n} x_i y_i,$$

so that $\|\mathbf{x}\|^2 =< \mathbf{x}, \mathbf{x} >$. Some authors write $\mathbf{x} \cdot \mathbf{y}$ for $< \mathbf{x}, \mathbf{y} >$.

When $\mathbf{e}_1, \dots, \mathbf{e}_n$ is the canonical basis of $\mathbb{R}^n$, with $(\mathbf{e}_1 \dots \mathbf{e}_n) \in \mathbb{Z}^{n \times n}$ being the identity $n \times n$ matrix I_n, we have $< \mathbf{e}_i, \mathbf{e}_j >= \delta_{ij}$ (Kronecker symbol).

Theorem (Gram–Schmidt). Every Euclidean space has an orthonormal basis: $E \simeq \mathbb{R}^{\dim E}$.

Sketch of proof. The result is true for $E = 0$. Otherwise, take $\mathbf{b}_1 \in E \smallsetminus \{0\}$, normalise by setting $\mathbf{e}_1 = \mathbf{b}_1/\|\mathbf{b}_1\|$.

This completes the proof if $\dim E = 1$. Otherwise, take $\mathbf{b}_2$ linearly independent of $\mathbf{e}_1$. If $< \mathbf{e}_1, \mathbf{b}_2 >= 0$ take $\mathbf{e}_2 = \mathbf{b}_2/\|\mathbf{b}_2\|$. If $< \mathbf{e}_1, \mathbf{b}_2 >\neq 0$, project on the orthogonal space to $\mathbf{e}_1$:

$$\mathbf{b}_2' = \mathbf{b}_2 - < \mathbf{e}_1, \mathbf{b}_2 > \mathbf{e}_1$$

and take $\mathbf{e}_2 = \mathbf{b}_2'/\|\mathbf{b}_2'\|$.

Continue by induction. See [La2002, Chap. XV]. □

Example of an Euclidean vector space. Eor x and y in $\mathbb{C}$, define

$$< x, y >= \mathrm{R}e(x\overline{y}) = \frac{1}{2}(x\overline{y} + x\overline{y})$$

where Rez is the real part of z and $\overline{z}$ is the complex conjugate of z. The map

$$\begin{array}{ccc} \mathbb{R}^2 & \to & \mathbb{C} \\ (a, b) & \to & a + bi \end{array}$$

is an isomorphism of Euclidean spaces:

$$< a + b\mathrm{i}, c + d\mathrm{i} >= \mathrm{R}e\big((a + b\mathrm{i})(c - d\mathrm{i})\big) = \mathrm{R}e\big(ac + bd + \mathrm{i}(bc - ad)\big) = ac + bd.$$

First definition of a lattice: *A lattice is a discrete subgroup of maximal rank in an Euclidean vector space.*

Hence the rank of a lattice in an Euclidean vector space E is the dimension of E over $\mathbb{R}$. The main example is $\mathbb{Z}^n$ in $\mathbb{R}^n$. More generally, if $(\mathbf{b}_1, \dots, \mathbf{b}_n)$ is a basis of an Euclidean vector space E, it follows from the above isomorphism that $\mathbb{Z}\mathbf{b}_1 + \dots + \mathbb{Z}\mathbf{b}_n$ is a lattice in E. This will give us the second definition of a lattice.

Beware that in some references, a lattice is only a discrete subgroup of E - here we assume that the rank is maximal.

Second course: 18/07/2025 14 : 00 − 14 : 50

Second definition of a lattice: A subgroup Λ in an Euclidean vector space E is *a lattice* if there exists a basis $(\mathbf{b}_1, \dots, \mathbf{b}_n)$ of E such that $\Lambda = \mathbb{Z}\mathbf{b}_1 + \cdots + \mathbb{Z}\mathbf{b}_n$.

We will sketch the proof of the equivalence with the first definition in the third course.

Write the components of $\mathbf{b}_1, \dots, \mathbf{b}_n$ as column vectors

$$\mathbf{b}_i = \begin{pmatrix} b_{i1} \\ b_{i2} \\ \vdots \\ b_{in} \end{pmatrix} \qquad i = 1, \dots, n.$$

To Λ we associate the $n \times n$ matrices

$$B = \begin{pmatrix} b_{11} & \dots & b_{n1} \\ b_{12} & \dots & b_{n2} \\ \vdots & \ddots & \vdots \\ b_{nn} & \dots & b_{nn} \end{pmatrix}$$

and the *Gram matrix:*

$$A = \big(< \mathbf{b}_i, \mathbf{b}_j >\big)_{1 \leqslant i,j \leqslant n}$$

which is a symmetric matrix. Since

$$< \mathbf{b}_i, \mathbf{b}_j >= b_{i1}b_{j1} + b_{i2}b_{j2} + \cdots + b_{in}b_{jn} = \big(b_{i1}, b_{i2}, \dots, b_{in}\big) \begin{pmatrix} b_{j1} \\ b_{j2} \\ \vdots \\ b_{jn} \end{pmatrix}$$

these two matrices are related by

$$A = B^t B.$$

Hence $\det A = (\det B)^2$. One defines the *discriminant of the lattice* Λ as $\mathrm{disc}(\Lambda) := \det A$. It does not depend on the choice of the basis $(\mathbf{b}_1, \dots, \mathbf{b}_n)$ of Λ (*exercise*).

The *fundamental domain* of $\mathbb{R}^n$ modulo Λ is the compact in E defined as

$$F = [0,1]\mathbf{b}_1 + \cdots + [0,1]\mathbf{b}_n = \{t_1\mathbf{b}_1 + \cdots + t_n\mathbf{b}_n \ \mid \ 0 \leqslant t_i \leqslant 1, \ i = 1, \dots, n\}.$$

For $n = 2$ this is a parallelogram (*draw a picture*). This set depends on the choice of the basis $(\mathbf{b}_1, \dots, \mathbf{b}_n)$ of Λ, but its volume does not. One defines the *covolume of* Λ as the volume of F for the Euclidean metric of E – this is the volume of the torus $\mathbb{R}^n/\Lambda$. Hence

$$\mathrm{covol}(\Lambda) = |\det B|.$$

This number is also called the *determinant* of the lattice Λ. The fact that is does not depend on the basis can also be seen from the formula

$$\mathrm{covol}(\Lambda) = \lim_{r \to \infty} \frac{\mathrm{vol}(B(0,r))}{\#\{y \in L \ \mid \ \|y\| \leqslant r\}}$$

(see [L2008, §5]).

