Math 669: Lattice Points in Geometry, Combinatorics and Optimization

Winter 1996

Contents.

Wednesday, January 10

---

1. Preview

(1.0) Preliminaries. The Euclidean space $\mathbb{R}^n$ is the vector space of all n-tuples $x = (x_1, \ldots, x_n) : x_i \in \mathbb{R}$. We fix the (standard) scalar product $\langle x, y \rangle = x_1 y_1 + \ldots + x_n y_n$ for $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$. Furthermore, $\|x\| = \sqrt{\sum_{i=1}^{n} x_i^2}$ is the norm in

$\mathbb{R}^n$. There is a volume form in $\mathbb{R}^n$: by $|u_1 \wedge \ldots \wedge u_n|$ we denote the volume of the "parallelepiped" $\Pi = \Big\{x = \alpha_1 u_1 + \ldots + \alpha_n u_n : 0 \le \alpha_i < 1, i = 1, \ldots, n\Big\}$ (for some reasons we prefer to consider such a "semi-open" parallelepiped). It is greater than zero if and only if $u_1, \ldots, u_n$ are linearly independent. A set $X \subset \mathbb{R}^n$ is called *convex* if and only if for any two points $x, y \in X$ the set contains the whole interval $[x, y] = \big\{\lambda x + (1-\lambda) y : 0 \le \lambda \le 1\big\}$.

(1.1) Definition. Let $u_1, \ldots, u_n$ be linear independent vectors in $\mathbb{R}^n$. The *lattice* Λ generated by $u_1, \ldots, u_n$ is the set of all integer combinations $u = m_1 u_1 + \ldots + m_n u_n$: $m_1, \ldots, m_n \in \mathbb{Z}$. A set $\Lambda \subset \mathbb{R}^n$ is called a *lattice* if and only if it is the lattice generated by some linearly independent vectors $u_1, \ldots, u_n$. In this case we call $u_1, \ldots, u_n$ a *basis* of the lattice.

We note that

a) Λ is an additive subgroup of $\mathbb{R}^n$, that is $x - y \in \Lambda$ provided $x, y \in \Lambda$;

b) Λ is *discrete*, that is there is an $r > 0$ such that the ball $B_r(0) = \big\{x \in \mathbb{R}^n : \|x\| \le r\big\}$ doesn't contain any point from Λ other than 0.

PROBLEMS.

1°. The set $\mathbb{Z} \subset \mathbb{R}$ of all integers is a lattice. The set $\mathbb{Z}^n \subset \mathbb{R}^n$ of all integral vectors is a lattice, called *integral lattice.*

2. Prove that every lattice is a discrete additive subgroup in $\mathbb{R}^n$.

Hint: Every lattice $\Lambda \subset \mathbb{R}^n$ is the image of $\mathbb{Z}^n$ under a non-degenerate linear transformation of $\mathbb{R}^n$.

3*. Every additive discrete subgroup $\Lambda \subset \mathbb{R}^n$ which spans the whole vectors space $\mathbb{R}^n$ is a lattice.

(1.2) Overview. As an algebraic structure, lattice Λ is just a free Abelian group of a finite rank. What makes lattices interesting is that they are embedded in $\mathbb{R}^n$ and hence they acquire metric properties.

We are going to spend some (little) time on studying lattices as free Abelian groups. The main result we are after is the so-called "Smith Normal Form" (also known as "invariant divisors" theorem): if $\Lambda_0 \subset \Lambda$ is a sublattice then there is a basis $e_1, \ldots, e_n$ of Λ and a basis $u_1, \ldots, u_n$ of Λ_0 such that $u_i = m_i e_i$ for positive integers $m_1, \ldots, m_n$ such that $m_1 | m_2 | \ldots | m_{n-1} | m_n$.

Then we turn to the metric properties of lattices. The central result is the celebrated "Minkowski First Theorem": a convex centrally symmetric body of the volume greater than 2^n contains a nonzero integral point. Here is a typical question where this theorem helps (enormously): given a lattice $\Lambda \subset \mathbb{R}^n$, what is the length of a shortest nonzero lattice vector? We will prove that every lattice has a basis $u_1, \ldots, u_n$ which is nearly orthogonal: $\|u_1\| \cdots \|u_n\| \le const(n) |u_1 \wedge \ldots \wedge u_n|$. We will prove a "flatness theorem" (there are many of them): if a convex (not necessarily centrally symmetric) body does not contain any lattice point then it has small width in some lattice direction and looks like a pancake squeezed between two layers of lattice points.

The bulk of the time we will spend on the combinatorics of lattices. Lattices go best with *polytopes.* We start with the Pick formula: the number of lattice points in an integral polygon is equal to its area plus half the number of points on its boundary plus 1. Then we turn to general McMullen's theorems on lattice-invariant valuations. Ultimate purpose is to explain why various combinatorial numbers behave polynomially. Here is a typical example: a *magic square* of size r and weight n is an $r \times r$ table filled by nonnegative integers such that all row and column sums are equal to n. Then we prove that the number $P_r(n)$ of magic squares of a fixed size r is a polynomial in n of the degree $(r-1)^2$. Furthermore, $P_r(-1) = P_r(-2) = \ldots = P_r(-r+1) = 0$.

Finally, we discuss some recent results on lattice points (initiated by M. Brion's paper of 1988). Surprisingly enough, these results concern various generalizations of the formula for the sum of the (finite) geometric series. Let us consider an integer interval $[0 : n] = \{0, 2, \ldots, n\}$. With every point k from the interval we associate the monomial x^k. Then as we know $\sum_{k=0}^{n} x^k = \frac{1-x^{n+1}}{1-x}$. Let us consider the sums over the rays $[0, +\infty)$ and $(-\infty, n]$. We get

$$\sum_{k=0}^{+\infty} x^k = \frac{1}{1-x} \quad \text{converges for } |x| < 1;$$

$$\sum_{k=-\infty}^{n} x^k = \frac{x^n}{1-x^{-1}} = \frac{-x^{n+1}}{1-x} \quad \text{converges for } |x| > 1.$$

If we disregard convergence as irrelevant to combinatorics, we can write a funny formula:

$$\sum_{k=0}^{n} x^k = \sum_{k=0}^{+\infty} x^k + \sum_{k=-\infty}^{n} x^k.$$

Brion's theorem concerns a multidimensional generalization of the above identity. Instead of the interval, we consider an integral polytope (for example, a triangle on the plane with integral vertices). Instead of x^k we assign to every integral point $k = (k_1, \ldots, k_n)$ a monomial $x_1^{k_1} \cdots x_n^{k_n}$ (a monomial $x^{k_1} y^{k_2}$ for an integral point on the plane). Instead of the rays we consider cones at the vertices of the polytope (so take the sum over all integral points in the angles of the triangle). The remarkable fact is that the formula remains true in this general setting.

PROBLEMS.

1°. Check the Pick formula for the square with the vertices $(0,0), (0,n), (n,0), (n,n)$.

2^*. Prove the Pick formula.

3°. The number $P_2(n)$ of 2×2 magic squares is a polynomial in n and $P_2(-1) = 0$.

4. Find $P_3(n)$.

2. Determinant of a Lattice

We recall (see Definition 1.1) that a *basis* of a lattice $\Lambda \subset \mathbb{R}^n$ is a set of linearly independent vectors $u_1, \ldots, u_n \in \Lambda$ such that every vector $u \in \Lambda$ can be represented (necessarily in a unique way) as $u = m_1 u_1 + \ldots + m_k u_k$, where $m_i \in \mathbb{Z}$ are integers.

(2.1) Definition. Let $u_1, \ldots, u_n$ be a basis of a lattice Λ. The parallelepiped

$$\Pi = \Big\{ \sum_{i=1}^{n} \alpha_i u_i : \ 0 \leq \alpha_i < 1 \Big\}$$

is called a *fundamental parallelepiped*
(or the fundamental parallelepiped of the basis $u_1, \ldots, u_n$).

(2.2) Theorem. *Let us fix a lattice $\Lambda \subset \mathbb{R}^n$. The volume $|u_1 \wedge \ldots \wedge u_n|$ of the fundamental parallelepiped does not depend on the basis of Λ.*

Proof. Let $u_1, \ldots, u_n$ and $v_1, \ldots, v_n$ be two bases of Λ. Then $u_i = m_{i1} v_1 + \ldots + m_{in} v_n$ for $i = 1, \ldots, n$ and some integers m_{ij} and $v_j = k_{j1} u_1 + \ldots + k_{jn} u_n$ for $j = 1, \ldots, n$ and some integers k_{ij}. We have two integer matrices $M = (m_{ij}) : i, j = 1, \ldots, n$ and $K = (k_{ij}) : i, j = 1, \ldots, n$. We must have $MK = I$, the identity matrix, which implies $\det M \cdot \det K = 1$. Since M and K are integral matrices, $\det M$ and $\det K$ are integers. Therefore $\det M = \det K = 1, -1$ are the only two possibilities. Now $|v_1 \wedge \ldots \wedge v_n| = |\det K||u_1 \wedge \ldots u_n| = |u_1 \wedge \ldots u_n|$. $\square$

(2.3) Definition. The volume of a fundamental parallelepiped of a lattice Λ is called the *determinant* of Λ and denoted $\det \Lambda$.

A fundamental parallelepiped has one important property:

(2.4) Lemma. *Let Π be a fundamental parallelepiped of a lattice $\Lambda \subset \mathbb{R}^n$. Then for any point $x \in \mathbb{R}^n$ there exist a unique pair $v \in \Lambda$, $y \in \Pi$ such that $x = v + y$.*

Proof. Let $u_1, \ldots, u_n$ be the basis of Λ with the fundamental parallelepiped Π. Since $u_1, \ldots, u_n$ is a basis of $\mathbb{R}^n$ we have $x = \alpha_1 u_1 + \ldots + \alpha_n u_n$ for some real $\alpha_1, \ldots, \alpha_n$. Let us denote by $\{\cdot\}$ the fractional part and by $[\cdot]$ the integer part of a number. So $[\alpha]$ is the largest integer which does not exceed α and $\{\alpha\} = \alpha - [\alpha]$. We may choose

$$v = [\alpha_1] u_1 + \ldots + [\alpha_n] u_n \qquad \text{and} \quad y = \{\alpha_1\} u_1 + \ldots + \{\alpha_n\} u_n.$$

Then $x = y + v, v \in \Lambda$ and $y \in \Pi$.

Let us prove uniqueness. Suppose that $x = v_1 + y_1 = v_2 + y_2$. Then $y_2 - y_1 = v_1 - v_2$ is a nonzero lattice vector, say v. So if $y_1 = \alpha_1 u_1 + \ldots + \alpha_n u_n$ and $y_2 = \beta_1 u_1 + \ldots + \beta_n u_n$ then $v = \gamma_1 u_1 + \ldots + \gamma_n u_n$, where $\gamma_i = \alpha_i - \beta_i$. Since $0 \leq \alpha_i, \beta_i < 1$ we get that $|\gamma_i| < 1$ for all i. On the other hand, since $v \in \Lambda$, we must have γ_i to be integers. Hence $\gamma_i = 0$ for $i = 1, \ldots, n$ and $v = 0$ which is a contradiction. $\square$

(2.5) Corollary. *Translates $\Pi + u : u \in \Lambda$ of a fundamental parallelepiped Π cover the whole space $\mathbb{R}^n$ without overlapping.*

$\square$

PROBLEMS.

1. The vectors $u_1 = (5,3)$ and $u_2 = (8,5)$ form a basis of the lattice $\mathbb{Z}^2$ whereas the vectors $u_1 = (5,3)$ and $u_2 = (6,4)$ do not form a basis of $\mathbb{Z}^2$.

2. Integral vectors $u_1, \ldots, u_n$ constitute a basis of $\mathbb{Z}^n$ if and only if $|u_1 \wedge \ldots \wedge u_n| = 1$.

3. Lattice vectors $u_1, \ldots, u_n \in \Lambda$ constitute a basis of Λ if and only if $|u_1 \wedge \ldots \wedge u_n| = \det L$.

4. Linear independent vectors $u, v \in \mathbb{Z}^2$ constitute a basis of $\mathbb{Z}^2$ if and only if the triangle with the vertices $0, u$ and v does not contain any integral point other than $0, u$ and v.

5*. The natural generalization of Problem 4 is incorrect: there exist 3 linearly independent vectors $u, v, w \in \mathbb{Z}^3$ such that the tetrahedron with the vertices $0, u, v, w$ does not contain any integral point other than $0, u, v, w$ but u, v, w is *not* a basis of $\mathbb{Z}^3$.

