MATH 669: COMBINATORICS, GEOMETRY AND COMPLEXITY OF INTEGER POINTS

Alexander Barvinok

Abstract. These are rather condensed notes, not really proofread or edited, presenting key definitions and results of the course that I taught in Winter 2011 term. Problems marked by $^\circ$ are easy and basic, problems marked by * may be difficult.

Typeset by $\mathcal{A}_{\mathcal{M}}\mathcal{S}$-TEX

Contents

1. Lattices: definition and examples 3
2. Lattice subspaces 4
3. A basis of a lattice 5
4. The determinant of a lattice 7
5. A sublattice of a lattice 9
6. Minkowski Theorem 11
7. The volume of a unit ball 13
8. An application: Lagrange's four squares theorem 14
9. An application: rational approximations of real numbers 16
10. Sphere packings 19
11. The Leech lattice 21
12. The Minkowski - Hlawka Theorem 24
13. The reciprocity relation for the packing radius 27
14. The Korkin-Zolotarev basis of a lattice 28
15. The covering radius of a lattice 30
16. An application: Kronecker's Theorem 33
17. The Poisson summation formula for lattices 34
18. The covering radius via the Poisson summation formula 36
19. The packing density via the Poisson summation formula 39
20. Approximating a convex body by an ellipsoid 40
21. The Flatness Theorem 42
22. The successive minima of a convex body 43
23. An almost orthogonal basis of the lattice 47
24. Successive minima via the Poisson summation formula 49
25. The Lenstra - Lenstra - Lovász basis of a lattice 52
26. Some applications of the Lenstra - Lenstra - Lovász basis 56
27. The algebra of polyhedra and the Euler characteristic 59
28. Linear transformations and polyhedra 62
29. Minkowski sum 64
30. The structure of polyhedra 65
31. Rational generating functions for integer points in polyhedra 69
32. Tangent cones 76
33. The Ehrhart polynomial of an integer polytope 79
34. The reciprocity relation for cones 82
35. The reciprocity relation for the Ehrhart polynomial 85
36. Polarity for cones 87
37. The constant term of the Ehrhart polynomial 90
38. Unimodular cones 92

1. Lattices: definition and examples

We work in a finite-dimensional real vector space V endowed with an inner product $\langle x, y\rangle$ (hence V is Euclidean space) and the corresponding Euclidean norm $\|x\| = \sqrt{\langle x, x\rangle}$.

(1.1) Definitions. A *lattice* $\Lambda \subset V$ is a discrete additive subgroup of V which spans V. That is, $\operatorname{span}(\Lambda) = V$, $x - y \in \Lambda$ for all $x, y \in \Lambda$ (additive subgroup) and there is an $\epsilon > 0$ such that $B_\epsilon \cap \Lambda = \{0\}$, where $B_\epsilon = \{x \in V : \ \|x\| \leq \epsilon\}$ is the ball of radius ϵ (discrete). The dimension of the ambient space V is called the *rank* of lattice Λ and denoted $\operatorname{rank} \Lambda$.

Lattices $\Lambda_1 \subset V_1$ and $\Lambda_2 \subset V_2$ are *isomorphic* if there is an invertible linear transformation $\phi : V_1 \longrightarrow V_2$ such that $\|\phi(x)\| = \|x\|$ for all $x \in V_1$ (so that ϕ is an isometry) and $\phi(\Lambda_1) = \Lambda_2$.

(1.2) Problem. Let $\Lambda \subset V$ be a lattice. Show that $\Lambda \cap K$ is a finite set for every bounded set $K \subset V$.

(1.3) Examples.

(1.3.1) Lattice $\mathbb{Z}^n$. Let $V = \mathbb{R}^n$ with the standard inner product

$$\langle x, y\rangle = \sum_{i=1}^n x_i y_i \quad \text{where} \quad x = (x_1, \ldots, x_n) \quad \text{and} \quad y = (y_1, \ldots, y_n).$$

Let $\mathbb{Z}^n \subset \mathbb{R}^n$ be the set consisting of the points with integer coordinates,

$$\mathbb{Z}^n = \Big\{(x_1, \ldots, x_n) : \quad x_i \in \mathbb{Z} \quad \text{for} \quad i = 1, \ldots, n\Big\}.$$

(1.3.2) Lattice A_n. Let us identify V with the hyperplane $H \subset \mathbb{R}^{n+1}$ defined by the equation $x_1 + \ldots + x_{n+1} = 0$. We let

$$A_n = \mathbb{Z}^{n+1} \cap H.$$

(1.3.3) Lattice D_n. Let $V = \mathbb{R}^n$ and let

$$D_n = \Big\{(x_1, \ldots, x_n) \in \mathbb{Z}^n : \quad x_1 + \ldots + x_n \equiv 0 \mod 2\Big\}.$$

(1.3.4) Lattice D_n^+. Suppose that n is even. Let $D_n \subset \mathbb{R}^n$ be the lattice of Example 1.3.3 and let us define $u \in \mathbb{R}^n$ by

$$u = \underbrace{\Big(\frac{1}{2}, \ldots, \frac{1}{2}\Big)}_{n \text{ times}}.$$

We let

$$D_n^+ = D_n \cup (D_n + u).$$

(1.3.5) Lattices E_8, E_7 and E_6. We denote $E_8 = D_8^+$, $E_7 = E_8 \cap H$, where $H \subset \mathbb{R}^8$ is the hyperplane defined by the equation $x_1 + \ldots + x_8 = 0$, and $E_6 = E_8 \cap L$, where $L \subset \mathbb{R}^8$ is the subspace defined by the equations $x_1 + x_8 = x_2 + x_3 + x_4 + x_5 + x_6 + x_7 = 0$.

(1.4) Problem. Prove that $\mathbb{Z}^n$, A_n, D_n, D_n^+, E_8, E_7 and E_6 are indeed lattices.

2. Lattice subspaces

(2.1) Definitions. Let $\Lambda \subset V$ be a lattice and let $L \subset V$ be a subspace. We say that L is a Λ-*subspace* or just a *lattice subspace* if L is spanned by points from Λ, or, equivalently, if $\Lambda \cap L$ is a lattice in L.

For a set $A \subset V$ and a point $x \in V$, we define the distance

$$\operatorname{dist}(x, A) = \inf_{y \in A} \|x - y\|.$$

In what follows, we denote by $\lfloor \alpha \rfloor$ the largest integer not exceeding a real number α and we denote $\{\alpha\} = \alpha - \lfloor \alpha \rfloor$. Clearly,

$$0 \ \leq \ \{\alpha\} \ < 1 \quad \text{for all} \quad \alpha \in \mathbb{R}.$$

The main result of this section is that if $L \subset V$ is a lattice subspace such that $L \neq V$ then among all lattice points not in L there is a point nearest to L.

(2.2) Lemma. *Let $\Lambda \subset V$ be a lattice and let $L \subset V$, $L \neq V$, be a Λ-subspace. Then there exists a point $v \in \Lambda \setminus L$ such that*

$$\operatorname{dist}(v, L) \ \leq \ \operatorname{dist}(w, L) \quad \textit{for all} \quad w \in \Lambda \setminus L.$$

Proof. Let $k = \dim L$ and let $u_1, \ldots, u_k$ be a basis of L consisting of lattice points, so $u_i \in \Lambda$ for $i = 1, \ldots, k$. Let

$$\Pi = \left\{ \sum_{i=1}^{k} \lambda_i u_i : \quad 0 \leq \lambda_i \leq 1 \quad \text{for} \quad i = 1, \ldots, k \right\}$$

be the parallelepiped spanned by $u_1, \ldots, u_k$. We claim that among the lattice points that are not in L there is a point nearest to Π. For $\rho > 0$, let us consider the ρ-neighborhood of Π,

$$\Pi_\rho = \Big\{ x \in V : \quad \operatorname{dist}(x, \Pi) \leq \rho \Big\}.$$

Clearly, Π_ρ is bounded and hence $\Pi_\rho \cap \Lambda$ is a finite set, cf. Problem 1.2. Let us choose a sufficiently large ρ so that

$$\Pi_\rho \cap (\Lambda \setminus L) \neq \emptyset$$

and let us choose a point $v \in \Pi_\rho \cap (\Lambda \setminus L)$ nearest to Π. Clearly,

$$\operatorname{dist}(v, \Pi) \ \leq \ \operatorname{dist}(w, \Pi) \quad \text{for all} \quad w \in \Lambda \setminus L. \tag{2.2.1}$$

Let us choose any $w \in \Lambda \setminus L$ and let $x \in L$ be the point such that

$$\operatorname{dist}(w, L) = \|w - x\|.$$

We can write

$$x = \sum_{i=1}^{k} \alpha_i u_i = u + y \quad \text{where} \quad u = \sum_{i=1}^{k} \lfloor \alpha_i \rfloor u_i \quad \text{and} \quad y = \sum_{i=1}^{k} \{\alpha_i\} u_i.$$

Clearly, $u \in \Lambda \cap L$ and $y \in \Pi$. Moreover, $w - u \in \Lambda \setminus L$ and by (2.2.1)

$$\begin{aligned} \operatorname{dist}(w, L) =& \|w - x\| = \|(w-u) - (x-u)\| = \|(w-u) - y\| \ \geq\ \operatorname{dist}(w-u,\ \Pi) \\ &\geq\ \operatorname{dist}(v, \Pi) \ \geq\ \operatorname{dist}(v, L), \end{aligned}$$

which completes the proof. □

(2.3) Problems.

1. Let $\Lambda \subset V$ be a lattice and let $L \subset V$ be a Λ-subspace. Let us consider a decomposition $V = L \oplus W$ and the projection $pr : V \longrightarrow W$ with the kernel L. Prove that $pr(\Lambda)$ is a lattice in W.

2. Let $L \subset \mathbb{R}^2$ be a line with an irrational slope. Prove that there exist points $w \in \mathbb{Z}^2 \setminus L$ arbitrarily close to L.

3. Let $L \subset \mathbb{R}^2$ be a line with an irrational slope and let $pr : \mathbb{R}^2 \longrightarrow L$ be the orthogonal projection. Prove that $pr\left(\mathbb{Z}^2\right)$ is dense in L.

3. A basis of a lattice

We prove the following main result.

(3.1) Theorem. *Let V be a d-dimensional Euclidean space, $d > 0$.*

(1) *Let $\Lambda \subset V$ be a lattice. Then there exist vectors $u_1, \ldots, u_d \in \Lambda$ such that every point $u \in \Lambda$ admits a unique representation*

$$u = \sum_{i=1}^{d} m_i u_i \quad \textit{where} \quad m_i \in \mathbb{Z} \quad \textit{for} \quad i = 1, \ldots, d.$$

The set $\{u_1, \ldots, u_d\}$ is called a basis of Λ.

(2) *Let $u_1, \ldots, u_d$ be a basis of V and let*

$$\Lambda = \left\{ \sum_{i=1}^{d} m_i u_i \quad \textit{where} \quad m_i \in \mathbb{Z} \right\}.$$

Then $\Lambda \subset V$ is a lattice.

Proof. We prove Part (1) by induction on d. Suppose that $d = 1$ so that we identify $V = \mathbb{R}$. Since Λ is discrete, there exists the smallest positive number $a \in \Lambda$. We claim that every point $x \in \Lambda$ can be written as $x = ma$ for some $m \in \mathbb{Z}$. Replacing x by $-x$, if necessary, without loss of generality we may assume that $x > 0$. Then we can write

$$x = \mu a = \lfloor \mu \rfloor a + \{\mu\} a \quad \text{for some} \quad \mu > 0.$$

We observe that $\lfloor \mu \rfloor a \in \Lambda$ and hence $\{\mu\} a \in \Lambda$. Since $0 \leq \{\mu\} a < a$ we must have $\{\mu\} = 0$. Therefore μ is integer and a is a basis of Λ.

Suppose that $d > 1$. Let us choose $d - 1$ linearly independent lattice points and let L be the subspace spanned by those points. Hence L is a Λ-subspace and $L \cap \Lambda$ is a lattice in L. By the induction hypothesis, we can choose a basis $u_1, \ldots, u_{d-1}$ of lattice $L \cap \Lambda$ in L. By Lemma 2.2, there is a point $u_d \in \Lambda \setminus L$ such that

$$\operatorname{dist}(u_d, L) \ \leq \ \operatorname{dist}(w, L) \quad \text{for all} \quad w \in \Lambda \setminus L.$$

We claim that $u_1, \ldots, u_{d-1}, u_d$ is a basis of Λ. Indeed, let us choose any $u \in \Lambda$, so we can write

$$u = \sum_{i=1}^{d} \alpha_i u_i \quad \text{for some} \quad \alpha_1, \ldots, \alpha_d \in \mathbb{R}.$$

Let

$$v = u - \lfloor \alpha_d \rfloor u_d = \{\alpha_d\} u_d + \sum_{i=1}^{d-1} \alpha_i u_i.$$

Clearly, $v \in \Lambda$ and

$$\operatorname{dist}(v, L) = \operatorname{dist}\left(\{\alpha_d\} u_d, \ L\right) = \{\alpha_d\} \operatorname{dist}\left(u_d, \ L\right) \ < \ \operatorname{dist}\left(u_d, \ L\right),$$

from which it follows that $v \in L$. Hence $\{\alpha_d\} = 0$ and $\alpha_d \in \mathbb{Z}$. Then $u - \alpha_d u_d \in \Lambda \cap L$ and by the induction hypothesis we must have $\alpha_1, \ldots, \alpha_{d-1} \in \mathbb{Z}$, which completes the proof of Part (1).

To prove Part (2), let us consider the map $T : \mathbb{R}^d \longrightarrow V$,

$$T\left(\alpha_1, \ldots, \alpha_d\right) = \sum_{i=1}^{d} \alpha_i u_i.$$

Then $\Lambda = T\left(\mathbb{Z}^d\right)$. Clearly, Λ is an additive subgroup of V which spans V, and since T is invertible, Λ is discrete. □

(3.2) Problems.

1. Construct bases of lattices $\mathbb{Z}^n$, A_n and D_n, see Example 1.3.

2. Prove that

$$u_1 = (2,0,0,0,0,0,0,0)\,,\ u_2 = (-1,1,0,0,0,0,0,0)\,,\ u_3 = (0,-1,1,0,0,0,0,0)\,,$$
$$u_4 = (0,0,-1,1,0,0,0,0)\,,\ u_5 = (0,0,0,-1,1,0,0,0)\,,\ u_6 = (0,0,0,0,-1,1,0,0)\,,$$
$$u_7 = (0,0,0,0,0,0,-1,1,0)\,,\ u_8 = \left(\frac{1}{2},\ \frac{1}{2},\ \frac{1}{2},\ \frac{1}{2},\ \frac{1}{2},\ \frac{1}{2},\ \frac{1}{2},\ \frac{1}{2}\right)$$

is a basis of E_8, see Example 1.3.5.

3. Let $\Lambda \subset \mathbb{R}^2$ be a lattice. Prove that there is a basis u, v of Λ such that the angle α between u and v satisfies $\pi/3 \ \leq\ \alpha\ \leq\ \pi/2$.

4. Let Λ be a lattice. A set of vectors $u_1, \ldots, u_k \in \Lambda$ is called *primitive* if $u_1, \ldots, u_k$ is a basis of $\Lambda \cap \operatorname{span}\{u_1, \ldots, u_k\}$. Prove that a primitive set can be appended to a basis of the lattice.

4. The determinant of a lattice

(4.1) Definition. Let $\Lambda \subset V$ be a lattice and let $u_1, \ldots, u_d$ be a basis of Λ. The set

$$\Pi = \left\{ \sum_{i=1}^d \alpha_i u_i : \quad 0 \leq \alpha_i < 1 \quad \text{for} \quad i = 1, \ldots, d \right\}$$

is called *the fundamental parallelepiped* of basis $u_1, \ldots, u_d$ and *a fundamental parallelepiped* of lattice Λ.

(4.2) Lemma. *Let $\Lambda \subset V$ be a lattice and let Π be a fundamental parallelepiped of Λ. Then every point $x \in V$ can be written uniquely as $x = u + y$ for $u \in \Lambda$ and $y \in \Pi$. In other words, lattice shifts $\{\Pi + u : \quad u \in \Lambda\}$ cover the ambient space V without overlapping.*

Proof. Let Π be the fundamental parallelepiped of a basis $u_1, \ldots, u_d$ of Λ. An arbitrary point $x \in V$ can be written as

$$x = \sum_{i=1}^d \alpha_i u_i \quad \text{for some} \quad \alpha_1, \ldots, \alpha_d \in \mathbb{R}.$$

Letting

$$u = \sum_{i=1}^d \lfloor \alpha_i \rfloor u_i \quad \text{and} \quad y = \sum_{i=1}^d \{\alpha_i\}\, u_i,$$

we conclude that $x = u + y$, where $u \in \Lambda$ and $y \in \Pi$.

To prove uniqueness, suppose that $x = u_1 + y_1 = u_2 + y_2$ where $u_1, u_2 \in \Lambda$ and $y_1, y_2 \in \Pi$. Therefore,

$$y_1 = \sum_{i=1}^d \alpha_i u_i \quad \text{and} \quad y_2 = \sum_{i=1}^d \beta_i u_i \quad \text{for some} \quad 0 \leq \alpha_i, \beta_i < 1 \quad \text{for} \quad i = 1, \ldots, d.$$

Then $y_1 - y_2 = u_2 - u_1 \in \Lambda$ from which we must have that $\alpha_i - \beta_i \in \mathbb{Z}$ for $i = 1, \ldots, d$. Therefore, $\alpha_i = \beta_i$ for $i = 1, \ldots, d$ and hence $y_1 = y_2$ and $u_1 = u_2$. $\square$

(4.3) Theorem. *Let $\Lambda \subset V$ be a lattice. Then every fundamental parallelepiped Π of Λ has the same volume, called the determinant of Λ and denoted $\det \Lambda$. Furthermore, $\det \Lambda$ can be obtained as follows.*

Let $B_\rho = \{x \in V : \quad \|x\| \leq \rho\}$ be the ball of radius ρ. Then

$$\lim_{\rho \longrightarrow +\infty} \frac{|\Lambda \cap B_\rho|}{\operatorname{vol} B_\rho} = \frac{1}{\det \Lambda}.$$

In other words, $\det \Lambda$ is "the volume per lattice point". More generally, if $x \in V$ is a point and $x + \Lambda = \{x + u : \quad u \in \Lambda\}$ is a translation of Λ then

$$\lim_{\rho \longrightarrow +\infty} \frac{|(x+\Lambda) \cap B_\rho|}{\operatorname{vol} B_\rho} = \frac{1}{\det \Lambda}.$$

Proof. Let Π be a fundamental parallelepiped of Λ. Let

$$X_\rho = \bigcup_{u \in B_\rho \cap \Lambda} (\Pi + u).$$

By Lemma 4.2, we have

$$\operatorname{vol} X_\rho = |B_\rho \cap \Lambda| \operatorname{vol} \Pi.$$

Since Π is bounded, we have $\Pi \subset B_\alpha$ for some $\alpha > 0$ and so $X_\rho \subset B_{\rho+\alpha}$. On the other hand, by Lemma 4.2 every point in $B_{\rho-\alpha}$ lies in some translation $\Pi + u$, where necessarily $\|u\| \leq \alpha$. Hence $B_{\rho-\alpha} \subset X_\rho$.

Summarizing,

$$\operatorname{vol} B_{\rho-\alpha} \ \leq \ \operatorname{vol} X_\rho = |B_\rho \cap \Lambda| \operatorname{vol} \Pi \ \leq \ B_{\rho+\alpha}.$$

Since

$$\lim_{\rho \longrightarrow +\infty} \frac{\operatorname{vol} B_{\rho \pm \alpha}}{\operatorname{vol} B_\rho} = \lim_{\rho \longrightarrow +\infty} \left(\frac{\rho \pm \alpha}{\rho}\right)^{\dim V} = 1, \tag{4.3.1}$$

we conclude that

$$\lim_{\rho \longrightarrow +\infty} \frac{|B_\rho \cap \Lambda|}{\operatorname{vol} B_\rho} = \frac{1}{\operatorname{vol} \Pi}.$$

In particular $\operatorname{vol} \Pi$ does not depend on the choice of the fundamental parallelepiped Π.

More generally, for an arbitrary $x \in V$ and $\xi = \|x\|$, we have

$$x + (B_{\rho-\xi} \cap \Lambda) \ \subset \ B_\rho \cap (x + \Lambda) \ \subset \ x + (B_{\rho+\xi} \cap \Lambda),$$

from which

$$|B_{\rho-\xi} \cap \Lambda| \ \leq \ |B_\rho \cap (x+\Lambda)| \ \leq \ |B_{\rho+\xi} \cap \Lambda|.$$

Using (4.3.1), we conclude that

$$\lim_{\rho \longrightarrow +\infty} \frac{|B_\rho \cap (x+\Lambda)|}{\operatorname{vol} B_\rho} = \lim_{\rho \longrightarrow +\infty} \frac{|B_\rho \cap \Lambda|}{\operatorname{vol} B_\rho} = \frac{1}{\det \Lambda}.$$

$\square$

(4.4) Problems.

1. Let $\Lambda \subset V$ be a lattice and let

$$\Phi = \Big\{ x \in V : \quad \|x\| \ \leq \ \|x - u\| \quad \text{for all} \quad u \in \Lambda \Big\}.$$

Prove that $\operatorname{vol} \Phi = \det \Lambda$.

2. Let $\Lambda \subset V$ be a lattice and let us define

$$\Lambda^* = \Big\{ x \in V : \ \langle x, u \rangle \in \mathbb{Z} \Big\}.$$

Prove that Λ^* is a lattice (it is called *dual* or *reciprocal*) to Λ and that

$$(\det \Lambda^*) \, (\det \Lambda) = 1.$$

3. Prove that $(\Lambda^*)^* = \Lambda$.
4. Prove that $(\mathbb{Z}^n)^* = \mathbb{Z}^n$ and that $E_8^* = E_8$.

5. A sublattice of a lattice

(5.1) Definitions. Let $\Lambda \subset V$ be a lattice. Suppose that $\Lambda_0 \subset \Lambda$ is another lattice in V, so $\operatorname{rank} \Lambda_0 = \operatorname{rank} \Lambda$. Then Λ_0 is a subgroup of Λ (we say that Λ_0 is a *sublattice* of Λ). We consider *cosets* $a + \Lambda_0 = \big\{ a + u : \quad u \in \Lambda_0 \big\}$ for $a \in \Lambda$. Every two cosets either coincide or do not intersect. The cosets form an abelian group under addition, called the *quotient* and denoted Λ / Λ_0. The order $|\Lambda / \Lambda_0|$ of the quotient is called the *index* of Λ_0 in Λ.

(5.2) Theorem. *Let Λ be a lattice and let $\Lambda_0 \subset \Lambda$ be a sublattice. Let Π be a fundamental parallelepiped of Λ_0. Then the set $\Pi \cap \Lambda_0$ contains each coset Λ / Λ_0 representative exactly once. Furthermore,*

$$|\Pi \cap \Lambda| = |\Lambda / \Lambda_0| = \frac{\det \Lambda_0}{\det \Lambda}.$$

In particular, the index $|\Lambda / \Lambda_0|$ is finite.

Proof. By Lemma 4.2, for every $x \in \Lambda$ there is a unique pair of $y \in \Pi$ and $u \in \Lambda_0$ such that $x = y + u$. Hence we must have that $y \in \Lambda$, so y is a coset representative of x in Π. This proves that $|\Pi \cap \Lambda| = |\Lambda / \Lambda_0|$.

Let S be a set of the coset representatives, so

$$\Lambda = \bigcup_{s \in S} (s + \Lambda_0) \, .$$

Let B_ρ be a ball of radius ρ. Hence

$$|B_\rho \cap \Lambda| = \sum_{s \in S} |B_\rho \cap (s + \Lambda_0)| \, .$$

By Theorem 4.3,

$$\lim_{\rho \longrightarrow +\infty} \frac{|B_\rho \cap \Lambda|}{\operatorname{vol} B_\rho} = \frac{1}{\det \Lambda} \quad \text{and} \quad \lim_{\rho \longrightarrow +\infty} \frac{|B_\rho \cap (s + \Lambda_0)|}{\operatorname{vol} B_\rho} = \frac{1}{\det \Lambda_0}.$$

which proves that

$$\frac{\det \Lambda_0}{\det \Lambda} = |\Lambda / \Lambda_0|.$$

□

(5.3) Problems.

1°. Let $u_1, \ldots, u_d \in \mathbb{Z}^d$ be linearly independent integer vectors and let

$$\Pi = \left\{ \sum_{i=1}^{d} \alpha_i u_i : \quad 0 \leq \alpha_i < 1 \quad \text{for} \quad i = 1, \ldots, d \right\}.$$

Prove that $\left| \Pi \cap \mathbb{Z}^d \right| = \operatorname{vol} \Pi$.

2. Prove that linearly independent vectors $u, v \in \mathbb{Z}^2$ form a basis of $\mathbb{Z}^2$ if and only if the triangle with the vertices $0, u, v$ does not contain any point from $\mathbb{Z}^2$ other than $0, u$ and v.

3. Construct an example of linearly independent vectors $u, v, w \in \mathbb{Z}^3$ with an arbitrary large volume of the tetrahedron with the vertices $0, u, v$ and w and no integer points in the tetrahedron other than $0, u, v$ and w.

4. Prove Pick's formula: if $P \subset \mathbb{R}^2$ is a convex polygon with integer vertices and non-empty interior then

$$\left| P \cap \mathbb{Z}^2 \right| = \operatorname{vol} P + \frac{1}{2} \left| \partial P \cap \mathbb{Z}^2 \right| + 1,$$

where ∂P is the boundary of P.

5. Let $u_1, \ldots, u_d$ be a basis of lattice $\Lambda \subset V$ and let $v_1, \ldots, v_d \in V$ be some vectors. Let $v_i = \sum_{j=1}^{d} \mu_{ij} u_j$ for $i = 1, \ldots, d$ and let $M = (\mu_{ij})$ be the $d \times d$ matrix of the coefficients μ_{ij}. Prove that $v_1, \ldots, v_d$ is a basis of M if and only if M is an integer matrix and $\det M = \pm 1$.

6. Prove the existence of the Smith normal form: if Λ_0 is a sublattice of Λ then there exists a basis $u_1, \ldots, u_d$ of Λ and positive integers $m_1, \ldots, m_d$ such that m_i divides m_{i+1} for $i = 1, \ldots, d-1$ and $v_1 = m_1 u_1, \ldots, v_d = m_d u_d$ is a basis of Λ_0.

7. Let $a_1, \ldots, a_d$ be coprime integers and let n be a positive integer. Let $\Lambda \subset \mathbb{Z}^d$ be the set of points $(m_1, \ldots, m_d)$ defined by the congruence

$$a_1 m_1 + \ldots + a_d m_d \equiv 0 \mod n.$$

Prove that Λ is a sublattice of $\mathbb{Z}^d$ and that $\det \Lambda = n$.

8. Let $a_1, \ldots, a_{d+1}$ be coprime integers and let V be the d-dimensional Euclidean space identified with the hyperplane $H \subset \mathbb{R}^{d+1}$ defined by the equation $a_1 x_1 + \ldots + a_{d+1} x_{d+1} = 0$. Let $\Lambda = \mathbb{Z}^{d+1} \cap H$. Prove that Λ is a lattice in V and that $\det \Lambda = \sqrt{a_1^2 + \ldots + a_{d+1}^2}$.

9. For lattices of Example 1.3 prove that $\det \mathbb{Z}^n = 1$, $\det A_n = \sqrt{n+1}$, $\det D_n = 2$, $\det D_n^+ = 1$, $\det E_7 = \sqrt{2}$ and $\det E_6 = \sqrt{3}$.

10. For $k \leq d$ let $\{v_1, \ldots, v_k\}$ be a linearly independent subset of $\mathbb{Z}^d$. Let us consider the $k \times d$ matrix M whose (i,j)-th entry is the j-th coordinate of v_i. Prove that the set $\{v_1, \ldots, v_k\}$ is primitive (see Problem 4 of Section 3.2) if and only if the greatest common divisor of all $k \times k$ minors of M is 1.

6. Minkowski Theorem

We start with a lemma, also known as Blichfeldt's Theorem.

(6.1) Lemma. *Let $\Lambda \subset V$ be a lattice and let X be a measurable set such that $\operatorname{vol} X > \det \Lambda$. Then there are points $x, y \in X$ such that $x - y \in \Lambda \setminus \{0\}$.*

Proof. Let us choose a fundamental parallelepiped Π of Λ. For $u \in \Lambda$ let us define

$$X_u = \Big\{ z \in \Pi : \ z + u \in X \Big\} = \Big((\Pi + u) \cap X \Big) - u.$$

By Lemma 4.2, the set X is a disjoint union

$$X = \bigcup_{u \in \Lambda} \left(X_u + u \right),$$

and hence

$$\sum_{u \in \Lambda} \operatorname{vol} X_u = \operatorname{vol} X > \det \Lambda = \operatorname{vol} \Pi.$$

Therefore, there are two points $u, v \in \Lambda$ such that $X_u \cap X_v \neq \emptyset$ and $u \neq v$. Therefore, there is a point $z \in \Pi$ such that $x = z + u \in X$ and $y = z + v \in X$. Then we have $x - y = u - v \in \Lambda \setminus \{0\}$. □

(6.2) Problems.

1. Let $X \subset V$ be a measurable set such that $\operatorname{vol} X > m \det \Lambda$ for some positive integer m. Prove that there exist $m+1$ distinct points $x_1, \ldots, x_{m+1} \in X$ such that $x_i - x_j \in \Lambda$ for all i and j.

2. Let $f : V \longrightarrow \mathbb{R}$ be a non-negative integrable function and let $\Lambda \subset V$ be a lattice. Prove that there is a $z \in V$ such that

$$\sum_{u \in \Lambda} f(u + z) \ \geq \ \frac{1}{\det \Lambda} \int_V f(x) \, dx.$$

3. Let $X \subset V$ be a compact set such that $\operatorname{vol} X = \det \Lambda$. Prove that there are points $x, y \in X$ such that $x - y \in \Lambda \setminus \{0\}$. Give an example showing that the statement is not true if X is not compact.

(6.3) Definitions. A set $A \subset V$ is called *convex* if for every $x, y \in A$, we have $[x, y] \subset A$, where $[x, y] = \big\{\alpha x + (1-\alpha)y : \ 0 \leq \alpha \leq 1\big\}$ is the interval with the endpoints x and y. A set $A \subset V$ is called *symmetric* if $-x \in A$ whenever $x \in A$ (we write $A = -A$ in this case).

Now we prove the famous Minkowski Theorem.

(6.4) Theorem. *Let $\Lambda \subset V$ be a lattice and let $\dim V = d$. Let $A \subset V$ be a symmetric convex set such that $\operatorname{vol} A > 2^d \det \Lambda$. Then there exists a point $u \in \Lambda \setminus \{0\}$ such that $u \in A$.*

Proof. Let

$$X = \frac{1}{2}A = \left\{\frac{1}{2}x : \ x \in A\right\}.$$

Then $\operatorname{vol} X = 2^{-d} \operatorname{vol} A > \det \Lambda$ and hence by Lemma 6.1 there are points $x, y \in X$ such that $x - y = u \in \Lambda \setminus \{0\}$. Hence

$$u = \frac{1}{2}(2x) + \frac{1}{2}(-2y).$$

We have $2x, 2y \in A$ and since A is symmetric, we also have $-2y \in A$. Finally, since A is convex, we conclude that $u \in A$. □

(6.5) Problems.

1. Prove that if $\operatorname{vol} A = 2^d \det \Lambda$ and if A is convex, symmetric and compact then A contains a non-zero lattice point.

2. Let $\Lambda \subset V$ be a lattice and let $A \subset V$ be a symmetric convex set such that $\operatorname{vol} A > m2^d \det \Lambda$, where $d = \dim V$ and m is a positive integer. Prove that A contains at least m pairs of distinct non-zero lattice points $\pm u_i$ for $i = 1, \ldots, m$.

3. Let $\Lambda \subset V$ be a lattice, where $\dim V = d$ and let

$$K = \Big\{x \in V : \ \|x\| \leq \|x - u\| \quad \text{for all} \quad u \in \Lambda\Big\}.$$

Let $A = 2K$. Prove that A is convex, symmetric, that $\operatorname{vol} A = 2^d \det \Lambda$ and that A does not contain a non-zero lattice point in its interior.

4. Let Λ be a lattice of rank d and let $X \subset \Lambda$ be set such that $|X| > 2^d$. Prove that there are two distinct points $x, y \in X$ such that $(x + y)/2 \in \Lambda$.

5. A set $X \subset \Lambda$ is called lattice-convex if $X = \Lambda \cap A$, where $A \subset V$ is a convex set. Let $\operatorname{rank} \Lambda = d$ and let $\{X_i\}$ be a finite family of lattice-convex sets such that the intersection of every 2^d of the sets is non-empty. Prove that the intersection of all sets X_i is non-empty (Doignon's Theorem).