The *shortest vectors* of Λ are the elements λ in Λ such that

$$\|\lambda\| = \min\{\|\mathbf{x}\| \mid \mathbf{x} \in \Lambda \smallsetminus \{0\}\}.$$

We will denote by $\ell(\Lambda)$ the length of the shortest vectors: $\ell(\Lambda) = \|\lambda\|$. For the lattice $\mathbb{Z}^n$ in $\mathbb{R}^n$ we have $\ell(\mathbb{Z}^n) = 1$.

The *shortest vector problem* [L2008, §8] is to find shortest vectors in a given lattice Λ.

The *nearest vector problem* [L2008, §6]. is the following: given a lattice Λ in an Euclidean vector space E and an element $\mathbf{t}$ in E, find $\mathbf{x}$ in Λ such that

$$\|\mathbf{x} - \mathbf{t}\| = \min\{\|\mathbf{y} - \mathbf{t}\| \mid \mathbf{y} \in \Lambda \smallsetminus \{0\}\}.$$

A trivial example is the lattice $\mathbb{Z}^n$ in $\mathbb{R}^n$: given $\mathbf{t} = (t_1, \ldots, t_n) \in \mathbb{R}^n$, take $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{Z}^n$ where x_i is a nearest integer to t_i (sometimes written as $x_i = \lfloor t_i \rceil$).

In general, these two problems are hard (see the courses on cryptography).

Sphere packing. [L2001, §3].

Let $\ell = \ell(\Lambda)$. The spheres centered at the points of Λ with radius $\ell/2$ produce a *sphere packing* of E. From

$$\lim_{r\to\infty} \frac{\#\{x \in \Lambda \mid x + B(0, \ell/2) \subset B(0, r)\}}{\mathrm{vol}(B(0,r))} = \frac{1}{\mathrm{covol}(\Lambda)}.$$

we deduce that the limit

$$\lim_{r\to\infty} \frac{\mathrm{vol}\left(\bigcup_{\mathbf{x}\in\Lambda} (\mathbf{x} + B(0,\ell/2)) \cap B(0,r)\right)}{\mathrm{vol}(B(0,r))}$$

is

$$d(\Lambda) := \frac{c_n(\ell/2)^n}{\mathrm{covol}(\Lambda)}$$

which is the *density of this sphere packing*.

For instance the density of the sphere packing associated to the lattice $\mathbb{Z}^n$ in $\mathbb{R}^n$ is 1 for $n = 1$, $\pi/4$ for $n = 2$, $\pi/6$ for $n = 3$, and generally $c_n/2^n$.

Recall that the *dual vector space* $E^* = \mathrm{Hom}(E, \mathbb{R})$ of a vector space E is a $\mathbb{R}$–vector space of the same dimension [DF2004, §11.3]. For E an Euclidean vector space, the map

$$\begin{array}{ccc} E & \to & E^* = \mathrm{Hom}(E, \mathbb{R}) \\ \mathbf{y} & \mapsto & \mathbf{y}^* : (\mathbf{x} \mapsto < \mathbf{x}, \mathbf{y} >) \end{array}$$

is an isomorphism. When $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ is a basis of E, then a basis of E^* is $(\mathbf{b}_1^*, \ldots, \mathbf{b}_n^*)$, where $< \mathbf{b}_i, \mathbf{b}_j^* >= \delta_{ij}$. Hence the $n \times n$ matrices B and B^* with columns $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ and $(\mathbf{b}_1^*, \ldots, \mathbf{b}_n^*)$ respectively are related by $B^t B^* = I_n$:

$$B^* = (B^t)^{-1}.$$

Let E be an Euclidean vector space and D a vector subspace of E. The restriction of $< \cdot, \cdot >$ to D endows D with a structure of Euclidean space. The dual of D is $D^* = \mathrm{Hom}(D, \mathbb{R})$. Let $D^\perp$ be the kernel of the map

$$\begin{array}{ccc} E & \to & D^* \\ \mathbf{x} & \mapsto & (\mathbf{y} \mapsto < \mathbf{x}, \mathbf{y} >), \end{array}$$

namely

$$D^\perp = \{\mathbf{x} \in E \mid < \mathbf{x}, \mathbf{y} >= 0 \text{ for all } \mathbf{y} \in D\}.$$

From $D \cap D^\perp = \{0\}$ we deduce that the composite map $D \to E \to E/D^\perp$ is injective. Composing with the injective map $E/D^\perp \to D^*$ gives an isomorphism between D and D^*.

Each $\mathbf{w} \in E$ has a unique decomposition $\mathbf{w} = \mathbf{x} + \mathbf{y}$ with $\mathbf{x} \in D$ and $\mathbf{y} \in D^\perp$: indeed given $\mathbf{w} \in E$ there is a unique $\mathbf{x} \in D$ such that $< \mathbf{w}, \mathbf{z} >=< \mathbf{x}, \mathbf{z} >$ for all $\mathbf{z} \in D$. Then $\mathbf{y} = \mathbf{w} - \mathbf{x}$ satisfies $< \mathbf{y}, \mathbf{z} >= 0$ for all $\mathbf{z} \in D$, hence $\mathbf{y} \in D^\perp$. This is the *orthogonal decomposition* with respect to D which occured in the proof of the Gram–Schmidt Theorem.

The quotient $E/D \simeq D^\perp$ is canonically an Euclidean vector space. And E^* is canonically isomorphic to E.