6. Let $\#\big\{\Lambda \cap B_r(0)\big\}$ be the number of lattice points in the ball of radius r. Then

$$\lim_{r \longrightarrow +\infty} \frac{\#\big\{\Lambda \cap B_r(0)\big\}}{\mathrm{vol} B_r(0)} = \Big(\det \Lambda\Big)^{-1}.$$

7*. Here is the most exquisite definition of the determinant of a lattice. Since $\Lambda \subset \mathbb{R}^n$ is a subgroup of $\mathbb{R}^n$ we may consider the quotient $\mathbb{R}^n/\Lambda$. This is an Abelian group which can be viewed as an n-dimensional torus T^n (the product of n circles). The projection $\mathbb{R}^n \longrightarrow T^n$ can be made locally measure preserving. Then $\det \Lambda$ is the volume $\mathrm{vol}\, T^n$ of the quotient.

Friday, January 12

---

3. Discrete Subgroups

Here we give an invariant definition of a lattice (see Problems 2-3 in Section 1.1). We start with some problems.

PROBLEMS.

1°. Let $\Lambda \subset \mathbb{R}^n$ be a discrete subgroup of $\mathbb{R}^n$, meaning that $x - y \in \Lambda$ for any pair of $x, y \in \Lambda$ and that a certain ball $B_r(0) = \big\{x \in \mathbb{R}^n : \|x\| \leq r\big\}$ for some $r > 0$ does not contain any point of Λ other than 0. Prove that for any $u \in \Lambda$ a translation $B_r(u) = B_r(0) + u$ does not contain any point from Λ other than u.

2. If $\Lambda \subset \mathbb{R}^n$ is a discrete additive subgroup then every ball $B_r(0)$ contains only finitely many points from Λ.

(3.1) Theorem. *A set $\Lambda \subset \mathbb{R}^n$ is a lattice if and only if it is a discrete additive subgroup of $\mathbb{R}^n$ whose linear hull is the whole space $\mathbb{R}^n$.*

Proof. The first part: lattice $\Longrightarrow$ discrete additive subgroup is easy (Problem 2 in Section 1.1). The proof is based on the two observations: $\mathbb{Z}^n$ is a discrete additive subgroup and every lattice is the image of $\mathbb{Z}^n$ under a non-degenerate linear transformation of $\mathbb{R}^n$.

The second part: discrete additive subgroup $\Longrightarrow$ lattice is a bit more tricky (Problem 3 in Section 1.1). Let's prove it. Suppose Λ is a subgroup in question. We are going to construct a basis $u_1, \ldots, u_n$ of Λ, so that every point $v \in \Lambda$ can be represented in the unique way as $v = m_1 u_1 + \ldots + m_n u_n$ for some integral $m_1, \ldots, m_n$. We do it step by step. First, let us choose any nonzero vector $b_1 \in \Lambda$. Let us choose u_1 to be the vector from Λ in the form $u_1 = \beta b_1$ with the smallest $\beta > 0$. So u_1 is the shortest nonzero vector from Λ on the interval $[0, b_1]$ (since Λ is discrete, such an u_1 exists, cf. Problem 2 above). Suppose $u_1, \ldots, u_{k-1}$ are chosen for some $k \leq n$. We choose u_k as follows. Let us choose a vector $b_k \in \Lambda$, so that $u_1, \ldots, u_{k-1}, b_k$ are linearly independent (this is possible since Λ spans the whole space $\mathbb{R}^n$). Now let

$$\Pi = \bigl\{\alpha_1 u_1 + \ldots + \alpha_{k-1} u_{k-1} + \alpha_k b_k : 0 \leq \alpha_i \leq 1\bigr\}$$

be the parallelepiped spanned by $u_1, \ldots, u_{k-1}, b_k$. We choose u_k to be a vector from $\Lambda \cap \Pi$ with the smallest nonzero coefficient β in the decomposition

$$u_k = \alpha_1 u_1 + \ldots + \alpha_k u_k + \beta b_k$$

(such a vector exists, because Π is bounded and Λ is discrete, cf. Problem 2 above).

Let L_k be the linear subspace in $\mathbb{R}^n$ generated by $u_1, \ldots, u_k$ and $\Lambda_k = \Lambda \cap L_k$, We claim that Λ_k is a lattice (as a subset of the k-dimensional Euclidean space L_k) with the basis $u_1, \ldots, u_k$. We prove this by induction on k.

Suppose that $k = 1$. Then L_1 is a line and $\Lambda_1 = \Lambda \cap L_1$ is a discrete additive subgroup of L_1. Let us choose any $v \in \Lambda_1$. Then $v = \alpha u_1$ for some real α. Denoting by $[\alpha]$ the integer part of α, we observe that $[\alpha] u_1 \in \Lambda_1$ (since $u_1 \in \Lambda_1$). Since Λ_1 is a subgroup, we must have $\alpha_1 u_1 - [\alpha_1] u_1 = \{\alpha_1\} u_1 \in \Lambda_1$. If $\{\alpha\} \neq 0$ then $\{\alpha_1\} u_1$ is a nonzero vector from Λ on the interval $[0, b_1]$ which is shorter than u_1. We get a contradiction. So $\{\alpha\} = 0$ meaning that α is an integer. So Λ_1 is a lattice generated by u_1.

Suppose that the result is proven for $k-1$. Let us choose $v \in \Lambda_k$. Then $v = w + \alpha_k u_k$ for some $w \in L_{k-1}$ and some real α_k. Since $u_k \in \Lambda_k$, Λ_k is a subgroup and $[\alpha_k] u_k \in \Lambda_k$, we have $v_1 = w + \{\alpha_k\} u_k \in \Lambda_k$. Since $u_k \in \Pi$, we have $u_k = w_1 + \beta b_k$ for some $0 < \beta \leq 1$ and some $w_1 \in L_{k-1}$ Therefore we can write $v_1 = w_2 + \{\alpha_k\}\{\beta\} b_k$ for some $w_2 \in L_{k-1}$. Suppose that $w_2 = \alpha_1 u_1 + \ldots + \alpha_{k-1} u_{k-1}$ for some real $\alpha_1, \ldots, \alpha_{k-1}$. Since $v_1 \in \Lambda_k$, Λ_k is a subgroup and the point $[\alpha_1] u_1 + \ldots + [\alpha_{k-1}] u_{k-1}$ belongs to Λ_k, we get that

$$v_2 = \{\alpha_1\} u_1 + \ldots + \{\alpha_{k-1}\} u_{k-1} + \{\alpha_k\} \beta b_k$$

is a point from Λ_k. Obviously, $v_2 \in \Pi$. On the other hand, the coefficient $\{\alpha_k\}\beta$ of v_2 in front of b_k is strictly smaller than the coefficient β of u_k in front of b_k. Hence we must have $\{\alpha_k\} = 0$, that is α_k has to be integral. Then $w = v - \alpha_k u_k \in \Lambda_{k-1}$ and we may apply the induction conjecture to w. So $w = \alpha_1 u_1 + \ldots \alpha_{k-1} u_{k-1}$ for some integers $\alpha_1, \ldots, \alpha_{k-1}$ and the proof follows. □

PROBLEMS.

1°. Let $\Lambda \subset \mathbb{R}^n$ be a lattice and $X = \{x_i \in \Lambda\}$ be a set (finite or infinite) of points from Λ which contains n linearly independent points. Let Λ_0 be the set of all finite integral linear combinations $\sum_{i \in I} m_i x_i : \ m_i \in \mathbb{Z}$ of the points from X. Then Λ_0 is a lattice.

2. A set $S \subset \mathbb{R}^n$ is called a *semigroup* if and only if for any two $x, y \in S$ we have $x + y \in S$. A set of points $X \subset S$ is said to be a set of *generators* of S if and only if every $s \in S$ can be represented as a finite linear combination with nonnegative integral coefficients $s = \sum_{i \in I} m_i x_i$, where $x_i \in X, m_i \in \mathbb{Z}$ and $m_i \geq 0$ for all i.

Show that there is a semigroup $S \subset \mathbb{Z}^2$ which does not have a finite set of generators.

Hint: Consider $S = \{(m,n) : 0 \leq n \leq \sqrt{2}m,\ m \text{ and } n \text{ are nonnegative integers }\}$.

3. Let α be a positive number. Consider the set $S = \{(m,n) : 0 \leq n \leq \alpha m,\ m \text{ and } n$ are nonnegative integers $\}$. Then S is a semigroup which has a finite set of generators if and only if α is rational.

4. Every semigroup $S \subset \mathbb{Z}$ has a finite set of generators.

Wednesday, January 17

---

4. Sublattices

We start with some problems.

PROBLEMS

1°. Let $u_1, \ldots, u_n$ be a basis of a lattice $\Lambda \subset \mathbb{R}^n$ and a be an integer number. Let us choose $1 \leq i \neq j \leq n$. Then $u_1, \ldots, u_{i-1}, u_i + a u_j, u_{i+1}, \ldots, u_n$ is a basis of Λ.

2°. An integer $n \times n$ matrix A is called *unimodular* if and only if $|\det A| = 1$. Prove that A is unimodular if and only if A and A^{-1} are integer matrices.

3°. Prove that the set $GL(n, \mathbb{Z})$ of all $n \times n$ unimodular matrices is a group, that is $AB^{-1} \in GL(n, \mathbb{Z})$ for any two $A, B \in GL(n, \mathbb{Z})$.

4. Let $a = (a_1, \ldots, a_n)$ be a string of integers whose greatest common divisor is 1. Then one can find a unimodular matrix A whose first row is a.

(4.1) Definition. Let $\Lambda \subset \mathbb{R}^n$ be a lattice and $\Lambda_0 \subset \Lambda$. If Λ_0 is a lattice we say that Λ_0 is a *sublattice* of Λ. Since Λ_0 is a subgroup of an Abelian group, we may define the quotient group $\Lambda : \Lambda_0$. Its cardinality is called the *index* of Λ_0 in Λ and denoted $|\Lambda : \Lambda_0|$.

Thus if $|\Lambda : \Lambda_0| = s$ then Λ can be represented as a union of s non-intersecting cosets $\Lambda = \bigcup_{i=1}^{s} \Big(\Lambda_0 + a_i\Big)$, where $a_1, \ldots, a_s \in \Lambda$.

PROBLEM.

1°. Let $\Lambda_0 \subset \mathbb{Z}^2$ be the subset consisting of all pairs (m, n), where m is even and n is divisible by 3. Then Λ_0 is a sublattice in $\mathbb{Z}^2$ of the index 6.

The following fundamental result is known as the "invariant divisors" Theorem or the "Smith Normal Form" Theorem.

(4.2) Theorem. *Let Λ_0 be a sublattice of a lattice $\Lambda \subset \mathbb{R}^n$. Then there exists a basis $u_1, \ldots, u_n$ of Λ and a basis $v_1, \ldots, v_n$ of Λ_0 such that $v_i = m_i \cdot u_i : \ i = 1, \ldots, n$, where $m_1, \ldots, m_n$ are positive integers such that m_i divides m_j for $j > i$.*

Proof. For a basis $u = (u_1, \ldots, u_n)$ of Λ and a basis $v = (v_1, \ldots, v_n)$ of Λ_0 we define the matrix $M(u, v)$ as an integer $n \times n$ matrix (m_{ij}) of the decompositions

$$v_1 = m_{11}u_1 + \ldots + m_{1n}u_n, \quad \ldots, \quad v_n = m_{n1}u_1 + \ldots + m_{nn}u_n.$$

Let $\mathcal{M}$ be the set of all possible matrices $M(u, v)$. We prove by induction that for every $k = 1, \ldots, n$ there exists a matrix $M \in \mathcal{M}$ such that

(4.2.1) all non-diagonal entries in the first k rows and first k columns of M are zeros;

(4.2.2) $m_{11}, \ldots, m_{kk}$ are positive integers where m_{ii} divides m_{jj} for $j > i$ and m_{kk} divides all the entries m_{ij} with $i > k$ or $j > k$.

We get the theorem when $k = n$.

Let us prove the statement for $k = 1$. First, we claim that there is $M \in \mathcal{M}$ with $m_{11} > 0$. Indeed, let us take any matrix $M(u, v) \in \mathcal{M}$. There exists at least one nonzero element m_{ij}. If $m_{ij} < 0$ then taking a new basis $v' = (v_1, \ldots, -v_i, \ldots, v_n)$ of Λ_0 we get a matrix $M \in \mathcal{M}$ with $m_{ij} > 0$. Reordering the vectors $u_1, \ldots, u_n$ and $v_1, \ldots, v_n$ we get an $M(u, v)$ with $m_{11} > 0$.

Let us take a matrix $M \in \mathcal{M}$ with the smallest positive $m_{11} = m_1$. We claim that every entry m_{1j} and every entry m_{i1} is divisible by m_1. Suppose that for some j we have m_{1j} is not divisible by m_1. Then $m_{1j} = sm_1 + r$ for some integer s and some positive integer $r < m_1$. Let us define a new basis $u' = (u_1', u_2, \ldots, u_n)$, where $u_1' = u_1 + su_j$ of Λ. Then $u_1 = u_1' - su_j$ and in the decomposition of v_1 with respect to the basis $u_1', \ldots, u_n$ the coefficient m_{ij}' is equal to $m_{ij} - sm_{11} = r < m_1$. After interchanging u_1' and u_j we get a matrix from $\mathcal{M}$ for which the first diagonal element is smaller than m_1, which is a contradiction. Therefore every m_{1j} is divisible by m_{11}. Similarly, we prove that every m_{i1} is divisible by m_1. Indeed, suppose that for some i we have $m_{i1} = sm_1 + r$ for some integer s and a positive $r < m_1$. Let us define a new basis $v' = (v_1, \ldots, v_i', \ldots, v_n)$, where $v_i' = v_i - sv_1$ of Λ_0. Then the coefficient m_{i1}' of the decomposition of v_i' with respect to the basis $u_1, \ldots, u_n$ is equal to $m_{i1} - sm_1 = r < m_1$. After interchanging v_1 and v_i' we get a matrix from $\mathcal{M}$ with the first diagonal element smaller than m_1 which is a contradiction.