6^*. Let $A \subset V$ be a compact symmetric convex set such that $\operatorname{vol} A = 2^d \det \Lambda$ and A does not contain a non-zero lattice point in its interior. Prove that there are $n \leq 2^d - 1$ vectors $u_i \in \Lambda \setminus \{0\}$ and real numbers α_i, $i = 1, \ldots, n$ such that

$$A = \Big\{x \in V : \ |\langle u_i, x\rangle| < \alpha_i \quad \text{for} \quad i = 1, \ldots, n\Big\}$$

(Minkowski's Theorem).

7*. Let $A \subset \mathbb{R}^d$ be a compact symmetric convex set which does not contain a non-zero point of $\mathbb{Z}^d$. Prove that

$$2^d = \operatorname{vol} A + 4^d (\operatorname{vol} A)^{-1} \sum_{u \in \mathbb{Z}^d \setminus \{0\}} \left| \int_{\frac{1}{2}A} \exp\{-2\pi i \langle u, x \rangle\} \ dx \right|^2$$

(Siegel's Theorem).

Hint: Define the indicator $[X]$ of a set $X \subset \mathbb{R}^d$ as the function $[X] : \mathbb{R}^d \longrightarrow \mathbb{R}$ where

$$[X](x) = \begin{cases} 1 & \text{if } x \in X \\ 0 & \text{if } \ x \notin X. \end{cases}$$

Let

$$\phi(x) = \sum_{u \in \mathbb{Z}^d} \left[u + \frac{1}{2} A \right],$$

and apply Parseval's formula to ϕ.

7. The volume of a unit ball

We need the formula for the volume of the unit ball in $\mathbb{R}^d$. Recall that the Gamma function is defined by the formula

$$\Gamma(x) = \int_0^{+\infty} t^{x-1} e^{-t} \ dt \quad \text{for} \quad x > 0.$$

(7.1) Problems.

1. Prove that $\Gamma(x+1) = x\Gamma(x)$. Deduce that $\Gamma(x) = (x-1)!$ for positive integer x.

2*. Prove that $\Gamma\left(\frac{1}{2}\right) = \sqrt{\pi}$.

3*. Deduce Stirling's formula

$$\Gamma(x+1) = \sqrt{2\pi x} x^x e^{-x} \left(1 + O\left(x^{-1}\right)\right) \quad \text{as} \quad x \longrightarrow +\infty.$$

(7.2) Lemma. *Let β_d be the volume of the unit ball*

$$\mathbb{B}^d = \left\{ x \in \mathbb{R}^d : \ \|x\| \leq 1 \right\}$$

in $\mathbb{R}^d$. Then

$$\beta_d = \frac{\pi^{d/2}}{\Gamma\left(1 + \frac{d}{2}\right)}.$$

Proof. Let
$$\mathbb{S}^{d-1}(\rho) = \left\{x \in \mathbb{R}^d : \ \|x\| = \rho\right\}$$
denote the sphere of radius ρ and let κ_{d-1} denote the surface area of the unit sphere $\mathbb{S}^{d-1}(1)$, so the surface area of $\mathbb{S}^{d-1}(\rho)$ is $\kappa_{d-1}\rho^{d-1}$. Let us denote temporarily

$$\int_{-\infty}^{+\infty} e^{-x^2} \ dx = \lambda.$$

Then, using the polar coordinates and a substitution $t = \rho^2$, we can write

$$\begin{aligned}\lambda^d = &\int_{\mathbb{R}^d} e^{-\|x\|^2} \ dx = \kappa_{d-1} \int_0^{\rho} e^{-\rho^2} \rho^{d-1} \ d\rho = \frac{\kappa_{d-1}}{2} \int_0^{+\infty} t^{(d-2)/2} e^{-t} \ dt \\ = &\frac{\kappa_{d-1}}{2} \Gamma\left(\frac{d}{2}\right),\end{aligned}$$

from which
$$\kappa_{d-1} = \frac{2\lambda^d}{\Gamma\left(\frac{d}{2}\right)}.$$

Therefore,
$$\beta_d = \int_0^1 \kappa_{d-1}\rho^{d-1} \ d\rho = \frac{\kappa_{d-1}}{d} = \frac{\lambda^d}{\Gamma\left(1 + \frac{d}{2}\right)}.$$
Since $\beta_2 = \pi$ we conclude that $\lambda = \sqrt{\pi}$ and the proof follows. $\square$

8. An application: Lagrange's four squares theorem

As an application of Minkowski's Theorem (Theorem 6.4), we prove Lagrange's Theorem that every positive integer is a sum of four squares of integers. The proof below was given by Davenport.

(8.1) Lemma. *Let $a_1, \ldots, a_k \in \mathbb{Z}^d \setminus \{0\}$ be integer vectors, let $m_1, \ldots, m_k$ be positive integers and let us define*

$$\Lambda = \Big\{x \in \mathbb{Z}^d : \ \langle a_i, x\rangle \equiv 0 \mod m_i \quad \textit{for} \quad i = 1, \ldots, k\Big\}.$$

Then Λ is a lattice in $\mathbb{R}^d$ and $\det \Lambda \ \leq \ m_1 \cdots m_k$.

Proof. Clearly, Λ is a discrete additive subgroup of $\mathbb{Z}^d$. Moreover, Λ spans $\mathbb{R}^d$ since $m\mathbb{Z}^d \subset \Lambda$ for $m = m_1 \cdots m_k$.

Let us estimate the index of Λ in $\mathbb{Z}^d$. A coset of $\mathbb{Z}^d/\Lambda$ consists of the points $x \in \mathbb{Z}^d$ for which the values of $\langle a_i, x\rangle$ have prescribed remainders modulo m_i. Since the number of all possible k-tuples of remainders doesn't exceed $m_1 \cdots m_k$, we conclude that $|\mathbb{Z}^d/\Lambda| \leq m_1 \cdots m_k$. Since $\det \mathbb{Z}^d = 1$, the proof follows by Theorem 5.2. $\square$

(8.2) Theorem. *A positive integer n is a sum of four squares of integers.*

Proof. Suppose first that n is a prime. We claim that one can find integers a and b such that

$$a^2 + b^2 + 1 \equiv 0 \mod n.$$

If $n = 2$, we can choose $a = 1$ and $b = 0$. If n is an odd prime then the $(n+1)/2$ numbers $a^2 : \ 0 \leq a < n/2$ must be distinct modulo n, since if $a_1^2 \equiv a_2^2 \mod n$ for some $0 \leq a_1, a_2 < n/2$ we must have $(a_1 - a_2)(a_1 + a_2) \equiv 0 \mod n$, which implies that $a_1 = a_2$. Similarly, the $(n+1)/2$ numbers $-1 - b^2 : \ 0 \leq b < n/2$ must be distinct modulo n. Therefore, for some a and b we must have $a^2 \equiv -1 - b^2 \mod n$ or, equivalently, $a^2 + b^2 + 1 \equiv \mod n$.

Let us define a lattice $\Lambda \subset \mathbb{Z}^4$ by

$$\Lambda = \left\{ (x_1, x_2, x_3, x_4) \in \mathbb{Z}^4 : \quad \begin{matrix} x_1 \equiv ax_3 + bx_4 \mod n \\ x_2 \equiv bx_3 - ax_4 \mod n \end{matrix} \right\}.$$

By Lemma 8.1, Λ is indeed lattice and $\det \Lambda \leq n^2$.

Moreover, for any $(x_1, x_2, x_3, x_4) \in \Lambda$, we have

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv \left(a^2 + b^2 + 1\right) x_3^2 + \left(a^2 + b^2 + 1\right) x_4^2 \equiv 0 \mod n.$$

Let

$$B = \left\{ (x_1, x_2, x_3, x_4) \in \mathbb{R}^4 : \quad x_1^2 + x_2^2 + x_3^2 + x_4^2 < 2n \right\}$$

be the open ball of radius $\sqrt{2n}$. By Lemma 7.2, we have

$$\operatorname{vol} B = 2\pi^2 n^2 > 16n^2 \geq 2^4 \det \Lambda.$$

Therefore, by Theorem 6.4, there is a non-zero vector $(x_1, x_2, x_3, x_4) \in B \cap \Lambda$. Since we have

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \mod n \quad \text{and} \quad x_1^2 + x_2^2 + x_3^2 + x_4^2 < 2n,$$

we must have

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = n,$$

which is the desired representation.

Since every positive integer $n > 1$ is a product of primes, the result for general integer n follows from the identity

$$\begin{gathered} \left(x_1^2 + x_2^2 + x_3^2 + x_4^2\right)\left(y_1^2 + y_2^2 + y_3^2 + y_4^2\right) = z_1^2 + z_2^2 + z_3^2 + z_4^2 \quad \text{where} \\ z_1 = x_1y_1 - x_2y_2 - x_3y_3 - x_4y_4, \\ z_2 = x_1y_2 + x_2y_1 + x_3y_4 - x_4y_3, \\ z_3 = x_1y_3 - x_2y_4 + x_3y_1 + x_4y_2, \\ z_4 = x_1y_4 + x_2y_3 - x_3y_2 + x_4y_1. \end{gathered}$$

□

(8.3) Problems.

1. Let k be a positive integer. Prove that if there is a solution to the congruence $x^2+1 \equiv 0 \mod k$ then k is the sum of two squares of integers. Deduce that every prime number $k \equiv 1 \mod 4$ is the sum of two squares of integers.

2*. Prove the Jacobi formula:

$$\left(\sum_{k=-\infty}^{+\infty} q^{k^2}\right)^4 = 1 + 8\sum_{k=1}^{+\infty} \frac{q^k}{(1+(-q)^k)^2}$$

and deduce from it that the number of integer vector solutions (x_1, x_2, x_3, x_4) of the equation

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = n,$$

where n is a positive integer, is equal to 8 times the sum of the divisors of n that are not multiples of 4.

Hint: For a short proof, see G. Andrews, S.B. Ekhad, and D. Zeilberger, A short proof of Jacobi's formula for the number of representations of an integer as a sum of four squares, *Amer. Math. Monthly* 100 (1993), no. 3, 274–276.

9. An application: rational approximations of real numbers

Let us fix a real α. Then for any positive integer q we can find an integer p such that

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{2q}.$$

It turns out that for infinitely many values of q we can do essentially better.

(9.1) Theorem. *Let us choose a real α. Then, for any positive integer M there exists an integer $q \geq M$ and an integer p such that*

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^2}.$$

Proof. Without loss of generality we assume that α is irrational. Let us choose a positive integer Q and consider the parallelogram A in $\mathbb{R}^2$ defined by the inequalities $|x| \leq Q$ and $|\alpha x - y| \leq 1/Q$.Then A is compact, convex, symmetric and $\operatorname{vol} A = 4$. Therefore, A contains a non-zero integer point (q, p) (cf. Problem 1 of Section 6.5). We must have $q \neq 0$ since otherwise we necessarily have $p = 0$. Since A is symmetric, we can always choose $q > 0$. Then we have

(9.1.1) $$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{qQ}$$

and $0 < q \leq Q$, from which it follows that

$$\left| \alpha - \frac{p}{q} \right| \leq \frac{1}{q^2}.$$

It remains to show that q can be chosen arbitrarily large. Since α is irrational, for any positive integer M we can choose a sufficiently large Q so that (9.1.1) cannot be satisfied with any $1 < q < M$. □

(9.2) Problem.
1. Prove that for any real $\alpha_1, \ldots, \alpha_n$ there exists an arbitrarily large integer $q > 0$ and integers $p_1, \ldots, p_n$ such that

$$\left| \alpha_k - \frac{p_k}{q} \right| \leq \frac{1}{q^{1+\frac{1}{n}}} \quad \text{for} \quad k = 1, \ldots, n.$$

(9.3) Continued fractions. The following construction of continued fractions allows one to obtain approximations such that

$$\left| \alpha - \frac{p}{q} \right| \leq \frac{1}{q^2\sqrt{5}}$$

for arbitrarily large q. The constant $1/\sqrt{5}$ cannot be made smaller.

Given a real α, we let

$$\alpha = \lfloor \alpha \rfloor + \{\alpha\} \quad \text{and} \quad a_0 = \lfloor \alpha \rfloor$$

If $\{\alpha\} = 0$, we stop. Otherwise, we let

$$\beta = \frac{1}{\{\alpha\}}, \quad \beta = \lfloor \beta \rfloor + \{\beta\} \quad \text{and} \quad a_1 = \lfloor \beta \rfloor.$$

If $\{\beta\} = 0$, we stop, otherwise we update

$$\beta := \frac{1}{\{\beta\}}$$

and proceed as above. In the end, we get a potentially infinite fraction

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ldots}}}$$

We write

$$\alpha = [a_0; a_1, a_2, \ldots].$$

For example,

$$\sqrt{2} = 1 + \sqrt{2} - 1 = 1 + \frac{1}{\sqrt{2}+1} = 1 + \cfrac{1}{2 + \cfrac{1}{\sqrt{2}+1}} = 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \dots}}}.$$

We obtain the *k-th convergent* of α by cutting the continued fraction at a_k:

$$[a_0; a_1, a_2, \dots, a_k] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\dots + \cfrac{1}{a_k}}}} = \frac{p_k}{q_k}.$$

For example,

$$[1; 2, 2, 2] = \frac{17}{12} \quad \text{and} \quad [1; 2, 2, 2, 2] = \frac{41}{29}.$$

It turns out that convergents provide very good rational approximations to real numbers. Note, for example, that

$$\sqrt{2} - \frac{17}{12} \approx -0.0025 \quad \text{and} \quad \sqrt{2} - \frac{41}{29} \approx 0.00042.$$

Similarly, $\pi = [3; 7, 15, 1, \dots,]$,

$$[3, 7] = \frac{22}{7}, \quad [3; 7, 15, 1] = \frac{355}{113} \quad \text{and} \quad \pi - \frac{22}{7} \approx -0.0013, \quad \pi - \frac{355}{113} \approx 2.66 \times 10^{-7}.$$

(9.4) Problems.

In the problems below, we let

$$\alpha = [a_0; a_1, \dots, a_k, \dots] \quad \text{and} \quad [a_0; a_1, \dots, a_k] = \frac{p_k}{q_k}.$$

1. Prove that

$$p_k = a_k p_{k-1} + p_{k-2} \quad \text{and} \quad q_k = a_k q_{k-1} + q_{k-2} \quad \text{for} \quad k \geq 2.$$

2. Prove that

$$p_{k-1} q_k - p_k q_{k-1} = (-1)^k \quad \text{for} \quad k \geq 1.$$

3. Prove that

$$q_k p_{k-2} - p_k q_{k-2} = (-1)^{k-1} a_k \quad \text{for} \quad k \geq 2.$$

4. Prove that
$$\left|\alpha - \frac{p_k}{q_k}\right| \leq \frac{1}{q_k q_{k+1}} \quad \text{for} \quad k \geq 0.$$

5*. Prove that for $k \geq 2$ at least one of the three inequalities
$$\left|\alpha - \frac{p_k}{q_k}\right| \leq \frac{1}{q_k^2\sqrt{5}}, \quad \left|\alpha - \frac{p_{k-1}}{q_{k-1}}\right| \leq \frac{1}{q_{k-1}^2\sqrt{5}} \quad \text{or} \quad \left|\alpha - \frac{p_{k-2}}{q_{k-2}}\right| \leq \frac{1}{q_{k-2}^2\sqrt{5}}$$
holds.

6. Let $\alpha = \frac{1+\sqrt{5}}{2}$. Prove that $\alpha = [1; 1, \ldots, 1, \ldots]$ and that
$$\left|\alpha - \frac{p_k}{q_k}\right| = \frac{1}{q_k^2\left(\sqrt{5} + \epsilon_k\right)},$$
where $\epsilon_k \longrightarrow 0$ as $k \longrightarrow +\infty$.

See A. Ya. Khinchin, *Continued Fractions*, Dover Publication, Mineola, New York, 1997.

10. Sphere packings

(10.1) Definitions. Let $\Lambda \subset V$ be a lattice of rank d. The *packing radius* $\rho(\Lambda)$ of Λ is the largest number ρ such that for no two open balls of radius ρ centered at the lattice points intersect. Equivalently, $2\rho(\Lambda)$ is the length of the shortest non-zero vector in Λ. The *packing density* $\sigma(\Lambda)$ is defined as
$$\sigma(\Lambda) = \frac{\pi^{d/2}\rho^d(\Lambda)}{\Gamma\left(1+\frac{d}{2}\right)\det\Lambda}.$$
In other words, the packing density of Λ is the proportion of the space occupied by the balls centered at the lattice points and of radius $\rho(\Lambda)$.

Lattices $\Lambda_1 \subset V_1$ and $\Lambda_2 \subset V_2$ are called *similar* (denoted $\Lambda_1 \sim \Lambda_2$) if there is a constant $\gamma > 0$ and a linear transformation $T : V_1 \longrightarrow V_2$ such that $\|T(x)\| = \gamma\|x\|$ for all $x \in V_1$ and $\Lambda_2 = T(\Lambda_1)$.

Lattices having high packing densities are of interest.

(10.2) Problems.

1. Prove that
$$\rho\left(\mathbb{Z}^n\right) = \frac{1}{2},\ \rho\left(A_n\right) = \rho\left(D_n\right) = \frac{\sqrt{2}}{2} \quad \text{for} \quad n \geq 2,$$
$$\rho\left(D_n^+\right) = \frac{\sqrt{2}}{2} \quad \text{for} \quad n \geq 8$$
$$\rho\left(D_2^+\right) = \frac{1}{2\sqrt{2}},\ \rho\left(D_4^+\right) = \frac{1}{2},\ \rho\left(D_6\right) = \sqrt{\frac{3}{8}} \quad \text{and}$$
$$\rho\left(E_6\right) = \rho\left(E_7\right) = \frac{\sqrt{2}}{2}.$$

2. Prove that similar lattices have equal packing density.

3. Prove that $D_2 \sim \mathbb{Z}^2$ that D_3 is isomorphic to A_3, that D_4^+ is isomorphic to $\mathbb{Z}^4$ and that $D_4^* \sim D_4$.

4. Prove that

$$\sigma(\mathbb{Z}) = 1, \ \sigma\left(A_2\right) = \frac{\pi}{\sqrt{12}} \approx 0.9069, \ \sigma\left(A_3\right) = \sigma\left(D_3\right) = \frac{\pi}{\sqrt{18}} \approx 0.7405$$
$$\sigma\left(D_4\right) = \frac{\pi^2}{16} \approx 0.6169, \ \sigma\left(D_5\right) = \frac{\pi^2}{15\sqrt{2}} \approx 0.4653, \ \sigma\left(E_6\right) = \frac{\pi^3}{48\sqrt{3}} \approx 0.3729,$$
$$\sigma\left(E_7\right) = \frac{\pi^3}{105} \approx 0.2953 \quad \text{and} \quad \sigma\left(E_8\right) = \frac{\pi^4}{384} \approx 0.2537.$$

5. Check the inequalities

$$\begin{aligned}
&\sigma\left(A_2\right) > \sigma\left(\mathbb{Z}^2\right) \\
&\sigma\left(A_3\right) = \sigma\left(D_3\right) > \sigma\left(\mathbb{Z}^3\right) \\
&\sigma\left(D_4\right) > \sigma\left(A_4\right) > \sigma\left(\mathbb{Z}^4\right) \\
&\sigma\left(D_5\right) > \sigma\left(A_5\right) > \sigma\left(\mathbb{Z}^5\right) \\
&\sigma\left(E_6\right) > \sigma\left(D_6\right) > \sigma\left(A_6\right) > \sigma\left(\mathbb{Z}^6\right) \\
&\sigma\left(E_7\right) > \sigma\left(D_7\right) > \sigma\left(A_7\right) > \sigma\left(\mathbb{Z}^7\right) \quad \text{and} \\
&\sigma\left(E_8\right) > \sigma\left(D_8\right) > \sigma\left(A_8\right) > \sigma\left(\mathbb{Z}^8\right).
\end{aligned}$$

6. Let V be a d-dimensional Euclidean space and let X be an (infinite) set such that $\|x-y\| \geq 2$ for any $x, y \in X$ such that $x \neq y$. We define the density of the unit sphere packing with centers at X as

$$\sigma(X) = \limsup_{r \longrightarrow +\infty} \frac{\pi^{d/2}\left|B_r \cap X\right|}{\Gamma\left(1+\frac{d}{2}\right) \operatorname{vol} B_r},$$

where B_r is the ball of radius r centered at the origin.

Prove that one can find such a set X so that $\sigma(X) \geq 2^{-d}$ (the Gilbert - Varshamov bound).

7. Let $\Lambda \subset \mathbb{R}^3$ be a lattice with basis

$$(1,0,0), \ \left(\frac{1}{2}, \frac{\sqrt{3}}{2}, 0\right), \ \left(0,0,\sqrt{\frac{8}{3}}\right)$$

and let

$$u = \left(\frac{1}{2}, \frac{1}{\sqrt{12}}, \sqrt{\frac{2}{3}}\right).$$

Let

$$X = \Lambda \cup (u + \Lambda).$$

Prove that X is not a lattice and that $\sigma(X) = \sigma(D_3)$.

8. Identify the 24 shortest non-zero vectors of D_4.

9. Identify the 240 shortest non-zero vectors of E_8.

10. Let

$$\|x\|_\infty = \max_{i=1,\ldots,d} |x_i| \quad \text{for} \quad x = (x_1, \ldots, x_d).$$

Prove that for any lattice $\Lambda \subset \mathbb{R}^d$ there is a vector $x \in \Lambda \setminus \{0\}$ such that

$$\|x\|_\infty \ \leq \ (\det \Lambda)^{1/d}.$$

11. Prove that

$$\rho(\Lambda) \ \leq \ \frac{1}{2}\sqrt{d}\,(\det \Lambda)^{1/d}$$

for a lattice Λ of rank d.

11. The Leech lattice

Our goal is to construct a remarkable lattice of rank 24, called the Leech lattice. We follow the construction of R. Wilson, Octonions and the Leech lattice, *Journal of Algebra*, **322**(2009), 2186–2190.

(11.1) Octonions. We introduce the algebra of *octonions*, following H.S.M. Coxeter, Integral Cayley numbers, *Duke Math. J.*, **13**(1946), 561–578.

We define octonions as formal linear combinations

$$x_0 + x_1 e_1 + x_2 e_2 + x_3 e_3 + x_4 e_4 + x_5 e_5 + x_6 e_6 + x_7 e_7,$$

where $x_0, x_1, x_2, x_3, x_4, x_5, x_6, x_7 \in \mathbb{R}$. We multiply octonions according to the following rules.

First,

$$1e_i = e_i 1 = e_i \quad \text{and} \quad e_i^2 = -1 \quad \text{for} \quad i = 1, \ldots, 7.$$

Next,

$$e_i e_j = -e_j e_i \quad \text{for all} \quad i \neq j.$$

Furthermore

$$e_1e_2 = e_4,\ e_2e_3 = e_5,\ e_3e_4 = e_6,\ e_4e_5 = e_7,\ e_5e_6 = e_1,\ e_6e_7 = e_2,\ e_7e_1 = e_3$$

(note that the remaining six identities can be obtained from the first identity by a cyclic shift of the indices), and the products of the generators from the following seven triples are associative

$$\begin{aligned} &\{e_1, e_2, e_4\},\ \{e_2, e_3, e_5\},\ \{e_3, e_4, e_6\},\ \{e_4, e_5, e_7\}, \\ &\{e_5, e_6, e_1\},\ \{e_6, e_7, e_2\},\ \{e_7, e_1, e_3\}, \end{aligned} \tag{11.1.1}$$

so, for example,

$$(e_1e_2)\,e_4 = e_1\,(e_2e_4)\,, \quad \text{etc.}$$

Finally, the product of any triple involving only two or one generator e_i is associative, so, for example,

$$(e_6e_3)\,e_6 = e_6\,(e_3e_6)\,.$$

These rules suffice to figure out any product e_ie_j. For example,

$$\begin{aligned}
&e_1e_6 = (e_5e_6)\,e_6 = e_5\,(e_6e_6) = -e_5,\\
&e_2e_6 = -e_6e_2 = -e_6\,(e_6e_7) = -\,(e_6e_6)\,e_7 = e_7,\\
&e_3e_6 = e_3\,(e_3e_4) = (e_3e_3)\,e_4 = -e_4 \quad \text{and}\\
&e_4e_6 = -e_6e_4 = -\,(e_3e_4)\,e_4 = -e_3\,(e_4e_4) = e_3.
\end{aligned}$$

We define the *conjugate*

$$\begin{gathered}
\overline{x_0 + x_1e_1 + x_2e_2 + x_3e_3 + x_4e_4 + x_5e_5 + x_6e_6 + x_7e_7} = \\
x_0 - x_1e_1 - x_2e_2 - x_3e_3 - x_4e_4 - x_5e_5 - x_6e_6 - x_7e_7
\end{gathered}$$

and the *norm*

$$\begin{gathered}
\|x_0 + x_1e_1 + x_2e_2 + x_3e_3 + x_4e_4 + x_5e_5 + x_6e_6 + x_7e_7\| = \\
\sqrt{x_0^2 + x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2 + x_6^2 + x_7^2},
\end{gathered}$$

thus making the space of octonions Euclidean space $\mathbb{R}^8$.

(11.2) Problems.

1°. Build a 7×7 multiplication table for $e_1, e_2, e_3, e_4, e_5, e_6$ and e_7.

2°. Let $\{i, j, k\}$ be a triple of distinct indices, not equal to one of the triples of (11.1.1). Prove the anti-associativity relation:

$$(e_ie_j)\,e_k = -e_i\,(e_je_k)\,.$$

3. Prove that $\overline{(x \cdot y)} = \overline{y} \cdot \overline{x}$ for every two octonions x and y.

4. Prove the *Moufang laws*:

$$\begin{aligned}
z(x(zy)) &= ((zx)z)y\\
x(z(yz)) &= ((xz)y)z\\
(zx)(yz) &= (z(xy))z = z((xy)z)
\end{aligned}$$

for every three octonions x, y and z.

5. Prove that the algebra generated by any two octonions is associative.

6. Prove that $\|x\|^2 = x\overline{x}$ for every octonion x.

7. Prove that $\|xy\| = \|x\|\|y\|$ for every two octonions x and y.

(11.3) The Leech lattice. First, we construct a copy of lattice E_8 in the space of octonions. As in Example 1.3.3, we define D_8 as the lattice consisting of all points

$$\begin{gathered} x_0 + x_1e_1 + x_2e_2 + x_3e_3 + x_4e_4 + x_5e_5 + x_6e_6 + x_7e_7, \\ \text{where} \quad x_i \in \mathbb{Z} \quad \text{for} \quad i = 0, \ldots, 7 \qquad\qquad \text{and} \\ x_0 + x_1 + x_2 + x_3 + x_4 + x_5 + x_6 + x_7 + x_7 \equiv 0 \mod 2. \end{gathered}$$

Next, we let

$$u = \frac{1}{2}\Big(-1 + e_1 + e_2 + e_3 + e_4 + e_5 + e_6 + e_7\Big).$$

We let

$$L = D_8 \cup (u + D_8)\,.$$

Now, we consider the space V of all triples (x, y, z), where x, y and z are octonions. We make it 24-dimensional Euclidean space by introducing the norm

$$\|(x, y, z)\| = \sqrt{\frac{\|x\|^2 + \|y\|^2 + \|z\|^2}{2}}.$$

Now we define the *Leech lattice* $\Lambda_{24} \subset V$ as the set of all triples (x, y, z) such that

$$\begin{aligned} &x, y, z \ \in \ L; \\ &x + y, x + z, y + z \ \in \ L\overline{u}; \\ &x + y + z \ \in \ Lu. \end{aligned}$$

Here by Lu, respectively $L\overline{u}$, we understand the lattice obtained by multiplying lattice L point-wise by u, respectively by $\overline{u}$.

(11.4) Problems.

1°. Check that L is isomorphic to E_8.

2. Prove that $Le_i = L$ for $i = 1, \ldots, 7$ and that $Lu \subset L$.

3°. Prove that if $(x, y, z) \in \Lambda_{24}$ then vectors (x, z, y), (y, x, z), (y, z, x), (z, x, y) and (z, y, x) also lie in Λ_{24}.

4. Prove that $2L \subset Lu$, $2L \subset L\overline{u}$ and that $Lu + L\overline{u} \subset L$ (in fact, $Lu \cap L\overline{u} = 2L$ and $Lu + L\overline{u} = L$).

5. Prove that for every $x \in L$ we have

$$\begin{aligned} &(2x,\ 0,\ 0) \in \Lambda_{24} \\ &(xu,\ x,\ -x) \in \Lambda_{24} \\ &(x\overline{u},\ x\overline{u},\ 0) \in \Lambda_{24}. \end{aligned}$$

6. Prove that $\|x\|^2$ is an even integer for every $x \in \Lambda_{24}$. Deduce that $\Lambda_{24} \subset \Lambda_{24}^*$.

7*. Prove that $\Lambda_{24}^* = \Lambda_{24}$.

8. Prove that $\|x\| \geq 2$ for all $x \in \Lambda_{24}$.

9*. Prove that if $(x, y, z) \in \Lambda_{24}$ then $(x, ye_i, ze_i) \in \Lambda_{24}$ for $i = 1, \ldots, 7$. Deduce that if $(x, y, z) \in \Lambda_{24}$ then $(x, y, -z) \in \Lambda_{24}$.

10*. Let us denote $1 = e_0$. Prove that if x is a shortest non-zero vector in L then

$$\begin{aligned}
&(2x,\ 0,\ 0) \in \Lambda_{24}, \\
&(x\overline{u},\ x\overline{u}e_i,\ 0) \in \Lambda_{24} \quad \text{for} \quad i = 0, \ldots, 7 \quad \text{and} \\
&((xu)e_i,\ xe_j,\ (xe_i)e_j) \in \Lambda_{24} \quad \text{for} \quad i, j = 0, \ldots, 7.
\end{aligned}$$

Accounting for permutations of the coordinates and sign changes, there are

$$3 \cdot 240 + 3 \cdot 240 \cdot 16 + 3 \cdot 240 \cdot 16 \cdot 16 = 196,560$$

shortest non-zero vectors of length 2 in Λ_{24}.

11°. Conclude from Problems 5, 7 and 8 above that $\rho\left(\Lambda_{24}\right) = 1$, $\det \Lambda = 1$ and hence

$$\sigma\left(\Lambda_{24}\right) = \frac{\pi^{12}}{12!} \approx 0.001929574313.$$

12. The Minkowski - Hlawka Theorem

Our goal is to prove that there is a lattice of rank d with a high packing density. We will prove that for every d and $\sigma < 2^{-d}$ there is a lattice of packing density at least σ. A simple modification of our construction improves the bound to any $\sigma < 2^{-d+1}$ and then to $\sigma = 2^{-d+1}$. There is a further (much more technical) improvement to $\sigma = \zeta(d)2^{1-d}$ for $d \geq 2$, where $\zeta(d) = \sum_{n=1}^{+\infty} n^{-d}$.

(12.1) Lemma. *Let $M \subset V$ be a Lebesgue measurable set, let $\Lambda \subset V$ be a lattice and let Π be a fundamental parallelepiped of Λ. For $x \in V$, let $x + \Lambda = \{x + u :\ u \in \Lambda\}$ be the translation of Λ and let $|M \cap (x + \Lambda)|$ be the number of points from $x + \Lambda$ in M. Then*

$$\int_{\Pi} |M \cap (x + \Lambda)| \ dx = \operatorname{vol} M.$$

More generally, for an integer $k \neq 0$, we have

$$\int_{\Pi} |M \cap (kx + \Lambda)| \ dx = \operatorname{vol} M.$$

Proof. For $u \in \Lambda$ let us introduce a function $f_u : \Pi \longrightarrow \mathbb{R}$ by

$$f_u(x) = \begin{cases} 1 & \text{if } x + u \in M \\ 0 & \text{if } x + u \notin M. \end{cases}$$

Then

$$|M \cap (x + \Lambda)| = \sum_{u \in \Lambda} f_u(x)$$

and hence

$$\int_\Pi |M \cap (x + \Lambda)| \ dx = \sum_{u \in \Lambda} \int_\Pi f_u(x) \ dx = \sum_{u \in \Lambda} \operatorname{vol}\big((\Pi + u) \cap M\big) = \operatorname{vol} M,$$

where the last equality follows by Lemma 4.2.

To handle the general case, without loss of generality we assume that $k > 0$ (if $k < 0$ we consider the parallelepiped $-\Pi$ instead). Substituting $y = kx$, we obtain

$$\int_\Pi |M \cap (kx + \Lambda)| \ dx = k^{-d} \int_{k\Pi} |M \cap (y + \Lambda)| \ dy \quad \text{for} \quad d = \dim V.$$

The parallelepiped $k\Pi$ is the union of k^d pairwise disjoint lattice translations $\Pi + u :$ $u \in \Lambda$ of the parallelepiped Π. Since the function $g(y) = |M \cap (y + \Lambda)|$ satisfies $g(y + u) = g(y)$ for all $y \in \Lambda$, we conclude that

$$k^{-d} \int_{k\Pi} |M \cap (y + \Lambda)| \ dy = \int_\Pi |M \cap (y + \Lambda)| \ dy = \operatorname{vol} M.$$

□

The following is the Minkowski - Hlawka Theorem.