When Λ is a lattice in E, its *dual lattice* is

$$\Lambda^* = \{\mathbf{y} \in E \mid < \mathbf{x}, \mathbf{y} > \in \mathbb{Z} \text{ for all } \mathbf{x} \in \Lambda\}.$$

This gives a map

$$\begin{array}{ccc} \Lambda \times \Lambda^* & \to & \mathbb{Z} \\ (\mathbf{x}, \mathbf{y}) & \mapsto & < \mathbf{x}, \mathbf{y} > . \end{array}$$

The Gram matrices A and A^*, and the matrices B and B^*, associated with Λ and Λ^* respectively, are related by

$$A^* = (B^*)^t B^* = B^{-1}(B^t)^{-1} = (B^t B)^{-1} = A^{-1}.$$

Hence

$$\mathrm{disc}(\Lambda^*)\mathrm{disc}(\Lambda) = 1, \qquad \mathrm{covol}(B^*)\mathrm{covol}(B) = 1.$$

Remark. For a lattice Λ in $\mathbb{R}^2$, $d(\Lambda) = d(\Lambda^*)$.

Exercise 6 shows that this property is not true for latices of rank 3.

Proof. Let

$$B = \begin{pmatrix} u_1 & u_2 \\ v_1 & v_2 \end{pmatrix}$$

be a matrix with vector columns a basis of Λ. The dual lattice Λ^* has for basis the vectors of the matrix

$$B^* = \frac{1}{u_1 v_2 - u_2 v_1} \begin{pmatrix} v_2 & -v_1 \\ u_2 & -u_1 \end{pmatrix}.$$

It follows that the lengths $\ell^* := \ell(\Lambda^*)$ and $\ell := \ell(\Lambda)$ of the shortest vectors of Λ^* and Λ respectively are related by

$$\ell^* = \frac{\ell}{\mathrm{covol}(\Lambda)}.$$

Since

$$\mathrm{covol}(\Lambda^*) = \frac{1}{\mathrm{covol}(\Lambda)},$$

one deduces that the densities $d(\Lambda^*)$ and $d(\Lambda)$ of the packings associated to Λ and Λ^* are the same:

$$d(\Lambda^*) = \frac{c_2(\ell^*/2)^2}{\mathrm{covol}(\Lambda^*)} = \frac{c_2(\ell/2)^2}{\mathrm{covol}(\Lambda)} = d(\Lambda).$$

□

For more information on lattices of rank 2, see [L2008, §9].

Sublattices.

If Λ and Λ' are two lattices with $\Lambda' \subset \Lambda$, then Λ/Λ' is a finite group, which means that Λ' has finite index $[\Lambda : \Lambda']$ in Λ. A fundamental domain for Λ' is the union of $[\Lambda : \Lambda']$ fundamental domains of Λ (example: a fundamental domain for $m\mathbb{Z}$ in $\mathbb{R}$ is the interval $[0, m]$). Hence

$$\mathrm{covol}(\Lambda') = [\Lambda : \Lambda']\mathrm{covol}(\Lambda).$$

Let $\Lambda' \subset \Lambda$ be two lattices. Let $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ be a basis of Λ over $\mathbb{Z}$, $(\mathbf{b}'_1, \ldots, \mathbf{b}'_n)$ a basis of Λ' over $\mathbb{Z}$ and $B, B' \in \mathbb{Z}^{n\times n}$ the $n \times n$ matrices with column vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n$ and $\mathbf{b}'_1, \ldots, \mathbf{b}'_n$ respectively. From $\Lambda' \subset \Lambda$ it follows that there is a $n \times n$ matrix $M = (m_{ij})_{1\leqslant i,j\leqslant n} \in \mathbb{Z}^{n\times n}$ such that

$$\mathbf{b}'_i = m_{i1}\mathbf{b}_1 + \cdots + m_{in}\mathbf{b}_n \quad (1 \leqslant i \leqslant n).$$

Hence $\Lambda' = M\Lambda$, $B' = MB$, $\det B' = (\det M)(\det B)$, $|\det M| = [\Lambda : \Lambda']$,

$$\mathrm{disc}\Lambda' = \det A' = (\det M)^2 \det A = [\Lambda : \Lambda']^2\mathrm{disc}\Lambda.$$

Example. Let Λ be a lattice of rank n. Let $m \geqslant 1$. The quotient $\Lambda/m\Lambda$ is isomorphic to $(\mathbb{Z}/m\mathbb{Z})^n$, hence $[\Lambda : m\Lambda] = m^n$:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & m\Lambda & \longrightarrow & \Lambda & \longrightarrow & \Lambda/m\Lambda & \longrightarrow & 0 \\ & & \downarrow\wr & & \downarrow\wr & & \downarrow\wr & & \\ 0 & \longrightarrow & (m\mathbb{Z})^n & \longrightarrow & \mathbb{Z}^n & \longrightarrow & (\mathbb{Z}/m\mathbb{Z})^n & \longrightarrow & 0. \end{array}$$

Third course: 22/07/2025 11 : 10 − 12 : 00

Recall the two definitions of lattices (courses 1 and 2).

We already saw that if Λ satisfies the second definition, $\Lambda = \mathbb{Z}\mathbf{b}_1 + \cdots + \mathbf{b}_n \subset E$, then Λ is a discrete subgroup of maximal rank of E.

Here is a sketch of proof of the converse. A full proof is given in [L2001, Proposition 3.3].

We will use the *theorem on elementary divisors* which describes the structure of submodules of a free module over a principal ring [La2002, Chap.III §7], [Sa2013, Chap. 1 §5 Theorem 1]. We need only the special case of the ring $\mathbb{Z}$ and a subgroup of $\mathbb{Z}^n$ [DF2004, §5.2 Theorem 5].