So in a matrix $M \in \mathcal{M}$ with the smallest positive m_{11} we have m_{i1} and m_{1j} divisible by m_{11}. Let $u_1, \ldots, u_n$ and $v_1, \ldots, v_n$ be the corresponding pair of bases. Let $m_{i1} = s_i m_{11}$ and $m_{1i} = d_i m_{11}$ for $i = 2, \ldots, n$. Modifying $v_i' = v_i - s_i v_1$ for $i = 2, \ldots, n$ and $u_1' = u_1 + d_2 u_2 + \ldots + d_n u_n$ we get a pair u', v' of bases such that for $M = M(u', v')$ we have $m_{i1} = m_{1i} = 0$ for $i > 2$ and m_{11} is the smallest positive number that can occupy the first diagonal entry of a matrix from $\mathcal{M}$. We claim now that every m_{ij} is divisible by m_{11}. Indeed, suppose that $m_{ij} = sm_{11} + r$ for some integer s, some positive integer $s < r$ and some i, j. Let $u_1, \ldots, u_n$ and $v_1, \ldots, v_n$ be a pair of bases corresponding to the matrix M. We can modify the bases $u_1' = u_1 + su_j$, $v_i' = v_i + v_1$ so that the new coefficient m_{ij} would become $m_{ij} - sm_{11} = r$. After reordering the bases, we could get r as the top diagonal element of a matrix from $\mathcal{M}$ which is a contradiction.

So we have proven (4.2.1)-(4.2.2) for $k = 1$. To prove it for a general k we define the set $\mathcal{M}_{k-1}$ of all possible matrices $M(u, v)$ which satisfy the conditions (4.2.1)-(4.2.2), find a matrix $M \in \mathcal{M}_{k-1}$ with the smallest positive element $m_{k+1,k+1}$ and proceed as above. $\square$

PROBLEMS.

1. Consider the lattice $\Lambda = \mathbb{Z}^2$ and its sublattice Λ_0 described in Problem 1° in (4.1). There is a basis u_1, u_2 of $\mathbb{Z}^2$ and a basis v_1, v_2 of Λ_0 such that $v_1 = u_1$ and $v_2 = 6u_2$.

Hint: Consider $u_1 = v_1 = (2, 3)$, $u_2 = (1, 1)$ and $v_2 = (6, 6)$.

2°. Let $\mathcal{M}$ be the class of all matrices $M(u, v)$ as defined in Theorem 4.2. The following operations preserve $\mathcal{M}$:

- permutation of rows or columns of $M \in \mathcal{M}$;
- multiplication of rows or columns by -1
- adding one row (column) multiplied by an integer to another row (column).

(4.3) Theorem. *Let Λ_0 be a sublattice of $\Lambda \subset \mathbb{R}^n$. The index $|\Lambda : \Lambda_0|$ can be found as*

(4.3.1) the number $|\Lambda \cap \Pi|$ of points from Λ in any fundamental parallelepiped

$$\Pi = \{\alpha_1 v_1 + \ldots + \alpha_n v_n : \ 0 \leq \alpha_i < 1\}, \quad v_1, \ldots, v_n \ \text{ is a basis of } \Lambda_0$$

of Λ_0;

(4.3.2) the absolute value of the determinant $\det M$ of the matrix $M = (m_{ij})$:

$$v_1 = m_{11} u_1 + \ldots + m_{1n} u_n, \quad \ldots, \quad v_n = m_{n1} u_1 + \ldots + m_{nn} u_n$$

for any basis $u_1, \ldots, u_n$ of Λ and any basis $v_1, \ldots, v_n$ of Λ_0;

(4.3.3) the ratio $(\det \Lambda_0) : (\det \Lambda)$.

Proof. We use Lemma 2.4 to prove 4.3.1. Namely, for every $x \in \Lambda$ there exists a unique pair $v \in \Lambda_0$ and $y \in \Pi$ such that $x = v + y$. Since $x \in \Lambda$ and $v \in \Lambda_0 \subset \Lambda$ we must have

$y \in \Lambda$. Thus we can write $\Lambda = \bigcup_{y \in \Pi \cap \Lambda} y + \Lambda_0$, where different cosets $y_1 + \Lambda_0$ and $y_2 + \Lambda_0$ do not intersect. So 4.3.1 is proven.

To prove (4.3.2)-(4.3.3) we note that $|v_1 \wedge \ldots \wedge v_n| = |\det M||u_1 \wedge \ldots \wedge u_n|$ and thus $\det M = \det \Lambda_0 : \det \Lambda$. In particular, (4.3.2) and (4.3.3) are equivalent. Let us choose a special pair of bases for Λ and Λ_0 for which the matrix M is diagonal, namely the bases from Theorem 4.2. A point $u \in \Lambda$ belongs to the fundamental parallelepiped $\Pi = \Big\{\alpha_1 m_1 u_1 + \ldots + \alpha_n m_n u_n : \ 0 \leq \alpha_i < 1\Big\}$ of Λ_0 if and only if $\alpha_i \in \Big\{0, \frac{1}{m_i}, \frac{2}{m_i}, \ldots, \frac{m_i - 1}{m_i}\Big\}$. Hence the number $|\Lambda \cap \Pi|$ of points from Λ in Π is equal to $m_1 \cdots m_n = \det M$. We apply (4.3.1) now. □

We get a remarkable corollary.

(4.4) Corollary. *Let $v_1, \ldots, v_n \in \mathbb{Z}^n$ be linearly independent integral vectors. The number of integral points in the "semi-open" parallelepiped*

$$\Pi = \Big\{\alpha_1 v_1 + \ldots + \alpha_n v_n : \ 0 \leq \alpha_i < 1 \textit{ for } i = 1, \ldots, n\Big\}$$

is equal to the volume $|v_1 \wedge \ldots \wedge v_n|$ of Π.

Proof. We apply Theorem 4.3 to the lattices $\Lambda = \mathbb{Z}^n$ and Λ_0 generated by $v_1, \ldots, v_n$. □

PROBLEMS

1. Deduce (4.3.2)-(4.3.3) from (4.3.1) and Problem 6 in Section 2.5 without using Theorem 4.2.

2°. Let $\Lambda \subset \mathbb{R}^n$ be a lattice. Linearly independent points $u_1, \ldots, u_n \in \Lambda$ constitute a basis of Λ if and only if the parallelepiped $\Pi = \big\{\alpha_1 u_1 + \ldots + \alpha_n u_n : 0 \leq \alpha_i < 1\big\}$ doesn't contain any lattice point other than 0. Equivalently, its volume is equal to $\det \Lambda$ (cf. Problem 3, Section 2.5).

3. This is how we can prove the Pick formula: the number of integral points in a convex polygon with integral vertices is equal to its area plus half the points on the boundary plus 1:

a) Let $a, b \in \mathbb{Z}^2$ be linearly independent integral vectors and $c = a + b$. Prove that the number of integral points in the triangle with the vertices $0, a, b$ is the same as in the triangle with the vertices a, b, c.

Hint: If x is an integral point in one triangle then $c - x$ is an integral point in the other.

b) Using Corollary 4.4 for a semi-open integral parallelogram (the number of integral points is equal to the area) and a), prove the Pick formula for a triangle with integral vertices.

c) Prove the Pick formula in the whole generality using induction on the number of vertices of the polygon and b).

5. Dual Lattice

(5.1) Theorem. *Let $\Lambda \subset \mathbb{R}^n$ be a lattice. The set*

$$\Lambda^* = \Big\{ x \in \mathbb{R}^n : \langle x, y \rangle \in \mathbb{Z} \text{ for any } y \in \Lambda \Big\}$$

is a lattice in $\mathbb{R}^n$, called the dual or reciprocal lattice. If $u_1, \ldots, u_n$ is a basis of Λ then the set of vectors $u_1^*, \ldots, u_n^*$ such that

$$\langle u_i, u_j^* \rangle = \begin{cases} 1 & \text{if } i = j; \\ 0 & \text{if } i \neq j, \end{cases}$$

is a basis of Λ^*, called dual to $u_1, \ldots, u_n$. Furthermore, $\det \Lambda^* = \Big(\det \Lambda\Big)^{-1}$.

Proof. Let us choose any $y \in \Lambda$, $y = m_1 u_1 + \ldots + m_n u_n$, where m_i are integers. Then $\langle y, u_i^* \rangle = m_i \in \mathbb{Z}$, so $u_i^* \in \Lambda^*$. Furthermore, integral linear combinations of u_i^* also belong to Λ^*. Let us choose any $x \in \Lambda^*$. Then $\langle x, u_i \rangle = m_i \in \mathbb{Z}$ for $i = 1, \ldots, n$. Consider $z = m_1 u_1^* + \ldots + m_n u_n^*$. Then $\langle x - z, u_i \rangle = 0$ for any $i = 1, \ldots, n$, so $x = z$. Therefore Λ^* is the lattice generated by $u_1^*, \ldots, u_n^*$. Now it is easily seen that

$$\det \Lambda^* = |u_1^* \wedge \ldots \wedge u_n^*| = |u_1 \wedge \ldots \wedge u_n|^{-1} = \Big(\det \Lambda\Big)^{-1}.$$

□

PROBLEMS.

1°. If Λ_0 is a sublattice of Λ then Λ^* is a sublattice of Λ_0^*. Furthermore, $|\Lambda : \Lambda_0| = |\Lambda_0^* : \Lambda^*|$. Furthermore, $\Lambda : \Lambda_0$ and $\Lambda_0^* : \Lambda^*$ are isomorphic as groups.

2°. $\Big(\mathbb{Z}^n\Big)^* = \mathbb{Z}^n$.

3°. $\big(\Lambda^*\big)^* = \Lambda$.

4. A lattice Λ is called *self-dual* if and only if $\Lambda^* = \Lambda$. So, in Problem 2 above we saw that $\mathbb{Z}^n$ is self-dual. Here are some other examples of self-dual lattices:

a) The lattice E_8. Let us define $E_8 \subset \mathbb{R}^8$ as the set of all vectors $(x_1, \ldots, x_8)$, where $x_1 + \ldots + x_8$ is an even integer and either every x_i is an integer or every x_i is an integer plus $\dfrac{1}{2}$. Then E_8 is a self-dual lattice. Furthermore, $\langle u, u \rangle$ is an even integer for any $u \in E_8$ (such self-dual lattices are called *even* lattices). Prove that E_8 has a basis:

$u_1 = (2, 0, 0, 0, 0, 0, 0, 0)$, $u_2 = (-1, 1, 0, 0, 0, 0, 0, 0)$,

$u_3 = (0, -1, 1, 0, 0, 0, 0, 0)$,$u_4 = (0, 0, -1, 1, 0, 0, 0, 0)$,

$u_5 = (0,0,0,-1,1,0,0,0)$, $u_6 = (0,0,0,0,-1,1,0,0)$,
$u_7 = (0,0,0,0,0,-1,1,0)$, $u_8 = (1/2,1/2,1/2,1/2,1/2,1/2,1/2,1/2)$.

b) The lattice D_{12}^+. Let us define $D_{12}^+ \subset \mathbb{R}^{12}$ as the subset consisting of the vectors of the following two types: type 1: integer vectors $(x_1,\ldots,x_{12})$ with $x_1+\ldots+x_{12}$ being an even integer; type 2: a vector of type 1 plus $(1/2,\ldots,1/2)$. Then D_{12}^+ is a self-dual lattice. This lattice is *odd* since there is a vector $u \in D_{12}^+$ with an odd value of $\langle u,u\rangle$.

c)* The Leech lattice Λ_{24}. The lattice $\Lambda_{24} \subset \mathbb{R}^{24}$ has the basis $u_i = \dfrac{1}{\sqrt{8}} v_i$, where v_i are given below (we give non-zero components only, indicating their positions by indices, thus $4_{1,3}$ means that the only non-zero entry is 4 in the first and third position and 2_{1-8} means that the only non-zero entry is 2 in the positions 1,2,3,4,5,6,7,8).