(12.2) Theorem. *$M \subset \mathbb{R}^d$ be a bounded Jordan measurable set, where $d > 1$. Then, for any $\delta > \operatorname{vol} M$ there is a lattice $\Lambda \subset V$ such that $\det \Lambda = \delta$ and $M \cap (\Lambda \setminus \{0\}) = \emptyset$.*

Proof. Without loss of generality we assume that $\operatorname{vol} M < 1$ and $\delta = 1$. Let $e_1, \ldots, e_d$ be the standard basis of $\mathbb{R}^d$ and let H be the coordinate hyperplane $x_d = 0$.

Let us choose a sufficiently small $\alpha > 0$ (to be defined later) and consider the translations

$$H_k = H + k\alpha e_d, \quad k \in \mathbb{Z}.$$

We denote $M_k = M \cap H_k$. We choose $\alpha > 0$ in such a way that for every $x \in M$, $x = (x_1, \ldots, x_d)$, we have

$$|x_i| \ < \ \alpha^{-1/(d-1)} \quad \text{for} \quad i = 1, \ldots, d-1 \tag{12.2.1}$$

and

$$\alpha \sum_{k=-\infty}^{+\infty} \operatorname{vol}_{d-1} M_k < 1. \tag{12.2.2}$$

While (12.2.1) can be satisfied with a sufficiently small α since M is bounded, (12.2.2) can be satisfied since $\operatorname{vol} M < 1$ and M is Jordan measurable.

Let

$$u_i = \alpha^{-1/(d-1)} e_i \quad \text{for} \quad i = 1, \ldots, d-1$$

and let $\Lambda_0 \subset H$ be the lattice with basis $u_1, \ldots, u_{d-1}$. Hence $\det \Lambda_0 = 1/\alpha$ and $M \cap (\Lambda_0 \setminus \{0\}) = \emptyset$ by (12.2.1).

Let Π be the fundamental parallelepiped of $u_1, \ldots, u_{d-1}$. For $x \in \Pi$ let us define $u_d(x) = \alpha e_d + x$ and let $\Lambda(x) \subset \mathbb{R}^d$ be the lattice with basis $u_1, \ldots, u_{d-1}, u_d(x)$. Then $\det \Lambda(x) = 1$ for all $x \in \Pi$. We have

$$|M \cap \Lambda(x)| = \sum_{k=-\infty}^{+\infty} |M_k \cap \Lambda(x)| .$$

Choosing the origin in H_k at $\alpha k e_d$, we identify $H_k = \mathbb{R}^{d-1}$ and $\Lambda(x) \cap H_k = kx + \Lambda_0$. Hence by Lemma 12.1, for $k \neq 0$ we have

$$\int_\Pi |M_k \cap \Lambda(x)| \ dx = \int_\Pi |M_k \cap (kx + \Lambda_0)| \ dx = \operatorname{vol}_{d-1} M_{k-1}.$$

Since $\operatorname{vol}_{d-1} \Pi = 1/\alpha$, by (12.2.2), we conclude that

$$\frac{1}{\operatorname{vol}_{d-1} \Pi} \int_\Pi \left(\sum_{k \in \mathbb{Z} \setminus \{0\}} |M_k \cap \Lambda(x)| \right) \ dx < 1.$$

Therefore, there is an $x \in \Pi$ such that $|M_k \cap \Lambda(x)| = \emptyset$ for all $k \in \mathbb{Z} \setminus \{0\}$. □

(12.3) Corollary. *For any $\sigma < 2^{-d}$ there is a lattice Λ of rank d with the packing density $\sigma(\Lambda) > 2^{-d}$.*

Proof. Let $B \subset \mathbb{R}^d$ be the standard Euclidean ball centered at the origin and of radius 1. By Theorem 12.2, there is a lattice $\Lambda \subset \mathbb{R}^d$ such that $\Lambda \cap B = \{0\}$ and $\det \Lambda = \sigma^{-1} 2^{-d} \operatorname{vol} B$. Hence we have $\rho(\Lambda) \geq 1/2$ for the packing radius of Λ and

$$\sigma(\Lambda) = \frac{\operatorname{vol} B \cdot \rho^d(\Lambda)}{\det \Lambda} = \sigma.$$

□

Rescaling

$$\Lambda' = \left(\frac{2^d \sigma}{\operatorname{vol} B} \right)^{1/d} \Lambda$$

we obtain a lattice $\Lambda' \subset \mathbb{R}^d$ with $\det \Lambda' = 1$ and

$$\rho\left(\Lambda'\right) = \frac{1}{2} \left(\frac{2^d \sigma}{\operatorname{vol} B} \right)^{1/d} \approx \sqrt{\frac{d}{8 \pi e}}$$

by Stirling's formula.

(12.4) Problems.

1. Let $\phi : V \longrightarrow \mathbb{R}$ be a Lebesgue integrable function and let $\Lambda \subset V$ be a lattice. Prove that there exists a $z \in V$ such that

$$\sum_{u \in \Lambda} \phi(z+u) \leq \frac{1}{\det \Lambda} \int_V \phi(x) \ dx.$$

2. Let $\phi : V \longrightarrow \mathbb{R}$ be a Riemann integrable function vanishing outside a bounded region in V and let $\epsilon > 0$ be a number. Prove that there exists a lattice $\Lambda \subset V$ such that $\det \Lambda = 1$ and

$$\sum_{u \in \Lambda \setminus \{0\}} \phi(u) \leq \epsilon + \int_V \phi(x) \ dx.$$

3. Let $M \subset V$ be a bounded symmetric (that is, $M = -M$) Jordan measurable set such that $\operatorname{vol} M < 2$. Prove that there is a lattice $\Lambda \subset V$ such that $\det \Lambda = 1$ and $M \cap (\Lambda \setminus \{0\}) = \emptyset$.

13. The reciprocity relation for the packing radius

(13.1) Lemma. *Let Λ be a lattice of rank d and let Λ^* be the dual lattice. Then for the packing radii of Λ and Λ^* we have*

$$\rho(\Lambda) \cdot \rho\left(\Lambda^*\right) \ \leq \ \frac{d}{4}.$$

Proof. It follows by the Minkowski Theorem (see Problem 11 of Section 10.2) that

$$\rho\left(\Lambda\right) \ \leq \ \frac{1}{2}\sqrt{d}\left(\det \Lambda\right)^{1/d} \quad \text{and} \quad \rho\left(\Lambda^*\right) \ \leq \ \frac{1}{2}\sqrt{d}\left(\det \Lambda^*\right)^{1/d}.$$

Since $(\det \Lambda)\left(\det \Lambda^*\right) = 1$ (see Problem 2 of Section 4.4), the proof follows. □

More precisely, it follows by the Minkowski Theorem (Theorem 6.4) or, equivalently, from the fact that the packing density of a lattice does not exceed 1, that

$$\begin{aligned} \rho(\Lambda) \ &\leq \ \frac{1}{\sqrt{\pi}}\left(\Gamma\left(1+\frac{d}{2}\right)\right)^{1/d}\left(\det \Lambda\right)^{1/d} \quad \text{and} \\ \rho\left(\Lambda^*\right) \ &\leq \ \frac{1}{\sqrt{\pi}}\left(\Gamma\left(1+\frac{d}{2}\right)\right)^{1/d}\left(\det \Lambda^*\right)^{1/d}, \end{aligned}$$

which implies that

$$\rho\left(\Lambda\right) \cdot \rho\left(\Lambda^*\right) \ \leq \ \frac{d}{2\pi e}\left(1+O\left(\frac{1}{d}\right)\right).$$

(13.2) Problems.

1°. Show by example that $\rho(\Lambda) \cdot \rho(\Lambda^*)$ can be arbitrarily small.

2°. Let $\Lambda_0 \subset \Lambda$ be a sublattice. Prove that

$$\rho(\Lambda) \ \leq \ \rho(\Lambda_0) \ \leq \ |\Lambda/\Lambda_0|\, \rho(\Lambda).$$

3°. Let Λ be a lattice of rank d and let $u_1, \ldots, u_d$ be linearly independent vectors from Λ^*. Prove that for any $v \in \Lambda \setminus \{0\}$ we have

$$\max_{i=1,\ldots,d} \|v\| \cdot \|u_i\| \ \geq \ 1.$$

14. The Korkin-Zolotarev basis of a lattice

(14.1) Lemma. *Let $\Lambda \subset V$ be a lattice and let $\Lambda^* \subset V$ be the dual lattice. Let $u_1, \ldots, u_d$ be a basis of Λ and let $v_1, \ldots, v_d$ be vectors such that*

$$\langle u_i, v_j \rangle = \begin{cases} 1 & \text{if } i+j=d+1 \\ 0 & \text{otherwise.} \end{cases}$$

Then $v_1, \ldots, v_d$ is a basis of Λ^*. Moreover, let $H = v_1^{\perp}$ be the orthogonal complement of v_1 and let $\Lambda_0 \subset H$ be the lattice with basis $u_1, \ldots, u_{d-1}$. Let $pr : V \longrightarrow H$ be the orthogonal projection. Then $\Lambda_0^* = pr(\Lambda^*)$ and $pr(v_2), \ldots, pr(v_d)$ is a basis of Λ_0^*.

Proof. Clearly, $v_1, \ldots, v_d \in \Lambda^*$. Moreover, for any $v \in \Lambda^*$, we can write

$$v = \sum_{i=1}^{d} \langle v, u_i \rangle v_{d+1-i},$$

and hence $v_1, \ldots, v_d$ is a basis of Λ^*.

For every $v \in \Lambda^*$ and every $u \in \Lambda_0$ we have

$$\langle u, \ pr(v) \rangle = \langle u, v \rangle \ \in \ \mathbb{Z}.$$

In particular, $pr(v_2), \ldots, pr(v_d) \in \Lambda_0^*$. Moreover, for every $v \in \Lambda_0^*$ we have

$$v = \sum_{i=1}^{d-1} \langle v, u_i \rangle pr(v_{d+1-i}),$$

and hence $pr(v_2), \ldots, pr(v_d)$ is indeed a basis of Λ_0^*.

The following pair of bases is of a particular interest.

(14.2) Definition. Let Λ be a lattice. An ordered basis $u_1, \ldots, u_d$ constructed as in Theorem 3.1 is called a *Korkin-Zolotarev basis* of Λ. That is, u_1 is a shortest non-zero vector in Λ, and for $k = 2, \ldots, d$ vector u_k is a closest vector to $L_{k-1} = \operatorname{span}(u_1, \ldots, u_{k-1})$ among all vectors in $\Lambda \setminus L_{k-1}$. An ordered basis $u_1, \ldots, u_d$ of Λ such that

$$\langle u_i, v_j \rangle = \begin{cases} 1 & \text{if } i + j = d + 1 \\ 0 & \text{otherwise,} \end{cases}$$

where $v_1, \ldots, v_d$ is a Korkin-Zolotarev basis of Λ^*, is called a *reciprocal Korkin-Zolotarev basis* of Λ.

Many interesting properties of Korkin-Zolotarev and reciprocal Korkin-Zolotarev bases of lattices are established in

J.C. Lagarias, H.W. Lenstra, Jr., C.-P. Schnorr, Korkin-Zolotarev bases and successive minima of a lattice and its reciprocal lattice, *Combinatorica* **10** (1990), no. 4, 333 – 348.

Here are some of them.

(14.3) Problems.

1°. Let $u_1, \ldots, u_d$ be a Korkin-Zolotarev basis of lattice Λ. For $k < d$ let $L_k = \operatorname{span}(u_1, \ldots, u_k)$ and let $\Lambda_k \subset L_k$ be the lattice with basis $u_1, \ldots, u_k$. Prove that $u_1, \ldots, u_k$ is a Korkin-Zolotarev basis of Λ_k.

2°. Let $u_1, \ldots, u_d$ be a Korkin-Zolotarev basis of a lattice $\Lambda \subset V$. Let $H = u_1^\perp$ be the orthogonal complement to u_1, let $pr : V \longrightarrow H$ be the orthogonal projection and let $\Lambda' = pr(\Lambda)$ be a lattice, $\Lambda' \subset H$. Let $u_i' = pr\,(u_{i+1})$ for $i = 1, \ldots, d-1$. Prove that $u_1', \ldots, u_{d-1}'$ is a Korkin-Zolotarev basis of Λ'.

3°. Let $u_1, \ldots, u_d$ be a reciprocal Korkin-Zolotarev basis of lattice Λ. For $k < d$ let $L_k = \operatorname{span}(u_1, \ldots, u_k)$ and let $\Lambda_k \subset L_k$ be the lattice with basis $u_1, \ldots, u_k$. Prove that $u_1, \ldots, u_k$ is a reciprocal Korkin-Zolotarev basis of Λ_k.

4. Let $u_1, \ldots, u_d$ be a basis of a lattice Λ. Let

$$L_k = \operatorname{span}(u_1, \ldots, u_k) \quad \text{for} \quad k = 1, \ldots, d \quad \text{and let} \quad L_0 = \{0\}.$$

Prove that for any $u \in \Lambda \setminus \{0\}$ we have

$$\|u\| \ \geq \ \min_{k=1,\ldots,d} \operatorname{dist}(u_k,\ L_{k-1}).$$

In particular,

$$\rho(\Lambda) \ \geq \ \frac{1}{2} \min_{k=1,\ldots,d} \operatorname{dist}(u_k,\ L_{k-1}).$$

5. Let $u_1, \ldots, u_d$ be a reciprocal Korkin-Zolotarev basis of a lattice Λ and let the subspaces L_k be defined as in Problem 4. Prove that

$$\rho(\Lambda) \ \leq \ \frac{d}{2} \min_{k=1,\ldots,d} \operatorname{dist}(u_k,\ L_{k-1}).$$

Hint: Using Lemma 13.1 prove that

$$\rho(\Lambda) \ \leq \ \frac{d}{2} \operatorname{dist}(u_d, \ L_{d-1}).$$

Then use Problem 3 above.

15. The covering radius of a lattice

(15.1) Definition. Let $\Lambda \subset V$ be a lattice. The number

$$\mu(\Lambda) = \max_{x \in V} \operatorname{dist}(x, \Lambda)$$

is called the *covering* radius of the lattice.

(15.2) Problems.

1. Prove that

$$\mu\left(\mathbb{Z}^d\right) = \frac{\sqrt{d}}{2}, \quad \mu(D_3) = 1 \quad \text{and} \quad \mu(D_n) = \frac{\sqrt{n}}{2} \quad \text{for} \quad n \geq 4.$$

2. Prove that $\mu(E_8) = 1$.

3. A point $x \in V$ at which the local maximum of the function $x \longmapsto \operatorname{dist}(x, \Lambda)$ is attained is called a *hole* of lattice Λ. If the maximum is global, the hole is called *deep*, otherwise it is called *shallow*.

Prove that $(1, 0, 0)$ is a deep hole of D_3 (it is called an *octahedral hole*) and that $(1/2, 1/2, 1/2)$ is a shallow hole of D_3 (it is called a *tetrahedral hole*).

4. Show that points $x = (1/2, \ldots, 1/2)$ and $y = (1, 0, \ldots, 0)$ are holes of D_n and that x is deep and y is shallow if $n > 4$, x is shallow and y is deep, if $n < 4$, and both x and y are deep if $n = 4$.

5. Show that $(1, 0, 0, 0, 0, 0, 0, 0)$ is a deep hole of E_8, while $(5/6, 1/6, 1/6, 1/6, 1/6, 1/6, 1/6, 1/6)$ is a shallow hole of E_8.

6. Show that $(1/4, 1/4, 1/4, 1/4, 1/4, 1/4, -3/4, -3/4)$ is a deep hole of E_7.

7. Show that $(0, -2/3, -2/3, 1/3, 1/3, 1/3, 1/3, 0)$ is a deep hole of E_6.

The following important result is known as a *transference theorem.* The proof is taken from J.C. Lagarias, H.W. Lenstra, Jr., C.-P. Schnorr, Korkin-Zolotarev bases and successive minima of a lattice and its reciprocal lattice, *Combinatorica* **10** (1990), no. 4, 333 – 348.

(15.3) Theorem. *Let Λ be a lattice of rank d and let Λ^* be the dual lattice. Then*

$$\frac{1}{4} \ \leq \ \mu(\Lambda)\rho(\Lambda^*) \ \leq \ c(d),$$

where we can choose

$$c(d) = \frac{1}{4}\sqrt{\sum_{k=1}^{d} k^2} \ \leq \ \frac{d^{3/2}}{4}.$$

Proof. We prove the lower bound first. Let us choose linearly independent vectors $u_1, \ldots, u_d \in \Lambda$ as follows: u_1 is a shortest non-zero vector from Λ and for $k = 2, \ldots, d$ we choose u_k to be a shortest vector form Λ such that vectors $u_1, \ldots, u_{k-1}, u_k$ are linearly independent. We claim that

$$\operatorname{dist}\left(\frac{1}{2}u_d,\ \Lambda\right) = \frac{1}{2}\|u_d\|. \tag{15.3.1}$$

Indeed, suppose that for some $u \in \Lambda$ we have

$$\left\| u - \frac{1}{2}u_d \right\| \ < \ \frac{1}{2}\|u_d\|.$$

Then $\|u\| < \|u_d\|$ and hence we must have

$$u \in \operatorname{span}\left(u_1, \ldots, u_{d-1}\right).$$

But then we have

$$2u - u_d \in \Lambda \quad \text{and} \quad 2u - u_d \notin \operatorname{span}\left(u_1, \ldots, u_{d-1}\right).$$

Moreover,

$$\|2u - u_d\| < \|u_d\|,$$

which is a contradiction with the choice of u_d. The contradiction proves that (15.3.1) indeed holds and hence

$$\mu(\Lambda) \ \geq \ \frac{1}{2}\|u_d\| = \max_{i=1,\ldots,d} \frac{1}{2}\|u_i\|.$$

Let v be a shortest non-zero vector from Λ^*. Then

$$\langle u_i, v\rangle \in \mathbb{Z} \quad \text{for} \quad i = 1, \ldots, d \quad \text{and} \quad \langle u_{i_0}, v\rangle \neq 0 \quad \text{for some} \quad i_0.$$

This proves that $\|v\|\|u_{i_0}\| \ \geq \ 1$ and hence

$$\mu(\Lambda)\rho\left(\Lambda^*\right) \ \geq \ \frac{1}{4}\|v\| \max_{i=1,\ldots,d} \|u_i\| \ \geq \ \frac{1}{4},$$

as desired.

Now we prove the upper bound by induction on d. If $d=1$ then $\Lambda = \alpha\mathbb{Z}$ for some $\alpha > 0$ and $\Lambda^* = \alpha^{-1}\mathbb{Z}$. Therefore, $\mu(\Lambda) = \alpha/2$ and $\rho(\Lambda^*) = 1/2\alpha$, so the product is $1/4$, as required.

Suppose that $d > 1$. Let us choose a shortest vector $u \in \Lambda \setminus \{0\}$, so $\|u\| = 2\rho(\Lambda)$. Let $H = u^{\perp}$ be the orthogonal complement to u and let $pr : V \longrightarrow H$ be the orthogonal projection. Let $\Lambda_1 = pr(\Lambda)$, so $\Lambda_1 \subset H$ is a lattice, see Problem 1 of Section 2.3. Let $\Lambda_1^* \subset H$ be the dual lattice. Since for every $v \in \Lambda_1^*$ and every $x \in \Lambda$ we have

$$\langle x, v \rangle = \langle pr(x), v \rangle \in \mathbb{Z},$$

we have $\Lambda_1^* \subset \Lambda^*$ and hence $\rho(\Lambda_1^*) \geq \rho(\Lambda^*)$.

Let us choose an arbitrary $x \in V$ and let $y = pr(x)$. Let $y_1 \in \Lambda_1$ be a closest lattice point to y so, $\|y - y_1\| \leq \mu(\Lambda_1)$. The line through y_1 parallel to u intersects Λ by a set of equally spaced points, each being of distance $\|u\|$ from the next. Therefore, there is a point $w \in \Lambda$ such that $pr(w) = v$ and

$$\|(x + y_1 - y) - w\| \ \leq \ \frac{1}{2}\|u\| = \rho(\Lambda).$$

By the Pythagoras Theorem

$$\|x - w\|^2 = \|(x + y_1 - y) - w\|^2 + \|y - y_1\|^2 \ \leq \ \rho^2(\Lambda) + \mu^2(\Lambda_1).$$

Thus

$$\mu^2(\Lambda) \ \leq \ \rho^2(\Lambda) + \mu^2(\Lambda_1).$$

Applying Lemma 13.1 and the induction hypothesis, we conclude that

$$\begin{aligned}
\mu^2(\Lambda)\rho^2(\Lambda^*) &\leq \rho^2(\Lambda)\rho^2(\Lambda^*) + \mu^2(\Lambda_1)\rho^2(\Lambda^*) \\
&\leq \rho^2(\Lambda)\rho^2(\Lambda^*) + \mu^2(\Lambda_1)\rho^2(\Lambda_1^*) \\
&\leq \frac{d^2}{16} + c^2(d-1) = c(d).
\end{aligned}$$

□

(15.4) Problems.

1°. Let $u_1, \ldots, u_d$ be linearly independent vectors in Λ. Prove that

$$\mu(\Lambda) \ \leq \ \frac{1}{2}\sum_{i=1}^{d}\|u_i\|.$$

2. Let $\Lambda \subset V$ be a lattice with basis $u_1, \ldots, u_d$. Let $L_0 = \{0\}$, $L_k = \operatorname{span}(u_1, \ldots, u_k)$ and let w_k be the complement to the orthogonal projection of u_k onto L_{k-1} for $k = 1, \ldots, d$. Prove that for any $x \in V$ there is $u \in \Lambda$ such that

$$x - u = \sum_{i=1}^{d} \alpha_i w_i \quad \text{where} \quad |\alpha_i| \leq \frac{1}{2} \quad \text{for} \quad i = 1, \ldots, d.$$

3. In Problem 2 above, prove that

$$\operatorname{dist}(x, \Lambda) \ \geq \ \min_{i=0,\dots,d} \left\| \frac{1}{2} w_i + \sum_{j=i+1}^{d} \alpha_j w_j \right\|,$$

where we agree that $w_0 = 0$ and that $\sum_{j=i+1}^{d} \alpha_j w_j = 0$ when $i = d$.

4. Suppose that in Problems 2 and 3 above, $u_1, \dots, u_d$ is a reciprocal Korkin-Zolotarev basis. Prove that

$$\operatorname{dist}(x, \Lambda) \ \leq \ d^{3/2} \min_{i=0,\dots,d} \left\| \frac{1}{2} w_i + \sum_{j=i+1}^{d} \alpha_j w_j \right\|.$$

Hint: See J.C. Lagarias, H.W. Lenstra, Jr., C.-P. Schnorr, Korkin-Zolotarev bases and successive minima of a lattice and its reciprocal lattice, *Combinatorica* **10** (1990), no. 4, 333 – 348.

16. An application: Kronecker's Theorem

The following result is Kronecker's Theorem.

(16.1) Theorem. *Let $\theta_1, \dots, \theta_n$ be real numbers such that if*

$$\sum_{i=1}^{n} m_i \theta_i \quad \text{is integer} \quad \text{for integer} \quad m_1, \dots, m_n,$$

then necessarily

$$m_1 = \ldots = m_n = 0.$$

Then for any real numbers

$$0 < \alpha_1, \dots, \alpha_n < 1$$

and any $\epsilon > 0$ there is an integer m such that

$$|\alpha_i - \{m\theta_i\}| \ \leq \epsilon \quad \text{for} \quad i = 1, \dots, n.$$

Proof. For $\tau > 0$ let us consider a lattice $\Lambda_\tau \subset \mathbb{R}^{n+1}$ with basis

$$u_1 = (1, 0, \dots, 0), \ u_2 = (0, 1, 0, \dots, 0), \ \dots, \ u_n = (0, \dots, 0, 1, 0) \quad \text{and}$$
$$u_{n+1} = \left(\theta_1, \dots, \theta_n, \tau^{-1}\right).$$

We need to show that as $\tau \longrightarrow +\infty$, we can find a point from Λ_τ arbitrarily close to $(\alpha_1, \dots, \alpha_n, 0)$. The result will follow if we show that

$$\lim_{\tau \longrightarrow +\infty} \mu\left(\Lambda_\tau\right) = 0. \tag{16.1.1}$$

By Theorem 15.3 it suffices to show that

$$\lim_{\tau \longrightarrow +\infty} \rho\left(\Lambda_\tau^*\right) = +\infty. \tag{16.1.2}$$

Let $a \in \Lambda_\tau^* \setminus \{0\}$. Then $a = (m_1, \ldots, m_n; \beta)$ for some integer $m_1, \ldots, m_n$ such that

$$m_1\theta_1 + \ldots + m_n\theta_n + \beta\tau^{-1} \in \mathbb{Z}.$$

If $m_1 = \ldots = m_n = 0$ then necessarily $|\beta| \geq \tau$ and hence $\|a\| \geq \tau$. Suppose that $m_1^2 + \ldots + m_n^2 > 0$. Let us choose an arbitrary $\gamma > 0$ and let us consider the set of all integer combinations

$$\begin{aligned} m_1\theta_1 + \ldots + m_n\theta_n \quad \text{where} \quad & m_i \in \mathbb{Z}, \quad m_1^2 + \ldots + m_n^2 > 0 \quad \text{and} \\ & |m_i| < \gamma \quad \text{for all} \quad i = 1, \ldots, n. \end{aligned}$$

This is a finite set of non-integer numbers and let $\delta = \delta(\gamma) > 0$ be the minimum distance from an element of the set to an integer. Then we must have $\beta \geq \delta(\gamma)\tau$ and hence for any $a \in \Lambda_\tau^*$ and any $\gamma > 0$ we have

$$\|a\| \ \geq \ \min\bigl\{\tau, \ \delta(\gamma)\tau, \ \gamma\bigr\}.$$

This establishes (16.1.2) and hence (16.1.1). □

17. The Poisson summation formula for lattices

(17.1) The Fourier transform and the Poisson summation formula. Let $f : \mathbb{R}^n \longrightarrow \mathbb{C}$ be a function from $L^2(\mathbb{R}^n, dx) \cap L^1(\mathbb{R}^n, dx)$. The *Fourier transform* $\hat{f}$ of f is defined by the formula

$$\hat{f}(y) = \int_{\mathbb{R}^n} e^{-2\pi i \langle x, y \rangle} f(x) \ dx.$$

We have then

$$f(x) = \int_{\mathbb{R}^n} e^{2\pi i \langle x, y \rangle} \hat{f}(y) \ dy.$$

In particular, we will use

$$\text{For} \quad f(x) = e^{-\pi\|x\|^2} \quad \text{we have} \quad \hat{f}(y) = e^{-\pi\|y\|^2}. \tag{17.1.1}$$

Suppose that f and $\hat{f}$ are decaying sufficiently fast, that is

$$|f(x)|, \ |\hat{f}(x)| \ \leq \ \frac{C}{\left(1 + \|x\|\right)^{n+\delta}} \quad \text{for all} \quad x \in \mathbb{R}^n \tag{17.1.2}$$

and some $C > 0$ and $\delta > 0$. Then the *Poisson summation formula* holds:

$$\sum_{m \in \mathbb{Z}^n} f(m) = \sum_{m \in \mathbb{Z}^n} \hat{f}(m). \tag{17.1.3}$$

(17.2) Lemma. *Let $\Lambda \subset \mathbb{R}^n$ be a lattice and let $\Lambda^* \subset \mathbb{R}^n$ be the dual lattice. Let $f : \mathbb{R}^n \longrightarrow \mathbb{C}$ be a function, let $\hat{f} : \mathbb{R}^n \longrightarrow \mathbb{C}$ be its Fourier transform and suppose that condition (17.1.2) holds. Then*

$$\sum_{m \in \Lambda} f(m) = \frac{1}{\det \Lambda} \sum_{l \in \Lambda^*} \hat{f}(l).$$

Proof. Let $e_1, \ldots, e_n$ be the standard basis of $\mathbb{Z}^n$ and let $u_1, \ldots, u_n$ be a basis of Λ. Let us define an operator $T : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ by $T(e_i) = u_i$ for $i = 1, \ldots, n$. Then $T(\mathbb{Z}^n) = \Lambda$ and $\det T = \det \Lambda$.

Let us define a function $g : \mathbb{R}^n \longrightarrow \mathbb{C}$ by $g(x) = f(T(x))$. Substituting $x = T^{-1}(z)$, we obtain

$$\begin{aligned}\hat{g}(y) =& \int_{\mathbb{R}^n} e^{-2\pi i \langle x, y \rangle} g(x) \ dx = \int_{\mathbb{R}^n} e^{-2\pi i \langle x, y \rangle} f(T(x)) \ dx \\ =& \frac{1}{\det \Lambda} \int_{\mathbb{R}^n} e^{-2\pi i \left\langle T^{-1}(z), \ y \right\rangle} f(z) \ dz = \frac{1}{\det \Lambda} \int_{\mathbb{R}^n} e^{-2\pi i \left\langle z, \ \left(T^{-1}\right)^* y \right\rangle} f(z) \ dz \\ =& \frac{1}{\det \Lambda} \hat{f}\left((T^{-1})^*(y) \right),\end{aligned}$$

where $\left(T^{-1}\right)^*$ denotes the conjugate linear operator to T^{-1}.

Let us denote

$$v_j = \left(T^{-1}\right)^* e_{n-j+1} \quad \text{for} \quad j = 1, \ldots, n.$$

Then

$$\langle u_i, v_j \rangle = \left\langle T(e_i), \ \left(T^{-1}\right)^* (e_{n+j-1}) \right\rangle = \langle e_i, \ e_{n-j+1} \rangle = \begin{cases} 1 & \text{if } i + j = n + 1 \\ 0 & \text{otherwise.} \end{cases}$$

By Lemma 14.1 it follows that $v_1, \ldots, v_n$ is a basis of Λ^* and hence

$$\left(T^{-1}\right)^* (\mathbb{Z}^n) = \Lambda^*.$$

Applying formula (17.1.3) to g and $\hat{g}$ (note that (17.1.2) still holds), we complete the proof. $\square$

(17.3) Lemma. *Let V be a d-dimensional Euclidean space, let $\Lambda \subset V$ be a lattice and let $\Lambda^* \subset V$ be the dual lattice. Then for any $\tau > 0$ and any $x \in V$, we have*

$$\tau^{d/2} \sum_{m \in \Lambda} \exp\left\{ -\pi \tau \|x - m\|^2 \right\} = \frac{1}{\det \Lambda} \sum_{l \in \Lambda^*} \exp\left\{ -\pi \|l\|^2 / \tau + 2\pi i \langle l, x \rangle \right\}.$$

Proof. First, we observe that for any $\tau > 0$ and $g(x) = f(\tau x)$ via substitution $z = \tau x$ we have

$$\hat{g}(y) = \int_{\mathbb{R}^n} e^{-2\pi i \langle x, y \rangle} f(\tau x) \ dx = \tau^{-n} \int_{\mathbb{R}^n} e^{-2\pi i \left\langle z, \ \tau^{-1} y \right\rangle} f(z) \ dz = \tau^{-n} \hat{f}\left(\tau^{-1} y\right).$$

In particular, choosing $f(x) = e^{-\pi\|x\|^2}$, $g(x) = f\left(\tau^{1/2}x\right)$ and using (17.1.1), we obtain:

$$\text{For} \quad g(x) = e^{-\pi\tau\|x\|^2} \quad \text{we have} \quad \hat{g}(y) = \tau^{-n/2} e^{-\pi\|y\|^2/\tau}.$$

Next, we observe that for any $a \in \mathbb{R}^n$ and $g(x) = f(x-a)$ via substitution $z = x-a$ we have

$$\hat{g}(y) = \int_{\mathbb{R}^n} e^{-2\pi i\langle x,y\rangle} f(x-a)\ dx = \int_{\mathbb{R}^n} e^{-2\pi i\langle z+a,\ y\rangle} f(z)\ dz = e^{-2\pi i\langle a,y\rangle}\hat{f}(y).$$

In particular, choosing $f(x) = e^{-\pi\tau\|x\|^2}$ and $g(x) = e^{-\pi\tau\|x-a\|^2}$, we obtain:

$$\text{For} \quad g(x) = e^{-\pi\tau\|x-a\|^2} \quad \text{we have} \quad \hat{g}(y) = \tau^{-n/2} e^{-2\pi i\langle a,y\rangle} e^{-\pi\|y\|^2/\tau}.$$

The result now follows from Lemma 17.2 and the observation that both sides of the identity we intend to prove are invariant under the substitution $x \longmapsto -x$. □

18. The covering radius via the Poisson summation formula

Our goal is to prove a better estimate of constant $c(d)$ in Theorem 15.3 using results of Section 17. We follow

W. Banaszczyk, New bounds in some transference theorems in the geometry of numbers, *Mathematische Annalen*, **296** (1993), 625–635

with some modifications.