> *Let Λ be a subgroup of $\mathbb{Z}^n$. There exists a non-negative integer $s \leqslant n$, a basis $\mathbf{y}_1, \cdots, \mathbf{y}_n$ of $\mathbb{Z}^n$ and positive integers $a_1, \ldots, a_s$ such that $a_1\mathbf{y}_1, \ldots, a_s\mathbf{y}_s$ is a basis of Λ and a_i divides a_{i+1} for $i = 1, \ldots, s-1$. If $s = n$, then Λ is a subgroup of $\mathbb{Z}^n$ of finite index $a_1 \cdots a_n$.*

Sketch of proof: a discrete subgroup has a basis. Let Λ be a discrete subgroup of maximal rank of an Euclidean vector space E of dimension n. Let r be the dimension of the $\mathbb{R}$-subspace of E spanned by Λ. Let $\mathbf{x}_1, \ldots, \mathbf{x}_r$ be elements $\mathbb{R}$–linearly independent in Λ and let

$$P = \{t_1\mathbf{x}_1 + \cdots + t_r\mathbf{x}_r \in E \ \mid \ 0 \leqslant t_i \leqslant 1\}.$$

Since the set $P \cap \Lambda$ is compact (closed and bounded) and discrete, it is finite.

One checks that $P \cap \Lambda$ spans G over $\mathbb{Q}$ as follows. For $\mathbf{y} = t_1\mathbf{x}_1 + \cdots + t_r\mathbf{x}_r \in \Lambda$ and $m \in \mathbb{Z}$, define

$$\mathbf{y}_m := m\mathbf{y} - \lfloor mt_1 \rfloor \mathbf{x}_1 - \cdots - \lfloor mt_r \rfloor \mathbf{x}_r = \{mt_1\}\mathbf{x}_1 + \cdots + \{mt_r\}\mathbf{x}_r \in P \cap \Lambda.$$

Since $P \cap \Lambda$ is finite, there are two integers m and m' such that $1 \leqslant m - m' \leqslant \#P \cap \Lambda$ and $\mathbf{y}_m = \mathbf{y}_{m'}$, hence such that $(m' - m)\mathbf{y} \in \mathbb{Z}\mathbf{x}_1 + \cdot + \mathbb{Z}\mathbf{x}_r$. As a consequence Λ is a subgroup of finite index of $\mathbb{Z}\mathbf{x}_1 + \cdot + \mathbb{Z}\mathbf{x}_r$.

We now use the above result on subgroups of a free $\mathbb{Z}$–module, with n replaced by r: there exists an integer $s \leqslant r$, a basis $\mathbf{b}_1, \cdots, \mathbf{b}_r$ of $\mathbb{Z}\mathbf{x}_1 + \cdot + \mathbb{Z}\mathbf{x}_r$ and positive integers $a_1, \ldots, a_s$ such that $a_1\mathbf{b}_1, \ldots, a_s\mathbf{b}_s$ is a basis of Λ. Since Λ has maximal rank n, we have $s = r = n$. □

We now come to the third definition of a lattice. If Λ is a discrete subgroup of E of maximal rank, define $q(\mathbf{x}) = \|\mathbf{x}\|^2$. Then we have

$$q(\mathbf{x} + \mathbf{y}) + q(\mathbf{x} - \mathbf{y}) = 2q(\mathbf{x}) + 2q(\mathbf{y})$$

and $q(\mathbf{x}) \neq 0$ if $\mathbf{x} \neq 0$. Further, for all $r > 0$, the set of $\mathbf{x} \in \Lambda$ with $q(\mathbf{x}) \leqslant r$ is finite. Furthermore,

$$< \mathbf{x}, \mathbf{y} >= \frac{1}{4}(q(\mathbf{x} + \mathbf{y}) - q(\mathbf{x} - \mathbf{y})).$$

Third definition of a lattice: A *lattice* is a pair (Λ, q) where Λ is finitely generated group and q a *quadratic form*, namely a map $q : \Lambda \to \mathbb{R}$ satisfying, for $\mathbf{x}$ and $\mathbf{y}$ in Λ,
(1) $q(\mathbf{x} + \mathbf{y}) + q(\mathbf{x} - \mathbf{y}) = 2q(\mathbf{x}) + 2q(\mathbf{y})$,
(2) $q(\mathbf{x}) \neq 0$ if $\mathbf{x} \neq 0$,
(3) for all $r > 0$, the set of $\mathbf{x} \in \Lambda$ with $q(\mathbf{x}) \leqslant r$ is finite.

An *isomorphism* between two lattices (Λ_1, q_1) and (Λ_2, q_2) is an isomorphism $f : \Lambda_1 \to \Lambda_2$ of the two $\mathbb{Z}$–modules (abelian groups) which is compatible with the quadratic forms q_1 and q_2:

$$f(q_1(\mathbf{x})) = q_2(f(\mathbf{x})), \quad \mathbf{x} \in \Lambda_1.$$

We just pointed out that a lattice according to the first definition satisfies the third one. We give a sketch of proof of the converse (see [L2001, Prop. 4.1], [L2008, p. 130]).

Sketch of proof. Let Λ satisfy the third definition. From (1) we deduce $q(0) = 0$. Next, by induction, we check, for $m \in \mathbb{Z}$,

$$q(m\mathbf{x}) = m^2 q(\mathbf{x}).$$

As a consequence of (3), we have $q(\mathbf{x}) > 0$ for all $\mathbf{x} \neq 0$. We deduce that Λ is torsion free: if $m\mathbf{x} = 0$ with $m \neq 0$, then $q(m\mathbf{x}) = 0$, hence $q(\mathbf{x}) = 0$ and $\mathbf{x} = 0$. We deduce that Λ is a free $\mathbb{Z}$–module, it has a basis over $\mathbb{Z}$.