$v_1 = 8_1, v_2 = 4_{1,2}, v_3 = 4_{1,3}, v_4 = 4_{1,4}, v_5 = 4_{1,5}, v_6 = 4_{1,6}, v_7 = 4_{1,7}, v_8 = 2_{1-8}$,
$v_9 = 4_{1,9}, v_{10} = 4_{1,10}, v_{11} = 4_{1,11}, v_{12} = 2_{1-4,9-12}$,
$v_{13} = 4_{1,13}, v_{14} = 2_{1,2,5,6,9,10,13,14}, v_{15} = 2_{1,3,5,7,9,11,13,15}, v_{16} = 2_{1,4,5,8,9,12,13,16}$,
$v_{17} = 4_{1,17}, v_{18} = 2_{1,3,5,8,9,10,17,18}, v_{19} = 2_{1,4,5,6,9,11,17,19}, v_{20} = 2_{1,2,5,7,9,12,17,20}$,
$v_{21} = 2_{2-5,9,13,17,21}, v_{22} = 2_{9,10,13,14,17,18,21,22}, v_{23} = 2_{9,11,13,15,17,19,21,23}$,
$v_{24} = (-3_1, 1_{2-24})$.

Then Λ_{24} is an even self-dual lattice. Furthermore, the minimal length of a non-zero vector from Λ_{24} is 2.

5°. If Λ is self-dual then $\det \Lambda = 1$.

6. Let $\Lambda_1 \subset \mathbb{R}^{n_1}$ and $\Lambda_2 \subset \mathbb{R}^{n_2}$ be lattices. Let $\Lambda \subset \mathbb{R}^{n_1} \oplus \mathbb{R}^{n_2} = \mathbb{R}^{n_1+n_2}$ be the set of all pairs $x \oplus y$, where $x \in \Lambda_1$ $y \in \Lambda_2$. Then Λ is a lattice (denoted $\Lambda = \Lambda_1 \oplus \Lambda_2$). If Λ_1, Λ_2 are self-dual then Λ is self-dual.

7. Lattices $\Lambda_1, \Lambda_2 \subset \mathbb{R}^n$ are called *isomorphic* if there exists an orthogonal transformation of $\mathbb{R}^n$ which maps Λ_1 onto Λ_2. Prove that the lattices $E_8 \oplus \mathbb{Z}^4$, D_{12}^+ and $\mathbb{Z}^{12}$ are pairwise non-isomorphic.

6. Linear Algebra of Lattices

We start with some problems.

PROBLEMS.

1. Let $\Lambda_0 \subset \Lambda$ be a sublattice and $k = |\Lambda : \Lambda_0|$. Then $k\Lambda = \{kx : x \in \Lambda\}$ is a sublattice in Λ_0.

2. Find the Smith normal form (that is, a pair of bases and divisors m_1, m_2, m_3) of the sublattice $\Lambda_0 \subset \mathbb{Z}^3$ generated by the vectors $v_1 = (2,0,3)$, $v_2 = (2,2,2)$, $v_3 = (3,2,0)$.

3. Let $\Lambda_0 \subset \Lambda$ be a sublattice. For any basis $u_1,\ldots,u_n$ of Λ there exists a basis $v_1,\ldots,v_n$ of Λ_0 such that

$$v_k = m_{k1}u_1 + \ldots + m_{kk}u_k, \quad k = 1,\ldots,n$$

for some integers m_{ij}, where $0 \le m_{jk} < m_{kk}$ for all j,k (the *Hermite Normal Form*).

Furthermore, for every basis $v_1, \ldots, v_n$ of Λ_0 there is a basis $u_1, \ldots, u_n$ of Λ such that

$$v_k = m_{k1}u_1 + \ldots + m_{kk}u_k, \quad k = 1, \ldots, n$$

for some integers m_{ij} where $0 \leq m_{kj} < m_{kk}$ for all j, k (the *Hermite Normal Form* again).

Hint: For a pair of bases u and v consider the matrix $M(u, v)$ as defined in the proof of Theorem 4.2. What operations on M are we allowed to perform provided u remains the same? v remains the same?

(6.1) Definitions. Let $\Lambda \subset \mathbb{R}^n$ be a lattice. A linear subspace $L \subset \mathbb{R}^n$ is called a *lattice subspace* provided $L \cap \Lambda$ is a lattice in L. A set of points $v_1, \ldots, v_k \in \Lambda$ is called *primitive* provided $v_1, \ldots, v_k$ constitute a basis in the lattice $\Lambda \cap L$, where L is the linear subspace generated by $v_1, \ldots, v_k$.

PROBLEM.

1°. A k-dimensional subspace $L \subset \mathbb{R}^n$ is a lattice subspace if and only if L contains k linearly independent points from Λ.

(6.2) Lemma. *A primitive set $v_1, \ldots, v_k \subset \Lambda$ can be appended to a basis $v_1, \ldots, v_n$ of Λ.*

Proof. For every basis $u = \{u_1, \ldots, u_n\}$ of Λ let us consider the $k \times n$ matrix $M(u) = (m_{ij})$:

$$v_i = m_{i1}u_1 + \ldots + m_{in}u_n : \quad i = 1, \ldots, k.$$

Let $\mathcal{M}$ be the set of all possible matrices $M(u)$. The following operations on matrices preserve the set $\mathcal{M}$: we can interchange two columns of M, multiply columns by -1, multiply a column by an integer and add to another column (cf. Proof of Theorem 4.2 and Problem 2 from that section). Then choose $M \in \mathcal{M}$ with the smallest positive $m_1 = m_{11}$. Then all the elements m_{1j} should be divisible by m_1. If $m_{1j} = s_j m_1 + r$ for some $0 < r < m_1$ then we can multiply the first column by s_j and subtract from the j-th column. Permuting the first and the j-th column we get the first corner entry r strictly smaller than m_1, which is a contradiction. So $m_{1j} = s_j m_1$ for all j. Multiplying the first column by s_j and subtracting from the j-th column we get to the situation where $m_{1j} = 0$ for all $j > 1$. Repeating this procedure, we get to the "column echelon form" where $m_{ij} = 0$ for $j > i$. Let $u_1, \ldots, u_n$ be the corresponding basis and $L \subset \mathbb{R}^n$ be the linear hull of $v_1, \ldots, v_k$. Then $u_1, \ldots, u_k \in L$. Since $v_1, \ldots, v_k$ is a basis of $L \cap \Lambda$, we can express $u_1, \ldots, u_k$ as integer linear combinations of $v_1, \ldots, v_k$. Therefore, $v_1, \ldots, v_k, u_{k+1}, \ldots, u_n$ is a basis of Λ. □

PROBLEM.

1. Deduce another proof of Lemma 6.2 from our proof of Theorem 3.1.

(6.3) Theorem. *Let $\Lambda \subset \mathbb{R}^n$ be a lattice and $L \subset \mathbb{R}^n$ be a lattice subspace. Then*

$$L^* = \{x \in \mathbb{R}^n : \langle x, y \rangle = 0 \textit{ for any } y \in L\}$$

is a lattice subspace with respect to the lattice Λ^*.

Proof. Let $u_1, \ldots, u_k$ be a basis of $\Lambda \cap L$. Let us append it to a basis $u_1, \ldots, u_n$ of Λ (Lemma 6.2). Consider the dual basis $u_1^*, \ldots, u_n^*$ (Theorem 5.1) of Λ^*. Then $u_{k+1}^*, \ldots, u_n^*$ is a basis of $L^* \cap \Lambda^*$. □

PROBLEMS.

1°. Let $\Lambda \subset \mathbb{R}^n$ be a lattice and L be a lattice subspace. A translation $L + t, t \in \mathbb{R}^n$ either does not contain lattice points or is generated by lattice points as an affine subspace.

2°. Let $a_1, \ldots, a_k \in \mathbb{Z}^n$ be linearly independent integral vectors. The system of linear equations $\langle a_i, x\rangle = b_i, \ i = 1, \ldots, k$ either does not have an integer solution $x \in \mathbb{Z}^n$ or the set of integer solutions generate an $(n-k)$-dimensional affine subspace in $\mathbb{R}^n$.

3. A set of integral vectors

$$v_1 = (m_{11}, \ldots, m_{1n}), \quad \ldots, \quad v_k = (m_{k1}, \ldots, m_{kn})$$

in $\mathbb{Z}^n$ is primitive if and only if the greatest common divisor of all $k \times k$ minors of the $k \times n$ matrix $M = (m_{ij})$ is 1.

Hint: To prove "only if" part append $v_1, \ldots, v_k$ to a basis of $\mathbb{Z}^n$ and use the Laplace expansion of the determinant. To prove "if" part, choose $\alpha_1 v_1 + \ldots + \alpha_k v_k \in \mathbb{Z}^n$. Using Cramer's rule show that for any minor d of M and any α_i one has $d \cdot \alpha_i \in \mathbb{Z}$ implying that $\alpha_i \in \mathbb{Z}$.

Monday, January 22

---

7. The Minkowski Theorem

(7.1) Theorem (Blichfeldt's Theorem.) *Let $\Lambda \subset \mathbb{R}^n$ be a lattice and $X \subset \mathbb{R}^n$ be a measurable set such that* vol $X >$ det Λ. *Then there exist two points $x \neq y \in X$ such that $x - y \in \Lambda$.*

Proof. Let us choose a basis $u_1, \ldots, u_n$ of Λ and let

$$\Pi = \Big\{\alpha_1 u_1 + \ldots + \alpha_n u_n : 0 \leq \alpha_i < 1\Big\}$$

be the fundamental parallelepiped. For every lattice point $u \in \Lambda$ let us define a set $X_u \subset \Pi$ as follows:

$$X_u = \Big\{y \in \Pi : y + u \in X\Big\}.$$

Then X_u are measurable since $X_u = \Pi \cap (X - u)$. Furthermore, the sets $X_u + u : u \in \Lambda$ cover X without overlapping (see Corollary 2.5). Therefore

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

We claim that some two subsets X_u and X_v have a non-empty intersection. Indeed, let χ_u be the characteristic function of X_u

$$\chi_u(x) = \begin{cases} 1 & \text{if } x \in X_u; \\ 0 & \text{elsewhere,} \end{cases} \qquad \text{and} \qquad \chi = \sum_{u \in \Lambda} \chi_u.$$

Then

$$\int_\Pi \chi(x)\ dx = \sum_{u\in\Lambda} \int_\Pi \chi_u(x)\ dx = \sum_{u\in\Lambda} \text{vol } X_u > \text{vol } \Pi.$$

Therefore for some $x \in \Pi$ we have $\chi(x) > 1$, so $\chi(x) \geq 2$ so X_u and X_v have non-empty intersection for some $u \neq v$. Let $z \in X_u \cap X_v$. Then $z + u = x \in X$ and $z + v = y \in X$. Then $x - y = u - v \in \Lambda$. □

There are numerous generalizations of the Blichfeldt Theorem. Here are some of them.

PROBLEMS.

1. Suppose that $\text{vol } X = \det \Lambda$ and X is compact. Then there exist two points $x \neq y \in X$ such that $x - y$ is a lattice point.

2. Suppose that $\text{vol } X > m \det \Lambda$ or $\text{vol } X = m \det \Lambda$ and X is compact. Then 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.

3. Let χ be a non-negative measurable function on $\mathbb{R}^n$ and $\Lambda \subset \mathbb{R}^n$ be a lattice. Then there exists a point z such that

$$\sum_{u\in\Lambda} \chi(u+z) \geq \frac{1}{\det \Lambda} \int_{\mathbb{R}^n} \chi(x)\ dx.$$

(7.2) Theorem "First Minkowski Theorem". *Let $\Lambda \subset \mathbb{R}^n$ be a lattice and $K \subset \mathbb{R}^n$ be a convex set such that*

(7.2.1) *K is centrally symmetric, that is $-x \in K$ whenever $x \in K$;*

(7.2.2) $\text{vol } K > 2^n \det \Lambda$.

Then K contains a non-zero lattice point u.

Furthermore, if K is compact then the inequality (7.2.2) can be relaxed to

$$\text{vol } K \geq 2^n \det \Lambda.$$

Proof. First, we prove the theorem under assumptions (7.2.1)-(7.2.2) Consider the set

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

Then $\text{vol } X = 2^{-n}(\text{vol K}) > \det \Lambda$. Therefore by Theorem 7.2.1 there exist a pair $x, y \in X$ such that $x - y = u \in \Lambda \setminus \{0\}$ is a non-zero lattice vector. Now $2x, 2y \in K$ and since K is centrally symmetric $-2y \in K$. Then

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

since K is convex. Suppose that K is compact and $\mathrm{vol}\, K = 2^n \det \Lambda$. Then for any $r > 0$ and $rK = \bigl\{ rx : x \in K \bigr\}$ we have $\mathrm{vol}\, rK = r^n K > 2^n \det \Lambda$, so there is a non-zero lattice point $u(r) \in rK$. Since K is compact, the family $\{u(r)\}$ for $r > 0$ has a limit point which has to be a non-zero lattice point from K. □

PROBLEMS.

1°. Show that if K is not compact then the inequality (7.2.2) can't be relaxed.

2°. Show that if K is not centrally symmetric then the theorem is no longer true.