(18.1) Lemma. *Let $\Lambda \subset V$ be a lattice of rank d. Then for all $0 < \tau < 1$ and for all $x \in V$ we have*

$$\sum_{m\in\Lambda} e^{-\pi\tau\|x-m\|^2} \ \leq\ \tau^{-d/2} \sum_{m\in\Lambda} e^{-\pi\|m\|^2}.$$

Proof. Applying Lemma 17.3 twice, we obtain

$$\begin{aligned}
\sum_{m\in\Lambda} e^{-\pi\tau\|x-m\|^2} \ &= \frac{1}{\tau^{d/2}\det\Lambda} \sum_{l\in\Lambda^*} \exp\left\{-\pi\|l\|^2/\tau + 2\pi i\langle l,x\rangle\right\} \\
&\leq \frac{1}{\tau^{d/2}\det\Lambda} \sum_{l\in\Lambda^*} \exp\left\{-\pi\|l\|^2/\tau\right\} \\
&\leq \frac{1}{\tau^{d/2}\det\Lambda} \sum_{l\in\Lambda^*} \exp\left\{-\pi\|l\|^2\right\} \\
&= \tau^{-d/2} \sum_{m\in\Lambda} e^{-\pi\|m\|^2}.
\end{aligned}$$

□

(18.2) Lemma. *Let $\Lambda \subset V$ be a lattice of rank d and let $\gamma > 1/2\pi$ be a real number. Then for all $x \in V$ we have*

$$\sum_{\substack{m \in \Lambda: \\ \|x-m\| > \sqrt{\gamma d}}} e^{-\pi \|x-m\|^2} \ \leq \ \left(e^{-\pi\gamma + \frac{1}{2}} \sqrt{2\pi\gamma}\right)^d \sum_{m \in \Lambda} e^{-\pi \|m\|^2}.$$

In particular,

$$\sum_{\substack{m \in \Lambda: \\ \|x-m\| > \sqrt{d}}} e^{-\pi \|x-m\|^2} \ \leq \ 5^{-d} \sum_{m \in \Lambda} e^{-\pi \|m\|^2}.$$

Proof. For $0 < \tau < 1$, applying Lemma 18.1, we get

$$\begin{aligned}
\sum_{\substack{m \in \Lambda: \\ \|x-m\| > \sqrt{\gamma d}}} e^{-\pi \|x-m\|^2} &\leq e^{-\pi\tau\gamma d} \sum_{\substack{m \in \Lambda: \\ \|x-m\| > \sqrt{\gamma d}}} e^{-\pi \|x-m\|^2} e^{\pi\tau \|x-m\|^2} \\
&\leq e^{-\pi\tau\gamma d} \sum_{m \in \Lambda} e^{-\pi(1-\tau)\|x-m\|^2} \\
&\leq e^{-\pi\tau\gamma d} (1-\tau)^{-d/2} \sum_{m \in \Lambda} e^{-\pi\|m\|^2}.
\end{aligned}$$

Optimizing on τ, we choose

$$\tau = 1 - \frac{1}{2\pi\gamma}$$

and obtain the desired estimate. □

Now we can sharpen the upper bound in Theorem 15.3.

(18.3) Theorem. *Let $\Lambda \subset V$ be a lattice of rank d. Then*

$$\mu(\Lambda)\rho(\Lambda^*) \ \leq \ \frac{d}{2}.$$

Proof. Suppose that for some lattice Λ of rank d we have

$$\mu(\Lambda)\rho(\Lambda^*) \ > \ \frac{d}{2}.$$

If we scale $\Lambda_1 = \alpha\Lambda$ for $\alpha > 0$, the dual lattice gets scaled $\Lambda_1^* = \alpha^{-1}\Lambda_1^*$ and the covering and packing radii scale accordingly, $\mu(\Lambda_1) = \alpha\mu(\Lambda)$ and $\rho(\Lambda_1^*) = \alpha^{-1}\rho(\Lambda_1)$. Hence, without loss of generality, we may assume that

$$\mu(\Lambda) \ > \ \sqrt{d} \quad \text{and} \quad \rho(\Lambda^*) \ > \ \frac{\sqrt{d}}{2}.$$

Let $x \in V$ be a point such that $\operatorname{dist}(x, \Lambda) > \sqrt{d}$. Applying Lemma 18.2, we deduce

$$\sum_{m \in \Lambda} e^{-\pi\|x-m\|^2} = \sum_{\substack{m \in \Lambda: \\ \|x-m\| > \sqrt{d}}} e^{-\pi\|x-m\|^2} \ \leq \ 5^{-d} \sum_{m \in \Lambda} e^{-\pi\|m\|^2}.$$

Applying Lemma 17.3, we obtain

$$\sum_{m \in \Lambda} e^{-\pi\|x-m\|^2} \ \leq \ \frac{1}{5^d \det \Lambda} \sum_{l \in \Lambda^*} e^{-\pi\|l\|^2}. \tag{18.3.1}$$

Applying Lemma 18.2 to Λ^*, we conclude that

$$\sum_{l \in \Lambda^*} e^{-\pi\|l\|^2} = 1 + \sum_{l \in \Lambda^* \setminus \{0\}} e^{-\pi\|l\|^2} \ = \ 1 + \sum_{\substack{l \in \Lambda^*: \\ \|l\| > \sqrt{d}}} e^{-\pi\|l\|^2} \ \leq 1 + 5^{-d} \sum_{l \in \Lambda^*} e^{-\pi\|l\|^2},$$

from which

$$\sum_{l \in \Lambda^*} e^{-\pi\|l\|^2} \ \leq \ \frac{5^d}{5^d - 1} \quad \text{and} \quad \sum_{l \in \Lambda^* \setminus \{0\}} e^{-\pi\|l\|^2} \ \leq \ \frac{1}{5^d - 1}. \tag{18.3.2}$$

Therefore, from (18.3.1) we conclude

$$\sum_{m \in \Lambda} e^{-\pi\|x-m\|^2} \ \leq \ \frac{1}{(5^d - 1) \det \Lambda}. \tag{18.3.3}$$

Similarly, from (18.3.2),

$$\left| \sum_{l \in \Lambda^*} e^{-\pi\|l\|^2 + 2\pi i \langle l, x \rangle} \right| \geq \ 1 - \sum_{l \in \Lambda^* \setminus \{0\}} e^{-\pi\|l\|^2} \ \geq \ \frac{5^d - 2}{5^d - 1}.$$

On the other hand, by Lemma 17.3,

$$\sum_{m \in \Lambda} e^{-\pi\|x-m\|^2} = \frac{1}{\det \Lambda} \sum_{l \in \Lambda^*} e^{-\pi\|l\|^2 + 2\pi i \langle l, x \rangle} \ \geq \ \frac{5^d - 2}{(5^d - 1) \det \Lambda},$$

which contradicts (18.3.3). □

(18.4) Problems.

1. Prove that

$$\sum_{m \in \Lambda} e^{-\pi\|x-m\|^2} \ \geq \ e^{-\pi\|x\|^2} \sum_{m \in \Lambda} e^{-\pi\|m\|^2}.$$

2°. Let $\Lambda \subset V$ be a lattice and let $x \in V$ be a point. Prove that for any $v \in \Lambda^*$ we have

$$\operatorname{dist}(x, \Lambda) \ \geq \ \frac{\operatorname{dist}(\langle x, v\rangle,\ \mathbb{Z})}{\|v\|}.$$

3. Let $\Lambda \subset V$ be a lattice of rank d. Prove that for every point $x \in V$ there is a vector $v \in \Lambda^* \setminus \{0\}$ such that

$$\operatorname{dist}(x, \Lambda) \ \leq \ 6d \frac{\operatorname{dist}(\langle x, v\rangle,\ \mathbb{Z})}{\|v\|}.$$

Hint: Without loss of generality we may assume that $\operatorname{dist}(x, \Lambda) = \sqrt{d}$. From Lemma 17.3 and Lemma 18.2 deduce that there is a $v \in \Lambda^* \setminus \{0\}$ such that $\|v\| \leq \sqrt{d}$ and $\operatorname{dist}(\langle x, v\rangle,\ \mathbb{Z}) \geq 1/6$.

19. The packing density via the Poisson summation formula

The following result is from

H. Cohn and N. Elkies, New upper bounds on sphere packings. I. *Ann. of Math. (2)* **157** (2003), no. 2, 689 – 714.

(19.1) Theorem. *Let $f : \mathbb{R}^n \longrightarrow \mathbb{R}$ be a measurable function such that*

$$|f(x)|,\ |\hat{f}(x)| \ \leq \ \frac{C}{(1 + \|x\|)^{n+\delta}} \quad \text{for all} \quad x \in \mathbb{R}^n$$

and some $C > 0$ and $\delta > 0$. Suppose further that

$$f(x) \leq 0 \quad \text{provided} \quad \|x\| \geq 1$$

and that

$$\hat{f}(y) \geq 0 \quad \text{for all} \quad y \in \mathbb{R}^n.$$

Then the packing density $\sigma(\Lambda)$ of every lattice $\Lambda \subset \mathbb{R}^n$ satisfies

$$\sigma(\Lambda) \ \leq \ \frac{\pi^{\frac{n}{2}}}{\Gamma\left(1 + \frac{n}{2}\right)} \frac{f(0)}{2^n \hat{f}(0)}.$$

Proof. Without loss of generality we may assume that $\rho(\Lambda) = 1/2$ and hence

$$\sigma(\Lambda) = \frac{\pi^{\frac{n}{2}}}{\Gamma\left(1 + \frac{n}{2}\right) 2^n \det \Lambda}.$$

Applying Lemma 17.2, we conclude

$$f(0) \ \geq \ \sum_{u \in \Lambda} f(u) = \frac{1}{\det \Lambda} \sum_{l \in \Lambda^*} \hat{f}(l) \ \geq \ \frac{\hat{f}(0)}{\det \Lambda}$$

and hence

$$\frac{1}{\det \Lambda} \ \leq \ \frac{f(0)}{\hat{f}(0)}.$$

□

(19.2) Problems.

1. Consider a sphere packing in $\mathbb{R}^n$ such that the set of the centers of the spheres is a union of finitely many pairwise disjoint lattice shifts $x_i + \Lambda$ for some lattice $\Lambda \subset \mathbb{R}^n$ and some points $x_1, \dots, x_m \in \mathbb{R}^n$ such that $x_i - x_j \notin \Lambda$ provided $i \neq j$. Prove that the packing density σ satisfies

$$\sigma \ \leq \ \frac{\pi^{\frac{n}{2}}}{\Gamma\left(1+\frac{n}{2}\right)} \frac{f(0)}{2^n \hat{f}(0)},$$

where f is a function of Theorem 19.1.

2. Deduce from Problem 1 above that the bound of Theorem 19.1 holds for any (lattice or non-lattice) sphere packing.

3. Let Λ be a lattice of rank d such that $\det \Lambda = 1$. Prove that for any $\beta > (2\pi)^{-1}$ there exists a positive integer $d_0 = d_0(\beta)$ such that Λ contains a non-zero vector of length at most $\sqrt{\beta d}$ provided $d \geq d_0$.

Hint: Note that if the length of a shortest non-zero vector from Λ exceeds $\sqrt{\beta d}$ then the length of a shortest non-zero vector from the scaled lattice $\alpha\Lambda$ exceeds $\alpha\sqrt{\beta d}$. Use Lemma 18.2 and Lemma 17.3.

4. Deduce from Problem 3 above that for any $\gamma > 0.5\sqrt{e} \approx 0.824$ there exists $d_1 = d_1(\gamma)$ such that the packing density of any lattice Λ of rank d satisfies $\sigma(\Lambda) < \gamma^d$ provided $d \geq d_1$.

20. Approximating a convex body by an ellipsoid

(20.1) Definitions. Let V be Euclidean space. A *convex body* $K \subset V$ is a convex compact set with a non-empty interior. A *ball* $B \subset V$ is the set

$$B = \Big\{ x \in V : \quad \|x - x_0\| \leq r \Big\},$$

where $x_0 \in V$ is a point called the *center* of B and $r > 0$ is the *radius* of B. An *ellipsoid* $E \subset V$ is a set $E = T(B)$, where $B \subset V$ is a ball and $T : V \longrightarrow V$ is an invertible linear transformation. Point $y_0 = T(x_0)$, where x_0 is the center of B, is called the *center* of E.

The main result of this section, known as F. John's Theorem, is that an arbitrary convex body can be reasonably well approximated by an appropriate ellipsoid.

(20.2) Theorem. *Let V be a d-dimensional Euclidean space and let $K \subset \mathbb{R}^d$ be a convex body. Then there is an ellipsoid $E \subset V$ centered at some point $x_0 \in K$ such that*

$$E \ \subset \ K \ \subset \ x_0 + d\,(E - x_0)\,.$$

Sketch of Proof. We choose E to be the ellipsoid of the maximum volume among those contained in K. That such an ellipsoid exists (it is, in fact, unique) follows by a compactness argument.

Without loss of generality, we may assume that the center of E is the origin. Moreover, applying an invertible linear transformation (which results in all volumes scaled proportionately), we may assume that E is the unit ball

$$E = \Big\{ x \in V : \ \|x\| \leq 1 \Big\}.$$

Our goal is to prove that $\|x\| \leq d$ for all $x \in K$. Assuming the contrary, we may identify $V = \mathbb{R}^d$ and assume that there is a point $x = (r, 0, \ldots, 0)$, $x \in K$, for some $r > d$. We intend to obtain a contradiction by constructing an ellipsoid $E_1 \subset K$ such that $\operatorname{vol} E_1 > \operatorname{vol} E$.

We look for an ellipsoid E_1 in the form

$$E_1 = \left\{ (x_1, \ldots, x_d) : \quad \frac{(x_1 - \tau)^2}{\alpha^2} + \frac{1}{\beta^2} \sum_{i=2}^d x_i^2 \ \leq \ 1 \right\} \quad \text{where}$$

$$\alpha = \tau + 1 \quad \text{and} \quad \beta^2 = \frac{(r-\tau)^2 - (\tau+1)^2}{r^2 - 1}.$$

We claim that for all $0 \leq \tau < (r-1)/2$, ellipsoid E_1 is contained in K. Because of symmetry, it suffices to check that the section of E_1 by the (x_1, x_2) coordinate plane is contained in the section of K by the (x_1, x_2) coordinate plane, which is an elementary geometry problem.

Moreover,

$$\ln \frac{\operatorname{vol} E_1}{\operatorname{vol} B} = (d-1) \ln \beta + \ln \alpha = \frac{d-1}{2} \ln \beta^2 + \ln \alpha.$$

For a sufficiently small $\tau > 0$, we have

$$\ln \alpha = \tau + O\left(\tau^2\right) \quad \text{and} \quad \ln \beta^2 = -\frac{2\tau}{r-1} + O\left(\tau^2\right).$$

If $r > d$ then for a sufficiently small $\tau > 0$ we get $\operatorname{vol} E_1 > \operatorname{vol} E$, which is a contradiction. $\square$

(20.3) Problems.

1. Fill in the gaps in the proof of Theorem 20.2.

2. Prove that every convex body K contains a unique ellipsoid of the maximum volume.

3. Let K be a d-dimensional symmetric convex body, so $K = -K$ and let $E \subset K$ be the ellipsoid of the maximum volume contained in K. Prove that the center of E is the origin and that $K \subset \sqrt{d} E$.

4. Prove that every convex body K is contained in a unique ellipsoid E of the minimum volume. Prove that if x_0 is the center of E then

$$\frac{1}{d}(E - x_0) + x_0 \ \subset \ K \ \subset \ E.$$

5. Prove that for the minimum volume ellipsoid of Problem 4 we have

$$\frac{1}{\sqrt{d}}(E - x_0) + x_0 \ \subset \ K \ \subset \ E,$$

if K is symmetric.

21. The Flatness Theorem

We rephrase Theorem 18.3 as follows.

(21.1) Lemma. *Let $\Lambda \subset V$ be a lattice, where $\dim V = d$, and let*

$$B = \Big\{ x \in V : \ \|x - x_0\| \leq r \Big\}$$

be a ball centered at some point $x_0 \in V$ and of radius r such that $B \cap \Lambda = \emptyset$. Then there exists a vector $v \in \Lambda^* \setminus \{0\}$ such that

$$\max_{x \in B} \langle v, x \rangle - \min_{x \in B} \langle v, x \rangle \ \leq \ c(d),$$

where one can choose $c(d) = 2d$.

Proof. Since $B \cap \Lambda = \emptyset$, we have $\mu(\Lambda) > r$. Therefore by Theorem 18.3 we have $\rho\left(\Lambda^*\right) < d/2r$ and hence there exists a vector $v \in \Lambda^* \setminus \{0\}$ such that $\|v\| < d/r$. Then

$$\max_{x \in B} \langle v, x \rangle \ \leq \ \langle v, x_0 \rangle + d \quad \text{and} \quad \min_{x \in B} \langle v, x \rangle \ \geq \ \langle v, x_0 \rangle - d,$$

from which the proof follows. □

Next, we extend Lemma 21.1 to ellipsoids.

(21.2) Lemma. *Let $\Lambda \subset V$ be a lattice, where $\dim V = d$, and let $E \subset V$ be an ellipsoid such that $E \cap \Lambda = \emptyset$. Then there exists a vector $v \in \Lambda^* \setminus \{0\}$ such that*

$$\max_{x \in E} \langle v, x \rangle - \min_{x \in E} \langle v, x \rangle \ \leq \ c(d),$$

where one can choose $c(d) = 2d$.

Proof. Let $T : V \longrightarrow V$ be an invertible linear transformation and let $B \subset V$ be a ball such that $E = T(B)$. Let $\Lambda_1 = T^{-1}(\Lambda)$. Then $\Lambda_1 \subset V$ is a lattice and $B \cap \Lambda_1 = \emptyset$. By Lemma 21.2, there exists a vector $w \in \Lambda_1^*$ such that

$$\max_{x \in B} \langle w, x \rangle - \min_{x \in B} \langle w, x \rangle \ \leq \ c(d), \tag{21.2.1}$$

where one can choose $c(d) = 2d$.

Let $v = \left(T^{-1}\right)^* (w)$. For every $u \in \Lambda$ we have

$$\langle u, v \rangle = \langle T^{-1}(u), w \rangle \ \in \ \mathbb{Z}$$

and hence $v \in \Lambda^* \setminus \{0\}$. Moreover, for every $y \in E$ we have $y = T(x)$ for some $x \in B$ and hence

$$\langle v, y \rangle = \langle T^*(v), x \rangle = \langle w, x \rangle,$$

and the proof follows by (21.2.1). □

The following result is known as the *Flatness Theorem.*

(21.3) Theorem. *Let $\Lambda \subset V$ be a lattice, where $\dim V = d$, and let $K \subset V$ be a convex body such that $K \cap \Lambda = \emptyset$. Then there is a vector $v \in \Lambda^* \setminus \{0\}$ such that*

$$\max_{x \in K} \langle v, x \rangle - \min_{x \in K} \langle v, x \rangle \ \leq \ c(d),$$

where one can choose $c(d) = 2d^2$.

Proof. Let $E \subset K$ be the ellipsoid of Theorem 20.2, so $K \subset d(E - x_0) + x_0$. Since $E \cap \Lambda = \emptyset$, by Lemma 21.2 there exists a vector $v \in \Lambda^* \setminus \{0\}$ such that

$$\max_{x \in E} \langle v, x \rangle - \min_{x \in E} \langle v, x \rangle \ \leq \ 2d.$$

Since

$$\max_{x \in K} \langle v, x \rangle \ \leq \ \max_{x \in d(E - x_0) + x_0} \langle v, x \rangle = d \max_{x \in E} \langle v, x \rangle - (d-1) \langle v, x_0 \rangle$$

and

$$\min_{x \in K} \langle v, x \rangle \ \geq \ \min_{x \in d(E - x_0) + x_0} \langle v, x \rangle = d \min_{x \in E} \langle v, x \rangle - (d-1) \langle v, x_0 \rangle,$$

the proof follows. □

(21.4) Problems.

1. Let $P \subset \mathbb{R}^2$ be a convex polygon with vertices in $\mathbb{Z}^2$. Suppose that P does not contain any point from $\mathbb{Z}^2$ other than its vertices. Prove that there exists a vector $w \in \mathbb{Z}^2 \setminus \{0\}$ such that

$$\max_{x \in P} \langle w, x \rangle - \min_{x \in P} \langle w, x \rangle \ \leq \ 1.$$

2*. Let $P \subset \mathbb{R}^3$ be a convex polytope with vertices in $\mathbb{Z}^3$. Suppose that P does not contain any point from $\mathbb{Z}^3$ other than its vertices. Prove that there exists a vector $w \in \mathbb{Z}^3 \setminus \{0\}$ such that

$$\max_{x \in P} \langle w, x \rangle - \min_{x \in P} \langle w, x \rangle \ \leq \ 1.$$

22. The successive minima of a convex body

(22.1) Definition. Let $K \subset V$ be a symmetric convex body and let $\Lambda \subset V$ be a lattice. Let $\dim V = d$. For $i = 1, \ldots, d$ we define the *i-th successive minimum*

$$\lambda_i = \lambda_i(K) = \inf \Big\{ \lambda > 0 : \quad \dim \operatorname{span}(\lambda K \cap \Lambda) \geq i \Big\}.$$

Clearly,

$$\lambda_1 \leq \lambda_2 \leq \ldots \leq \lambda_d.$$

Minkowski's Theorem (see Theorem 6.4) states that

$$\lambda_1^d \operatorname{vol} K \ \leq \ 2^d \det \Lambda.$$

In this section we prove a sharpening of this result, also due to Minkowski, that

$$\lambda_1 \cdots \lambda_d \operatorname{vol} K \ \leq \ 2^d \det \Lambda.$$

(22.2) Lemma. *Let us consider the map* $\Phi_n : \mathbb{R}^n \longrightarrow [0,1)^n$,

$$\Phi_n (x_1, \ldots, x_n) = (\{x_1\}, \ldots, \{x_n\}),$$

where $\{\cdot\}$ *denotes the fractional part of a number.*

Let $X \subset \mathbb{R}^n$ *be a Lebesgue measurable set. Then for every* $z \in \mathbb{R}^n$, *we have*

$$\operatorname{vol} \Phi_n(X+z) = \operatorname{vol} \Phi_n(X).$$

Proof. It suffices to prove the identity when z has only one non-zero coordinate and that coordinate lies in the interval $(0,1)$. Hence without loss of generality we may assume that

$$z = (0, \ldots, 0, \alpha)$$

for some $0 < \alpha < 1$.

Let $X = X_- \cup X_+$, where

$$X_- = \Big\{x \in X : \quad \{x_n\} < 1 - \alpha\Big\} \quad \text{and} \quad X_+ = \Big\{x \in X : \quad \{x_n\} \geq 1 - \alpha\Big\}.$$

Clearly,

$$X_- \cap X_+ = \emptyset \quad \text{and} \quad \operatorname{vol} X = \operatorname{vol} X_- + \operatorname{vol} X_+.$$

Moreover,

$$\begin{aligned} \Phi_n (X_- + z) &= \Phi_n (X_-) + (0, \ldots, 0, \alpha) \quad \text{and} \\ \Phi_n (X_+ + z) &= \Phi_n (X_-) + (0, \ldots, \alpha - 1) \end{aligned}$$

and hence

$$\operatorname{vol} \Phi_n (X_- + z) = \operatorname{vol} \Phi_n (X_-) \quad \text{and} \quad \operatorname{vol} \Phi_n (X_+ + z) = \operatorname{vol} \Phi_n (X_+).$$

Finally, $\Phi_n (X_- + z)$ and $\Phi_n (X_+ + z)$ are disjoint sets, since for any vector $x = (x_1, \ldots, x_n)$ we have $\{x_n\} \geq \alpha$ if $x \in \Phi_n (X_- + z)$ and $\{x_n\} < \alpha$ if $x \in \Phi_n (X_+ + z)$. Since $\Phi_n (X_+)$ and $\Phi_n (X_-)$ are also disjoint, we have

$$\begin{aligned} \operatorname{vol} \Phi_n(X+z) &= \operatorname{vol} \Phi_n (X_- + z) + \operatorname{vol} \Phi_n (X_+ + z) \\ &= \operatorname{vol} \Phi_n (X_-) + \operatorname{vol} \Phi_n (X_+) \\ &= \operatorname{vol} \Phi_n(X). \end{aligned}$$

$\square$

(22.3) Lemma. *Let $X \subset \mathbb{R}^n$ be a convex set. Then for any $\alpha \geq 1$ we have*

$$\operatorname{vol} \Phi_n(\alpha X) \ \geq \ \operatorname{vol} \Phi_n(X).$$

Proof. Let $z \in \mathbb{R}^n$ be a point such that $0 \in X + z$. Then $(X+z) \subset \alpha(X+z)$ and so $\Phi_n(X+z) \subset \Phi_n(\alpha X + \alpha z)$. Applying Lemma 22.2, we get

$$\operatorname{vol} \Phi_n(\alpha X) = \operatorname{vol} \Phi_n(\alpha X + \alpha z) \ \geq \ \operatorname{vol} \Phi_n(X+z) = \operatorname{vol} \Phi_n(X).$$

□

(22.4) Lemma. *For $1 \leq i \leq n$ let us consider the map $\Phi_i : \mathbb{R}^n \longrightarrow [0,1)^i \times \mathbb{R}^{n-i}$,*

$$\Phi_i\left(x_1, \ldots, x_n\right) = \left(\{x_1\}, \ldots, \{x_i\}, x_{i+1}, \ldots, x_n\right).$$

Let $X \subset \mathbb{R}^n$ be a convex set. Then for any $\alpha \geq 1$ we have

$$\operatorname{vol} \Phi_i(\alpha X) \ \geq \ \alpha^{n-i} \Phi_i(X).$$

Proof. Let $pr : \mathbb{R}^n \longrightarrow \mathbb{R}^{n-i}$ be the projection,

$$pr\left(x_1, \ldots, x_n\right) = \left(x_{i+1}, \ldots, x_n\right)$$

and let $Y = pr(X)$. Then, by Fubini's Theorem,

$$\operatorname{vol} \Phi_i(X) = \int_Y \operatorname{vol}_i \Phi_i\left(pr^{-1}(y) \cap X\right) \ dy \quad \text{and}$$
$$\operatorname{vol} \Phi_i(\alpha X) = \int_{\alpha Y} \operatorname{vol}_i \Phi_i\left(pr^{-1}(y) \cap \alpha X\right) \ dy.$$

Making substitution $y = \alpha x$ in the second integral, we obtain

$$\Phi_i(\alpha X) = \alpha^{n-i} \int_Y \operatorname{vol}_i \Phi_i\left(pr^{-1}(\alpha x) \cap \alpha X\right) \ dx,$$

which we formally rewrite as

$$\Phi_i(\alpha X) = \alpha^{n-i} \int_Y \operatorname{vol}_i \Phi_i\left(pr^{-1}(\alpha y) \cap \alpha X\right) \ dy,$$

Now, $pr^{-1}(y) \cap X$ consists of all points $(x_1, \ldots, x_i, y_{i+1}, \ldots, y_n) \in X$ while $pr^{-1}(\alpha y) \cap \alpha X$ consists of all points $(\alpha x_1, \ldots, \alpha x_i; \alpha y_{i+1}, \ldots, \alpha y_n) \in \alpha X$. Applying Lemma 22.3, we obtain

$$\operatorname{vol}_i \Phi_i\left(pr^{-1}(\alpha y) \cap \alpha X\right) \ \geq \ \operatorname{vol}_i \Phi_i\left(pr^{-1}(y) \cap X\right) \quad \text{for all} \quad y \in Y$$

and the proof follows. □

Now we can prove Minkowski's Theorem.

(22.5) Theorem. *Let $K \subset V$ be a symmetric convex body and let $\Lambda \subset V$ be a lattice. Then*

$$\lambda_1 \cdots \lambda_d \operatorname{vol} K \ \leq \ 2^d \det \Lambda,$$

where $d = \dim V$ and $\lambda_1, \ldots, \lambda_d$ are the successive minima.

Proof. Applying a linear transformation, we may assume that $V = \mathbb{R}^d$ and $\Lambda = \mathbb{Z}^d$.

Let us consider dilations λK as $\lambda > 0$ grows and let $u_1, \ldots, u_d \in \mathbb{Z}^d$ be linearly independent vectors in the order of appearance, where ties are broken arbitrarily. We choose a new basis $b_1, \ldots, b_d$ of $\mathbb{Z}^d$ in such a way that for $i = 1, \ldots, d$ vectors $b_1, \ldots, b_i$ constitute a basis of the lattice $\mathbb{Z}^d \cap \operatorname{span}(u_1, \ldots, u_i)$, cf. Problem 4 of Section 3.2.

The linear transformation that maps the standard basis vectors $e_1, \ldots, e_d$ to $b_1, \ldots, b_d$ does not change the volume of K or the lattice $\mathbb{Z}^d$. Hence we can assume additionally that the coordinates of $u_1, \ldots, u_d$ look as follows:

$$u_1 = (*, 0, \ldots, 0), u_2 = (*, *, 0, \ldots, 0), \ldots, u_d = (*, \ldots, *).$$

Let A be the interior of K, so $\operatorname{vol} A = \operatorname{vol} K$ and if $u \in \lambda_i A \cap \Lambda$ then the coordinates of u, starting with the i-th position, are 0's.

Let

$$X = \frac{1}{2} A.$$

Let Φ_i be the map of Lemma 22.4. Then $\Phi_i\left(\lambda_i X\right)$ is obtained from $\Phi_{i-1}\left(\lambda_i X\right)$ via the transformation $x_i \longmapsto \{x_i\}$. This transformation is one-to-one since if there are two distinct points $x, y \in \lambda_i X$ with the same image then

$$u = x - y = 2\left(\frac{1}{2}x + \frac{1}{2}(-y)\right) \in \lambda_i A$$

and the i-th coordinate of u is a non-zero integer, while all other coordinates are 0's, which is a contradiction. Then we can conclude from Lemma 22.4 that

$$\begin{aligned} \operatorname{vol} \Phi_i\left(\lambda_i X\right) = \operatorname{vol} \Phi_{i-1}\left(\lambda_i X\right) &= \operatorname{vol} \Phi_{i-1}\left(\left(\frac{\lambda_i}{\lambda_{i-1}}\right) \lambda_{i-1} X\right) \\ &\geq \left(\frac{\lambda_i}{\lambda_{i-1}}\right)^{d-i+1} \operatorname{vol} \Phi_{i-1}\left(\lambda_{i-1} X\right). \end{aligned}$$

Similarly, the transformation $x_i \longmapsto \{x_1\}$ is one-to-one on $\lambda_1 X$ and hence

$$\operatorname{vol} \Phi_1\left(\lambda_1 X\right) = \operatorname{vol} \lambda_1 X = \lambda_1^d \operatorname{vol} X.$$

Summarizing,

$$\operatorname{vol} \Phi_n\left(\lambda_n X\right) \ \geq \ \lambda_1^d \operatorname{vol} X \prod_{i=2}^{d} \left(\frac{\lambda_i}{\lambda_{i-1}}\right)^{d-i+1} = \lambda_1 \cdots \lambda_d \operatorname{vol} X.$$

Therefore,

$$\lambda_1 \cdots \lambda_d \operatorname{vol} X \leq 1,$$

as claimed. $\square$

23. An almost orthogonal basis of the lattice

One corollary of Theorem 22.5 is that every lattice has an "almost orthogonal" basis.

(23.1) Lemma. *Let Λ be a lattice of rank d and let $u_1, \ldots, u_d$ be linearly independent vectors. Then there exists a basis $v_1, \ldots, v_d$ of Λ such that*

$$v_k = \sum_{i=1}^{k} \alpha_{ki} u_i \quad \textit{where}$$

$$0 < \alpha_{kk} \leq 1 \quad \textit{and} \quad |\alpha_{ki}| \leq \frac{1}{2} \quad \textit{for} \quad i = 1, \ldots, k-1 \quad \textit{and} \quad k = 1, \ldots, d.$$

Proof. Let us define

$$L_k = \operatorname{span}\Big(u_1, \ldots, u_k\Big) \quad \text{and} \quad \Lambda_k = \Lambda \cap L_k \quad \text{for} \quad k = 1, \ldots, d.$$

We choose v_1 to be a basis of Λ_1. Clearly, we must have $v_1 = \alpha_{11} u_1$ for some $|\alpha_{11}| \leq 1$. If $\alpha_{11} < 0$, we replace v_1 by $-v_1$. Generally, having constructed $v_1, \ldots, v_{k-1}$ as a basis of Λ_{k-1}, we append it to a basis $v_1, \ldots, v_k$ of Λ_k (cf. the proof of Theorem 3.1). Hence we have

$$v_k = \sum_{i=1}^{k} \alpha_{ki} u_i. \tag{23.1.1}$$

If $\alpha_{kk} < 0$, we replace

$$v_k := -v_k.$$

Writing the right hand side of (23.1.1) as an integer linear combination of $v_1, \ldots, v_k$, we conclude that $\alpha_{kk} m = 1$ for some integer m and hence $0 < \alpha_{kk} \leq 1$, as required If $|\alpha_{ki}| > 1/2$ for some $i < k$, we replace

$$v_k := v_k - m_{ki} u_i,$$

where m_{ki} is the nearest integer to α_{ki}. Since u_i is an integer combination of $v_1, \ldots, v_i$ where $i < k$, we get a vector v_k from Λ_k. Moreover, the volume of the parallelepiped spanned by $v_1, \ldots, v_k$ does not change, so we still have a basis of Λ_k. $\square$

(23.2) Theorem. *Let $\Lambda \subset V$ be a lattice of rank d. Then there is a basis $v_1, \ldots, v_d$ of Λ such that*

$$\prod_{i=1}^{d} \|v_i\| \ \leq \ C(d) \det \Lambda,$$

where one can choose

$$C(d) = \frac{(d+1)!\Gamma\left(1+\frac{d}{2}\right)}{\pi^{d/2}}.$$

Proof. Let $B \subset V$ be the ball of radius 1 centered at the origin. Let us consider the dilations λB for $\lambda > 0$ and let $u_1, \ldots, u_d \in \Lambda$ be linearly independent vectors, in the order of appearance, as λ grows, where the ties are broken arbitrarily. Hence

$$\|u_1\| \leq \|u_2\| \leq \ldots \leq \|u_d\|$$

and by Theorem 22.5 we have

$$\prod_{i=1}^{d} \|u_i\| \ \leq \ \frac{2^d \det \Lambda}{\operatorname{vol} B} \ = \ \frac{2^d \Gamma\left(1+\frac{d}{2}\right)}{\pi^{d/2}} \det \Lambda. \tag{23.2.1}$$

Now we construct a basis $v_1, \ldots, v_d$ of Λ as in Lemma 23.2.