For $\mathbf{x}$ and $\mathbf{y}$ in Λ define

$$< \mathbf{x}, \mathbf{y} >= \frac{1}{4}(q(\mathbf{x}+\mathbf{y}) - q(\mathbf{x}-\mathbf{y})).$$

Let E be the $\mathbb{R}$–space spanned by Λ, namely $\Lambda \otimes_{\mathbb{Z}} \mathbb{R}$. One checks that Λ is dense in E. We extend $< \cdot, \cdot >$ to E. Let E_0 be the set of $\mathbf{x} \in E$ with $q(\mathbf{x}) = 0$. Then E/E_0 is an Euclidean space. Finally one checks that $E_0 = 0$. Hence Λ is a discrete $\mathbb{Z}$–module in E of maximal rank. □

Packing

In a lattice of covolume 1, the length of the shortest vectors can be as small as we wish (consider a lattice in $\mathbb{R}^2$ with basis $(\epsilon, 0)$, $(0, 1/\epsilon)$). This length cannot be too large (see [L2001, Prop. 4.2]):

Lemma. There exists $\mathbf{x} \in \Lambda$ with $0 < \|\mathbf{x}\| \leqslant \frac{2}{c_n^{1/n}} \mathrm{covol}(\Lambda)^{1/n}$.

Notice that $\frac{2}{c_n^{1/n}} \leqslant \sqrt{n}$.

Fix n. For Λ lattice in $\mathbb{R}^n$ of covolume 1, let $\ell(\Lambda)$ be the length of a shortest vector in Λ.

Hermite constant:

$$\gamma_n = \sup_{\Lambda} \ell(\Lambda)^2.$$

From the Lemma we deduce the upper bound $\gamma_n \leqslant n$.

Here are the only known exact values:

$n =$	1	2	3	4	5	6	7	8	24
$\gamma_n^n =$	1	4/3	2	4	8	64/3	$64 = 2^6$	$256 = 2^8$	4^{24}

Remark: changing the norm produces different sphere packing. Example: for $\mathbb{R}^n$ with the sup norm, the associated packing is a partition of $\mathbb{R}^n$ by fundamentals parallelograms (hypersquares) with density 1.

Further topics which would deserve to be included.

• LLL reduction algorithm (A. K. Lenstra, H. W. Lenstra, Jr. and L. Lovász, 1982). See [L2001], [TW2006, Chap. 18], [L2008], [G2018, Chap. 17].

• Theorems of Blichfeld and Minkowski. See [Sc1980, Chap. II §12], [L2008, §6], [Sa2013, §4.1], [N2013, Chap. I], [St2020, §5 Geometry of numbers].

• Lattices and codes. Unimodular lattices, integral lattices in $\mathbb{R}^n$, even lattices, root lattices. See [CS1999], [TW2006, §18], [Eb2013, §§1 and 4].

• Diophantine approximation, Geometry of numbers, Blichfeldt's Theorem, Dirichlet's Theorems on convex bodies. See [Sc1980, Chap. II §1], [L2008, §7].

• Finiteness results in algebraic number theory, Dirichlet's unit Theorem, class number. See [L2008, §3], [Sa2013, Chap. 4], [N2013, Chap. I], [St2020, §5 Geometry of numbers, Number rings as lattices].

• Lattices and their theta functions [El2019]. See the course by Samuele Anni on Modular Forms
http://www.rnta.eu/Yogyakarta2025/courses.html

Exercises on Lattices

1. Let Λ be the lattice of $\mathbb{R}^2$ with basis $\begin{pmatrix}1\\2\end{pmatrix}$ and $\begin{pmatrix}3\\-1\end{pmatrix}$.
(a) What is the covolume of Λ?
(b) What is the length of the shortest vectors of Λ?
(c) What is the density of the corresponding sphere packing?
(d) Let $\Lambda^\star$ be the dual lattice. What is the covolume of $\Lambda^\star$? Give a basis of $\Lambda^\star$, the length of the shortest vectors and the density of the sphere packing.

2. Let $u_1, \ldots, u_n$ be nonzero real numbers. Let Λ be the lattice in $\mathbb{R}^n$ with basis

$$\begin{pmatrix}u_1\\0\\\vdots\\0\end{pmatrix}, \begin{pmatrix}0\\u_2\\\vdots\\0\end{pmatrix}, \ldots, \begin{pmatrix}0\\0\\\vdots\\u_n\end{pmatrix}.$$

Let $\mathbf{t} = \begin{pmatrix}t_1\\\vdots\\t_n\end{pmatrix} \in \mathbb{R}^n$. Find the nearest vectors to $\mathbf{t}$ in Λ.

3. Let A be the subring $\mathbb{Z}[\sqrt{3}]$ of $\mathbb{R}$. For $x = a + b\sqrt{3} \in A$, write $x' = a - b\sqrt{3}$. Let

$$L := \left\{ \begin{pmatrix}x\\x'\end{pmatrix} \in \mathbb{R}^2 \;\mid\; x \in A \right\}.$$

Check that L is a lattice in $\mathbb{R}^2$. What is its covolume? What is the length of the shortest vectors? What is the density of the corresponding sphere packing?

4. Let $n \geqslant 2$.
(a) Let $a_1, \ldots, a_n$ and d be rational integers with $d > 0$. Let Λ be the set of $(x_1, \ldots, x_n)$ in $\mathbb{Z}^n$ which satisfy

$$a_1x_1 + \cdots + a_nx_n \equiv 0 \mod d.$$

(a1) Show that Λ is a lattice in $\mathbb{R}^n$. What is its covolume?
(a2) Assume that a_1 and d are relatively prime. Find positive integers $u_1, \ldots, u_{n-1}$ such that

$$\begin{pmatrix}u_1\\1\\0\\\vdots\\0\end{pmatrix}, \begin{pmatrix}u_2\\0\\1\\\vdots\\0\end{pmatrix}, \ldots, \begin{pmatrix}u_{n-1}\\0\\0\\\vdots\\1\end{pmatrix}, \begin{pmatrix}d\\0\\0\\\vdots\\0\end{pmatrix}$$

is a basis of Λ.
(a3) Assume $n = 2$. Let δ be the gcd of a_1 and d. Find a positive integer u such that

$$\begin{pmatrix} u \\ \delta \end{pmatrix}, \begin{pmatrix} d/\delta \\ 0 \end{pmatrix}$$

is a basis of Λ.
(b) Assume $a_1 = \cdots = a_n = 1$ and $d = 2$, so that Λ is the set of $(x_1, \ldots, x_n)$ in $\mathbb{Z}^n$ which satisfy

$$x_1 + \cdots + x_n \equiv 0 \mod 2.$$

This lattice is denoted D_n.
(b1) Give a basis of D_n.
(b2) We use the Euclidean norm on $\mathbb{R}^n$:

$$\|(x_1, \ldots, x_n)\| = \left(\sum_{i=1}^{n} x_i^2 \right)^{1/2}.$$

Show that for any $\mathbf{v}$ and $\mathbf{w}$ in D_n with $\mathbf{v} \neq \mathbf{w}$, we have $\|\mathbf{v} - \mathbf{w}\| \geqslant \sqrt{2}$.
(b3) Show that the spheres of radius $\sqrt{2}/2$ with centers in D_n give a sphere packing in $\mathbb{R}^n$. Compute the density.