3. Let $\Lambda \subset \mathbb{R}^n$ be a lattice, $K \subset \mathbb{R}^n$ be a centrally symmetric convex set with $\mathrm{vol}\, K > m 2^n \det \Lambda$ for some positive integer m. Then K contains at least m pairs of non-zero lattice points $u_i, -u_i : i = 1, \ldots, m$.

4. Let $K \subset \mathbb{R}^n$ be a convex body containing the origin as its interior point. We say that the *symmetry coefficient* of K is at least σ provided $\sigma > 0$ and for every $x \in K$ we have $-\sigma x \in K$. If $\mathrm{vol}\, K > (1 + \sigma^{-1})^n \det \Lambda$ then K contains a non-zero lattice point u.

5*. Show that the inequality of Problem 4 can be relaxed to $\mathrm{vol}\ \mathrm{K} > (1 + \sigma^{-1})^n (1 - (1 - \sigma)^n) \det \Lambda$.

6. If $K \subset \mathbb{R}^n$ is a convex body then for some $x \in \mathbb{R}^n$ the symmetry coefficient of the translation $K - x$ is at least $1/n$ (one can choose x to be the center of gravity of K).

7*. If $K \subset \mathbb{R}^2$ is a convex compact set whose center of gravity coincides with the origin and $\mathrm{vol}\, K > \frac{9}{2} \det \Lambda$ then K contains a non-zero lattice point.

8. The following proof of the Minkowski Theorem was suggested by C.L. Siegel. Let $K \subset \mathbb{R}^n$ be a compact centrally symmetric convex body which does not contain a non-zero point from $\mathbb{Z}^n$. Then

$$2^n = \mathrm{vol}\, K + 4^n \Bigl(\mathrm{vol}\, K\Bigr)^{-1} \sum_{u \in \mathbb{Z}^n \setminus \{0\}} \Bigl| \int_{\frac{1}{2}K} \exp\{-2\pi i \langle u, x \rangle\}\, dx \Bigr|^2.$$

Hint: Let

$$\phi(x) = \sum_{u \in \mathbb{Z}^n} \chi(u + x), \quad \text{where} \quad \chi(x) = \begin{cases} 1 & \text{if } 2x \in K, \\ 0 & \text{elsewhere} \end{cases}$$

be the characteristic function of $\frac{1}{2}K$. Then ϕ is a periodic function on $\mathbb{R}^n$ and we may apply Parseval's formula to ϕ.

See C.L. Siegel, *Lectures on the Geometry of Numbers*, Springer-Verlag, Berlin, New York, 1989 and P. Gruber and C. Lekkerkerker, *Geometry of Numbers*, 2nd ed., North-Holland, New York, 1987.

(7.3) Corollary. *Let $\Lambda \subset \mathbb{R}^n$ be a lattice. Then there exists a non-zero $u \in \Lambda$ such that*

$$\|u\| \leq \frac{2}{\sqrt{\pi}} \Bigl(\Gamma\bigl(1 + \frac{n}{2}\bigr)\Bigr)^{\frac{1}{n}} \Bigl(\det \Lambda\Bigr)^{\frac{1}{n}} \approx \sqrt{\frac{2n}{e\pi}} \Bigl(\det \Lambda\Bigr)^{\frac{1}{n}}.$$

Proof. Let us consider the ball $B_r(0) = \{x : \|x\| \le r\}$. We have

$$\text{vol } B_r(0) = \frac{r^n \pi^{\frac{n}{2}}}{\Gamma(1+\frac{n}{2})}.$$

Furthermore, $B_r(0)$ is compact and centrally symmetric. Therefore, by Theorem 7.2 $B_r(0)$ contains a non-zero lattice point provided vol $B_r(0) \ge 2^n \det \Lambda$, that is

$$r \ge 2\Big(\det \Lambda\Big)^{\frac{1}{n}} \Big(\Gamma(1+\frac{n}{2})\Big)^{\frac{1}{n}} \pi^{-\frac{1}{2}}.$$

Since $\Gamma\big(1+\frac{n}{2}\big) \approx \Big(\frac{n}{2e}\Big)^{\frac{n}{2}}$ (Stirling's formula), the proof follows. $\square$

PROBLEMS.

1. Let $\|u\|_\infty = \max\big\{|u_1|, \ldots, |u_n|\big\}$. Prove that there exists a non-zero $u \in \Lambda$ with $\|u\|_\infty \le \Big(\det \Lambda\Big)^{\frac{1}{n}}$. This estimate is sharp in the worst case.

2°. There exists a non-zero $u \in \Lambda$ such that $\|u\| \le \sqrt{n}(\det \Lambda)^{1/n}$.

3^*. Prove that there exists $\gamma > 0$ such that for every n there exists a lattice $\Lambda \subset \mathbb{R}^n$ with the property $\|u\| \ge \gamma\sqrt{n}\Big(\det \Lambda\Big)^{1/n}$ for all $u \in \Lambda \setminus \{0\}$.

4^*. Can you come up with an algorithm which for any given n constructs the lattice $\Lambda \subset \mathbb{R}^n$ from Problem 3?

5^*. Is there a $\beta > 0$ such that there exists a polynomial time algorithm which for any lattice $\Lambda \subset \mathbb{R}^n$, given by its basis, constructs a non-zero $u \in \Lambda$ such that $\|u\| \le \beta\sqrt{n}\Big(\det \Lambda\Big)^{1/n}$?

6. Let $A = (a_{ij})$ be an $n \times n$ real matrix and $\Delta = |\det A| > 0$. Let us define n linear forms $l_1, \ldots, l_n$ on $\mathbb{R}^n$:

$$l_i(x) = a_{i1}x_1 + \ldots + a_{in}x_n.$$

If $b_1, \ldots, b_n$ are positive numbers such that $b_1 \cdots b_n \ge \Delta$ then there exists a non-zero $x \in \mathbb{Z}^n$ such that $|l_i(x)| \le b_i$ for $i = 1, \ldots, n$.

7. Problem 6 implies that there exists $x \in \mathbb{Z}^n \setminus \{0\}$ such that

$$\prod_{i=1}^{n} |l_i(x)| \le \Delta.$$

Prove that in fact there exists $x \in \mathbb{Z}^n \setminus \{0\}$ such that $|l_1(x) \cdots l_n(x)| \le \dfrac{n!}{n^n}\Delta$.

Hint: Apply Theorem 7.2 to the convex body

$$K(r) = \Big\{x \in \mathbb{R}^n : \frac{1}{n}\sum_{i=1}^{n} |l_i(x)| \le r\Big\}.$$

8*. Find the smallest κ_n such that for any n linear forms $l_1, \ldots, l_n$ on $\mathbb{R}^n$ there exists a non-zero $x \in \mathbb{Z}^n$ such that $|l_1(x) \cdots l_n(x)| \leq \kappa_n \Delta$.

It is known that $\kappa_2 = \frac{1}{\sqrt{5}}$ and that $\kappa_3 = \frac{1}{7}$.

Wednesday, January 24

---

8. Some Applications of the Minkowski Theorem

We start with a simple Lemma.

(8.1) Lemma. *Let $c_1, \ldots, c_m \in \mathbb{Z}^m$ be integral vectors and $k_1, \ldots, k_m$ be positive integers. Consider the set*

$$\Lambda = \Big\{ x \in \mathbb{Z}^n : \ \langle x, c_i \rangle \equiv 0 \ (\mathrm{mod}\ k_i), \ i = 1, \ldots, m \Big\}.$$

Then Λ is a lattice and $\det \Lambda_0 \leq k_1 \cdots k_m$.

Proof. Obviously, Λ is a discrete additive subgroup of $\mathbb{R}^n$. Let $k = k_1 \cdots k_m$ and

$$k\mathbb{Z}^n = \Big\{ kx : x \in \mathbb{Z}^n \Big\}.$$

Then $k\mathbb{Z}^n \subset \Lambda$ and therefore Λ spans the whole space $\mathbb{R}^n$, so Λ is a lattice. Now $\det \Lambda = |\mathbb{Z}^n : \Lambda| \cdot \det \mathbb{Z}^n = |\mathbb{Z}^n : \Lambda|$. We describe cosets $\mathbb{Z}^n : \Lambda$. For a vector $a = (a_1, \ldots, a_m)$, where $0 \leq a_i < k_i$ let us find $x_a \in \mathbb{Z}^n$ (if one exists) such that $\langle c_i, x_a \rangle \equiv a_i \ (\mathrm{mod}\ k_i)$. Then

$$\mathbb{Z}^n = \bigcup_a \Big(x_a + \Lambda \Big),$$

and, therefore $|\mathbb{Z}^n : \det \Lambda| \leq k_1 \cdots k_m$. □

PROBLEM.

1°. Let $D_n \subset \mathbb{R}^n$ be the lattice consisting of all integral vectors $x = (x_1, \ldots, x_n) \in \mathbb{Z}^n$ such that $x_1 + \ldots + x_n$ is an even integer. Then $\det D_n = 2$.

(8.2) Theorem. *Every positive integer number n can be represented as a sum $n = x_1^2 + x_2^2 + x_3^2 + x_4^2$, where x_i are integers.*

Proof. It suffices to prove the result if $n = p_1 \cdots p_m$ is the product of distinct primes (why?). We show that for every prime p there are numbers a_p, b_p such that $a_p^2 + b_p^2 + 1 \equiv 0(\text{mod p})$. Indeed, for $p = 2$ we take $a_p = 1$, $b_p = 0$. If p is odd then all the $(p+1)/2$ numbers $a^2 : 0 \leq a < p/2$ have pairwise different residues mod p since $a^2 \equiv b^2 (\mathrm{mod}\ p)$ implies $(a-b)(a+b) \equiv 0 (\mathrm{mod}\ p)$ which in turn implies $a \equiv b (\mathrm{mod}\ p)$ or $a \equiv -b (\mathrm{mod}\ p)$. Similarly, the $(p+1)/2$ numbers $-1 - b^2 : \ 0 \leq b < p/2$ have pairwise different residues mod p. Therefore there is a pair a, b such that $a^2 + b^2 + 1 \equiv 0 \pmod p$. Now we consider the lattice $\Lambda \subset \mathbb{Z}^4$ consisting of all vectors (x_1, x_2, x_3, x_4) such that

$$x_1 \equiv a_p x_3 + b_p x_4 \pmod p, \quad x_2 = b_p x_3 - a_p x_4 \pmod p, \quad p = p_1, \ldots, p_m.$$

Lemma 8.1 implies that $\det \Lambda \leq (p_1 \cdots p_m)^2 = n^2$. Consider an open ball

$$B = \Big\{ x \in \mathbb{R}^n : x_1^2 + x_2^2 + x_3^2 + x_4^2 < 2n \Big\}.$$

We have

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

Therefore there is a point $x \in \Lambda$ such that $0 < x_1^2 + x_2^2 + x_3^2 + x_4^2 < 2n$. On the other hand, since $x \in \Lambda$ we get that

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv (a_p^2 + b_p^2 + 1)x_3^2 + (a_p^2 + b_p^2 + 1)x_4^2 \equiv 0 \pmod p \quad \text{for } p = p_1, \ldots p_m.$$

So $(x_1^2 + x_2^2 + x_3^2 + x_4^2)$ is divisible by n and, therefore $x_1^2 + x_2^2 + x_3^2 + x_4^2 = n$. $\square$

PROBLEMS.

1. If there is a solution to the congruence $x^2 + 1 \equiv 0 \pmod k$ then k is the sum of two squares. In particular, every prime number $p \equiv 1 \pmod 4$ is the sum of the squares of two integers.

2. Prove the Legendre Theorem: Let a_1, a_2, a_3 be pairwise coprime square free integers. If the congruences

$$a_1 + x^2 a_2 \equiv \pmod{a_3}, \quad a_2 + y^2 a_3 \equiv 0 \pmod{a_1}, \quad a_3 + z^2 a_1 \equiv 0 \pmod{a_2}$$

are solvable and there are integers u, v, w not all even such that $a_1 u^2 + a_2 v^2 + a_3 w^2 \equiv 0 \pmod 8$ for $a_1 a_2 a_3$ even or $a_1 u^2 + a_2 v^2 + a_3 w^2 \equiv 0 \pmod 4$ for $a_1 a_2 a_3$ odd then there is a non-zero integer vector x, y, z such that $a_1 x^2 + a_2 y^2 + a_3 z^2 = 0$.

3*. The number of integral solutions of the equation $x_1^2 + x_2^2 + x_3^2 + x_4^2 = n$ is 8 times the sum of all d such that d divides n and 4 does not divide n (Jacobi's formula, see, for example, D. Mumford, *Tata Lectures on Theta*, Boston, Birkhäuser, 1983).

See also J.W.S. Cassels, *An Introduction to the Geometry of Numbers*, Springer-Verlag, Berlin, 1959.

Next, we consider the problem of approximation of real numbers by rationals

PROBLEM.