We note that

$$\|v_k\| \ \leq \ \|u_k\| + \frac{1}{2} \sum_{i=1}^{k-1} \|u_i\| \ \leq \ \frac{(k+1)}{2} \|u_k\|$$

and the proof follows by (23.2.1). □

(23.3) Problems.

1. Let $\{\Lambda_n \subset V, \quad n = 1, 2, \ldots\}$ be a sequence of lattices and let $\Lambda \subset V$ be yet another lattice. We say that

$$\lim_{n \longrightarrow +\infty} \Lambda_n = \Lambda$$

if there exist bases $u_{n1}, \ldots, u_{nd}$ of Λ_n and a basis $u_1, \ldots, u_d$ of Λ such that

$$\lim_{n \longrightarrow +\infty} u_{ni} = u_i \quad \text{for} \quad i = 1, \ldots, d.$$

Prove the following *Mahler's Compactness Theorem:*

Let $\{\Lambda_i \subset V : \quad i \in I\}$ be an infinite family of lattices such that $\det \Lambda_i \leq C$ for all $i \in I$ and some real C and $\rho(\Lambda_i) \geq \delta$ for all $i \in I$ and some $\delta > 0$, where ρ is the packing radius. Prove that the family contains a sequence converging to some lattice $\Lambda \subset V$.

2. Let $\{\Lambda_n \subset V\}$ be a sequence of lattices and let $\Lambda \subset V$ be a lattice such that

$$\lim_{n \longrightarrow +\infty} \Lambda_n = \Lambda.$$

Prove that

$$\lim_{n \longrightarrow +\infty} \rho(\Lambda_n) = \rho(\Lambda) \quad \text{and} \quad \lim_{n \longrightarrow +\infty} \mu(\Lambda_n) = \mu(\Lambda)$$

for the packing and covering radii.

3. Let $U = u_1, \ldots, u_d$ be a basis of a lattice Λ, let

$$L_0 = \{0\} \quad \text{and} \quad L_k = \operatorname{span}\Big(u_1, \ldots, u_k\Big) \quad \text{for} \quad k = 1, \ldots, d$$

and let w_k be the orthogonal complement to the projection of u_k onto L_{k-1} for $k = 1, \ldots, d$. Hence we can write

$$u_k = w_k + \sum_{i=1}^{k-1} \alpha_{ki} w_i.$$

The basis is called *reduced* if

$$|\alpha_{ki}| \ \leq \ \frac{1}{2} \quad \text{for} \quad i = 1, \ldots, k-1 \quad \text{and} \quad k = 2, \ldots, d.$$

Prove that for every basis $u_1, \ldots, u_d$ of Λ there is a reduced basis $v_1, \ldots, v_d$ such that

$$\operatorname{span}\Big(v_1, \ldots, v_k\Big) = L_k \quad \text{and} \quad \operatorname{dist}(u_k, L_{k-1}) = \operatorname{dist}(v_k, L_{k-1})$$
$$\text{for} \quad k = 1, \ldots, d.$$

4. Let $u_1, \ldots, u_d$ be a reduced Korkin-Zolotarev basis (see Section 14) of Λ. Prove that

$$\|u_k\|^2 \ \leq \ \frac{k+3}{4} \lambda_k^2(\Lambda) \quad \text{for} \quad k = 1, \ldots, d,$$

where $\lambda_k(\Lambda)$ is the k-th successive minimum with respect to the unit ball. Deduce that one can choose

$$C(d) = \frac{\sqrt{(d+3)!}\Gamma\left(1 + \frac{d}{2}\right)}{\pi^{d/2}\sqrt{6}} \det \Lambda$$

in Theorem 23.2.

5. Let $u_1, \ldots, u_d$ be a reduced Korkin-Zolotarev basis of Λ. Prove that

$$\|u_k\|^2 \ \geq \ \frac{4}{k+3} \lambda_k^2(\Lambda) \quad \text{for} \quad k = 1, \ldots, d.$$

24. Successive minima via the Poisson summation formula

The following result is also known as a *transference theorem*. We follow

W. Banaszczyk, New bounds in some transference theorems in the geometry of numbers, *Mathematische Annalen*, 296 (**1993**), 625 – 635

with some modifications, as we don't pursue the best possible constants.

For a lattice $\Lambda \subset V$, we denote by $\lambda_i(\Lambda)$ the i-th successive minimum of Λ with respect to the Euclidean ball in V of radius 1.

(24.1) Theorem. *Let $\Lambda \subset V$ be a lattice of rank d. Then*

$$1 \ \leq \ \lambda_k(\Lambda)\lambda_{d-k+1}(\Lambda^*) \ \leq \ 2d \quad \textit{for} \quad k=1, \ldots, d.$$

Proof. Let $u_1, \ldots, u_d \in \Lambda$ and $v_1, \ldots, v_d \in \Lambda^*$ be linearly independent vectors in the order of increasing length, so

$$\|u_1\| \ \leq \ \ldots \ \leq \ \|u_d\| \quad \text{and} \quad \|v_1\| \ \leq \ \ldots \ \leq \ \|v_d\|$$

and

$$\lambda_k(\Lambda) = \|u_k\| \quad \text{and} \quad \lambda_{d-k+1}(\Lambda^*) = \|v_{d-k+1}\|.$$

Since

$$\dim \operatorname{span}\Big(u_1, \ldots, u_k\Big) = k \quad \text{and} \quad \dim \operatorname{span}\Big(v_1, \ldots, v_{d-k+1}\Big) = d-k+1,$$

there are vectors u_i with $i \leq k$ and v_j with $j \leq d-k+1$ such that $\langle u_i, v_j \rangle \neq 0$. Then $|\langle u_i, v_j \rangle| \geq 1$, since the scalar product is necessarily an integer. Thus we have

$$\lambda_k(\Lambda) \cdot \lambda_{d-k+1}(\Lambda^*) = \|u_k\| \cdot \|v_{d-k+1}\| \ \geq \ \|u_i\| \cdot \|v_j\| \ \geq \ |\langle u_i, v_j \rangle| \ \geq 1.$$

Next, we prove the upper bound. First, we note that by Lemma 18.2,

$$\sum_{\substack{l \in \Lambda^*: \\ \|l\| > \sqrt{d}}} e^{-\pi\|l\|^2} \ \leq \ 5^{-d} \sum_{l \in \Lambda} e^{-\pi\|l\|^2}$$

and hence

$$\sum_{\substack{l \in \Lambda^*: \\ \|l\| \leq \sqrt{d}}} e^{-\pi\|l\|^2} = \sum_{l \in \Lambda^*} e^{-\pi\|l\|^2} - \sum_{\substack{l \in \Lambda^*: \\ \|l\| > \sqrt{d}}} e^{-\pi\|l\|^2} \ \geq \ \left(1-5^{-d}\right) \sum_{l \in \Lambda^*} e^{-\pi\|l\|^2}.$$

Seeking a contradiction, let us suppose that $\lambda_k(\Lambda)\lambda_{d-k+1}(\Lambda^*) > 2d$. Scaling $\Lambda := \alpha\Lambda$ and $\Lambda^* := \alpha^{-1}\Lambda^*$ for $\alpha > 0$, we may assume that $\lambda_k(\Lambda) > 2\sqrt{d}$ and $\lambda_{d-k+1}(\Lambda^*) > \sqrt{d}$. Then we have

$$\begin{aligned} &\dim \operatorname{span}\Big(u \in \Lambda: \ \|u\| \leq 2\sqrt{d}\Big) \ \leq \ k-1 \quad \text{and} \\ &\dim \operatorname{span}\Big(v \in \Lambda^*: \ \|v\| \leq \sqrt{d}\Big) \ \leq \ d-k. \end{aligned}$$

Therefore there is an $x \in V$, $\|x\| = \sqrt{d}$, such that x is orthogonal to all vectors of Λ of length at most $2\sqrt{d}$ and x is orthogonal to all vectors of Λ^* of length at most

$\sqrt{d}$. Therefore we have

$$\begin{aligned}
\left|\sum_{l\in\Lambda^*} e^{-\pi\|l\|^2+2\pi i\langle l,x\rangle}\right| &= \left|\sum_{\substack{l\in\Lambda^*:\\ \|l\|\le\sqrt{d}}} e^{-\pi\|l\|^2+2\pi i\langle l,x\rangle} + \sum_{\substack{l\in\Lambda^*:\\ \|l\|>\sqrt{d}}} e^{-\pi\|l\|^2+2\pi i\langle l,x\rangle}\right| \\
&= \left|\sum_{\substack{l\in\Lambda^*:\\ \|l\|\le\sqrt{d}}} e^{-\pi\|l\|^2} + \sum_{\substack{l\in\Lambda^*:\\ \|l\|>\sqrt{d}}} e^{-\pi\|l\|^2+2\pi i\langle l,x\rangle}\right| \\
&\ge \sum_{\substack{l\in\Lambda^*:\\ \|l\|\le\sqrt{d}}} e^{-\pi\|l\|^2} - \sum_{\substack{l\in\Lambda^*:\\ \|l\|>\sqrt{d}}} e^{-\pi\|l\|^2} \\
&\ge \left(1-2\cdot 5^{-d}\right)\sum_{l\in\Lambda^*} e^{-\pi\|l\|^2}.
\end{aligned} \tag{24.1.1}$$

On the other hand,

$$\begin{aligned}
\sum_{\substack{m\in\Lambda:\\ \|x-m\|\le\sqrt{d}}} e^{-\pi\|x-m\|^2} &\le \sum_{\substack{m\in\Lambda:\\ \|m\|\le 2\sqrt{d}}} e^{-\pi\|x-m\|^2} = \sum_{\substack{m\in\Lambda:\\ \|m\|\le 2\sqrt{d}}} e^{-\pi\|x\|^2-\pi\|m\|^2} \\
&\le e^{-\pi d}\sum_{m\in\Lambda} e^{-\pi\|m\|^2}
\end{aligned}$$

and from Lemma 18.2

$$\begin{aligned}
\sum_{m\in\Lambda} e^{-\pi\|x-m\|^2} &= \sum_{\substack{m\in\Lambda:\\ \|x-m\|\le\sqrt{d}}} e^{-\pi\|x-m\|^2} + \sum_{\substack{m\in\Lambda:\\ \|x-m\|>\sqrt{d}}} e^{-\pi\|x-m\|^2} \\
&\le \left(e^{-\pi d}+5^{-d}\right)\sum_{m\in\Lambda} e^{-\pi\|m\|^2}.
\end{aligned} \tag{24.1.2}$$

Finally, by Lemma 17.3, we have

$$\begin{aligned}
\sum_{m\in\Lambda} e^{-\pi\|x-m\|^2} &= \frac{1}{\det\Lambda}\sum_{l\in\Lambda^*} e^{-\pi\|l\|^2+2\pi i\langle l,x\rangle} \quad \text{and} \\
\sum_{m\in\Lambda} e^{-\pi\|m\|^2} &= \frac{1}{\det\Lambda}\sum_{l\in\Lambda^*} e^{-\pi\|l\|^2},
\end{aligned}$$

which, together with (24.1.1) and (24.1.2) implies

$$e^{-\pi d} \ \ge\ 1-3\cdot 5^{-d},$$

which is a contradiction. $\square$

25. The Lenstra - Lenstra - Lovász basis of a lattice

In this section, we describe a construction by A.K. Lenstra, H.W. Lenstra Jr. and L. Lovász of a particularly convenient basis of a given lattice (also called the LLL basis or an LLL-reduced basis). The construction is computationally efficient (both in theory and in practice) and the resulting basis is "almost orthogonal" in the sense of Theorem 23.2 and has some other useful properties.

(25.1) Definitions. Let Λ be a lattice of rank d and let $u_1, \ldots, u_d$ be its basis. We define the subspaces

$$L_0 = \{0\} \quad \text{and} \quad L_k = \operatorname{span}\Big(u_1, \ldots, u_k\Big) \quad \text{for} \quad k = 1, \ldots, d.$$

For $k = 1, \ldots, d$, let w_k be the orthogonal complement to the projection of u_k onto L_{k-1}. Vectors $w_1, \ldots, w_d$ are also called the *Gram-Schmidt orthogonalization* (without normalization) of $u_1, \ldots, u_d$. Hence we can write

$$u_k = w_k + \sum_{i=1}^{k-1} \alpha_{ki} w_i. \tag{25.1.1}$$

We say that the basis $u_1, \ldots, u_d$ is *weakly reduced* if

$$|\alpha_{ki}| \ \leq \ \frac{1}{2} \quad \text{for all} \quad 1 \leq i < k \leq d. \tag{25.1.2}$$

We say that the basis $u_1, \ldots, u_d$ is *Lenstra-Lenstra-Lovász reduced* or *LLL-reduced* if

$$\operatorname{dist}^2(u_k, L_{k-1}) \ \leq \ \frac{4}{3} \operatorname{dist}^2(u_{k+1}, L_{k-1}) \quad \text{for} \quad k = 1, \ldots, d-1. \tag{25.1.3}$$

(25.2) Constructing an LLL basis. Given a basis $u_1, \ldots, u_d$ of a lattice Λ, we modify it by repeating the following two steps until we get an LLL-reduced basis.

Step 1. We compute vectors $w_1, \ldots, w_d$ and check if conditions (25.1.2) are satisfied. If (25.1.2) is violated for some k, we choose the largest i where it is violated, let

$$u_k' := u_k - m_{ki} u_i,$$

where m_{ki} is the nearest integer to α_{ki} so that $|\alpha_{ki} - m_{ki}| \leq 1/2$, and replace u_k by u_k' in the basis. This transformation produces a basis of Λ and does not change the subspaces of $L_0, \ldots, L_d$ of V or the vectors $w_1, \ldots, w_d$. In (25.1.1) it changes the coefficients α_{kj} with $j \leq i$. Therefore, applying the transformation at most $d(d-1)/2$ times, we enforce (25.1.2). Then we go to Step 2.

Step 2. If conditions (25.1.3) are satisfied, we stop and output the current basis $u_1, \ldots, u_d$. If (25.1.3) is violated for some k, we interchange u_k and u_{k+1} in the basis, that is, we let

$$u'_k := u_{k+1} \quad \text{and} \quad u'_{k+1} := u_k \tag{25.2.1}$$

and replace u_k and u_{k+1} in the basis by u'_k and u'_{k+1} respectively. This transformation may violate (25.1.2), so we go to Step 1, if necessary.

Clearly, if the algorithm ever stops, it produces an LLL-reduced basis. To show that it indeed stops, for a given basis $u_1, \ldots, u_d$ we introduce the lattices

$$\Lambda_k = \Lambda \cap L_k \quad \text{for} \quad k = 1, \ldots, d-1$$

and the quantity

$$D(u_1, \ldots, u_d) = \prod_{k=1}^{d-1} \det \Lambda_k.$$

We note that

$$\det \Lambda_k = \prod_{i=1}^{k} \|w_i\|$$

and that

$$\|w_k\| = \operatorname{dist}(u_k, L_{k-1}).$$

Step 1 does not change subspaces L_k and hence does not change the value of $D(u_1, \ldots, u_d)$. Switch (25.2.1) on Step 2 changes the subspace L_k and does not change any other subspaces L_i. Since (25.1.3) is violated, we have

$$\|w'_k\| = \operatorname{dist}(u_{k+1}, L_{k-1}) \ < \ \frac{\sqrt{3}}{2} \operatorname{dist}(u_k, L_{k-1}) = \|w_k\|$$

and hence $\det \Lambda_k$ decreases by at least a factor of $2/\sqrt{3}$. Consequently, the value of $D(u_1, \ldots, u_d)$ decreases by at least a factor of $2/\sqrt{3}$.

Therefore, it remains to show that $D(u_1, \ldots, u_d)$ cannot get arbitrarily small. Let λ be the length of a shortest non-zero vector in Λ. Then the length of a non-zero vector in Λ_k is at least λ and hence

$$\det \Lambda_k \ \geq \ \left(\frac{\lambda}{\sqrt{k}} \right)^k \quad \text{for} \quad k = 1, \ldots, d,$$

which proves that

$$D(u_1, \ldots, u_d) \ \geq \ \lambda^{d(d-1)/2} \prod_{k=1}^{d-1} k^{-k/2}.$$

Consequently, Step 2 of the algorithm can be performed only finitely many times and hence the algorithm stops and outputs an LLL-reduced basis.

In fact, the algorithm works *in polynomial time* and is very efficient in practice.

Here is a useful property of an LLL-reduced basis.

(25.3) Lemma. *Let $u_1, \ldots, u_d$ be an LLL-reduced basis and let $w_1, \ldots, w_d$ be the vectors defined in Section 25.1, so*

$$\|w_k\| = \operatorname{dist}(u_k,\ L_{k-1}) \quad \textit{where} \quad L_k = \operatorname{span}\Big(u_1, \ldots, u_{k-1}\Big).$$

Then

$$\|w_{k+1}\|^2 \ \geq \ \frac{1}{2}\|w_k\|^2 \quad \textit{for} \quad k = 1, \ldots, d-1.$$

Proof. From (25.1.1)–(25.1.3), we have

$$\begin{aligned}
\|w_k\|^2 =& \operatorname{dist}^2(u_k,\ L_{k-1}) \ \leq \ \frac{4}{3}\operatorname{dist}^2(u_{k+1},\ L_{k-1}) \\
=& \frac{4}{3}\|w_{k+1} + \alpha_{k+1k} w_k\|^2 = \frac{4}{3}\|w_{k+1}\|^2 + \frac{4}{3}\alpha_{k+1k}^2\|w_k\|^2 \\
\leq& \frac{4}{3}\|w_{k+1}\|^2 + \frac{1}{3}\|w_k\|^2
\end{aligned}$$

and the proof follows. □

(25.4) Corollary. *Let Λ be a lattice of rank d and let $u_1, \ldots, u_d$ be its LLL-reduced basis.*

Then

(1)

$$\prod_{k=1}^{d}\|u_k\| \ \leq \ 2^{\frac{d(d-1)}{4}} \det\Lambda,$$

(2)

$$\|u_1\| \ \leq \ 2^{\frac{d-1}{2}} \min_{u \in \Lambda \setminus \{0\}} \|u\|,$$

(3)

$$\|u_1\| \ \leq \ 2^{\frac{d-1}{4}} (\det\Lambda)^{1/d}.$$

Proof. From (25.1.1)–(25.1.2) and Lemma 25.3, we have

$$\begin{aligned}
\|u_k\|^2 =& \|w_k\|^2 + \sum_{i=1}^{k-1}\alpha_{ki}^2\|w_i\|^2 \ \leq \ \|w_k\|^2 + \frac{1}{4}\sum_{i=1}^{k-1}\|w_i\|^2 \\
\leq& \|w_k\|^2\left(1 + \frac{1}{4}\sum_{i=1}^{k-1}2^{k-i}\right) \ \leq \ 2^{k-1}\|w_k\|^2.
\end{aligned}$$

Since

$$\det\Lambda = \prod_{k=1}^{d}\|w_k\|,$$

the proof of Part (1) follows.

By Problem 4 of Section 14.3 and Lemma 25.3, for all $u \in \Lambda \setminus \{0\}$ we have

$$\|u\| \ \geq \min_{k=1,\ldots,d} \operatorname{dist}(u_k,\ L_{k-1}) = \min_{k=1,\ldots,d} \|w_k\| \ \geq \ 2^{\frac{1-d}{2}} \|w_1\| = 2^{\frac{1-d}{2}} \|u_1\|$$

and the proof of Part (2) follows.

Finally, by Lemma 25.3,

$$\det \Lambda = \prod_{k=1}^{d} \|w_k\| \ \geq \ \|w_1\|^d \prod_{k=1}^{d} 2^{\frac{1-k}{2}} = \|u_1\|^d 2^{\frac{(1-d)d}{4}}$$

and the proof of Part (3) follows. □

(25.5) Problems.

1. Let Λ be a lattice and let $u_1, \ldots, u_d$ be an LLL-reduced basis of Λ. Let $u \in \Lambda \setminus \{0\}$ be a shortest non-zero lattice vector. Suppose that

$$u = \sum_{k=1}^{d} m_k u_k$$

for some integer $m_1, \ldots, m_d$. Prove that we must have

$$|m_k| \ \leq \ 3^d \quad \text{for} \quad k = 1, \ldots, d.$$

2. Let Λ be a lattice and let $u_1, \ldots, u_d$ be an LLL-reduced basis of Λ. Let $v_1, \ldots, v_d$ be the reciprocal basis of Λ^*, so that

$$\langle u_i, v_j \rangle = \begin{cases} 1 & \text{if } \ i+j = d+1 \\ 0 & \text{otherwise.} \end{cases}$$

Prove that

$$\sum_{k=1}^{d} \|u_k\| \cdot \|v_{d-k+1}\| \ < \ \left(\frac{3}{\sqrt{2}}\right)^d.$$

3*. Let $\Lambda \subset V$ be a lattice and let $u_1, \ldots, u_d$ be an LLL-reduced basis of Λ. Given a point $x \in V$, let us write

$$x = \sum_{k=1}^{d} \mu_k u_k$$

for some real $\mu_1, \ldots, \mu_d$. Let $m_1, \ldots, m_d$ be integers such that

$$|\mu_k - m_k| \ \leq \ \frac{1}{2} \quad \text{for} \quad k = 1, \ldots, d$$

and let

$$u = \sum_{k=1}^{d} m_k u_k.$$

Prove that

$$\|u - x\| \ \leq \ \left(\frac{3}{\sqrt{2}}\right)^d \operatorname{dist}(x, \Lambda).$$

Hint: This result is due to L. Babai, see L. Babai, On Lovász lattice reduction and the nearest lattice point problem, *Combinatorica* **6** (1986), no. 1, 1–13.

4. Let Λ be a lattice and let $u_1, \ldots, u_d$ be an LLL-reduced basis of Λ. Prove that

$$2^{\frac{(1-k)}{2}} \lambda_k(\Lambda) \ \leq \ \|u_k\| \ \leq \ 2^{\frac{(d-1)}{2}} \lambda_k(\Lambda),$$

where $\Lambda_k(\Lambda)$ is the k-th successive minimum of Λ.

Hint: See A.K. Lenstra, H.W. Lenstra Jr. and L. Lovász, Factoring polynomials with rational coefficients, *Mathematische Annalen*, **261**(1982), 515–534.

26. Some applications of the Lenstra - Lenstra - Lovász basis

We sketch below some of the applications.

(26.1) Rational approximations of reals. By Problem 1 of Section 9.2 for any real $\alpha_1, \ldots, \alpha_n$ there exists an arbitrarily large integer $q > 0$ and integers $p_1, \ldots, p_n$ such that

$$\left|\alpha_k - \frac{p_k}{q}\right| \ \leq \ \frac{1}{q^{1+\frac{1}{n}}} \quad \text{for} \quad k = 1, \ldots, n.$$

Using the LLL algorithm, one can construct $p_1, \ldots, p_n$ and q efficiently, so that

$$\left|\alpha_k - \frac{p_k}{q}\right| \ \leq \ \frac{2^{(n+1)/4}}{q^{1+\frac{1}{n}}} \quad \text{for} \quad k = 1, \ldots, n. \tag{26.1.1}$$

Here is how: let us choose a small $\epsilon > 0$ and let us consider the lattice $\Lambda \subset \mathbb{R}^{n+1}$ with the basis $e_1, \ldots, e_n$ and

$$v = \left(-\alpha_1, \ldots, -\alpha_n, \epsilon^{n+1}\right),$$

where $e_1, \ldots, e_n$ is the standard basis vectors. In particular,

$$\det \Lambda = \epsilon^{n+1}.$$

Let us construct an LLL basis of Λ and let u_1 be the first vector of the basis. By Part (3) of Corollary 25.4, we have

$$\|u_1\| \ \leq \ 2^{n/4}\epsilon.$$

We can write

$$u_1 = p_1 e_1 + \ldots + p_n e_n + qv$$

for some integer $p_1, \ldots, p_n$ and q. Hence

$$|p_k - q\alpha_k| \ \leq \ 2^{n/4}\epsilon \quad \text{for} \quad k = 1, \ldots, n \tag{26.1.2}$$

and

$$|q| \ \leq 2^{\frac{n}{4}}\epsilon^{-n}. \tag{26.1.3}$$

If $\epsilon < 2^{-n/4}$ we must have $q \neq 0$ and by switching to $-u_1$, if necessary, we can assure that $q > 0$. From (26.1.3), we have

$$\epsilon \ \leq \ \sqrt{2}q^{-\frac{1}{n}}$$

and from (26.1.2) we deduce (26.1.1). To show that q can be made arbitrarily large, we note that this is certainly the case if all $\alpha_1, \ldots, \alpha_n$ are rational. If some α_k is irrational, then by choosing a sufficiently small $\epsilon > 0$ we can make sure that (26.1.2) does not hold unless q is sufficiently large.

This construction is from A.K. Lenstra, H.W. Lenstra Jr. and L. Lovász, Factoring polynomials with rational coefficients, *Mathematische Annalen*, **261**(1982), 515–534.

(26.2) Testing linear independents over integers. Let $\alpha_1, \ldots, \alpha_n$ be real numbers. We want to find out if there are integers $m_1, \ldots, m_n$, not all equal 0, such that

$$m_1\alpha_1 + \ldots + m_n\alpha_n = 0. \tag{26.2.1}$$

Let $t > 0$ be a real number and let us define

$$\Lambda_t = \left\{ \left(m_1, \ldots, m_n, \ t\sum_{i=1}^{n} \alpha_i m_i \right) : \quad m_1, \ldots, m_n \in \mathbb{Z} \right\}.$$

Then Λ_t is a lattice of rank n (with the ambient space $V_t = \operatorname{span}(\Lambda_t)$). Moreover, if (26.2.1) implies $m_1 = \ldots = m_n = 0$ then

$$\lim_{t \longrightarrow +\infty} \rho(\Lambda_t) = +\infty \tag{26.2.2}$$

whereas if (26.2.1) for some $m_1, \ldots, m_n$, not all equal 0, then the packing radius $\rho(\Lambda_t)$ stays bounded even as t grows. The length of first basis vector u_1 of an LLL basis of Λ approximates the length of the shortest non-zero vector in Λ_t within a factor of $2^{(n-1)/2}$, which is independent of t. This suggests a way to test whether (26.2.2) holds.

In particular, if $\alpha_i = \alpha^{i-1}$ for $i = 1, \ldots, n$, we can check whether α is a root of an integer polynomial with degree $n - 1$. If α is an algebraic number, all the computations can be carried out efficiently in the field $Q(\alpha)$. This, in turn, leads to a polynomial time algorithm for factoring of rational polynomials, see also A.K. Lenstra, H.W. Lenstra Jr. and L. Lovász, Factoring polynomials with rational coefficients, *Mathematische Annalen*, **261**(1982), 515–534.

(26.3) Solving the knapsack problem. Given (large) positive integers $a_1, \ldots, a_n$ and a (large) positive integer b we want to find a subset $S \subset \{1, \ldots, n\}$ such that

$$\sum_{i \in S} a_i = b. \tag{26.3.1}$$

This is a way to encrypt a 0-1 vector x, where $x_i = 1$ if $i \in S$ and $x_i = 0$ if $i \notin S$ by a set $(a_1, \ldots, a_n; b)$ in the "knapsack code".

While the problem is NP-complete in general, the following strategy works under certain circumstances. We define a lattice Λ of rank $n-1$ by

$$\Lambda = \Big\{(m_1, \ldots, m_n, k) \in \mathbb{Z}^{n+1} : \quad m_1 a_1 + \ldots + m_n a_n - kb = 0\Big\},$$

construct an LLL basis and look at the first basis vector u_1. If there is a solution to (26.3.1), by Part (3) of Corollary 25.4, we will have

$$\|u_1\| \leq 2^{(n-1)/2}\sqrt{n+1}$$

and hence every coordinate of u_1 will not exceed $2^{(n-1)/2}$ in the absolute value.

Under a certain "general position" condition, there is a unique 0-1 solution to the equation

$$m_1 a_1 + \ldots + m_n a_n - kb = 0$$

and every solution which is not an integer multiple of that unique solution has at least one coordinate which is bigger than 2^n in the absolute value. This happens, for example, if we choose a subset S, choose $a_1, \ldots, a_n$ independently at random from the interval $[1 : N]$ with $N > 2^{(n+2)n}$ and let $b = \sum_{k \in S} a_k$.

This result is from J.C. Lagarias and A.M. Odlyzko, Solving low-density subset sum problems, *J. Assoc. Comput. Mach.* **32** (1985), no. 1, 229246.

(26.4) Computationally efficient flatness theorem. Given a convex body $K \subset \mathbb{R}^d$ such that $K \cap \mathbb{Z}^d = \emptyset$, we want to construct efficiently a vector $v \in \mathbb{Z}^d$ such that

$$\max_{x \in K}\langle v, x\rangle - \min_{x \in K}\langle v, x\rangle \ \leq \ c(d)$$

for some constant $c(d)$. We don't discuss here how the body K is "given".

Analyzing the proof of the Flatness Theorem (Theorem 21.3), we realize that to construct the required vector $v \in \Lambda^*$ for a given convex body K efficiently, we have to construct the approximating ellipsoid E of K (which can be done though we don't discuss how), apply a linear transformation T which transfers E into a ball and lattice $\mathbb{Z}^d$ into some other lattice Λ, then find a shortest non-zero vector w in Λ^* and let $v = T^*(w)$. If instead of the shortest vector w, we find a reasonably short vector, such as the first vector in an LLL-reduced basis, we get a computationally efficient flatness theorem with a different constant $c(d)$. From Part (2) of Corollary 25.4, we conclude that we can have $c(d) = d^{O(1)}2^{(d+1)/2}$. This is the idea of H.W. Lenstra's polynomial time algorithm in integer programming in fixed dimension, see H.W. Lenstra Jr. Integer programming with a fixed number of variables, *Math. Oper. Res.* **8** (1983), no. 4, 538 – 548.

(26.5) Problem.

1. Construct an efficient (polynomial time) algorithm to find a basis in the lattice Λ of Section 26.3.

27. The algebra of polyhedra and the Euler characteristic

(27.1) Definitions. Let V be Euclidean space. A *polyhedron* $P \subset V$ is the set of solutions to a system of finitely many linear inequalities:

$$P = \Big\{x \in V : \quad \langle c_i, x\rangle \leq \alpha_i \quad \text{for} \quad i \in I\Big\},$$

where I is a finite set, $c_i \in V$ and $\alpha_i \in \mathbb{R}$ for all $i \in I$.

Let us fix a lattice $\Lambda \subset V$. A polyhedron is called Λ-*rational* if $c_i \in \Lambda^*$ and $\alpha_i \in \mathbb{Z}$ for all $i \in I$. In the most common case, we'll have $V = \mathbb{R}^d$ and $\Lambda = \mathbb{Z}^d$, in which case the polyhedron is called *rational*.

For a set $A \subset V$ we define its *indicator* as a function $[A] : V \longrightarrow \mathbb{R}$, where

$$[A](x) = \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{if } x \notin A. \end{cases}$$

We define the *algebra of polyhedra* $\mathcal{P}(V)$ as a vector space (over $\mathbb{R}$) spanned by the indicators $[P]$ of polyhedra $P \subset V$. Similarly, we define the *algebra of rational polyhedra* $\mathcal{P}\left(\mathbb{Q}^d\right)$ as a vector space (over $\mathbb{R}$) spanned by the indicators of rational polyhedra $P \subset \mathbb{R}^d$. We define the *algebra of closed convex sets* $\mathcal{C}(V)$ as a vector space (over $\mathbb{R}$) spanned by the indicators $[A]$ of closed convex sets $A \subset V$ and we define the *algebra of compact convex sets* $\mathcal{C}_b(V)$ as a vector space (over $\mathbb{R}$) spanned by the indicators $[A]$ of compact convex sets $A \subset V$.

Let W be a real vector space. A linear transformation

$$\mathcal{T} : \mathcal{P}(V), \mathcal{P}\left(\mathbb{Q}^d\right), \mathcal{C}(V), \mathcal{C}_b(V) \longrightarrow W$$

is called a *valuation* on the corresponding algebra.

(27.2) Theorem. *There exists a unique valuation $\chi : \mathcal{C}(V) \longrightarrow \mathbb{R}$, called the Euler characteristic, such that $\chi([A]) = 1$ for all non-empty closed convex sets $A \subset V$.*

Proof. Clearly, χ is unique, if exists: we must have

$$\chi(f) = \sum_{i \in I : A_i \neq \emptyset} \alpha_i \quad \text{provided} \quad f = \sum_{i \in I} \alpha_i [A_i], \tag{27.2.1}$$

where $A_i \subset V$ are closed convex sets and $\alpha_i \in \mathbb{R}$.