5. Check that the three subsets Λ_0, Λ_1, Λ_2 of $\mathbb{Z}^3$ defined by

$$\begin{aligned} \Lambda_0 &= \{(x, y, z) \in \mathbb{Z}^3 \mid x \equiv y \equiv z \equiv 0 \mod 7\}, \\ \Lambda_1 &= \{(x, y, z) \in \mathbb{Z}^3 \mid 2x + 3y \equiv z \equiv 0 \mod 7\}, \\ \Lambda_2 &= \{(x, y, z) \in \mathbb{Z}^3 \mid 2x + 3y + 5z \equiv 0 \mod 7\} \end{aligned}$$

are lattices in $\mathbb{R}^3$. What are their covolume? Give a basis for each of them.

6. Let ϵ satisfy $0 < \epsilon < 1$. Let Λ be the lattice in $\mathbb{R}^3$ with basis

$$\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ \epsilon \end{pmatrix}.$$

Compute the covolume of Λ, the length of the shortest vectors and the density of the associated packing.
Repeat for the dual $\Lambda^\star$.

Solutions of the exercises on Lattices

1. The covolume is the absolute value of the determinant of the matrix

$$\begin{pmatrix} 1 & 3 \\ 2 & -1 \end{pmatrix}$$

hence is 7.

For $(a,b) \in \mathbb{Z}^2$, the square of the norm of $(a+3b, 2a-b)$ is $5a^2+2ab+10b^2$. Let us check that the minimum over $\mathbb{Z}^2 \smallsetminus \{0\}$ of this quadratic form is 5 (with $a = \pm 1$ and $b = 0$). This follows from the remark that for $(a,b) \in \mathbb{Z}^2$ one at least of the two inequalities

$$10b^2 \geqslant 2|ab| \qquad 5a^2 \geqslant 2|ab|$$

is true (consider the two cases $|a| \leqslant |b|$ and $|a| \geqslant |b|$). The same argument shows that for $(a,b) \in \mathbb{Z}^2$ different from $(0,0)$, $(1,0)$ and $(-1,0)$, we have $5a^2+2ab+10b^2 \geqslant 10$ (second shortest vector).

Hence the shortest vectors have length $\sqrt{5}$. The area of the disk of radius $\sqrt{5}/2$ is $5\pi/4$. Since the covolume of Λ is 7,, the density of the sphere packing is

$$\frac{5\pi}{28} = 0.56099\ldots$$

The covolume of $\Lambda^\star$ is $1/7$. The matrices B and $B^\star$ associated to Λ and $\Lambda^\star$ are

$$B = \begin{pmatrix} 1 & 3 \\ 2 & -1 \end{pmatrix} \quad \text{and} \quad B^\star = (B^t)^{-1} = \frac{1}{7}\begin{pmatrix} 1 & 2 \\ 3 & -1 \end{pmatrix}$$

Hence a basis of $\Lambda^\star$ is

$$\begin{pmatrix} 1/7 \\ 3/7 \end{pmatrix}, \quad \begin{pmatrix} 2/7 \\ -1/7 \end{pmatrix}.$$

The square of the norm of an element $(1/7)(a+2b, 3a-b)$ of $\Lambda^\star$ is

$$\frac{1}{49}\big((a+2b)^2 + (3a-b)^2\big) = \frac{1}{49}(10a^2 - 2ab + 5b^2).$$

The minimum over $\mathbb{Z}^2$ of the quadratic form $10a^2-2ab+5b^2$ is 5 (for $(a,b) = (0,\pm 1)$), hence the length of the shortest vectors of $\Lambda^\star$ is

$$\frac{\sqrt{5}}{7} = 0.319\ldots$$

The discs of radius $\sqrt{5}/14$ centered at the lattice points are pairwise disjoint, hence the density of the sphere packing is $5\pi/28 = 0.56099\ldots$.

2. For $1 \leqslant i \leqslant n$, let a_i be one of the nearest integer to t_i/u_i; if $2t_i/u_i \in \mathbb{Z}$ and $t_i/u_i \notin \mathbb{Z}$ then there are two solutions a_i, namely $\frac{t_i}{u_i} - \frac{1}{2}$ and $\frac{t_i}{u_i} + \frac{1}{2}$. Then

$$a_1 \begin{pmatrix} u_1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + a_2 \begin{pmatrix} 0 \\ u_2 \\ \vdots \\ 0 \end{pmatrix} + \cdots + a_n \begin{pmatrix} 0 \\ 0 \\ \vdots \\ u_n \end{pmatrix} = \begin{pmatrix} a_1u_1 \\ a_2u_2 \\ \vdots \\ a_nu_n \end{pmatrix}$$

is a nearest vector of $\mathbf{t}$ in Λ.

3. Since $\sqrt{3}$ is irrational, L is the $\mathbb{Z}$–sub–module of $\mathbb{R}^2$ with basis

$$\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} \sqrt{3} \\ -\sqrt{3} \end{pmatrix},$$

which is a basis of $\mathbb{R}^2$ over $\mathbb{R}$, hence L is a lattice in $\mathbb{R}^2$ (*draw a picture).* The covolume of L is the absolute value of the determinant

$$\begin{pmatrix} 1 & \sqrt{3} \\ 1 & -\sqrt{3} \end{pmatrix},$$

hence is $2\sqrt{3}$.