1°. Let $\alpha \in \mathbb{R}$ be a real number and let q be a positive integer. Then there exists an integer p such that

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

(8.3) Theorem. *There exists a $C > 0$ such that for any $\alpha \in \mathbb{R}$ one can find an arbitrarily large positive integer q and $p \in \mathbb{Z}$ such that*

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

Proof. Without loss of generality we may assume that α is irrational. Let us choose a positive integer $Q > 2$ and consider the set $K \subset \mathbb{R}^2$:

$$K = \left\{(x, y) : |\alpha x - y| \leq \frac{1}{Q}, \ |x| \leq Q\right\}.$$

Then K is a convex centrally symmetric body (parallelogram). Furthermore, vol $K \geq 4$. Therefore there is a non-zero integer point $(q, p) \in K$. Furthermore, $q \neq 0$ since otherwise $p = 0$. Because of the symmetry, we may assume that $q > 0$. It follows now that

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{qQ} \quad \text{and} \quad 0 < q \leq Q. \tag{8.3.1}$$

The inequalities (8.3.1) imply that

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^2} \tag{8.3.2}$$

and our goal is to establish that q can be made arbitrarily large in (8.3.2). Indeed, let M be a natural number. Since α is irrational, we can choose Q in (8.3.1) so big that the inequality (8.3.1) is not satisfied for any $q < M$ (since there are finitely many possibilities to approximate a number by a rational with a denominator $\leq M$ and not a single such approximation will be precise). That's why (8.3.1) and thus (8.3.2) should be satisfied with some $q > M$. □

PROBLEMS.

1*. The best possible value of C in Theorem 8.3 is $C = \dfrac{1}{\sqrt{5}}$. For the corresponding α one may take $\alpha = \dfrac{\sqrt{5}-1}{2}$.

Hint: To construct an approximation which satisfies the inequality of Theorem 8.3 with $C = \dfrac{1}{\sqrt{5}}$ we may use *continued fractions.* For given α write $\alpha = [\alpha] + \{\alpha\}$. Then write $\{\alpha\} = 1/\alpha_1$, where $\alpha_1 = 1/\{\alpha\}$ and proceed as above with α_1. After a number of steps forcefully let $\alpha_n = 0$ and fold the process back to get a rational approximation of α. If we do this with $\alpha = \frac{\sqrt{5}-1}{2}$ we get the sequence

$$\alpha = \frac{1}{1 + \frac{1}{1+\ldots}}$$

The corresponding n-th approximation is $\dfrac{F_n}{F_{n+1}}$, where F_k are Fibonacci numbers.

2. There exists $C > 0$ such that for any real numbers $\alpha_1, \ldots, \alpha_n$ one can find arbitrarily large positive integer q and integers $p_1, \ldots, p_n$ such that

$$\left|\alpha_i - \frac{p_i}{q}\right| \leq \frac{C}{q^{1+\frac{1}{n}}} \quad \text{for } i = 1, \ldots, n.$$

3*. What is the best value of C in Problem 2?

4*. Construct an algorithm for finding an approximation from Problem 2. Is there a procedure similar to continued fractions from Problem 1?

Remark: we should discuss how real numbers $\alpha_1, \ldots, \alpha_n$ are given. We suppose that there is a "black box" which can compare real numbers and perform arithmetic operations on them.

See L. Lovász, *An Algorithmic Theory of Numbers, Graphs and Convexity*, SIAM, Philadelphia, PA, 1986.

Friday, January 26

---

9. The Minkowski - Hlawka Theorem

We start with a problem.

PROBLEM.

1. Let $\Lambda \subset \mathbb{R}^n$ be a lattice and $M \subset \mathbb{R}^n$ be a measurable set such that vol $M < \det \Lambda$. Then there exists $x \in \mathbb{R}^n$ such that $(M + x) \cap \Lambda = \emptyset$, so some translation of M does not contain any point from Λ.

(9.1) Lemma. *Let $M \subset \mathbb{R}^n$ be a measurable set, $\Lambda \subset \mathbb{R}^n$. Let us define a function $\nu : \mathbb{R}^n \longrightarrow \mathbb{Z}$,*

$$\nu(x) = \big|(M - x) \cap \Lambda\big|,$$

the number of lattice points in the translation $M - x$. Let Π be a fundamental parallelepiped of Λ. Then

$$\int_\Pi \nu(x)\ dx = \text{vol } M.$$

Proof. For a lattice point $u \in \Lambda$ let us define

$$\chi_u(x) = \begin{cases} 1 & \text{if } u \in M - x, \\ 0 & \text{otherwise.} \end{cases}$$

Then $\nu(x) = \sum_{u \in \Lambda} \chi_u(x)$ and

$$\int_\Pi \nu(x)\ dx = \sum_{u \in \Lambda} \int_\Pi \chi_u(x)\ dx = \sum_{u \in \Lambda} \text{vol } \Big((\Pi + u) \cap M\Big) = \text{vol } M.$$

The last equality follows by Corollary 2.5. $\square$

(9.2) Theorem (Minkowski - Hlawka Theorem). *Suppose that $n > 1$, and $M \subset \mathbb{R}^n$ is a bounded Jordan measurable set. Let us choose a $d > \operatorname{vol} M$. Then there exists a lattice $\Lambda \subset \mathbb{R}^n$ such that $\det \Lambda = d$ and $M \cap \Big(\Lambda \setminus \{0\}\Big) = \emptyset$, that is M does not contain any lattice point, except possibly 0.*

Proof. Without loss of generality we may assume that $\operatorname{vol} M < 1$ and we want to find a lattice Λ such that $\det \Lambda = 1$ and M does not contain a non-zero point from Λ. Let $e_1, \ldots, e_n$ be the standard orthonormal basis of $\mathbb{R}^n$ and let $\mathbb{R}^{n-1}$ be the space generated by $e_1, \ldots, e_{n-1}$, so we decompose $\mathbb{R}^n = \mathbb{R}^{n-1} \oplus \mathbb{R}$. Let us choose a small $\alpha > 0$ and consider a family of hyperplanes $H_m = \{x_n = m\alpha\}$, where $m \in \mathbb{Z}$. In particular, $H_0 = \mathbb{R}^{n-1}$. We choose α to be so small that

(9.2.1) every point from $M \cap H_0$ belongs to the cube $|x_i| < \alpha^{-\frac{1}{n-1}}$ in H_0 (we can choose such an α since M is bounded);

(9.2.2) let $S_i = M \cap H_i$. Then $\alpha \sum\limits_{i=-\infty}^{\infty} \operatorname{vol}_{n-1} S_i < 1$. Here vol_{n-1} is the $(n-1)$-dimensional volume in the hyperplane H_i. We can choose such an α because M is Jordan measurable and $\operatorname{vol} M < 1$, so the sum approximates $\operatorname{vol} M$ arbitrarily close if α is sufficiently small.

Now we are ready to announce the first $n-1$ basis vectors of Λ. They are $u_i = \alpha^{-\frac{1}{n-1}} e_i$, $i = 1, \ldots, n-1$.

Note that the volume of the $(n-1)$-dimensional cube generated by $u_1, \ldots, u_{n-1}$ is α^{-1}. Therefore, if we choose u_n somewhere on H_1, the determinant $|u_1 \wedge \ldots \wedge u_{n-1} \wedge u_n|$ of the lattice Λ will be equal to 1. So we claim that there exists $u_n \in H_1$ such that the lattice Λ generated by $u_1, \ldots, u_n$ does not contain any point of M, except possibly 0. Let $I_{n-1} = \big\{\beta_1 u_1 + \ldots + \beta u_{n-1} : \ 0 \leq \beta_i < 1\big\}$ be the parallelepiped spanned by $u_1, \ldots, u_{n-1}$. For a $y \in I_{n-1}$ let $u_n(y) = y + \alpha e_n$. So $u_n(y) \in H_1$ and we claim that for some $y \in I_{n-1}$ the lattice Λ_y generated by $u_1, \ldots, u_{n-1}, u_n(y)$ satisfies the desired properties. To prove this, let us introduce the functions ν and ν_k, where k is a non-zero integer:

$$\nu(y) = \Big|M \cap \Big(\Lambda_y \setminus \{0\}\Big)\Big|; \quad \nu_k(y) = |\Lambda_y \cap S_k|, \quad \text{where} \quad S_k = M \cap H_k.$$

So $\nu(y)$ is the number of points from $\Lambda_y \setminus \{0\}$ in M and $\nu_k(y)$ is the number of the points from Λ_y on the k-th level $M \cap H_k$ of the set M. Obviously, $\nu_k(y), \nu(y)$ are non-negative integers.

Claim:

$$\int_{I_{n-1}} \nu_k(y) \ dy = \operatorname{vol} S_k.$$

Proof. For $k = 1, -1$ the formula follows by Lemma 9.1. Indeed, let $\Lambda_0 \subset H_0$ be the sublattice generated by $u_1, \ldots, u_{n-1}$. Then

$$\nu_1(y) = \Big|S_1 \cap (\Lambda_0 + u_n)\Big| = \Big|(S_1 - u_n) \cap \Lambda_0\Big| = \Big|(S_1 - \alpha e_n - y) \cap \Lambda_0\Big|,$$

so we apply Lemma 9.1 to $S_1 - \alpha e_n \subset H_0$. Similarly, $\nu_{-1}(y) = \left|\big(S_{-1} + \alpha e_n + y\big) \cap \Lambda_0\right|$. Let us consider the case $k > 1$ (the case $k < -1$ is completely analogous). Again, we are going to use Lemma 9.1. Then

$$\nu_k(y) = \big|S_k \cap (\Lambda_0 + k u_n)\big| = \big|(S_k - k\alpha e_n - ky) \cap \Lambda_0\big|,$$

so letting $S'_k = S_k - k\alpha e_n$ and substituting $z = ky$ we get

$$\int_{I_{n-1}} \nu_k(y)\ dy = \int_{I_{n-1}} \big|(S'_k - ky) \cap \Lambda_0\big|\ dy = k^{-(n-1)} \int_{kI_{n-1}} \big|(S'_k - z) \cap \Lambda_0\big|\ dz.$$

On the other hand, the parallelepiped $kI_{n-1} = \big\{\beta_1 u_1 + \ldots + \beta_{n-1} u_{n-1} : 0 \leq \beta_{n-1} < k\big\}$ is the union of k^{n-1} non-intersecting lattice shifts $I_{n-1} + u :\ u \in \Lambda_0$ of I_{n-1} so we can apply Lemma 9.1. The claim is proven.

Now we observe that

$$\begin{aligned}\frac{1}{\mathrm{vol}\ I_{n-1}} \int_{y \in I_{n-1}} \nu(y)\ dy &= \alpha \sum_{k \in \mathbb{Z} \setminus \{0\}} \int_{y \in I_{n-1}} \nu_k(y)\ dy \quad \text{(by (9.2.1))} \\ &= \alpha \sum_{k \in \mathbb{Z} \setminus \{0\}} \mathrm{vol}_{n-1}(S_k) < 1 \quad \text{(by (9.2.2))}.\end{aligned}$$

So the average value of ν is strictly smaller than 1. Since ν takes non-negative integral values, for some y we must have $\nu(y) = 0$. Then the lattice Λ_y is the lattice we need. $\square$

PROBLEMS.

1. Let χ be a measurable function on $\mathbb{R}^n$ and $\Lambda \subset \mathbb{R}^n$ be a lattice. Then there exists a $z \in \mathbb{R}^n$ such that

$$\sum_{u \in \Lambda} \chi(u + z) \leq \frac{1}{\det \Lambda} \int_{\mathbb{R}^n} \chi(x)\ dx.$$

2. Let χ be a bounded Riemann integrable function vanishing outside a bounded region in $\mathbb{R}^n$, $n > 1$ and let ϵ be a positive number. Then there exists a lattice $\Lambda \subset \mathbb{R}^n$ of determinant 1 such that

$$\sum_{u \in \Lambda \setminus \{0\}} \chi(u) < \int_{\mathbb{R}^n} \chi(x)\ dx + \epsilon.$$

3. Let $M \subset \mathbb{R}^n$, $n > 1$ be a bounded centrally symmetric Jordan measurable set and $d > \dfrac{1}{2}\mathrm{vol}\ M$. Then there exists a lattice $\Lambda \subset \mathbb{R}^n$ such that $\det \Lambda = d$ and M does not contain any lattice point, except possibly 0.

Hint: Either M does not contain any non-zero lattice point or it contains at least two.

4* (Theorem of Minkowski-Hlawka). A set $S \subset \mathbb{R}^n$ is called a *star body* if and only if for any $x \in S$ and any $0 \leq \alpha < 1$ the point αx is an inner point of S. Let S be a centrally symmetric star body in $\mathbb{R}^n$, $n > 1$ and $d \geq \dfrac{\text{vol } S}{2\zeta(n)}$, where $\zeta(n) = \sum_{m=1}^{\infty} \dfrac{1}{m^n}$. Then there exists a lattice $\Lambda \subset \mathbb{R}^n$ such that $\det \Lambda = d$ and $S \cap \Big(\Lambda \setminus \{0\}\Big) = \emptyset$.