First, we prove the existence of $\chi : \mathcal{C}_b(V) \longrightarrow \mathbb{R}$ with the required properties. We proceed by induction on $\dim V$. If $\dim V = 0$ then we define $\chi(f) = f(0)$.

Suppose now that $d > 1$. Let us choose a non-zero vector $c \in V$ and let us slice V into affine hyperplanes

$$H_\tau = \Big\{ x \in V : \quad \langle c, x \rangle = \tau \Big\} \quad \text{for} \quad \tau \in \mathbb{R}.$$

Hence each affine hyperplane can be identified with a $(d-1)$-dimensional Euclidean space and there exists the Euler characteristic $\chi_\tau : \mathcal{C}_b(H_\tau) \longrightarrow \mathbb{R}$.

Given a function $f \in \mathcal{C}_b(V)$, we consider its restriction $f_\tau : H_\tau \longrightarrow \mathbb{R}$. We claim that for every $f \in \mathcal{C}_b(V)$ we have $f_\tau \in \mathcal{C}_b(H_\tau)$ and there is a one-sided limit

$$\lim_{\epsilon \longrightarrow 0+} \chi_{\tau-\epsilon}(f_{\tau-\epsilon}).$$

Moreover, we claim that for every $f \in \mathcal{C}_b(V)$ there are at most finitely many values of τ where the one-sided limit is not equal to $\chi_\tau(f_\tau)$.

Indeed,

$$f_\tau = \sum_{i \in I} \alpha_i [A_i \cap H_\tau] \quad \text{provided} \quad f = \sum_{i \in I} \alpha_i [A_i],$$

where $A_i \subset V$ are convex compact sets and $\alpha_i \in \mathbb{R}$, which proves that $f_\tau \in \mathcal{C}_b(H_\tau)$. Given $f \in \mathcal{C}_b(V)$ as above, let

$$J_\tau = \Big\{ i \in I : \quad A_i \neq \emptyset \quad \text{and} \quad \min_{x \in A_i} \langle c, x \rangle = \tau \Big\}.$$

It follows from (27.2.1) that

$$\chi_\tau(f_\tau) - \lim_{\epsilon \longrightarrow 0+} \chi_{\tau-\epsilon}(f_{\tau-\epsilon}) = \sum_{i \in J_\tau} \alpha_i.$$

We define $\chi : \mathcal{C}_b(V) \longrightarrow \mathbb{R}$ by

$$\chi(f) = \sum_{\tau \in \mathbb{R}} \Big(\chi_\tau(f_\tau) - \lim_{\epsilon \longrightarrow 0+} \chi_{\tau-\epsilon}(f_{\tau-\epsilon}) \Big). \tag{27.2.2}$$

The sum (27.2.2) is well-defined since only finitely many terms are non-zero. By the induction hypothesis, it follows that χ is a valuation. Moreover, if $f = [A]$, where $A \subset V$ is a non-empty compact convex set then $\chi([A]) = 1$, since the only non-zero term in (27.2.2) corresponds to $\tau = \min_{x \in A} \langle c, x \rangle$ and equals $1 - 0 = 1$.

It remains to extend χ onto $\mathcal{C}(V)$. Let $B_r \subset V$ denote the closed ball of radius r centered at the origin. For $f \in \mathcal{C}(V)$ we define

$$\chi(f) = \lim_{r \longrightarrow +\infty} \chi(f \cdot [B_r]). \tag{27.2.3}$$

We note that

$$f \cdot [B_r] = \sum_{i: A_i \cap B_r \neq \emptyset} \alpha_i \quad \text{provided} \quad f = \sum_{i \in I} \alpha_i [A_i],$$

from which it follows that $f \cdot [B_r] \in \mathcal{C}_b(V)$ and hence the limit (27.2.3) is well-defined and satisfies (27.2.1). $\square$

(27.3) Problems.

1°. Show that the indicators of closed convex sets in V are not linearly independent if $\dim V \geq 1$.

2°. Check that the spaces $\mathcal{P}(V), \mathcal{P}\left(\mathbb{Q}^d\right), \mathcal{C}(V)$ and $\mathcal{C}_b(V)$ are closed under pointwise multiplication of functions.

3. Prove the inclusion exclusion formula

$$\left[\bigcup_{i=1}^{n} A_i\right] = \sum_{\substack{I \subset \{1, \ldots, n\} \\ I \neq \emptyset}} (-1)^{|I|-1} \left[\bigcap_{i \in I} A_i\right]$$

for sets $A_i \subset V$.

4. Let $A_i, i=1, \ldots, n$ be a family of closed convex sets in V such that $\bigcup_{i=1}^{n} A_i$ is convex. Suppose that the intersection of any $k < n$ sets A_i is not empty. Prove that the intersection of some $k+1$ sets A_i is not empty.

5. Let $\Delta \subset \mathbb{R}^n$ be the standard $(n-1)$-dimensional simplex defined by the equation $x_1 + \ldots + x_n = 1$ and inequalities $x_i \geq 0$ for $i = 1, \ldots, n$. For $i = 1, \ldots, n$, let let $F_i \subset \Delta$ be the facet of Δ defined by the equation $x_i = 0$. Let $A_1, \ldots, A_n \subset \mathbb{R}^n$ be closed convex sets such that

$$\Delta \ \subset \ \bigcup_{i=1}^{n} A_i \quad \text{and} \quad A_i \cap F_i = \emptyset \quad \text{for} \quad i = 1, \ldots, n.$$

Prove that

$$\bigcap_{i=1}^{n} A_i \neq \emptyset.$$

6. Let $P \subset V$ be a bounded polyhedron with a non-empty interior $\operatorname{int} P$. Prove that $[\operatorname{int} P] \in \mathcal{P}(V)$ and that $\chi([\operatorname{int} P]) = (-1)^d$, where $d = \dim V$.

Hint: Use (27.2.2).

7*. For an affine hyperplane $H = \big\{x \in V : \ \langle c, x \rangle = \alpha\big\}$, where $c \neq 0$, let us define the closed halfspaces

$$H_+ = \big\{x \in V : \quad \langle c, x \rangle \geq \alpha\big\} \quad \text{and} \quad H_- = \big\{x \in V : \quad \langle c, x \rangle \leq \alpha\big\}.$$

Let W be a real vector space and suppose that with every polyhedron $P \subset V$ we associate an element $\phi(P) \in W$ such that

$$\phi(P) = \phi(P \cap H_+) + \phi(P \cap H_-) - \phi(P \cap H)$$

for every affine hyperplane H. Prove that there is a valuation $\Phi : \mathcal{P}(V) \longrightarrow W$ such that $\Phi([P]) = \phi(P)$ for every polyhedron $P \subset V$.

(28.1) Definition. A linear transformation $T : \mathbb{R}^n \longrightarrow \mathbb{R}^m$ is called *rational*, if the matrix of T in the standard bases of $\mathbb{R}^n$ and $\mathbb{R}^m$ is rational.

(28.2) Lemma. *Let $T : \mathbb{R}^d \longrightarrow \mathbb{R}^{d-1}$ be the projection*

$$T(x_1, \ldots, x_d) = (x_1, \ldots, x_{d-1}).$$

If $P \subset \mathbb{R}^d$ is a (rational) polyhedron then $T(P) \subset \mathbb{R}^{d-1}$ is a (rational) polyhedron.

Proof. Suppose that P is defined by a system of linear inequalities

$$\sum_{j=1}^{d} a_{ij} x_j \ \leq \ b_i \quad \text{for} \quad i = 1, \ldots, n.$$

Let

$$I_+ = \{i : \ a_{id} > 0\}, \quad I_- = \{i : \ a_{id} < 0\} \quad \text{and} \quad I_0 = \{i : \ a_{id} = 0\}.$$

Then, for $x = (x_1, \ldots, x_{d-1})$ we have $x \in T(P)$ if and only if

$$\sum_{j=1}^{d-1} a_{ij} x_j \ \leq \ b_i \quad \text{for all} \quad i \in I_0 \tag{28.2.1}$$

and there exists $x_d \in \mathbb{R}^d$ such that

$$x_d \ \leq \ \frac{b_i}{a_{id}} - \sum_{j=1}^{d-1} \frac{a_{ij}}{a_{id}} x_j \quad \text{for all} \quad i \in I_+ \quad \text{and}$$
$$x_d \ \geq \ \frac{b_i}{a_{id}} - \sum_{j=1}^{d-1} \frac{a_{ij}}{a_{id}} x_j \quad \text{for all} \quad i \in I_-.$$

Hence $x \in T(P)$ if and only if (28.2.1) holds and

$$\frac{b_{i_1}}{a_{i_1 d}} - \sum_{j=1}^{d-1} \frac{a_{i_1 j}}{a_{i_1 d}} x_j \ \leq \ \frac{b_{i_2}}{a_{i_2 d}} - \sum_{j=1}^{d-1} \frac{a_{i_2 j}}{a_{i_2 d}} \quad \text{for every} \quad i_i \in I_-, \ i_2 \in I_+. \tag{28.2.2}$$

If I_0 is empty then there are no equations (28.2.1) and if either of I_- and I_+ is empty then there are no equations (28.2.2).

The proof now follows. $\square$

(28.3) Theorem. *Let $T : V \longrightarrow W$ be a linear transformation. Then for every polyhedron $P \subset V$ the image $T(P) \subset W$ is a polyhedron. Furthermore, there is a unique valuation $\mathcal{T} : \mathcal{P}(V) \longrightarrow \mathcal{P}(W)$ such that $\mathcal{T}([P]) = [T(P)]$ for any polyhedron $P \subset V$.*

If $V = \mathbb{R}^n$, $W = \mathbb{R}^m$ and $T : \mathbb{R}^n \longrightarrow \mathbb{R}^m$ is a rational linear transformation and if $P \subset \mathbb{R}^n$ is a rational polyhedron then $T(P) \subset \mathbb{R}^m$ is a rational polyhedron.

Proof. If $T : V \longrightarrow W$ is an isomorphism and

$$P = \Big\{ x \in V : \quad \langle c_i, x \rangle \ \leq \ \alpha_i \quad \text{for} \quad i \in I \Big\}$$

then

$$T(P) = \Big\{ y \in W : \quad \big\langle \left(T^*\right)^{-1} c_i, \ y \big\rangle \ \leq \ \alpha_i \quad \text{for} \quad i \in I \Big\}$$

is a polyhedron. Furthermore, if T is rational and P is rational then $T(P)$ is rational.

If $T : V \longrightarrow W$ satisfies $\ker T = \{0\}$ and hence $T : V \longrightarrow \operatorname{image} T$ is an isomorphism. Hence if $P \subset V$ is a polyhedron then $T(P)$ is a polyhedron. If T and P are rational then $T(P)$ is rational.

Finally, if $T : V \longrightarrow W$ is an arbitrary linear transformation then T is a composition of a linear transformation $V \longrightarrow W \oplus V$, $x \longmapsto (Tx, x)$ with the trivial kernel and a sequence of the coordinate projections $W \oplus V \longrightarrow W$. Using Lemma 28.2, we conclude that if P is a (rational) polyhedron and T is a (rational) linear transformation, then $T(P)$ is (rational) polyhedron.

Clearly, $\mathcal{T} : \mathcal{P}(V) \longrightarrow \mathcal{P}(W)$ is unique, if it exists. To prove existence, we note that for any $f \in \mathcal{P}(V)$ and any $x \in W$ we have

$$f \cdot \left[T^{-1}(x)\right] = \sum_{i \in I} \alpha_i \left[A_i \cap T^{-1}(x)\right] \quad \text{where} \quad f = \sum_{i \in I} \alpha_i \left[A_i\right]$$

and $A_i \subset V$ are polyhedra and $\alpha_i \in \mathbb{R}$ are reals. Hence $f \cdot \left[T^{-1}(x)\right] \in \mathcal{P}(V)$ and we define

$$h = \mathcal{T}(f) \quad \text{where} \quad h(x) = \chi\big(f \cdot \left[T^{-1}(x)\right]\big). \tag{28.3.1}$$

It is straightforward to check that $\mathcal{T}([A]) = [T(A)]$ for a polyhedron $A \subset V$ and hence $\mathcal{T} : \mathcal{P}(V) \longrightarrow \mathcal{P}(W)$ is the required valuation. □

(28.4) Problems.

1. Let $T : V \longrightarrow W$ be a linear transformation. Prove that if $A \subset V$ is a compact convex set then $T(A) \subset W$ is a compact convex set and that there exists a unique valuation $\mathcal{T} : \mathcal{C}_b(V) \longrightarrow \mathcal{C}_b(W)$ such that $\mathcal{T}([A]) = [T(A)]$ for any non-empty compact convex set $A \subset V$.

2. Construct an example of a linear transformation $T : \mathbb{R}^2 \longrightarrow \mathbb{R}$ and a closed convex set $A \subset \mathbb{R}^2$ such that $T(A)$ is not closed.

(29.1) Definition. Let V be a vector space and let $A, B \subset V$ be sets. The *Minkowski sum* of A and B is defined as the set

$$A + B = \Big\{ a + b : \quad a \in A,\ b \in B \Big\}.$$

(29.2) Theorem. *Let V be Euclidean space.*

(1) *If $P_1, P_2 \subset V$ are polyhedra then $P_1 + P_2$ is a polyhedron.*

(2) *There exists a unique bilinear operation*

$$* : \quad \mathcal{P}(V) \times \mathcal{P}(V) \longrightarrow \mathcal{P}(V),$$

called convolution, such that $[P_1] * [P_2] = [P_1 + P_2]$ for any two non-empty polyhedra $P_1, P_2 \subset V$.

Proof. Let $P_1, P_2 \subset V$ be polyhedra. Let us consider the set $P_1 \times P_2 \subset V \oplus V$ defined by

$$P_1 \times P_2 = \Big\{ (x, y) : \quad x \in P_1,\ y \in P_2 \Big\}.$$

Clearly, P is a polyhedron.

Let us consider a linear transformation

$$T : V \oplus V \longrightarrow V, \quad T(x, y) = x + y. \tag{29.2.1}$$

Then $P_1 + P_2 = T(P_1 \times P_2)$ and hence $P_1 + P_2$ is a polyhedron by Theorem 28.3.

Clearly, convolution $*$ is unique, if exists. For functions $f, g \in \mathcal{P}(V)$, we define

$$f \times g : V \oplus V \longrightarrow \mathbb{R} \quad \text{where} \quad (f \times g)(x, y) = f(x) g(y).$$

Hence if

$$f = \sum_{i \in I} \alpha_i \, [P_i] \quad \text{and} \quad g = \sum_{j \in J} \beta_j \, [Q_j]$$

then

$$f \times g = \sum_{\substack{i \in I \\ j \in J}} \alpha_i \beta_j \, [P_i \times Q_j] \,,$$

from which it follows that $f \times g \in \mathcal{P}(V \oplus V)$.

Let $\mathcal{T} : \mathcal{P}(V \oplus V) \longrightarrow \mathcal{P}(V)$ be the valuation associated with linear transformation (29.2.1) via Theorem 28.3. We define

$$f * g = \mathcal{T}(f \times g).$$

$\square$

(29.3) Problems.

1°. Let $T : V \longrightarrow W$ be a linear transformation and let $\mathcal{T} : \mathcal{P}(V) \longrightarrow \mathcal{P}(W)$ be the associated valuation. Prove that $\mathcal{T}(f * g) = \mathcal{T}(f) * \mathcal{T}(g)$.

2°. Prove that $f * [0] = f$ for all $f \in \mathcal{P}(V)$.

3*. Let $P \subset \mathbb{R}^d$ be a bounded polyhedron with a non-empty interior $\operatorname{int} P$. Prove that

$$[P] * [-\operatorname{int} P] = (-1)^d [0],$$

where $-X = \{-x : \ x \in X\}$.

4. Prove that the Minkowski sum of compact convex sets is a compact convex set and that there exists a unique bilinear operation $* : \mathcal{C}_b(V) \times \mathcal{C}_b(V) \longrightarrow \mathcal{C}_b(V)$, called convolution, such that $[A] * [B] = [A + B]$ for any non-empty convex compact sets $A, B \subset V$.

5*. Let $\{A_i \subset V : \ i \in I\}$ be a finite family of convex compact sets and let $\{\alpha_i : \ i \in I\}$ be a finite family of real numbers such that

$$\sum_{i \in I} \alpha_i \, [A_i] = 0.$$

Prove that

$$\sum_{i: \ \alpha_i > 0} \alpha_i A_i = \sum_{i: \ \alpha_i < 0} (-\alpha_i) A_i,$$

where $\alpha X = \Big\{ \alpha x : \ x \in X \Big\}$ and the sums on both sides are the Minkowski sums.

30. The structure of polyhedra

(30.1) Definitions. Let V be a vector space and let $a, u \in V$ be vectors, where $u \neq 0$. The *ray emanating from a in the direction of u* is the set

$$\Big\{ a + tu : \quad t \geq 0 \Big\}.$$

The *line through a in the direction of u* us the set

$$\Big\{ a + tu : \quad t \in \mathbb{R} \Big\}.$$

Recall that the *interval with the endpoints a and b* is the set

$$[a, b] = \Big\{ ta + (1 - t)b : \quad 0 \leq t \leq 1 \Big\},$$

where $a, b \in V$.

A point $a \in P$ is called a *vertex* of a polyhedron P if whenever $a = (b + c)/2$ where $b, c \in P$, we must have $a = b = c$.

A point $b \in V$ is a *convex combination* of a finite set of points $\{a_i : \ i \in I\} \subset V$ if b can be written as

$$b = \sum_{i \in I} \lambda_i a_i \quad \text{where} \quad \sum_{i \in I} \lambda_i = 1 \quad \text{and} \quad \lambda_i \geq 0 \quad \text{for all} \quad i \in I.$$

The set of all convex combinations of points from a given set $A \subset V$ is called the *convex hull* of A and denoted $\operatorname{conv}(A)$. The convex hull of a finite set is called a *polytope.*

(30.2) Lemma. *Let V be Euclidean space and let $P \subset V$ be a polyhedron. Then P is unbounded if and only if it contains a ray.*

Proof. Clearly, if P contains a ray then P is unbounded. Suppose that

$$P = \Big\{ x \in V : \quad \langle c_i, x \rangle \leq \alpha_i, \ i \in I \Big\}.$$

Since P is unbounded, there is a sequence of points $x_n \in P$, $n = 1, 2, \ldots$ such that $\|x_n\| \longrightarrow +\infty$. Let $y_n = x/\|x_n\|$. Then $\|y_n\| = 1$ and hence there exists a unit vector $u \in V$ which is a limit point of the sequence $\{y_n\}$. Then necessarily $\langle c_i, u \rangle \leq 0$ for all $i \in I$ and hence for any $a \in P$ the ray emanating from a in the direction of u lies in P. □

(30.3) Lemma. *A polytope is a polyhedron. The convex hull of a finite set of rational points (that is, points with rational coordinates) in $\mathbb{R}^d$ is a rational polyhedron.*

Proof. Let $P = \operatorname{conv}(v_1, \ldots, v_n)$, where $v_1, \ldots, v_n \in V$ are points. Let $\Delta \subset \mathbb{R}^n$ be the standard simplex defined by the equation $x_1 + \ldots + x_n = 1$ and inequalities $x_i \geq 0$ for $i = 1, \ldots, n$. Then Δ is a polyhedron and also a polytope that is the convex hull of the standard basis vectors $e_1, \ldots, e_n$. Let us define a linear transformation $T : \mathbb{R}^n \longrightarrow V$ by $T(e_i) = v_i$ for $i = 1, \ldots, n$. Then $P = T(\Delta)$ and the proof follows by Theorem 28.3. □

(30.4) Lemma. *Let $P \subset V$ be a non-empty polyhedron. Then P contains a vertex if and only if P does not contain a line.*

Proof. Let $P = \big\{ x \in V : \ \langle c_i, x \rangle \leq \alpha_i, \ i \in I \big\}$ be a polyhedron. Suppose that P contains a line in the direction u. Then $\langle c_i, u \rangle = 0$ for all $i \in I$. If $x \in P$ is a point then $x \pm u \in P$ and $x = \big((x+u) + (x-u) \big)/2$, which proves that x is not a vertex.

To prove that if P does not contain lines it contains a vertex, we proceed by induction on $\dim V$. If $\dim V \leq 1$, the statement is clear. If $\dim V > 1$, let us consider a line l having a non-empty intersection with P. Since $l \not\subset P$, the intersection $P \cap l$ is either a ray emanating from some point $a \in P$ or an interval with an endpoint $a \in P$. In any case, we must have $\langle c_j, a \rangle = \alpha_j$ for some $j \in I$. Let $Q = P \cap H$, where $H \subset V$ is the affine hyperplane defined by the equation $\langle c_j, x \rangle = \alpha_j$. Identifying H with a $(d-1)$-dimensional Euclidean space, we conclude that there is a vertex v of Q. Suppose that $v = (u+w)/2$, where $u, w \in P$. Since $\langle c_j, u \rangle, \langle c_j, w \rangle \leq \alpha_j$ and $\langle c, v \rangle = \alpha_j$ we must have $\langle c_j, u \rangle = \langle c_j, w \rangle = \alpha_j$ and hence $u, w \in Q$. Therefore, $u = w$ and v is a vertex of Q. □

(30.5) Lemma. *Let*

$$P = \Big\{ x \in V : \quad \langle c_i, x \rangle \leq \alpha_i, \ i \in I \Big\}$$

be a polyhedron and let $v \in P$ be a point. Let

$$I_v = \Big\{ i \in I : \quad \langle c_i, v \rangle = \alpha_i \Big\}$$

(the inequalities indexed by $i \in I_v$ are called active on v). Then v is a vertex of P if and only if $\operatorname{span}\Big(c_i : \ i \in I_v\Big) = V$*. In particular, the set of vertices of a polyhedron is finite and if P is a rational polyhedron then the vertices of P are rational points.*

Proof. Suppose that $v = (u + w)/2$ for some $u, w \in P$. Since $\langle c_i, u \rangle, \langle c_i, w \rangle \leq \alpha_i$ and $\langle c_i, v \rangle = \alpha_i$ for $i \in I_v$, we must have $\langle c_i, u \rangle = \langle c_i, w \rangle = \alpha_i$ for all $i \in I_v$. Hence if $\operatorname{span}\Big(c_i : \ i \in I_v\Big) = V$ then necessarily $u = w = v$ and v is a vertex. If $\operatorname{span}\Big(c_i : \ i \in I_v\Big) \neq V$ then there is a $u \neq 0$ such that $\langle c_i, u \rangle = 0$ for all $i \in I_v$. Then for a sufficiently small $\epsilon > 0$ we have $v \pm \epsilon u \in P$ and $v = \big((v + \epsilon u) + (v - \epsilon u)\big)/2$ and hence v is not a vertex. $\square$

(30.6) Lemma. *Let $P \subset V$ be a bounded polyhedron. Then P is the convex hull of the set of its vertices and hence is a polytope.*

Proof. By Lemma 30.5, the set of vertices of P is finite and hence the convex hull of the set of vertices is a polytope. It remains to prove that every point $y \in P$ can be written as a convex combination of vertices of P. We proceed by induction of $\dim V$. If $\dim V = 0$, the result is clear. Suppose that $\dim V > 0$ and let

$$P = \Big\{ x \in V : \quad \langle c_i, x \rangle \leq \alpha_i, \ i \in I \Big\}.$$

If $\langle c_j, y \rangle = \alpha_j$ for some $j \in I$, we consider the affine hyperplane H defined by the equation $\langle c_j, x \rangle = \alpha_j$ and let $Q = P \cap H$. By the induction hypothesis, x is a convex combination of vertices of Q and, arguing as in the proof of Lemma 30.4, we conclude that the vertices of Q are also vertices of P.

If $\langle c_i, y \rangle < \alpha_i$ for all $i \in I$, we consider a line l through y. Since P is bounded, the intersection $l \cap P$ is an interval $[a, b]$ where $y \in [a, b]$ and $\langle c_j, a \rangle = \alpha_j$ and $\langle c_k, b \rangle = \alpha_k$ for some $j, k \in I$. Arguing as above, we prove that a and b are convex combinations of vertices of P and so is y. $\square$

(30.7) Definition. Let $K \subset V$ be a polyhedron. Then K is called a *polyhedral cone* (or just a *cone*) if $0 \in K$ and for every $x \in K$ and $\lambda \geq 0$ we have $\lambda x \in K$. Equivalently, K is a polyhedral cone, if

$$K = \Big\{ x \in V : \quad \langle c_i, x \rangle \leq 0, \ i \in I \Big\},$$

where I is a finite set.

(30.8) Lemma. *Let*

$$K = \Big\{ x \in V : \quad \langle c_i, x \rangle \leq 0, \ i \in I \Big\}$$

be a polyhedral cone and let

$$c = \sum_{i \in I} c_i.$$

Suppose that $K \neq \{0\}$ and that K does not contain lines. Then

(1) *For any $x \in K \setminus \{0\}$ we have $\langle c, x \rangle < 0$;*
(2) *Let $Q = \Big\{ x \in K : \quad \langle c, x \rangle = -1 \Big\}$. Then Q is a polytope and every vector $x \in K \setminus \{0\}$ can be uniquely written as $x = \lambda y$ for some $\lambda > 0$ and $y \in Q$;*
(3) *The set W of vectors $w \in V$ such that $\langle w, x \rangle < 0$ for all $x \in K \setminus \{0\}$ is non-empty and open.*

Proof. Clearly, $\langle c, x \rangle \leq 0$ for all $x \in K$. Suppose that $\langle c, x \rangle = 0$ for some $x \neq 0$. Then $\langle c_i, x \rangle = 0$ for all $i \in I$ and K contains a line through the origin in the direction of x, which is a contradiction. This also proves that $x = \lambda y$ for some $\lambda > 0$ and $y \in Q$. Hence it remains to prove that Q is a polytope. Clearly, Q is a polyhedron and in view of Lemma 30.3 it remains to show that Q is bounded. In view of Lemma 30.2, it suffices to show that Q does not contain rays. Indeed, if Q contains a ray in the direction of u for some $u \neq 0$ then we must have $\langle c_i, u \rangle \leq 0$ for all $i \in I$ and $\langle c, u \rangle = 0$, from which it follows that $\langle c, u_i \rangle = 0$ for all $i \in I$ and K contains a line in the direction of u, which is a contradiction.

The set W is non-empty since it contains c. Moreover, by Part (2) we have $w \in W$ if and only if $\langle w, v \rangle < 0$ for every vertex v of Q, from which W is open. $\square$

(30.9) Theorem. *Let $P \subset V$ be a non-empty polyhedron not containing lines and let*

$$K_P = \Big\{ u \in V : \quad x + \lambda u \in V \quad \textit{for all} \quad x \in P \quad \textit{and all} \quad \lambda \geq 0 \Big\}.$$

Let R be the polytope that is the convex hull of the set of vertices of P. Then K_P is a polyhedral cone without lines, called the recession cone of P and $P = K + R$.

Proof. Suppose that

$$P = \Big\{ x \in V : \quad \langle c_i, x \rangle \leq \alpha_i, \ i \in I \Big\}.$$

It is easy to check that

$$K_P = \Big\{ x \in V : \quad \langle c_i, x \rangle \leq 0, \ i \in I \Big\},$$

so K_P is indeed a polyhedral cone. Since P does not contain lines, K_P does not contain lines as well.

Clearly, $K + R \subset P$. It remains to show that every point $a \in P$ can be written as a sum of $x = u + b$ where $b \in R$ and $u \in K$. We proceed by induction on $\dim V$. If $\dim V = 0$, the result is clear. Let us assume that $\dim V > 0$. If $K_P = \{0\}$ then by Lemma 30.2 polyhedron P is bounded and the result follows by Lemma 30.6. If $K_P \neq \{0\}$, let us choose $u \in K_P \setminus \{0\}$. Then the intersection of a line through a in the direction of u with P is a ray $y + tu$, $t \geq 0$, where $\langle c_j, y \rangle = \alpha_j$ for some $j \in I$. Let H be the affine hyperplane defined by the equation $\langle c_j, x \rangle = \alpha_j$ and let $Q = P \cap H$. By the induction hypothesis, we can write $y = b + w$, where b is a convex combination of vertices of Q and $w \in K_Q$. As in the proof of Lemma 30.4, the vertices of Q are also vertices of P and hence $b \in R$. It is not hard to see that $K_Q \subset K_P$ and hence $w \in K_P$. Finally, we can write $a = y + w + tu$ for some $t \geq 0$. Since $w + ty \in K_P$, the proof follows. □

(30.10) Problems.

Let $A \subset V$ be a closed convex set. A set $F \subset A$ is called a *face* of A if there is a vector $c \in V$ and a number $\alpha \in \mathbb{R}$ such that $\langle c, x \rangle \leq \alpha$ for all $x \in A$ and $F = \big\{x \in V: \ \langle c, x \rangle = \alpha\big\}$.

1. Prove that a polyhedron has finitely many faces.

2*. Prove that if a closed convex set $A \subset V$ has finitely many faces then A is a polyhedron.

3. Let $P_1, P_2 \subset V$ be non-empty polyhedra and let $P = P_1 + P_2$. Prove that every face F of P can be written as $F = F_1 + F_2$ where F_1 is a face of P_1 and F_2 is a face of P_2.

4. Let $P_1, P_2 \subset V$ be non-empty polyhedra and let $P = P_1 \cap P_2$. Prove that every vertex v of P can be written as $v = F_1 \cap F_2$, where F_1 is a face of P_1, F_2 is a face of P_2 and $\dim F_1 + \dim F_2 \leq \dim V$.

31. Rational generating functions for integer points in polyhedra

(31.1) Definitions. For an integer point $m = (m_1, \ldots, m_d)$ and a vector $\mathbf{x} = (x_1, \ldots, x_d)$ we denote

$$\mathbf{x}^m = x_1^{m_1} \cdots x_d^{m_d},$$

a Laurent monomial in $x_1, \ldots, x_d$.

For a vector $c = (c_1, \ldots, c_d)$, we denote

$$\mathbf{e}^c = \left(e^{c_1}, \ldots, e^{c_d}\right).$$

(31.2) Lemma. *Let $u_1, \ldots, u_k \in \mathbb{Z}^d$ be linearly independent vectors and let*

$$K = \left\{ \sum_{i=1}^k \alpha_i u_i : \quad \alpha_i \geq 0 \quad \textit{for} \quad i = 1, \ldots, k \right\}$$

(such a set K is called a simple rational cone). Let

$$\Pi = \left\{ \sum_{i=1}^{k} \alpha_i u_i : \quad 0 \leq \alpha_i < 1 \quad \textit{for} \quad i = 1, \ldots, k \right\}.$$

Then the set

$$W = \left\{ \mathbf{x} \in \mathbb{C}^d : \quad |\mathbf{x}^{u_i}| < 1 \quad \textit{for} \quad i = 1, \ldots, k \right\}$$

is non-empty and open and for all $\mathbf{x} \in W$ the series

$$\sum_{m \in K \cap \mathbb{Z}^d} \mathbf{x}^m$$

converges absolutely and uniformly on compact subsets of W to a rational function

$$f(K, \mathbf{x}) = \left(\sum_{n \in \Pi \cap \mathbb{Z}^d} \mathbf{x}^n \right) \prod_{i=1}^{k} \frac{1}{1 - \mathbf{x}^{u_i}}.$$

Proof. Clearly, W is open. Since vectors $u_1, \ldots, u_k$ are linearly independent, there exists a $c \in \mathbb{R}^d$ such that $\langle c, u_i \rangle < 0$ for $i = 1, \ldots, k$. Then $\mathbf{e}^c \in W$, so W is non-empty.

We claim that every point $m \in K \cap \mathbb{Z}^d$ can be uniquely written as

$$m = n + \sum_{i=1}^{k} \mu_i u_i \tag{31.2.1}$$

for some $n \in \Pi \cap \mathbb{Z}^d$ and non-negative integers $\mu_1, \ldots, \mu_k$.

Indeed, given

$$m = \sum_{i=1}^{k} \alpha_i u_i \quad \text{where} \quad \alpha_i \geq 0 \quad \text{for} \quad i = 1, \ldots, k$$

we let

$$\mu_i = \lfloor \alpha_i \rfloor \quad \text{for} \quad i = 1, \ldots, k$$

and

$$n = \sum_{i=1}^{k} \{\alpha_i\} u_i = m - \sum_{i=1}^{k} \mu_i u_i$$

cf. also the proof of Theorem 3.1. Note that n is a difference of two integer vectors and hence is an integer vector and that $n \in \Pi$ since $0 \leq \{\alpha_i\} < 1$ for $i = 1, \ldots, k$. The representation (31.2.1) is unique since if

$$m = n_1 + \sum_{i=1}^{k} \mu_i u_i = n_2 + \sum_{i=1}^{k} \lambda_i u_i,$$

where $n_1, n_2 \in \Pi$ and λ_i, μ_i are non-negative integers then $n_1 - n_2$ is an integer combination of $u_1, \ldots, u_k$. On the other hand,

$$n_1 - n_2 = \sum_{i=1}^{k} \beta_i u_i \quad \text{where} \quad -1 < \beta_i < 1 \quad \text{for} \quad i = 1, \ldots, k.$$

Since vectors $u_1, \ldots, u_k$ are linearly independent, we conclude that $\beta_i = 0$ for $i = 1, \ldots, k$. Therefore, $n_1 = n_2$ and hence $\lambda_i = \mu_i$ for $i = 1, \ldots, k$.