The square of the norm of an element $(a + b\sqrt{3}, a - b\sqrt{3}) \in L$ is

$$(a + b\sqrt{3})^2 + (a - b\sqrt{3})^2 = 2(a^2 + 3b^2).$$

The minimum of $a^2 + 3b^2$ for $(a, b) \in \mathbb{Z}^2 \smallsetminus \{0\}$ is 1, hence the shortest vectors have length $\sqrt{2}$. The discs with radius $\sqrt{2}/2$ have area $\pi/2$. The density of the corresponding sphere packing is $\pi/4\sqrt{3} = 0.4534\ldots$.
N.B. The highest density for a lattice sphere packing in 2 dimensions is $\pi/2\sqrt{3} = 0.9068\ldots$ with the hexagonal lattice associated to $\mathbb{Z} + \mathbb{Z}(1 + \sqrt{3})/2$.

4.
(a1) Let δ_1 be the gcd of $a_1, \ldots, a_n, d$. We show that Λ is a lattice in $\mathbb{R}^n$ of covolume d/δ_1.

Firstly, assume that $a_1, \ldots, a_n$ are relatively prime, hence $\delta_1 = 1$. The map

$$\begin{array}{rccc} \varphi : & \mathbb{Z}^n & \longrightarrow & \mathbb{Z} \\ & (x_1, \ldots, x_n) & \longmapsto & a_1x_1 + \cdots + a_nx_n \end{array}$$

is therefore surjective. Let $s : \mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}$ be the canonical surjective map. So $s \circ \varphi : \mathbb{Z}^n \longrightarrow \mathbb{Z}/d\mathbb{Z}$ is surjective; its kernel is Λ. Hence Λ is a subgroup of $\mathbb{Z}^n$ of index d. Therefore Λ is a lattice of covolume d: a fundamental domain of Λ is the union of d fundamental domains of $\mathbb{Z}^n$.

In general, let δ be the gcd of $a_1, \ldots, a_n$. Hence δ_1 is the gcd of δ and d. Write $a_i' = \delta a_i$, $\delta = \delta_1\delta_2$, $d = \delta_1 d_1$ with $\gcd(a_1', \ldots, a_n') = 1$, $\gcd(\delta_2, d_1) = 1$. Then the condition

$$a_1x_1 + \cdots + a_nx_n \equiv 0 \mod d$$

is equivalent to

$$a_1'x_1 + \cdots + a_n'x_n \equiv 0 \mod d_1.$$

Hence Λ is a subgroup of $\mathbb{Z}^n$ of index d_1 and a lattice in $\mathbb{R}^n$ of covolume d_1.
(a2) Since a_1 and d are relatively prime, there exists an integer a_1' such that $a_1a_1' \equiv 1 \mod d$. Let u_i be a

positive integer congruent to $-a'_1 a_{i+1}$ modulo d. Then $a_i u_i + a_{i+1} \equiv 0 \mod d$. Since the absolute value of the determinant of the matrix

$$\begin{pmatrix} u_1 & u_2 & \dots & u_{n-1} & d \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}$$

is d, which is the covolume of Λ, we obtain a basis of Λ.
(a3) Write $a_1 = \delta \tilde{a_1}$, $d = \delta \tilde{d}$, with $\tilde{a_1}$ and $\tilde{d}$ relatively prime. Let a'_1 satisfy $a'_1 \tilde{a_1} \equiv 1 \mod \tilde{d}$. Let u_i be a positive integer congruent to $-a'_1 a_2$ modulo $\tilde{d}$. Then $\tilde{a_1} u \equiv -a_2 \mod \tilde{d}$, hence $a_1 u_1 + a_2 \delta \equiv 0 \mod d$. Since the absolute value of the determinant of the matrix

$$\begin{pmatrix} u_1 & d/\delta \\ \delta & 0 \end{pmatrix}$$

is d, which is the covolume of Λ, we obtain a basis of Λ.

(b1) Take $u_1 = \cdots = u_{n-1} = 1$ in (a2).
(b2) For $\mathbf{x} \in \mathbb{Z}^n$, we have $\|\mathbf{x}\|^2 \in \mathbb{Z}$, and $\|\mathbf{x}\| = 0$ if and only if $\mathbf{x} = 0$. The elements $\mathbf{x}$ in $\mathbb{Z}^n$ of norm 1 have all components but 1 which is 0, and the component which is not 0 is 1 or -1, hence for such an element we have

$$x_1 + \cdots + x_n = \pm 1.$$

We deduce that such an element does not belong to D_n, and therefore the elements of $D_n \smallsetminus \{0\}$ have norm $\geqslant \sqrt{2}$. For any $\mathbf{v}$ and $\mathbf{w}$ in D_n with $\mathbf{v} \neq \mathbf{w}$, we have $\mathbf{v} - \mathbf{w} \in \Lambda \smallsetminus \{0\}$, hence $\|\mathbf{v} - \mathbf{w}\| \geqslant \sqrt{2}$.
(b3) From the triangle inequality it follows that two spheres of radius $\sqrt{2}/2$ with centers two different elements of D_n have an empty intersection. The covolume of D_n is 2. Let

$$c_n = \frac{\pi^{n/2}}{\Gamma((n/2)+1)}$$

be the volume of the unit sphere in $\mathbb{R}^n$. The volume of the sphere of radius $\sqrt{2}/2$ is $c_n/2^{n/2}$ and the density of the packing is $\delta(D_n) = c_n/2^{(n/2)+1}$ for $n \geqslant 2$.