Hint: Let μ be the Möbius function, that is $\mu(m) = 0$ if m is not square free and $\mu(m) = (-1)^k$ if m is a product of k distinct primes. Let χ_0 be the characteristic function of S and

$$\chi(x) = \sum_{k=1}^{+\infty} \mu(k)\chi_0(kx) \quad \text{for } x \in \mathbb{R}^n.$$

Then

$$\int_{\mathbb{R}^n} \chi(x)\ dx = \frac{\text{vol S}}{\zeta(n)}$$

(use the fact that $\sum_{m=1}^{\infty} \dfrac{\mu(m)}{m^n} = \dfrac{1}{\zeta(n)}$) and

$$\sum_{u \in \Lambda \setminus \{0\}} \chi(x) = \sum_{u \text{ is primitive in } \Lambda} \chi_0(u)$$

(use the inversion formula from the number theory). Now apply Problem 2. See, for example, P. Gruber and C. Lekkerkerker, *Geometry of Numbers*, 2nd ed., North-Holland, New York, 1987.

(9.3) Corollary. *There exists a $\beta > 0$ such that for any n there exists a lattice $\Lambda \subset \mathbb{R}^n$ with*

$$\|u\| \geq \beta\sqrt{n}\Big(\det \Lambda\Big)^{\frac{1}{n}}$$

for any non-zero $u \in \Lambda$ (cf. Corollary 7.3).

Proof. Let us choose any $\beta < \dfrac{1}{\sqrt{2e\pi}}$. Let us consider the ball

$$B = \Big\{x \in \mathbb{R}^n : \|x\| \leq \beta\sqrt{n}\Big\}.$$

Then

$$\text{vol } B = \frac{\pi^{\frac{n}{2}}\beta^n n^{\frac{n}{2}}}{\Gamma\big(\frac{n}{2}+1\big)} < 1$$

for sufficiently large n. Then by Theorem 9.2 there exists a lattice $\Lambda \subset \mathbb{R}^n$ with $\det \Lambda = 1$ such that B does not contain a non-zero point from Λ. □

So for sufficiently large n we may use $\beta \approx \dfrac{1}{\sqrt{2\pi e}}$.

Monday, January 29

---

10. Sphere Packing

(10.1) Definitions. Let $\Lambda \subset \mathbb{R}^n$ be a lattice. The largest $\rho > 0$ such that the open balls $B_\rho(u) = \{x \in \mathbb{R}^n : \|x - u\| < \rho\}$, centered at the lattice points are pairwise non-intersecting is called the *packing radius* $\rho(\Lambda)$ of Λ. Let $\mathcal{B} = \bigcup\limits_{u \in \Lambda} B_\rho(u)$. The number

$$\sigma(\Lambda) = \lim_{r \longrightarrow +\infty} \frac{\text{vol } \big(\mathcal{B} \cap B_r(0)\big)}{\text{vol } B_r(0)}$$

is called the *packing density* of Λ.

Let $\Lambda_1, \Lambda_2 \subset \mathbb{R}^n$ be two lattices. We say that Λ_1 and Λ_2 are *isomorphic* (denoted $\Lambda_1 \simeq \Lambda_2$) if there exists an orthogonal transformation of $\mathbb{R}^n$ which maps Λ_1 onto Λ_2. We say that Λ_1 and Λ_2 are *similar* (denoted $\Lambda_1 \sim \Lambda_2$) if there is a lattice Λ_3 such that $\Lambda_1 \simeq \Lambda_3$ and $\Lambda_2 = k\Lambda_3 = \{ku : u \in \Lambda_3\}$ for some $k > 0$. Often we don't distinguish similar lattices (warning: sometimes we do).

PROBLEMS.

1°. Prove that the packing radius exists and that

$$\rho(\Lambda) = \frac{1}{2} \min\big\{\|u\| : \ u \in \Lambda \setminus \{0\}\big\}.$$

2. Prove that the packing density exists and that

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

3°. If $\Lambda_1 \sim \Lambda_2$ then $\sigma(\Lambda_1) = \sigma(\Lambda_2)$.

Sometimes we will denote the volume of the unit ball in $\mathbb{R}^n$ by κ_n, so $\kappa_n = \dfrac{\pi^{\frac{n}{2}}}{\Gamma\big(1 + \frac{n}{2}\big)}$.

(10.2) Some interesting lattices.

(10.2.1) The lattice $\mathbb{Z}^n$ of all integral vectors in $\mathbb{R}^n$.

(10.2.2) The lattice $A_n \subset \mathbb{R}^n$ can be defined as follows. Identify $\mathbb{R}^n$ with the hyperplane $H = \{x : x_1 + \ldots + x_n = 0\}$ in $\mathbb{R}^{n+1}$ and define $A_n = \mathbb{Z}^{n+1} \cap H$.

(10.2.3) The lattice $D_n \subset \mathbb{R}^n$ consisting of all integral vectors $(x_1, \ldots, x_n)$ such that $x_1 + \ldots + x_n$ is an even integer.

(10.2.4) The lattice $D_n^+ \subset \mathbb{R}^n$ where n is even consists of the vectors of the two classes:

Class I: vectors $(x_1, \ldots, x_n)$, where all x_i are integers and $x_1 + \ldots + x_n$ is an even integer;

Class II: vectors $\big(\frac{1}{2}, \ldots, \frac{1}{2}\big)$ plus a vector $(x_1, \ldots, x_n)$ from the first class.

(10.2.5) The lattice $E_8 = D_8^+$ (cf. Problem 4, a) from Section 5.1).

(10.2.6) The lattice $E_7 \subset \mathbb{R}^7$ defined as follows. Let us identify $\mathbb{R}^7$ with the hyperplane $H = \{x = (x_1, \ldots, x_8) : x_1 + x_2 + x_3 + x_4 + x_5 + x_6 + x_7 + x_8 = 0\}$. Then $E_7 = E_8 \cap H$.

(10.2.7) The lattice $E_6 \subset \mathbb{R}^6$ defined as follows. Let us identify $\mathbb{R}^6$ with the subspace $L = \{x = (x_1, \ldots, x_8) : x_1 + x_8 = x_2 + x_3 + x_4 + x_5 + x_6 + x_7 = 0\}$ and let $E_6 = E_8 \cap L$.

(10.2.8) The Coxeter-Todd lattice K_{12}. Let ω be the primitive root of unity of degree 3, so $\omega^3 = 1$. Consider the set $\mathcal{E}$ of all numbers $a + \omega b : a, b \in \mathbb{Z}$, called *Eisenstein integers.* Let us identify $\mathbb{C}^6 = \mathbb{R}^{12}$ and define $K_{12} \subset \mathbb{C}^6$ as the set of all combinations $\frac{1}{\sqrt{2}} \sum_{i \in I} \epsilon_i x_i$, where $\epsilon_i \in \mathcal{E}$ and x_i are the vectors having precisely one component $i\sqrt{3}$ or $-i\sqrt{3}$ and 5 other components to be $+1$ or -1 so that for every x_i the number of "$-$" signs is even.

(10.2.9) The Leech lattice Λ_{24} (compare Section 5.1, Problem 4, c). Let $Q = \Big\{0 < a < 23 : x^2 - a \equiv 0 \pmod{23}$ for some integer $x\Big\}$. Let us consider a 23-dimensional vector $g = (g_0, \ldots, g_{22})$ such that the i-th component of g is 1 if $i \in Q$ and 0 otherwise. Now let G be a set of all 22 cyclic shifts $g_0 \to g_1 \to g_2 \to \ldots \to g_{22} \to g_0$ obtained from g. Next, we interpret G as a set of vectors in a 23-dimensional vector space $\mathbb{Z}_2^{23}$ over the field $\mathbb{Z}_2$ and let $\mathcal{C}_{23}$ be a linear subspace in $\mathbb{Z}_2^{23}$ generated by G. Next, we consider the set $\mathcal{C}_{24}$ of all 24-dimensional vectors obtained from $\mathcal{C}_{23}$ by appending the 24-th coordinate by 1 to make the number of 1-s even. Finally, we define the Leech lattice Λ_{24} as the lattice in $\mathbb{R}^{24}$ generated by all vectors $\frac{1}{\sqrt{8}}(x_1, \ldots, x_{24})$, where exactly one x_i is 3 or -3 and the rest 23 coordinates are -1 or 1 and there is a vector $s \in \mathcal{C}_{24}$ such that if $s_i = 1$ then $x_i = 1$ or $x_i = -3$ and if $s_i = 0$ then $x_i = -1$ or $x_i = 3$.

(10.2.9) Laminated lattices Λ_n. Let us define $\Lambda_0 = \{0\} \subset \mathbb{R}^0$. Let us choose a laminated lattice Λ_{n-1}. Let $\mathcal{L} = \Big\{\Lambda$ is a lattice in $\mathbb{R}^n$: $\rho(\Lambda) = 1$ and there exists a hyperplane $H \subset \mathbb{R}^n$ such that $H \cap \Lambda \sim \Lambda_{n-1}\Big\}$. Let $\Lambda_n = \Lambda \in \mathcal{L}$, such that $\det \Lambda_n \leq \det \Lambda$ for any $\Lambda \in \mathcal{L}$.

PROBLEMS.

1. An alternative description of A_2: let $u_1, u_2 \in \mathbb{R}^2$ be two unit vectors with the angle $\pi/3 = 60°$ between them. They generate a lattice similar to A_2.

2. Prove that $\sigma(A_2) > \sigma(\mathbb{Z}^2)$.

Remark: In fact, $\sigma(A_2) = \dfrac{\pi}{\sqrt{12}} \approx 0.9069$ is the largest packing density of a two-dimensional lattice.

3. Prove that $A_3 \sim D_3$. Prove that $\sigma(A_3) > \sigma(\mathbb{Z}^3)$.

Remark: In fact, $\sigma(A_3) = \dfrac{\pi}{\sqrt{18}} \approx 0.7405$ is the largest packing density of a three-dimensional lattice.

4. Prove that $D_4 \sim (D_4)^*$ (similar to its dual).

5. Prove that $\sigma(D_4) > \sigma(A_4) > \sigma(\mathbb{Z}^4)$.

Remark: In fact, $\sigma(D_4) = \dfrac{\pi^2}{16} \approx 0.6169$ is known to be the largest packing density of a four-dimensional lattice.

6. Prove that $D_4^+ \sim \mathbb{Z}^4$.

7. Prove that $\sigma(D_5) > \sigma(A_5) > \sigma(\mathbb{Z}^5)$.

Remark: In fact, $\sigma(D_5) \approx 0.46526$ is known to be the largest packing density of a five-dimensional lattice.

8. Here is another construction of E_6. Let us identify $\mathbb{R}^6 = \mathbb{C}^3$. Let us choose $u_1 = (i\sqrt{3}, 0, 0)$, $u_2 = (0, i\sqrt{3}, 0)$, $u_3 = (1, 1, 1)$. Then E_6 is the set of all combinations $a_1u_1 + a_2u_2 + a_3$, where a_i are Eisenstein integers (see (10.2.8)).

9. Prove that $\sigma(E_6) > \sigma(D_6) > \sigma(A_6) > \sigma(\mathbb{Z}^6)$.

Remark: In fact, $\sigma(E_6) \approx 0.37295$ is known to be the largest packing density of a 6-dimensional lattice.

10. Prove that $\sigma(E_7) > \sigma(D_7) > \sigma(A_7) > \sigma(\mathbb{Z}^7)$.

Remark: In fact, $\sigma(E_7) \approx 0.29530$ is known to be the largest packing density of a 7-dimensional lattice.

11. Prove that $\sigma(E_8) > \sigma(D_8) > \sigma(A_8) > \sigma(\mathbb{Z}^8)$.

In fact, $\sigma(E_8) \approx 0.25367$ is known to be the largest packing density of a 8-dimensional lattice.

12°. Prove that D_n^+ (for even n) is indeed a lattice.

13. Find $\rho(A_n)$, $\rho(D_n)$, $\rho(D_n^+)$, $\rho(\mathbb{Z}^n)$, $\det A_n$, $\det D_n$, $\det D_n^+$, $\det \mathbb{Z}_n$ and prove that $\sigma(D_n^+) > \sigma(D_n) > \sigma(A_n) > \sigma(\mathbb{Z}^n)$ for a sufficiently large n.

14. Prove that K_{12} is a lattice.

15. Prove that $K_{12} \sim (K_{12})^*$.

16. Prove that $\sigma(K_{12}) > \sigma(D_{12}^+) > \sigma(D_{12})$.

Remark: In fact, $\sigma(K_{12}) = \dfrac{\pi^6}{19440} \approx 0.04945$ is the largest *known* packing density of a 12-dimensional lattice.

17. Prove that $\sigma(\Lambda_{24}) > \sigma(D_{24}^+)$.

Remark: In fact, $\sigma(\Lambda_{24}) \approx 0.001930$ is the largest *known* packing density of a 24-dimensional lattice. All the lattices with *known* highest packing density in dimensions ≤ 24 may be obtained as sections of Λ_{24}.