Therefore, we have the identity of formal power series

$$\begin{aligned}\sum_{m \in K \cap \mathbb{Z}^d} \mathbf{x}^m &= \left(\sum_{n \in \Pi \cap \mathbb{Z}^d} \mathbf{x}^n \right) \sum_{\substack{\mu_1, \ldots, \mu_k \in \mathbb{Z} \\ \mu_1, \ldots, \mu_k \geq 0}} \mathbf{x}^{\mu_1 u_1 + \ldots + \mu_k u_k} \\ &= \left(\sum_{n \in \Pi \cap \mathbb{Z}^d} \mathbf{x}^n \right) \prod_{j=1}^{k} \sum_{\substack{\mu \in \mathbb{Z} \\ \mu \geq 0}} \mathbf{x}^{\mu u_j}.\end{aligned} \tag{31.2.2}$$

Now we observe that (31.1.2) converges absolutely for all $\mathbf{x} \in W$ and uniformly on compact subsets of W. □

(31.3) Lemma. *Let*

$$K = \Big\{ x \in \mathbb{R}^d : \quad \langle c_i, x \rangle \leq 0, \ i = 1, \ldots, k \Big\},$$

where $c_i \in \mathbb{Z}^d$ for $i = 1, \ldots, k$, a rational cone without lines. Then there are points $u_1, \ldots, u_n \in K \cap \mathbb{Z}^d$ such that the set

$$W = \big\{ \mathbf{x} \in \mathbb{C}^d : \quad |\mathbf{x}^{u_i}| < 1 \quad \textit{for} \quad i = 1, \ldots, n \big\}$$

is non-empty and open and for all $\mathbf{x} \in W$ the series

$$\sum_{m \in K \cap \mathbb{Z}^d} \mathbf{x}^m$$

converges absolutely and uniformly on compact subsets of W to a rational function

$$f(\mathbf{x}) = \sum_{j \in J} \epsilon_j \frac{p_j(\mathbf{x})}{q_j(\mathbf{x})},$$

where $\epsilon_j = \pm 1$,

$$p_j(\mathbf{x}) = \sum_{n \in A_j} \mathbf{x}^n \quad \textit{and} \quad q_j(\mathbf{x}) = \prod_{i \in B_j} (1 - \mathbf{x}^{u_i})$$

for some finite sets $A_j \subset K \cap \mathbb{Z}^d$ and $B_j \subset \{1, \ldots, n\}$, where $|B_j| \leq d$.

Sketch of Proof. Without loss of generality we assume that $K \neq \{0\}$. Let

$$c = \sum_{i=1}^{k} c_i$$

and let

$$Q = \Big\{x \in K : \quad \langle c, x \rangle = -1\Big\}.$$

We note that Q is a polytope with rational vertices and by Lemma 30.8 every $x \in K \setminus \{0\}$ can be uniquely written as $x = \lambda y$ for some $y \in Q$ and $\lambda > 0$. Scaling $Q' = tQ$ for some integer t we obtain a polytope Q' with integer vertices $u_1, \ldots, u_n$ and such that every $x \in K \setminus \{0\}$ can be uniquely written as $x = \lambda y$ for some $y \in Q'$ and $\lambda > 0$. Triangulating Q' we represent K as a union of simple rational cones as in Lemma 31.2. By Lemma 30.8 there is a vector $c \in \mathbb{R}^d$ such that $\langle c, u_i \rangle < 0$ for all $i = 1, \ldots, k$. Then $\mathbf{e}^c \in W$, so W is non-empty. Clearly, W is open. The proof now follows from Lemma 31.2 and the inclusion-exclusion formula. $\square$

(31.4) Lemma. *Let $P \subset \mathbb{R}^d$ be a rational polyhedron without lines. Then there exists a non-empty open set $U \subset \mathbb{C}^d$ such that for every $\mathbf{x} \in U$ the series*

$$\sum_{m \in P \cap \mathbb{Z}^d} \mathbf{x}^m$$

converges absolutely and uniformly on compact subsets of W to a rational function

$$f(P, \mathbf{x}) = \sum_{i \in I} \frac{p_i(\mathbf{x})}{q_i(\mathbf{x})},$$

where $p_i(\mathbf{x})$ are Laurent polynomials in $\mathbf{x}$ and $q_i(\mathbf{x}) = (1 - \mathbf{x}^{u_{i1}}) \cdots (1 - \mathbf{x}^{u_{ik}})$ for some vectors $u_{ij} \in \mathbb{Z}^d \setminus \{0\}$.

Proof. Let us identify $\mathbb{R}^d$ with the affine hyperplane H defined by the equation $x_{d+1} = 1$ in $\mathbb{R}^{d+1}$. Let

$$P = \Big\{x \in \mathbb{R}^d : \quad \langle c_i, x \rangle \leq \alpha_i, \ i = 1, \ldots n\Big\},$$

where $c_i \in \mathbb{Z}^d$ and $\alpha_i \in \mathbb{Z}$ for $i = 1, \ldots, d$. Let us define a rational cone $K \subset \mathbb{R}^{d+1}$ as

$$K = \Big\{(x, \tau) : \quad \langle c_i, x \rangle - \alpha_i \tau \ \leq \ 0 \quad \text{for} \quad i = 1, \ldots, n \quad \text{and} \quad \tau \geq 0\Big\}.$$

Then $P = K \cap H$.

We claim that K does not contain lines. Indeed, if K contains a line in the direction $u = (u, \beta)$, for some $u \in \mathbb{R}^d$ and some $\beta \in \mathbb{R}$, we must have $\beta = 0$ since the last coordinate of every point in K is non-negative. Hence $u \neq 0$ and we must have $\langle c_i, u \rangle = 0$ for $i = 1, \ldots, n$. This, however, contradicts the assumption that P contains no lines.

We apply Lemma 31.3 to K. We note that the last coordinate of every integer point $n \in K$ is non-negative. Therefore, if a particular point $\mathbf{z} = (\mathbf{x}, y)$ lies in the non-empty open set $W \subset \mathbb{C}^{d+1}$, the existence of which is asserted by Lemma 31.3, then any point $(\mathbf{x}, \tilde{y})$ with $|\tilde{y}| \leq |y|$ lies in W as well. We define $U \subset \mathbb{C}^d$ as the projection of W onto the first d coordinates and conclude that

$$f(P, \mathbf{x}) = \frac{\partial}{\partial y} f\big(K, (\mathbf{x}, y)\big)\Big|_{y=0}.$$

$\square$

The following remarkable result was proved by A. Khovanskii and A. Pukhlikov, and, independently, by J. Lawrence in early 1990s.

(31.5) Theorem. *Let $R(\mathbf{x})$ be the real vector space of rational functions in $\mathbf{x} \in \mathbb{C}^d$ and let $\mathcal{P}\left(\mathbb{Q}^d\right)$ be the algebra of rational polyhedra. There exists a valuation*

$$\mathcal{F} : \mathcal{P}\left(\mathbb{Q}^d\right) \longrightarrow R(\mathbf{x})$$

such that

(1) *If $P \subset \mathbb{R}^d$ is a rational polyhedron without lines then $\mathcal{F}([P]) = f(P, \mathbf{x})$, where $f(P, \mathbf{x})$ is a rational function of Lemma 31.4;*
(2) *If $P \subset \mathbb{R}^d$ is a rational polyhedron with lines then $\mathcal{F}([P]) = 0$.*

Proof. First, we claim that $\mathcal{P}\left(\mathbb{Q}^d\right)$ is spanned by the indicators $[P]$, where $P \subset \mathbb{R}^d$ is a rational polyhedron not containing lines. To establish this, it suffices to show that the indicator $[P]$ of any rational polyhedron $P \subset \mathbb{R}^d$ is a linear combination of indicators of polyhedra without lines.

Let us represent

$$\left[\mathbb{R}^d\right] = \sum_{i \in I} \epsilon_i \left[Q_i\right] \tag{31.5.1}$$

where $\epsilon_i \in \{-1, 1\}$ and $Q_i \subset \mathbb{R}^d$ are rational polyhedra without lines (for example, we can cut $\mathbb{R}^d$ into orthants and use the inclusion-exclusion formula). Then

$$[P] = [P] \cdot \left[\mathbb{R}^d\right] = \sum_{i \in I} \epsilon_i \left[Q_i \cap P\right] \tag{31.5.2}$$

and $Q_i \cap P$ are rational polyhedra without lines.

Next, we prove that the correspondence $P \longrightarrow f(P, \mathbf{x})$ preserves linear relations among indicators of rational polyhedra without lines. Namely, if

$$\sum_{j \in J} \alpha_j \left[P_j\right] = 0 \tag{31.5.3}$$

for some real α_j and some rational polyhedra $P_j \subset \mathbb{R}^d$ then necessarily

$$\sum_{j \in J} \alpha_j f(P_j, \mathbf{x}) = 0. \tag{31.5.4}$$

We use decomposition (31.5.1). Multiplying (31.5.3) by $[Q_i]$ we get

$$\sum_{j \in J} \alpha_j \, [P_j \cap Q_i] = 0.$$

By Lemma 31.4, there is a non-empty open set $U_i \subset \mathbb{C}^d$ such that for all $\mathbf{x} \in U_i$ the series

$$\sum_{m \in Q_i \cap \mathbb{Z}^d} \mathbf{x}^m$$

converges absolutely and uniformly on compact subsets of W to a rational function $f(P_i, \mathbf{x})$. Then the series

$$\sum_{m \in P_j \cap Q_i \cap \mathbb{Z}^d} \mathbf{x}^m$$

also converges uniformly on compact subsets of W necessarily to a rational function $f(P_i \cap Q_j, \mathbf{x})$. Besides,

$$\sum_{j \in J} \alpha_j f(P_j \cap Q_i, \mathbf{x}) = 0, \tag{31.5.5}$$

since the same identity holds for power series.

Similarly, from (31.5.2) we obtain

$$f(P_j, \mathbf{x}) = \sum_{i \in I} \epsilon_i f(P_j \cap Q_i, \mathbf{x}). \tag{31.5.6}$$

Combining (31.5.5) and (31.5.6), we obtain

$$\begin{aligned} \sum_{j \in J} \alpha_j f(P_j, \mathbf{x}) =& \sum_{j \in J} \alpha_j \left(\sum_{i \in I} \epsilon_i f(P_j \cap Q_i, \mathbf{x}) \right) = \sum_{\substack{i \in I \\ j \in J}} \epsilon_i \alpha_j f\left(P_j \cap Q_i, \mathbf{x}\right) \\ =& \sum_{i \in I} \epsilon_i \left(\sum_{j \in J} \alpha_j f(P_j \cap Q_i, \mathbf{x}) \right) = 0, \end{aligned}$$

which proves (31.5.4).

Therefore, the correspondence $P \longmapsto f(P, \mathbf{x})$ extends to a valuation $\mathcal{F}$. It remains to prove that $\mathcal{F}([P]) = 0$ if P contains a line. First, we note that if $n + P$ is an integer translation of P then

$$\mathcal{F}([n + P]) = \mathbf{x}^n \mathcal{F}([P]). \tag{31.5.7}$$

Indeed, it suffices to check (31.5.7) for polyhedra without lines, where it is obvious. Next, we observe that if a rational polyhedron P contains a line, it contains a rational line and hence there is $n \in \mathbb{Z}^d \setminus \{0\}$ such that $P+n=P$. This proves that for such a polyhedron we have

$$\mathcal{F}([P]) = \mathbf{x}^n \mathcal{F}([P]),$$

and hence $\mathcal{F}([P]) = 0$. $\square$

(31.6) Problems.

1. Let $P \subset \mathbb{R}^d$ be a rational polyhedron without lines and let $K_P \subset \mathbb{R}^d$ be its recession cone (see Theorem 30.9). Let

$$W = \Big\{ \mathbf{x} \in \mathbb{C}^d : \quad |x^u| < 1 \quad \text{for all} \quad u \in K \setminus \{0\} \Big\}.$$

Prove that for every $\mathbf{x} \in W$ the series

$$\sum_{m \in P \cap \mathbb{Z}^d} \mathbf{x}^m$$

converges absolutely and uniformly on compact subsets of W to a rational function $f(P; \mathbf{x})$.

2. Let $u_1, \ldots, u_k \in \mathbb{Z}^d$ be linearly independent vectors, let cone K be defined as in Lemma 3.2 and let

$$\operatorname{int} K = \left\{ \sum_{i=1}^k \alpha_i u_i : \quad \alpha_i > 0 \quad \text{for} \quad i = 1, \ldots, k \right\}$$

be the relative interior of K. Let

$$\overline{\Pi} = \left\{ \sum_{i=1}^k \alpha_i u_i : \quad 0 < \alpha_i \leq 1 \right\}$$

and let us define a set $W \subset \mathbb{C}^d$ as in Lemma 31.2. Prove that the series

$$\sum_{m \in K \cap \mathbb{Z}^d} \mathbf{x}^m$$

absolutely converges for all $\mathbf{x} \in W$ uniformly on compact subsets of W to a rational function

$$f(\operatorname{int} K, \mathbf{x}) = \left(\sum_{n \in \overline{\Pi} \cap \mathbb{Z}^d} \mathbf{x}^n \right) \prod_{i=1}^k \frac{1}{1 - \mathbf{x}^{u_i}}.$$

Deduce that

$$f\left(\operatorname{int} K, \mathbf{x}^{-1}\right) = (-1)^k f(\operatorname{int} K, \mathbf{x}).$$

3. Let a and b be coprime positive integers and let $S \subset \mathbb{Z}$ be the set of all linear combinations of a and b with non-negative integer coefficients. Prove that

$$\sum_{m \in S} x^m = \frac{1 - x^{ab}}{(1 - x^a)(1 - x^b)} \quad \text{for} \quad |x| < 1.$$

4*. Let a, b and c be coprime positive integers and let $S \subset \mathbb{Z}$ be the set of all linear combinations of a, b and c non-negative integer coefficients. Prove that there exist positive integers p_1, p_2, p_3, p_4 and p_5, not necessarily distinct, such that

$$\sum_{m \in S} x^m = \frac{1 - x^{p_1} - x^{p_2} - x^{p_3} + x^{p_4} + x^{p_5}}{(1 - x^a)(1 - x^b)(1 - x^c)} \quad \text{for} \quad |x| < 1.$$

32. Tangent cones

(32.1) Definitions. Let $P \subset V$ be a polyhedron and let $v \in P$ be a point. The *cone of feasible directions* of P at v is defined as

$$\operatorname{fcone}(P, v) = \Big\{x \in V : \quad v + \epsilon x \in P \quad \text{for all sufficiently small} \quad \epsilon > 0\Big\}.$$

Equivalently, if

$$P = \Big\{x \in V : \quad \langle c_i, x \rangle \leq \alpha_i, \ i \in I\Big\}$$

and

$$I_v = \Big\{i \in I : \quad \langle c_i, v \rangle = \alpha_i\Big\}$$

then

$$\operatorname{fcone}(P, v) = \Big\{x \in V : \quad \langle c_i, x \rangle \leq 0 \quad \text{for} \quad i \in I_v\Big\}.$$

The *tangent cone* of P at v is

$$\operatorname{tcone}(P, v) = v + \operatorname{fcone}(P, v),$$

or, equivalently,

$$\operatorname{tcone}(P, v) = \Big\{x \in V : \quad \langle c_i, x \rangle \leq \alpha_i \quad \text{for} \quad i \in I_v\Big\}.$$

Let $f, g \in \mathcal{P}(V)$. We say that

$$f \equiv g \quad \text{modulo polyhedra with lines}$$

if

$$f - g = \sum_i \alpha_i [P_i],$$

where $P_i \subset V$ are polyhedra with lines. For $f, g \in \mathcal{P}\left(\mathbb{Q}^d\right)$ we say that

$$f \equiv g \quad \text{modulo rational polyhedra with lines}$$

if

$$f - g = \sum_i \alpha_i [P_i],$$

where $P_i \subset \mathbb{R}^d$ are rational polyhedra without lines.

(32.2) Lemma. *Let $T : V \longrightarrow W$ be a linear transformation, let $P \subset V$ be a polyhedron, let $Q = T(P)$, let $v \in P$ be a point and let $w = T(v) \in Q$ be its image. Then*

$$T\Big(\operatorname{tcone}(P, v)\Big) = \operatorname{tcone}(Q, w).$$

Proof. Without loss of generality we may assume that $v = 0$, in which case $w = 0$,

$$\operatorname{tcone}(P, v) = \bigcup_{t \geq 0} tP \quad \text{and} \quad \operatorname{tcone}(Q, w) = \bigcup_{t \geq 0} tQ.$$

Since $T(tP) = tT(P) = tQ$, the proof follows. □

Here is the main result of this section.

(32.3) Theorem. *Let $P \subset \mathbb{R}^d$ be a (rational) polyhedron. Then*

$$[P] \equiv \sum_v [\operatorname{tcone}(P, v)] \quad \textit{modulo (rational) polyhedra with lines,}$$

where the sum is taken over all vertices of P.

Proof. Let A be the affine hyperplane in $\mathbb{R}^n$ defined by the equation $x_1 + \ldots + x_n = 1$ and let $H_i \subset A$ be the halfspace defined by the inequality $x_i \geq 0$ for $i = 1, \ldots, n$. Then

$$\Delta = \bigcap_{i=1}^n H_i$$

is the standard simplex, which is also the convex hull of the standard basis vectors $e_1, \ldots, e_n$. We note that

$$A = \bigcup_{i=1}^n H_i$$

and hence by the inclusion-exclusion formula

$$(32.3.1) \qquad [A]=\sum_{\substack{I\subset\{1,\dots,n\}\\ I\neq\emptyset}}(-1)^{|I|-1}[H_I] \quad \text{where} \quad H_I=\bigcap_{i\in I}H_i.$$

Thus if $I=\{1,\dots,n\}$ then $H_I=\Delta$ and if $I=\{1,\dots,n\}\setminus\{e_i\}$ then $H_I=\operatorname{tcone}(\Delta,e_i)$. If $i,j\notin I$ for some $i\neq j$ then H_I contains a line in the direction of e_i-e_j. Hence

$$\Delta\equiv\sum_{i=1}^{n}[\operatorname{tcone}(\Delta,e_i)] \quad \text{modulo rational polyhedra with lines.}$$

Suppose now that P is a (rational) polytope, that is,

$$P=\operatorname{conv}(v_1,\dots,v_n),$$

where $v_1,\dots,v_n\in\mathbb{R}^d$ are the vertices of P. Let $T:\mathbb{R}^n\longrightarrow\mathbb{R}^d$ be a linear transformation such that $T(e_i)=v_i$ for $i=1,\dots,n$. Hence $T(\Delta)=P$. By Theorem 28.3, from (32.3.1) we conclude

$$[T(A)]=\sum_{\substack{I\subset\{1,\dots,n\}\\ I\neq\emptyset}}(-1)^{|I|-1}[T(H_I)].$$

Hence $T(H_I)=P$ if $I=\{1,\dots,n\}$, by Lemma 32.2

$$T(H_I)=T(\operatorname{tcone}(\Delta,e_i)=\operatorname{tcone}(P,v_i)$$

if $I=\{1,\dots,n\}\setminus\{i\}$ and $T(H_I)$ contains a line in the direction $v_i-v_j\neq 0$ if $i,j\notin I$ for $i\neq j$. Hence

$$[P]\equiv\sum_{i=1}^{n}[\operatorname{tcone}(P,v_i)] \quad \text{modulo rational polyhedra with lines.}$$

Finally, we consider the case of an arbitrary (rational) polyhedron P. If P contains a line then by Lemma 30.4 polyhedron P has no vertices and the identity holds trivially. If P contains a line then by Theorem 30.9 we may write $P=Q+K_P$, where Q is the convex hull of the set of vertices of P and K_P is the recession cone of P. Since we have already proved the desired identity for polytopes, we can write

$$[Q]\equiv\sum_{v}[\operatorname{tcone}(Q,v)] \quad \text{modulo (rational) polyhedra with lines.}$$

Using Theorem 29.2, we obtain

$$[P] \equiv \sum_v [\text{tcone}(Q, v) + K_P] \quad \text{modulo (rational) polyhedra with lines.}$$

It remains to show that for every vertex v of P we have

$$\text{tcone}(Q, v) + K_P = \text{tcone}(P, v). \tag{32.3.2}$$

Indeed, let us consider the direct product $Q \times K_P \subset \mathbb{R}^{2d}$ and a linear transformation $T : \mathbb{R}^{2d} \longrightarrow \mathbb{R}^d$

$$Q \times K_P = \Big\{ (x, y) : \quad x \in Q, y \in K_P \Big\}, \quad T(x, y) = x + y.$$

Hence $P = Q + K_P = T(Q \times K_P)$, $T(v, 0) = v$ and it is easy to check that

$$\text{tcone}\left(Q \times K_P, (v, 0)\right) = \text{tcone}(Q, v) \times K_P.$$

Applying Lemma 32.2, we deduce (32.3.2) and hence the theorem. □

We obtain the following corollary also known as *Brion's Theorem*, after M. Brion who proved it in 1988 using methods of algebraic geometry.

(32.4) Corollary. *Let $P \subset \mathbb{R}^d$ be a rational polyhedron and let $\mathcal{F}$ be the valuation of Theorem 31.5. Then*

$$\mathcal{F}([P]) = \sum_v \mathcal{F}\big([\text{tcone}(P, v)]\big),$$

where the sum is taken over all vertices v of P. If the vertices of P are integer vectors then

$$\mathcal{F}([P]) = \sum_v \mathbf{x}^v \mathcal{F}\big([\text{fcone}(P, v)]\big).$$

Proof. Follows by Theorem 31.5 and Theorem 32.3. □

33. The Ehrhart polynomial of an integer polytope

(33.1) Definition. A polytope $P \subset \mathbb{R}^d$ is called *integer* if the vertices of P are integer vectors.

(33.2) Theorem. *Let $P \subset \mathbb{R}^d$ be an integer polytope. For a positive integer n let nP be the dilation of P, so that*

$$nP = \big\{ nx : \quad x \in P \big\}.$$

Then there exists a polynomial $p(n)$, called the Ehrhart polynomial of P, such that

$$p(n) = \left|nP \cap \mathbb{Z}^d\right|$$

for positive integer m.

Proof. Let v_i, $i \in I$, be the vertices of P and let

$$K_i = \operatorname{fcone}(P, v_i) \quad \text{for} \quad i \in I$$

be the cone of feasible directions of P at v_i. Then nv_i, $i \in I$, are the vertices of nP and

$$\operatorname{fcone}(nP, v_i) = K_i \quad \text{for} \quad i \in I.$$

By Corollary 32.4, we have

$$\mathcal{F}([nP]) = \sum_{i \in I} \mathbf{x}^{nv_i} \mathcal{F}\big([K_i]\big). \tag{33.2.1}$$

We have

$$\mathcal{F}([nP]) = \sum_{m \in (nP) \cap \mathbb{Z}^d} \mathbf{x}^m$$

and hence the number of integer points in nP is the value of $\mathcal{F}([nP])$ at $\mathbf{x} = (1, \dots, 1)$. Using Lemma 31.3, we can write $\mathcal{F}\big([K_i]\big) = f(K_i, \mathbf{x})$ as sums of functions of the type $p(\mathbf{x})/q(\mathbf{x})$, where $p(\mathbf{x})$ is a Laurent polynomials in $\mathbf{x}$ and

$$q(\mathbf{x}) = (1 - \mathbf{x}^{u_1}) \cdots (1 - \mathbf{x}^{u_d})$$

for some $u_1, \dots, u_d \in \mathbb{Z}^d \setminus \{0\}$. We note that $\mathbf{x} = (1, \dots, 1)$ is a pole of $f(K_i, \mathbf{x})$.

Let us choose a vector $c \in \mathbb{R}^d$ such that $\langle c, u_{ij} \rangle \neq 0$ for all i and j. We choose $\mathbf{x}(t) = \mathbf{e}^{tc}$ in (33.2.1). Then the value of the left hand side is

$$\sum_{m \in (nP) \cap \mathbb{Z}^d} e^{t\langle c, m \rangle},$$

which is an analytic function of t and the constant term of its Taylor series expansion in a neighborhood of $t = 0$ is the number $\left|nP \cap \mathbb{Z}^d\right|$ of integer points in nP.

We observe that

$$\mathbf{x}(t)^{nv_i} = e^{t\langle nc, v_i \rangle} = \sum_{k=0}^{+\infty} \frac{\langle c, v_i \rangle^k}{k!} n^k t^k. \tag{33.2.2}$$

Next, we observe that

$$\prod_{j=1}^{d} \frac{1}{1 - \mathbf{x}^{u_j}(t)} = \prod_{j=1}^{d} \frac{1}{1 - e^{t\langle c, u_{ij} \rangle}}.$$

Since the function

$$\frac{t}{1-e^t}$$

is analytic at $t=0$, the function

$$t^d f\big(K_i, \mathbf{x}(t)\big)$$

is analytic at $t=0$ and we obtain the Laurent expansion in the neighborhood of $t=0$

$$f\big(K_i, \mathbf{x}(t)\big) = t^{-d} \sum_{k=0}^{+\infty} \alpha_{ki} t^k, \tag{33.2.3}$$

where the coefficients α_{ki} depend only on the cone of feasible directions of P at v_i. From (33.2.2) and (33.2.3) we conclude that the constant term of the Laurent expansion of the right hand side of (33.2.1) in a neighborhood of $t=0$ is

$$\sum_{i \in I} \sum_{\substack{k_1, k_2 \geq 0 \\ k_1 + k_2 = d}} \frac{\langle c, v_i \rangle^{k_1}}{k_1!} n^{k_1} \alpha_{k_2 i},$$

which is a polynomial in n. □

(33.3) Problems.

1. Prove that $\deg p = \dim P$.

2. Let $\{P_\alpha : \ \alpha \in A\}$ be a family of d-dimensional polytopes,

$$P_\alpha = \operatorname{conv}\Big(v_1(\alpha), \ldots, v_n(\alpha)\Big),$$

where $v_i(\alpha) \in \mathbb{Z}^d$ and the cones of feasible directions at $v_i(\alpha)$ do not depend on α:

$$\operatorname{fcone}\big(P_\alpha, \ v_i(\alpha)\big) = K_i \quad \text{for} \quad i = 1, \ldots, n$$

and all $\alpha \in A$. Prove that there exists a polynomial

$$p : \quad \underbrace{\mathbb{R}^d \times \cdots \times \mathbb{R}^d}_{n \text{ times}} \longrightarrow \mathbb{R}$$

such that

$$\big|P_\alpha \cap \mathbb{Z}^d\big| = p\big(v_1(\alpha), \ldots, v_n(\alpha)\big)$$

for all $\alpha \in A$.

3. Let $P \subset \mathbb{R}^d$ be a rational polytope such that kP is an integer polytope for some positive integer k. Prove that for a positive integer n

$$\big|nP \cap \mathbb{Z}^d\big| = \sum_{j=0}^{d} b_j(n) n^j,$$

where

$$b_j(n) = b_j(n+k)$$

for all positive integer n and all $0 \leq j \leq d$. In other words, the number of integer points in nP is a *quasi-polynomial*, called the *Ehrhart quasi-polynomial* of P.

(34.1) Lemma. *Let $P \subset \mathbb{R}^d$ be a (rational) polytope with a non-empty interior* $\operatorname{int} P$. *Then* $[\operatorname{int} P] \in \mathcal{P}\left(\mathbb{R}^d\right)$ *(respectively,* $[\operatorname{int} P] \in \mathcal{P}\left(\mathbb{Q}^d\right)$*, if P is rational) and*

$$\chi\left([\operatorname{int} P]\right) = (-1)^d.$$

Proof. By Lemma 30.3 polytope P is a (rational) polyhedron, so

$$P = \Big\{ x \in \mathbb{R}^d : \quad \langle c_i, x \rangle \leq \alpha_i, \ i = 1, \dots, n \Big\}.$$

Then $P \setminus \operatorname{int} P$ is a union of lower-dimensional (rational) polytopes lying in the affine hyperplanes

$$H_j = \Big\{ x : \quad \langle c_j, x \rangle = \alpha_j \Big\}.$$

Hence the inclusions

$$[\operatorname{int} P] \subset \mathcal{P}\left(\mathbb{R}^d\right), \ \mathcal{P}\left(\mathbb{Q}^d\right)$$

follow by induction on d.

To compute the Euler characteristic of $\operatorname{int} P$ we use formula (27.2.2) and induction on d. Clearly, the formula holds for $d = 1$. For $d > 1$, let $H_\tau \subset \mathbb{R}^d$ be the affine hyperplane defined by the equation $x_d = \tau$. Then, by (27.2.2), we have

$$\chi\left([\operatorname{int} P]\right) = \sum_{\tau \in \mathbb{R}} \left(\chi\left(\operatorname{int} P \cap H_\tau\right) - \lim_{\epsilon \longrightarrow 0+} \chi\left(\operatorname{int} P \cap H_{\tau - \epsilon}\right) \right). \tag{34.1.1}$$

By Lemma 30.6, for every τ the intersection $\operatorname{int} P \cap H_\tau$ is either empty or the interior of a $(d-1)$-dimensional polytope. Therefore, by the induction hypothesis, the only non-zero term of (34.1.1) corresponds to

$$\tau = \max_{(x_1, \dots, x_d) \in P} x_d$$

and equals

$$0 - (-1)^{d-1} = (-1)^d.$$

$\square$

The following result is known as the *reciprocity relation.*

(34.2) Theorem. *Let $K \subset \mathbb{R}^d$ be a (rational) polyhedral cone with a non-empty interior* $\operatorname{int} K$. *Then*

$$[K] \equiv (-1)^d [-\operatorname{int} K] \quad \textit{modulo (rational) polyhedra with lines,}$$

where

$$-\operatorname{int} K = \Big\{ -x : \quad x \in \operatorname{int} K \Big\}.$$

Proof. First, we consider the special case of the non-negative orthant $\mathbb{R}^n_+$. For $i = 1, \ldots, n$ let H_i^+ be the closed halfspace defined by the inequality $x_i \geq 0$ and let H_i^- be the complementary open halfspace defined by the inequality $x_i < 0$. Then

$$\left[\mathbb{R}^n_+\right] = \prod_{i=1}^n \left[H_i^+\right] = \prod_{i=1}^n \left([\mathbb{R}^n] - \left[H_i^-\right]\right) = \sum_{I \subset \{1, \ldots, n\}} (-1)^{|I|} \left[H_I^-\right], \tag{34.2.1}$$
$$\text{where} \quad H_I^- = \bigcap_{i \in I} H_i^-.$$

If $I = \{1, \ldots, n\}$ then $H_I = -\operatorname{int} \mathbb{R}^n_+$. If $j \notin I$ for some j then $[H_I]$ is a linear combination of indicators of polyhedra containing a line in the direction of the j-th basis vector e_j, and hence we conclude that

$$\left[\mathbb{R}^n_+\right] \equiv (-1)^n \left[-\operatorname{int} \mathbb{R}^n_+\right] \quad \text{modulo rational polyhedra with lines.}$$

Suppose now that $K \subset \mathbb{R}^d$ is a (rational) polyhedra cone with no lines and with a non-empty interior. By Lemma 30.8, we can write

$$K = \left\{ \sum_{i=1}^n \alpha_i u_i : \quad \alpha_i \geq 0 \quad \text{for} \quad i = 1, \ldots, n \right\}$$

and some $u_1, \ldots, u_n$ such that $Q = \operatorname{conv}\Big(u_1, \ldots, u_n\Big)$ is a polytope contained in an affine hyperplane not passing through the origin. If K is rational, we may additionally choose $u_i \in \mathbb{Z}^d \setminus \{0\}$ for $i = 1, \ldots, n$.

Let us consider a linear transformation $T : \mathbb{R}^n \longrightarrow \mathbb{R}^d$ such that $T(e_i) = u_i$ for $i = 1, \ldots, n$. Then

$$T\left(\mathbb{R}^n_+\right) = K.$$

By Theorem 28.3, there is a unique valuation

$$\mathcal{T} : \mathcal{P}\left(\mathbb{R}^n\right),\ \mathcal{P}\left(\mathbb{Q}^n\right) \longrightarrow \mathcal{P}\left(\mathbb{R}^d\right),\ \mathcal{P}\left(\mathbb{Q}^d\right)$$

such that $\mathcal{T}([P]) = [T(P)]$ for any (rational) polyhedron $P \subset \mathbb{R}^n$. In particular,

$$\mathcal{T}\left[\mathbb{R}^n_+\right] = [K]. \tag{34.2.2}$$

Let us compute $h = \mathcal{T}\left(\left[-\operatorname{int} \mathbb{R}^n_+\right]\right)$. From (28.3.1) we have

$$h(x) = \chi\left(\left[\left(-\operatorname{int} \mathbb{R}^n_+\right) \cap T^{-1}(x)\right]\right) \quad \text{for all} \quad x \in \mathbb{R}^d.$$

We observe that for all $x \in -\operatorname{int} K$ the intersection $\left(-\operatorname{int} \mathbb{R}^n_+\right) \cap T^{-1}(x)$ is the interior of a $(n-d)$-dimensional polytope while for all other x the intersection is empty. From Lemma 34.1, we conclude that

$$h = (-1)^{n-d} \left[-\operatorname{int} K\right].$$

Finally, if P is a (rational) polyhedron containing a line in the direction of a basis vector e_j then $T(P)$ is a (rational) polyhedron containing a line in the direction of vector u_j. Applying $\mathcal{T}$ to (34.2.1), we conclude that

$$[K] \equiv (-1)^n \cdot (-1)^{n-d}[-\operatorname{int} K] \equiv (-1)^d[-\operatorname{int} K]$$
$$\text{modulo (rational) polyhedra with lines,}$$

as desired.