Examples.
• $n = 1$, $\Gamma(1/2) = \sqrt{\pi}$, $\Gamma(3/2) = \frac{1}{2}\Gamma(1/2) = \frac{\sqrt{\pi}}{2}$, $c_1 = 2$. For $n = 1$ the covolume of $D_1 = 2\mathbb{Z}$ is 2, the shortest vectors have length 2 and the sphere packing has density 1.
• $n = 2$ (square packing) the density of D_2 is $\pi/4 = 0.7853\ldots$.
• $n = 3$ (face centered cubic packing in 3 dimension). The density of D_3 is

$$\frac{\pi^{3/2}}{4\sqrt{2}\Gamma(2.5)} = 0.7405\ldots$$

• $n = 4$, the density of D_4 is

$$\frac{\pi^2}{2^3\Gamma(3)} = \frac{\pi^2}{16} = 0.6168\ldots$$

• $n = 8$, the density of D_8 is

$$\frac{\pi^4}{32 \cdot \Gamma(4)} = \frac{\pi^4}{768} = 0.1268\ldots$$

5. We have $\Lambda_0 = 7\mathbb{Z}^3$ and

$$\Lambda_0 \subset \Lambda_1 \subset \Lambda_2 \subset \mathbb{Z}^3.$$

A basis of Λ_0 is

$$\begin{pmatrix} 7 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 7 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 7 \end{pmatrix},$$

a basis of Λ_1 is

$$\begin{pmatrix} 7 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 7 \end{pmatrix},$$

a basis of Λ_2 is

$$\begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 7 \end{pmatrix}.$$

The covolumes are respectively 7^3, 7^2 and 7.

6. The covolume of Λ is ϵ. The shortest vectors have length ϵ. The area of the sphere of radius $\epsilon/2$ is $\pi\epsilon^3/6$. Hence the density of the sphere packing associated to Λ is $\pi\epsilon^2/6$.

The inverse of the matrix

$$B = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & \epsilon \end{pmatrix} \quad \text{is} \quad B^{-1} = \begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & -1/\epsilon \\ 0 & 0 & 1/\epsilon \end{pmatrix}.$$

The transpose of B^{-1} is

$$(B^t)^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 0 & -1/\epsilon & 1/\epsilon \end{pmatrix}.$$

Hence a basis of the dual $\Lambda^\star$ is

$$\begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ -1/\epsilon \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1/\epsilon \end{pmatrix}.$$

The covolume est $1/\epsilon$, the shortest vectors have length 1, the sphere of radius $1/2$ has volume $\pi/6$, hence the packing density of $\Lambda^\star$ is $\pi\epsilon/6$.

References

[CS1999] John Conway & Neil J. A. Sloane.
Sphere Packings, Lattices and Groups. Grundlehren der mathematischen Wissenschaften **290** Springer Verlag (1999).
https://doi.org/10.1007/978-1-4757-6568-7

[DF2004] David S. Dummit & Richard Foote.
Abstract algebra. Third Ed., John Wiley and Sons, Inc. (2004)

[Eb2013] Wolfgang Ebeling.
Lattices and Codes. A Course Partially Based on Lectures by Friedrich Hirzebruch. Advanced Lectures in Mathematics (ALM), Springer Verlag 3rd Ed. (2013).
https://doi.org/10.1007/978-3-658-00360-9

[El2019] Noam Elkies.
Rational Lattices and their Theta Functions. Lecture notes for the 2019 Harvard university course.
https://people.math.harvard.edu/~elkies/M272.19/index.html
Lattice Basics
Lattice Basics II

[G2018] Steven D Galbraith.
Mathematics of Public Key Cryptography. Version 2.0, 2018.
https://www.math.auckland.ac.nz/~sgal018/crypto-book/main.pdf

[La2002] Serge Lang.
Algebra. Third Ed. Graduate Texts in Mathematics (GTM, volume **211**) (2002).
https://doi.org/10.1007/978-1-4613-0041-0

[L2001] Hendrik W. Lenstra.
Flags and Lattice Basis Reduction, In: Casacuberta, C., Miró-Roig, R.M., Verdera, J., Xambó-Descamps, S. (eds) European Congress of Mathematics. Progress in Mathematics, vol **201**, 37–51. Birkhäuser, Basel (2001).
https://doi.org/10.1007/978-3-0348-8268-2_3

[L2008] Hendrik W. Lenstra.
Lattices. Algorithmic Number Theory, MSRI Publications Volume **44** (2008), Chap. 12, 127–181. Ed. J.P. Buhler, P. Stevenhagen, Cambridge University Press
https://pub.math.leidenuniv.nl/~stevenhagenp/ANTproc/06hwl.pdf

[N2013] Jürgen Neukirch.
Algebraic Number Theory, Grundlehren der mathematischen Wissenschaften **322**, Springer Verlag (2013).
https://doi.org/10.1007/978-3-662-03983-0

[Sa2013] Pierre Samuel.
Algebraic Theory of Numbers. Translated from the French (Hermann 1967) by Allan J. Silberger. Dover Publications (2013).
https://web.math.ucsb.edu/~agboola/teaching/2021/fall/225A/samuel.pdf

[Sc1980] Wolfgang Schmidt.
Diophantine Approximation, Lecture Notes in Mathematics **785** (1980).
https://doi.org/10.1007/978-3-540-38645-2

[St2020] Peter Stevenhagen.
Number rings (2020).
https://websites.math.leidenuniv.nl/algebra/ant.pdf

[TW2006] Wade Trappe & Lawrence C. Washington.
Introduction to Cryptography with Coding Theory. Pearson Education International, Prentice Hall, 2006. See Chap. 17.
https://www.math.umd.edu/~lcw/book2.html

[W1995] Michel Waldschmidt.
Topologie des points rationnels. 176 p. Cours de Troisième Cycle 1994/95, Preprint Univ. P. et M. Curie, 175 p.
https://webusers.imj-prg.fr/~michel.waldschmidt/TPR.html

Michel WALDSCHMIDT
Sorbonne Université
Faculté Sciences et Ingenierie
CNRS, Institut Mathématique de Jussieu Paris Rive Gauche, IMJ-PRG
F – 75005 Paris, France
michel.waldschmidt@imj-prg.fr
http://www.imj-prg.fr/~michel.waldschmidt