Finally, if K contains a line then

$$[K] \equiv [-\operatorname{int} K] \equiv 0 \quad \text{modulo rational polyhedra with lines.}$$

$\square$

(34.3) Theorem. *Let $P \subset \mathbb{R}^d$ be a (rational) polytope with a non-empty interior* $\operatorname{int} P$. *Then*

$$[\operatorname{int} P] \equiv \sum_v [\operatorname{int} \operatorname{tcone}(P, v)] \quad \textit{modulo (rational) polyhedra with lines,}$$

where the sum is taken over all vertices v of P.

Proof. The proof combines the approaches of Theorem 32.3 and Theorem 34.2. First, we establish the identity for the standard simplex and then use a suitable projection. $\square$

(34.4) Corollary.

(1) *Let $K \subset \mathbb{R}^d$ be a rational cone with a non-empty interior* $\operatorname{int} K$ *and let $f(K, \mathbf{x}) = \mathcal{F}([K])$ and $f(\operatorname{int} K, \mathbf{x}) = \mathcal{F}([\operatorname{int} K])$ be the corresponding rational functions in $\mathbf{x} \in \mathbb{C}^d$. Then*

$$f\left(\operatorname{int} K, \mathbf{x}\right) = (-1)^d f\left(K, \mathbf{x}^{-1}\right),$$

where

$$\mathbf{x}^{-1} = \left(x_1^{-1}, \ldots, x_d^{-1}\right) \quad \textit{for} \quad \mathbf{x} = (x_1, \ldots, x_d).$$

(2) *Let $P \subset \mathbb{R}^d$ be a rational polytope with a non-empty interior. Then*

$$\mathcal{F}([P]) = \sum_v \mathcal{F}\big([\operatorname{int} \operatorname{tcone}(P, v)]\big),$$

where v ranges over all vertices of P. If the vertices of P are integer vectors then

$$\mathcal{F}([P]) = \sum_v \mathbf{x}^v \mathcal{F}\big([\operatorname{int} \operatorname{fcone}(P, v)]\big).$$

Proof. Part (1) follows by Theorem 34.2, Theorem 31.5 and the observation that

$$\sum_{m \in \operatorname{int} K \cap \mathbb{Z}^d} \mathbf{x}^m = \sum_{m \in -\operatorname{int} K \cap \mathbb{Z}^d} \mathbf{x}^{-m}.$$

Part (2) follows from Theorem 34.3 and Theorem 31.5. $\square$

The following result is called the *reciprocity relation* for Ehrhart polynomials.

(35.1) Theorem. *Let $P \subset \mathbb{R}^d$ be an integer polytope with a non-empty interior* $\operatorname{int} P$ *and let p be its Ehrhart polynomial, so that*

$$p(n) = \left|nP \cap \mathbb{Z}^d\right|$$

for positive integer n. Then

$$p(-n) = (-1)^d \left|\operatorname{int}(nP) \cap \mathbb{Z}^d\right|$$

for positive integer n.

Proof. We proceed as in the proof of Theorem 33.2. Let v_i, $i \in I$, be the vertices of P and let

$$K_i = \operatorname{fcone}(P, v_i) \quad \text{for} \quad i \in I$$

be the cone of feasible directions of P at v_i. From Corollaries 32.4 and 34.4, we get

$$\mathcal{F}([nP]) = \sum_{i \in I} \mathbf{x}^{nv_i} \mathcal{F}\left([K_i]\right) \quad \text{and} \quad \mathcal{F}([\operatorname{int} nP]) = \sum_{i \in I} \mathbf{x}^{nv_i} \mathcal{F}\left([\operatorname{int} K_i]\right)$$

and

$$\mathcal{F}([nP]) = \sum_{m \in (nP) \cap \mathbb{Z}^d} \mathbf{x}^m \quad \text{and} \quad \mathcal{F}([\operatorname{int} nP]) = \sum_{m \in (\operatorname{int} nP) \cap \mathbb{Z}^d} \mathbf{x}^m,$$

where the last identity follows since $[\operatorname{int} P]$ can be written as a linear combination of indicators of polytopes (the polytope P and its faces). Denoting

$$f\left(K_i, \mathbf{x}\right) = \mathcal{F}\left([K_i]\right) \quad \text{and} \quad f\left(\operatorname{int} K_i, \mathbf{x}\right) = \mathcal{F}\left([\operatorname{int} K_i]\right),$$

from Corollary 34.4, we have

$$f\left(\operatorname{int} K_i, \mathbf{x}\right) = (-1)^d f\left(K_i, \mathbf{x}^{-1}\right) \tag{35.1.1}$$

As in the proof of Theorem 33.2, let us choose a vector $c \in \mathbb{R}^d$ such that $\mathbf{x}(t) = \mathbf{e}^{tc}$ is a regular point of all functions $f(K_i, \mathbf{x})$ provided $t \neq 0$. Since $\mathbf{x}^{-1}(t) = \mathbf{x}(-t)$ it follows by (35.1.1) that $\mathbf{x}(t)$ is a regular point of all functions $f(\operatorname{int} K_i, \mathbf{x})$ as long as $t \neq 0$.

As in the proof of Theorem 33.2, functions $f(K_i, \mathbf{x}(t))$ admit a Laurent expansion in the neighborhood of $t = 0$:

$$f(K_i, \mathbf{x}(t)) = t^d \sum_{k=0}^{+\infty} \alpha_{ki} t^k.$$

Since $\mathbf{x}^{-1}(t) = \mathbf{x}(-t)$, from (35.1.1) we conclude that functions $f(\operatorname{int} K_i, \mathbf{x}(t))$ admit the Laurent expansions in the neighborhood of $t = 0$

$$f(\operatorname{int} K_i, \mathbf{x}(t)) = t^{-d} \sum_{k=0}^{+\infty} \alpha_{ki} (-t)^k.$$

As in the proof of Theorem 33.2, the number $p(n) = |nP \cap \mathbb{Z}^d|$ of integer points in nP is the constant term of the Taylor expansion of

$$\sum_{m \in (nP) \cap \mathbb{Z}^d} e^{t\langle c, m\rangle}$$

in a neighborhood of $t = 0$ and equals

$$\sum_{i \in I} \sum_{\substack{k_1 + k_2 \geq 0 \\ k_1 + k_2 = d}} \frac{\langle c, v_i\rangle^{k_1}}{k_1!} n^{k_1} \alpha_{k_2 i}. \tag{35.1.2}$$

Similarly, the number $|\operatorname{int} nP \cap \mathbb{Z}^d|$ of integer points in the interior of nP is the constant term of the Taylor expansion of

$$\sum_{m \in (\operatorname{int} nP) \cap \mathbb{Z}^d} e^{t\langle c, m\rangle}$$

and equals

$$\sum_{i \in I} \sum_{\substack{k_1 + k_2 \geq 0 \\ k_1 + k_2 = d}} \frac{\langle c, v_i\rangle^{k_1}}{k_1!} n^{k_1} (-1)^{k_2} \alpha_{k_2 i}. \tag{35.1.3}$$

Comparing (35.1.2) and (35.1.3) we conclude that

$$|\operatorname{int}(nP) \cap \mathbb{Z}^d| = (-1)^d p(-n).$$

$\square$

(35.2) Problem.

1. Let $\{P_\alpha : \alpha \in A\}$ be a family of d-dimensional polytopes with non-empty interiors,

$$P_\alpha = \operatorname{conv}\big(v_1(\alpha), \ldots, v_n(\alpha)\big),$$

where $v_i(\alpha) \in \mathbb{Z}^d$ and the cones of feasible directions at $v_i(\alpha)$ do not depend on α:

$$\operatorname{fcone}(P_\alpha, v_i(\alpha)) = K_i \quad \text{for} \quad i = 1, \ldots, n$$

and all $\alpha \in A$. By Problem 2 of Section 33.3 there exists a polynomial p such that

$$\big|P_\alpha \cap \mathbb{Z}^d\big| = p\big(v_1(\alpha), \ldots, v_n(\alpha)\big)$$

for all $\alpha \in A$. Prove that one can choose a polynomial p so that, additionally,

$$\big|\operatorname{int} P_\alpha \cap \mathbb{Z}^d\big| = (-1)^d p\big(-v_1(\alpha), \ldots, -v_n(\alpha)\big)$$

for all $\alpha \in A$.

(36.1) Definition. Let $K \subset V$ be a cone. The *polar cone* $K^\circ \subset V$ is defined by

$$K^\circ = \Big\{ x \in V : \quad \langle x, y \rangle \leq 0 \quad \text{for all} \quad y \in K \Big\}.$$

(36.2) Theorem.

(1) *Let $K \subset \mathbb{R}^d$ be a (rational) polyhedral cone. Then $K^\circ \subset \mathbb{R}^d$ is a (rational) polyhedral cone.*
(2) *We have $(K^\circ)^\circ = K$ for any polyhedral cone $K \subset \mathbb{R}^d$.*
(3) *A polyhedral cone K contains a line (respectively, lies in a hyperplane) if and only if K° lies in a hyperplane (respectively, contains a line).*
(4) *Let $\mathcal{K}\left(\mathbb{R}^d\right) \subset \mathcal{P}\left(\mathbb{R}^d\right)$ be the subspace spanned by the indicators of polyhedral cones. Then there exists a unique linear operator (valuation) $\mathcal{D} : \mathcal{K}\left(\mathbb{R}^d\right) \longrightarrow \mathcal{K}\left(\mathbb{R}^d\right)$ such that*

$$\mathcal{D}([K]) = ([K^\circ])$$

for any polyhedral cone $K \subset \mathbb{R}^d$.

Proof. To prove Part (1), first we consider the case when K has no lines. Then, by Lemma 30.8 we have

$$K = \left\{ \sum_{i=1}^{n} \alpha_i u_i \quad \text{where} \quad \alpha_i \geq 0 \quad \text{for} \quad i = 1, \ldots, n \right\}$$

for some vectors $u_1, \ldots, u_n \in \mathbb{R}^d$. Moreover, if K is rational we can choose u_i to be integer vectors. Then

$$K^\circ = \Big\{ x \in \mathbb{R}^d : \quad \langle x, u_i \rangle \leq 0 \quad \text{for} \quad i = 1, \ldots, n \Big\}.$$

Suppose now that K contains lines. We assume that

$$K = \Big\{ x \in \mathbb{R}^d : \quad \langle c_i, x \rangle \leq 0 \quad \text{for} \quad i \in I \Big\}$$

and let

$$L = \Big\{ x \in \mathbb{R}^d : \quad \langle c_i, x \rangle = 0 \quad \text{for} \quad i \in I \Big\}$$

be the largest subspace contained in K. Let $L^\perp \subset \mathbb{R}^d$ be the orthogonal complement to L and let $K_1 \subset L^\perp$ be the orthogonal projection of K onto $L^\perp$. Using Theorem 28.3 we conclude that K_1 is a (rational) polyhedral cone, necessarily without lines. It is not hard to argue that $K = K_1 + L$ and that $K^\circ = (K_1^\circ) \cap L^\perp$, from which Part (1) follows.

If $y \in K$ then $\langle x, y \rangle \leq 0$ for all $x \in K^\circ$ and hence $y \in (K^\circ)^\circ$. Suppose that $y \in (K^\circ)^\circ$ and suppose that

$$K = \Big\{ x \in \mathbb{R}^d : \quad \langle c_i, x \rangle \leq 0 \quad \text{for} \quad i \in I. \Big\}.$$

We note that $c_i \in K^\circ$ for all $i \in I$ and hence $\langle c_i, y \rangle \leq 0$ for all $i \in I$. It follows then that $y \in K$, which completes the proof of Part (2).

If K contains a line in the direction of $u \neq 0$ then K° lies in the hyperplane $u^\perp$. If $K \subset H$, where $H \subset \mathbb{R}^d$ is a hyperplane then K° contains a line in the direction orthogonal to H. Together with Part (2), this completes the proof of Part (3).

To prove Part (4), let us define $G : \mathbb{R}^d \times \mathbb{R}^d \longrightarrow \mathbb{R}$

$$G(x, y) = \begin{cases} 1 & \text{if } \langle x, y \rangle = 1 \\ 0 & \text{otherwise.} \end{cases}$$

We claim that for every $f \in \mathcal{K}\left(\mathbb{R}^d\right)$ and any $y \in \mathbb{R}^d$ the function $g_y(x) = f(x)G(x, y)$ lies in $\mathcal{P}\left(\mathbb{R}^d\right)$. Indeed, by linearity it suffices to check this when $f = [K]$, where $K \subset \mathbb{R}^d$ is a polyhedral cone, in which case $g_y = [K \cap H_y]$, where $H_y = \big\{ x \in \mathbb{R}^d : \quad \langle x, y \rangle = 1 \big\}$ is a hyperplane. This allows us to consider the Euler characteristic of g_y and hence to define a function $h : \mathbb{R}^d \longrightarrow \mathbb{R}$ by

$$h(y) = \chi(f) - \chi\big(g_y\big).$$

Next, we claim that if $f = [K]$ then $h = [K^\circ]$. Indeed, in this case $\chi(f) = 1$ while

$$\chi\left(g_y\right) = \begin{cases} 1 & \text{if } \ K \cap H_y \neq \emptyset \\ 0 & \text{if } \ K \cap H_y = \emptyset. \end{cases}$$

If $y \in K^\circ$ then clearly $K \cap H_y = \emptyset$ so $h(y) = 1$. If $y \notin K^\circ$ then there is an $x \in K$ such that $\langle x, y \rangle > 0$ and by scaling $x \longmapsto \lambda x$ for some $\lambda > 0$ we find a point $x \in K \cap H_y$. Hence $\chi\left(g_y\right) = 1$ in this case and $h(y) = 0$ if $y \notin K^\circ$. Therefore we can define a transformation

$$\mathcal{D} : \quad \mathcal{K}\left(\mathbb{R}^d\right) \longrightarrow \mathcal{K}\left(\mathbb{R}^d\right) \quad \text{where} \quad \mathcal{D}(f) = h.$$

The transformation is clearly linear and $\mathcal{D}\left([K]\right) = [K^\circ]$ for all polyhedral cones K. □

(36.3) Theorem. *Let $P \subset \mathbb{R}^d$ be a (rational) polytope. Then*

$$\sum_v [\operatorname{fcone}(P, v)] \equiv [0] \quad \textit{modulo (rational) polyhedra with lines},$$

where the sum is taken over all vertices v of P.

Proof. For a vertex v of P let us define a cone

$$K_v = \Big\{c \in \mathbb{R}^d : \quad \langle c, v \rangle \ \geq \ \langle c, w \rangle \quad \text{for all vertices} \quad w \neq v \quad \text{of} \quad P\Big\}.$$

In other words, K_v consists of all functions $x \longmapsto \langle c, x \rangle$ that attain their maximum on P at v. Hence

$$\bigcup_v K_v = \mathbb{R}^d,$$

where the union is taken over all vertices v of P. Moreover, the intersection of any two or more of cones K_v is a lower-dimensional cone since $K_{v_1} \cap K_{v_2}$ lies in the hyperplane $\langle c, v_1 - v_2 \rangle = 0$. Therefore,

$$\sum_v [K_v] \equiv \left[\mathbb{R}^d\right] \quad \text{modulo cones in hyperplanes,} \tag{36.3.1}$$

where the sum is taken over all vertices v of P. Next, it is not hard to see that

$$K_v = \Big(\text{fcone}(P, v)\Big)^\circ.$$

Hence by Part (2) of Theorem 36.2 we conclude that

$$K_v^\circ = \text{fcone}(P, v).$$

Applying the operator $\mathcal{D}$ of Part (4) of Theorem 36.2 to both parts of (36.3.1), we complete the proof. □

(36.4) Corollary. *Let $P \subset \mathbb{R}^d$ be a rational polytope. Then*

$$\sum_v \mathcal{F}\big([\text{fcone}(P, v)]\big) = 1,$$

where the sum is taken over all vertices v of P.

Proof. Follows from Theorem 31.5 and Theorem 36.3. □

(36.5) Problems.

1. Let $\mathcal{D}$ be the the operator of Theorem 36.2. Prove that

$$\mathcal{D}(f * g) = \mathcal{D}(f)\mathcal{D}(g) \quad \text{and that} \quad \mathcal{D}(fg) = D(f) * D(g),$$

where $*$ is the bilinear operation of Theorem 29.2.

2. Let $P \subset V$ be a polyhedron without lines. Prove that

$$\sum_v [\text{fcone}(P, v)] \equiv K_P \quad \text{modulo polyhedra with lines,}$$

where the sum is taken over all vertices v of P and K_P is the recession cone of P, see Theorem 30.9.

3. Let us fix $1 \leq k \leq d$ and let

$$A = \Big\{(x_1, \ldots, x_d) : \quad x_1, \ldots, x_k > 0 \quad \text{and} \quad x_{k+1}, \ldots, x_d \geq 0\Big\}.$$

Prove that $[A] \in \mathcal{K}\left(\mathbb{R}^d\right)$ and compute $\mathcal{D}([A])$.

37. THE CONSTANT TERM OF THE EHRHART POLYNOMIAL

(37.1) Theorem. *Let $P \subset \mathbb{R}^d$ be a non-empty integer polytope and let p be its Ehrhart polynomial, so that*

$$p(n) = \left|nP \cap \mathbb{Z}^d\right|$$

for a positive integer n. Then

$$p(0) = 1.$$

Proof. Let v_i, $i \in I$ be the vertices of P and let

$$K_i = \operatorname{fcone}(P, v_i) \quad \text{for} \quad i \in I.$$

As in the proof of Theorem 33.2, we conclude that

$$p(n) = \sum_{i \in I} \sum_{\substack{k_1, k_2 \geq 0 \\ k_1 + k_2 = d}} \frac{\langle c, v_i \rangle^{k_1}}{k_1!} n^{k_1} \alpha_{k_2 i},$$

where $c \in \mathbb{R}^d$ is a sufficiently generic vector and

$$f\left(K_i, \mathbf{x}(t)\right) = t^{-d} \sum_{k=0}^{+\infty} \alpha_{ki} t^k, \quad \text{for} \quad \mathbf{x}(t) = \mathbf{e}^{tc} \quad \text{and} \quad f\left(K_i, \mathbf{x}\right) = \mathcal{F}\left([K_i]\right).$$

Then

$$p(0) = \sum_{i \in I} \alpha_{di} = 1$$

since

$$\sum_{i \in I} f\left(K_i, \mathbf{x}(t)\right) = 1$$

By Corollary 36.4. □

(37.3) Problems.

1. Let $\{P_\alpha : \quad \alpha \in A\}$ be a family of d-dimensional polytopes,

$$P_\alpha = \operatorname{conv}\Big(v_1(\alpha), \ldots, v_n(\alpha)\Big),$$

where $v_i(\alpha) \in \mathbb{Z}^d$ for $i = 1, \ldots, n$ and

$$\operatorname{fcone}\left(P_\alpha, v_i(\alpha)\right) = K_i,$$

independently of α, see Problem 2 of Section 33.3. Prove that one choose a polynomial p in Problem 2, Section 33.3 and Problem 1 of Section 35.2, so that

$$\left|P_\alpha \cap \mathbb{Z}^d\right| = p\left(v_1(\alpha), \ldots, v_n(\alpha)\right) \quad \text{for all} \quad \alpha \in A.$$

and that

$$p(0, \dots, 0) = 1.$$

2. Let $\{P_\alpha : \quad \alpha \in A\}$ be a family of polytopes as in Problem 1 above and let $v_1, \dots, v_n \in \mathbb{Z}^d$ are not necessarily distinct points such that in an arbitrary small neighborhood of v_i there is a point $v_i' \in \mathbb{R}^d$ such that for $P' = \operatorname{conv}\Big(v_1', \dots, v_n'\Big)$ one has

$$\operatorname{fcone}(P, v_i') = K_i \quad \text{for} \quad i = 1, \dots, n.$$

In other words, P_α degenerates into an integer polytope P in such a way that the facets of P_α are moved parallel to themselves. Prove that one can choose a polynomial p in Problem 1 above such that

$$\left|P \cap \mathbb{Z}^d\right| = p\left(v_1, \dots, v_n\right)$$

and so that

$$\left|\operatorname{int} P \cap \mathbb{Z}^d\right| = (-1)^k p\left(-v_1, \dots, -v_n\right),$$

where $k = \dim P$ and $\operatorname{int} P$ is the relative interior of P.

3*. Let $P_1, \dots, P_k \subset \mathbb{R}^d$ be integer polytopes. Prove that there exists a k-variate polynomial p such that

$$\left|\Big(m_1 P_1 + \ldots + m_k P_k\Big) \cap \mathbb{Z}^d\right| = p\left(m_1, \dots, m_k\right),$$

for all non-negative integer $m_1, \dots, m_k$. Here "+" stands for the Minkowski sum and multiplication by m_i is a dilation. Moreover, prove that for $P = m_1 P_1 + \ldots + m_k P_k$ one has

$$\left|\operatorname{int} P \cap \mathbb{Z}^d\right| = (-1)^{\dim P} p\left(-m_1, \dots, -m_k\right),$$

where $m_1, \dots, m_k$ are non-negative integers and $\operatorname{int} P$ is the relative interior of P.

4. Prove that for every positive integer k there exists a univariate polynomial p of degree $(k-1)^2$ such that for every positive integer m the value $p(m)$ is equal to the number of $k \times k$ non-negative integer matrices with the row and column sums equal to m. Prove that, additionally,

$$p(0) = 1,\ p(-1) = \ldots = p(-k+1) = 0 \quad \text{and} \quad p(-m) = (-1)^{k-1} p(m-k)$$

for integer $m \geq k$.

5. Let $P \subset \mathbb{R}^3$ be the tetrahedron with the vertices $(0,0,0), (1,0,0), (0,1,0)$ and $(1,1,a)$, where $a > 0$ is an integer parameter and let p be its Ehrhart polynomial. Prove that

$$p(n) = \frac{a}{6} n^3 + n^2 + \frac{12 - a}{6} n + 1.$$

6. Let us fix a polynomial $\rho : \mathbb{R}^d \longrightarrow \mathbb{R}$ and let $\{P_\alpha : \quad \alpha \in A\}$ be a family of polytopes as in Problem 1. Prove that there exists a polynomial q such that

$$\sum_{m \in P_\alpha \cap \mathbb{Z}^d} \rho(m) = q\left(v_1(\alpha), \dots, v_n(\alpha)\right)$$

for all $\alpha \in A$.

(38.1) Definition. Let $u_1, \ldots, u_k \subset \mathbb{Z}^d$ be a primitive set, that is, $u_1, \ldots, u_k$ is a basis of the lattice $\mathbb{Z}^d \cap \operatorname{span}\Big(u_1, \ldots, u_k\Big)$. The cone

$$K = \left\{ \sum_{i=1}^{k} \alpha_i u_i : \quad \alpha_i \geq 0 \quad \text{for} \quad i = 1, \ldots, k \right\}$$

is called a *unimodular cone*. We say that K is *spanned* by $u_1, \ldots, u_k$ and denote it as

$$K = \operatorname{co}\Big(u_1, \ldots, u_k\Big).$$

If K is a unimodular cone spanned by a primitive set of vectors $u_1, \ldots, u_k$ then the fundamental parallelepiped

$$\Pi = \left\{ \sum_{i=1}^{k} \alpha_i u_i : \quad 0 \leq \alpha_i < 1 \quad \text{for} \quad i = 1, \ldots, k \right\}$$

contains no lattice points other than the origin (cf. Theorem 5.2) and by Lemma 31.2 for the generating function of integer points in K we have

$$f(K, \mathbf{x}) = \prod_{i=1}^{k} \frac{1}{1 - \mathbf{x}^{u_i}}.$$

(38.2) Decomposing a planar cone into unimodular cones using continued fractions. For $d = 2$, there is a rather efficient (polynomial time) algorithm to write the indicator of a cone $K \subset \mathbb{R}^d$ as an alternating sum of indicators of unimodular cones and hence to compute the generating function $f(K, \mathbf{x})$ of integer points in K.

We compute one example. Suppose that K is spanned by vectors $(1, 0)$ and $(31, 164)$. We write:

$$\frac{164}{31} = 5 + \frac{9}{31} = 5 + \frac{1}{3 + \frac{4}{9}} = 5 + \frac{1}{3 + \frac{1}{2 + \frac{1}{4}}},$$

and hence we write

$$\frac{164}{31} = [5; 3, 2, 4].$$

Next, we compute the convergents:

$$[5; 3, 2] = 5 + \frac{1}{3 + \frac{1}{2}} = \frac{37}{7}, \quad [5; 3] = 5 + \frac{1}{3} = \frac{16}{3} \quad \text{and} \quad [5] = \frac{5}{1}.$$

Let

$$K_{-1} = \operatorname{co}\left(\begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}0\\1\end{bmatrix}\right), \quad K_0 = \operatorname{co}\left(\begin{bmatrix}0\\1\end{bmatrix}, \begin{bmatrix}1\\5\end{bmatrix}\right), \quad K_1 = \operatorname{co}\left(\begin{bmatrix}1\\5\end{bmatrix}, \begin{bmatrix}3\\16\end{bmatrix}\right)$$
$$K_2 = \operatorname{co}\left(\begin{bmatrix}3\\16\end{bmatrix}, \begin{bmatrix}7\\37\end{bmatrix}\right) \quad \text{and} \quad K_3 = \operatorname{co}\left(\begin{bmatrix}7\\37\end{bmatrix}, \begin{bmatrix}31\\164\end{bmatrix}\right).$$

Then

$$[K] = [K_{-1}] - [K_0] + [K_1] - [K_2] + [K_3].$$

Besides, K_{-1}, K_0, K_1, K_2 and K_3 are unimodular cones since

$$\begin{aligned}1 = &\det\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix} = -\det\begin{bmatrix}0 & 1\\1 & 5\end{bmatrix} = \det\begin{bmatrix}1 & 3\\5 & 16\end{bmatrix} = -\det\begin{bmatrix}3 & 7\\16 & 37\end{bmatrix}\\ = &\det\begin{bmatrix}7 & 31\\37 & 164\end{bmatrix}.\end{aligned}$$

Thus

$$\begin{aligned}f(K, \mathbf{x}) = &f(K_{-1}, \mathbf{x}) - f(K_0, \mathbf{x}) + f(K_1, \mathbf{x}) - f(K_2, \mathbf{x}) + f(K_3, \mathbf{x})\\ = &\frac{1}{(1-x)(1-y)} - \frac{1}{(1-y)(1-xy^5)} + \frac{1}{(1-xy^5)(1-x^3y^{16})}\\ &- \frac{1}{(1-x^3y^{16})(1-x^7y^{37})} + \frac{1}{(1-x^7y^{37})(1-x^{31}y^{164})}.\end{aligned}$$

We note that by changing coordinates, we can represent an arbitrary rational cone in the form

$$K = \operatorname{co}\left(\begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}q\\p\end{bmatrix}\right) \tag{38.2.1}$$

for some coprime integers p and q.

(38.3) Problems.

1. For the cone (38.2.1), assuming that $p, q > 0$ are coprime integers, consider the continued fraction expansions

$$\frac{p}{q} = [a_0; a_1, \ldots, a_n].$$

For $i = 0, 1, \ldots, n$ consider convergents

$$[a_0; a_1, \ldots, a_i] = \frac{p_i}{q_i}$$

and define cones

$$K_{-1} = \operatorname{co}\left(\begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}\right), \quad K_0 = \operatorname{co}\left(\begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ p_0 \end{bmatrix}\right) \quad \text{and}$$

$$K_i = \operatorname{co}\left(\begin{bmatrix} q_{i-1} \\ p_{i-1} \end{bmatrix}, \begin{bmatrix} q_i \\ p_i \end{bmatrix}\right) \quad \text{for} \quad i = 1, \ldots, n.$$

Prove that each K_i is a unimodular cone and that

$$[K] = \sum_{i=-1}^{n} (-1)^{i+1} [K_i] \quad \text{if} \quad n \quad \text{is odd}$$

and

$$[K] = [R] + \sum_{i=1}^{n} (-1)^{i+1} [K_i] \quad \text{if} \quad n \quad \text{is even} \quad \text{where} \quad R = \operatorname{co}\left(\begin{bmatrix} q_n \\ p_n \end{bmatrix}\right).$$

Hint: Use Problem 2 of Section 9.4.

2. Let $K \subset \mathbb{R}^d$ be a unimodular cone with a non-empty interior. Prove that K° is a unimodular cone.

(38.4) Decomposing cones of higher dimensions. As long as the dimension d remains fixed, there is a polynomial time algorithm to write a given rational cone K as a signed combination of unimodular cones and hence to compute $f(K, \mathbf{x})$ as a rational function. We sketch the algorithm below.

First, we may assume that $K \subset \mathbb{R}^d$ is a cone with a non-empty interior (otherwise, we pass to the smallest subspace containing K). Triangulating, if needed, we reduce the case to that of a simple cone

$$K = \operatorname{co}\Big(u_1, \ldots, u_d\Big),$$

where $u_1, \ldots, u_d$ are linearly independent vectors. Let us define the *index* of K as the volume of the parallelepiped spanned by $u_1, \ldots, u_d$,

$$\operatorname{ind} K = |u_1 \wedge \ldots \wedge u_d|.$$

Hence $\operatorname{ind} K = 1$ if and only if K is unimodular. The algorithm consists in repeating a procedure which represents a non-unimodular cone as a signed combination of cones with smaller indices. The important feature of the procedure is that the number of the cones increases exponentially with the number of steps while the indices of the obtained cones decrease double exponentially.

Let us define

$$\Pi_0 = \left\{ \sum_{i=1}^{d} \alpha_i u_i : \quad |\alpha_i| \ \leq \ (\operatorname{ind} K)^{-1/d} \quad \text{for} \quad i = 1, \ldots, d \right\}.$$

Then Π_0 is a symmetric convex body and

$$\operatorname{vol}\Pi_0 = 2^d.$$

Hence by Minkowski Theorem (Theorem 6.4) there exists a non-zero vector $v \in \Pi$, which then can be found efficiently with the help of the Lenstra-Lenstra-Lovász basis. For $i \in \{1, \ldots, d\}$ let us define

$$K_i = \operatorname{co}\Big(u_1, \ldots, u_{i-1}, v, u_{i+1}, \ldots, u_d\Big)$$

provided vectors $u_1, \ldots, u_{i-1}, v, u_{i+1}, \ldots, u_d$ are linearly independent and $\epsilon_i = 1$ if replacing u_i by v in $u_1, \ldots, u_d$ preserves the orientation and $\epsilon_i = -1$ if replacing u_i by v in $u_1, \ldots, u_d$ reverses the orientation. Finally, let I be the set of all i for which vectors $u_1, \ldots, u_{i-1}, v, u_{i+1}, \ldots, u_d$ are linearly independent.

We can write

$$[K] \equiv \sum_{i \in I} \epsilon_i \, [K_i] \quad \text{modulo rational cones in hyperplanes} \tag{38.4.1}$$

and we note that

$$\operatorname{ind} K_i = |\alpha_i| \operatorname{ind} K \ \le \ (\operatorname{ind} K)^{(d-1)/d}.$$

If we iterate the procedure n times we obtain a decomposition of $[K]$ (modulo low-dimensional cone that can be handled separately) as a signed linear combination of at most d^n indicators of cones of indices not exceeding $(\operatorname{ind} K)^{\left(\frac{d-1}{d}\right)^n}$. Hence, if d is fixed in advance, we will need only

$$n = O\left(\log\log \operatorname{ind} K\right)$$

steps to achieve a unimodular decomposition (modulo lower-dimensional cones) with

$$(\log \operatorname{ind} K)^{O(1)}$$

cones.

The following "duality trick" allows one to discard lower-dimensional cones completely. Namely, let us apply the algorithm to the polar cone K°. Hence, from (38.4.1), we obtain

$$[K^\circ] \equiv \sum_{i \in I} \epsilon_i \, [K_i] \quad \text{modulo rational cones in hyperplanes,}$$

where K_i are unimodular cones. From Theorem 36.2, we get

$$[K] \equiv \sum_{i \in I} \epsilon_i \, [K_i^\circ] \quad \text{modulo rational cones with lines.}$$

Moreover, from Problem 2 of Section 38.3, we conclude that K_i° are unimodular cones. From Theorem 31.5, we obtain the corresponding identity for the generating functions:

$$f(K, \mathbf{x}) = \sum_{i \in I} \epsilon_i f\left(K_i^\circ, \mathbf{x}\right).$$