18*. Prove that a laminated lattice Λ_n exists for every n.

Remark: In fact, the laminated lattices Λ_1, Λ_2, Λ_3, Λ_4, Λ_5, Λ_6, Λ_7 and Λ_8 are unique (up to a similarity) and coincide with $\mathbb{Z}^1$, A_2, $A_3 \sim D_3$, D_4, D_5, E_6, E_7, E_8 correspondingly. The lattice K_{12} is not laminated. The Leech lattice Λ_{24} is the unique 24-dimensional laminated lattice.

19. Prove that the Minkowski-Hlawka Theorem (Theorem 9.2) implies that for every n there exists a lattice $\Lambda \subset \mathbb{R}^n$ with $\sigma(\Lambda) \geq 2^{-n}$. If we use Problem 3 from Section 9.2 we get $\sigma(\Lambda) \geq 2^{1-n}$. If we use Problem 4* we get $\sigma(\Lambda) \geq \dfrac{\zeta(n)}{2^{n-1}}$.

20*. Prove that for every n there exists a lattice $\Lambda \subset \mathbb{R}^n$ such that $\sigma(\Lambda)$ is the largest possible for an n-dimensional lattice.

21°. Prove that for any $n > 1$ the packing density $\sigma(\Lambda)$ of a lattice $\Lambda \subset \mathbb{R}^n$ can be arbitrarily small positive.

See J.H. Conway and N.J.A. Sloane, *Sphere Packings, Lattices, and Groups*, 2nd ed., Springer-Verlag, New York, 1993.

Wednesday, January 31

---

11. Extremal Convex Bodies

(11.1) Definition. Let $l : \mathbb{R}^n \longrightarrow \mathbb{R}$ be a non-zero linear function and α be a real number. So $l(x) = \langle c, x \rangle$ for some non-zero $c \in \mathbb{R}^n$. The set $H = \big\{x \in \mathbb{R}^n : l(x) = \alpha\big\}$ is called a *hyperplane*. The sets $H^+ = \big\{x \in \mathbb{R}^n : l(x) \geq \alpha\big\}$ and $H^- = \big\{x \in \mathbb{R}^n : l(x) \leq \alpha\big\}$ are called (closed) *halfspaces*.

PROBLEM.

1. Let $K \subset \mathbb{R}^n$ be a compact convex set and $p \notin K$. Then there exists a hyperplane $H \subset \mathbb{R}^n$ such that $p \in H$ and $H \cap K = \emptyset$.

Hint: Let $q \in K$ be a point such that $\|q - p\| = \min\big\{\|x - p\| : x \in K\big\}$. Take H to be the hyperplane passing through the midpoint of the interval $[q, p]$ and orthogonal to that interval.

2. Let $K \subset \mathbb{R}^n$ be a compact convex set and $p \in \partial P$ be a point on its boundary. Then there exists a hyperplane $H \subset \mathbb{R}^n$ such that $p \in H$ and H does not contain an inner point of K. Such a hyperplane is called a *supporting hyperplane*.

Hint: Consider a sequence $p_m \in \mathbb{R}^n$ such that $p_m \longrightarrow p$ and $p_m \notin K$. Take H to be the limit of the hyperplanes H_m from Problem 1 which separate p_m from K.

(11.2) Definitions. A *polyhedron* is a set $P \subset \mathbb{R}^n$ of the type

$$P = \Big\{x \in \mathbb{R}^n : \langle c_i, x \rangle \leq \alpha_i, \ i = 1, \ldots, m\Big\},$$

where $c_1, \ldots, c_m$ are non-zero vectors from $\mathbb{R}^n$ and $\alpha_1, \ldots, \alpha_m$ are real numbers. In other words, polyhedron is an intersection of finitely many closed halfspaces. The *dimension* of P is the dimension of the smallest affine subspace containing P. Let $P \subset \mathbb{R}^n$ be a polyhedron and H^+ be a subspace bounded by a hyperplane H, such that $P \subset H^+$. The intersection $F = P \cap H$ is called a *face* of P. A face of a polyhedron is a polyhedron. If $\dim F = (\dim P) - 1$ then F is called a *facet* of P.

PROBLEMS.

1. A polyhedron has only finitely many faces.
2°. Polyhedra are convex.

(11.3) Theorem. *Let $\Lambda \subset \mathbb{R}^n$ be a lattice and $K \subset \mathbb{R}^n$ be a centrally symmetric closed convex body containing 0 as its interior point. Suppose further that K contains no non-zero lattice points in its interior. Then there exists a centrally symmetric polyhedron P such that*

(11.3.1) *$K \subset P$ and P contains no non-zero lattice points in its interior;*

(11.3.2) *P has at most $2(2^n - 1)$ facets.*

Proof. First, we prove that there exists a centrally symmetric polyhedron P which satisfies (11.3.1). Let us choose an $r > 0$ such that K contains the ball $B_r = \{x : \|x\| \leq r\}$. First, we note that K has to be bounded, otherwise $\operatorname{vol} K = \infty > 2^n \det \Lambda$ and because of the Minkowski Theorem K contains a non-zero lattice point in its interior. For every non-zero lattice point u let us do the following procedure: let us consider the ray $[0, u)$ and the point $p_u = \partial K \cap [0, u)$. Then $p_u = -p_{-u}$ and there exist a supporting hyperplane H_u of K in p_u and a supporting hyperplane H_{-u} of K in p_{-u} such that $H_u = -H_{-u}$. Let us translate these hyperplanes $H_u \mapsto H_u(u)$ and $H_{-u} \mapsto H_{-u}(-u)$ so that they pass through u and $-u$ correspondingly and let $H_u^+(u), H_{-u}^+(-u)$ be the halfspaces bounded by those translated hyperplanes and containing K. Finally, let

$$P = \bigcap_{u \in \Lambda \setminus \{0\}} H_u^+(u).$$

It is immediate that P is a convex centrally symmetric set containing K such that P does not contain a non-zero lattice point. Let us prove that P is a polyhedron. By the Minkowski Theorem we must have $\operatorname{vol} P \leq 2^n \det \Lambda$. This implies that P is bounded, so $P, K \subset B_R = \{x \in \mathbb{R}^n : \|x\| \leq R\}$ for some $R > 0$. Now the distance from 0 to H_u is at least r and the distance from $H_u(u)$ to 0 is at least $\dfrac{\|u\|}{R} r$. So only the hyperplanes $H_u(u)$ with $\|u\| \leq R^2/r$ can intersect P. Since Λ is discrete, there are finitely many of them.

Second, we prove that one can choose a polyhedron P in such a way that (11.3.2) holds. If some facet of P does not contain contain a lattice point in its interior, we can translate the supporting hyperplanes of this facet and of the antipodal facet further away from 0 until we hit a lattice point or just remove this pair of hyperplanes. Using this argument we get a centrally symmetric polyhedron P such that P does not contain a non-zero lattice point in its interior and every facet of P contains a non-zero lattice point. We claim that now P contains at most $2(2^n - 1)$ facets. Let $2\Lambda = \{2u : u \in \Lambda\}$. Then $|\Lambda : 2\Lambda| = 2^n$. Suppose that P has more than $2(2^n - 1)$ facets. For every pair of facets $F, -F$ let us choose a point u_F from the interior of F and map it into its class in $\Lambda : 2\Lambda$. Since the number of pairs of facets is at least 2^n we either get a facet F such that $u_F \in 2\Lambda$ or two facets $F \neq -G, G$ such that $u_F - u_G \in 2\Lambda$. In the first case we get a point $\dfrac{1}{2} u_F \in \Lambda$

which belongs to the interior of P, which is a contradiction. In the second case, the point $\frac{1}{2}(u_F - u_G) \in \Lambda$ is a point from the interior of P which is a contradiction again. $\square$

(11.4) Corollary. *Let K be a closed centrally symmetric convex set which does not contain a non-zero lattice point in its interior and such that* vol $K = 2^n \det \Lambda$. *Then K is a polyhedron with at most $2(2^n - 1)$ facets.*

Proof. The polyhedron P from Theorem 11.3 must coincide with K. $\square$

Such convex bodies K are called *extremal.*

(11.5) Theorem. *Let $\Lambda \subset \mathbb{R}^n$ be a lattice. Let*

$$V = \Big\{ x \in \mathbb{R}^n : \|x\| \leq \|x - u\| \quad \text{for any } u \in \Lambda \Big\} \quad \text{and} \quad K = 2V$$

Then K is an extremal convex body. That is, K is centrally symmetric and convex, vol K $= 2^n \det \Lambda$ *and K does not contain a non-zero lattice point in its interior. In particular, K is a polyhedron with at most $2(2^n - 1)$ facets.*

Proof. It is immediate that K is centrally symmetric. Since the inequality $\|x\| \leq \|x - u\|$ is equivalent to the inequality $\|x\|^2 - \|x - u\|^2 \leq 0$, that is $\langle 2u, x \rangle \leq \|u\|^2$, V is the intersection of a (possibly infinitely many) halfspaces, so K is convex. If $u \in \Lambda$ is a point from the interior of K, then $x = (0.5 + \epsilon)u$ is a point from V for a sufficiently small $\epsilon > 0$. But then $\|u\| > \|u - x\|$ which is a contradiction. Finally, we have to check that vol $K = 2^n \det \Lambda$, or equivalently, vol $V = \det \Lambda$. Indeed, for any $u \in \Lambda$ we have

$$V + u = \Big\{ x \in \mathbb{R}^n : \|x - u\| \leq \|x - v\| \quad \text{for any } v \in \Lambda \Big\},$$

so the translations $\{V + u : u \in \Lambda\}$ cover $\mathbb{R}^n$ without overlapping in their interiors. Let χ_V be the characteristic function of V, so

$$\chi_V(x) = \begin{cases} 1 & \text{if } x \in V, \\ 0 & \text{if } x \notin V. \end{cases}$$

Let Π be a fundamental parallelepiped of Λ. Then

$$\det \Lambda = \int_\Pi 1 \ dx = \sum_{u \in \Lambda} \int_\Pi \chi_{V+u}(x) \ dx$$

$$= \sum_{u \in \Lambda} \int_{\Pi - u} \chi_V(x) \ dx = \int_{\mathbb{R}^n} \chi_V(x) \ dx = \text{vol } V$$

(recall that $\Pi + u$ cover the whole space $\mathbb{R}^n$ without overlapping). $\square$

The set V is called the *Voronoi cell* of Λ.

PROBLEMS.

1. Voronoi cell of the lattice $\mathbb{Z}^2$ is a square and Voronoi cell of A_2 is a regular hexagon.

2. If $\Lambda \subset \mathbb{R}^2$ is a lattice then its Voronoi cell is either a parallelogram or a hexagon.

3. A centrally symmetric convex hexagon is the Voronoi cell of a lattice $\Lambda \subset \mathbb{R}^2$.

4. The Voronoi cell of $\mathbb{Z}^n$ is a cube.

5. The Voronoi cell of D^4 is a regular 4-dimensional polytope called 24-cell. It has 24 facets and 24 vertices and every facet is a regular octahedron.

6. Let A_n^* be the lattice dual to A_n. The Voronoi cell of A_n^* is a permutohedron. After rescaling, it is the polytope obtained by taking the convex hull of all $(n+1)!$ points which are obtained from $(-n, -n+2, -n+4, \ldots, n-2, n)$ by permutations of the coordinates.

7*. The facets of an extremal polyhedron are centrally symmetric.

8*. Let V be the Voronoi cell of a lattice and let $V + u : u \in \Lambda$ be a translation of V. If the intersection $(V+u) \cap V$ is $(n-1)$-dimensional then this is a common facet of V and $V + u$.

9*. There are extremal polyhedra that are not Voronoi cells of lattices.

Friday, February 2

---

12. Minkowski's Second Theorem

(12.1) Definitions. Let $K \subset \mathbb{R}^n$ be a centrally symmetric compact convex set and $\Lambda \subset \mathbb{R}^n$ be a lattice. For a real μ we let $\mu K = \{\mu x : x \in K\}$. We define the *successive minima* $\mu_1, \ldots, \mu_n$ as follows:

$\mu_1 = \min\big\{\mu : \ \mu K$ contains a non-zero lattice point, say $u_1\big\}$;
$\mu_k = \min\big\{\mu : \mu K$ contains k linearly independent lattice points, say $u_1, \ldots, u_k\big\}$.

PROBLEMS.

1°. Minkowski's Convex Body Theorem implies that $\big(\mathrm{vol}\ K\big) \cdot \mu_1^n \leq 2^n \det \Lambda$.

2°. We have $\mu_1 \leq \mu_2 \leq \ldots \leq \mu_n$.

3. $\dfrac{2^n}{n!} \det \Lambda \leq \mu_1 \cdot \mu_2 \cdots \mu_n \cdot \mathrm{vol}\ K$.

4. Let $K = \{x \in \mathbb{R}^n : \|x\| \leq 1\}$ be the unit ball. Then $\det \Lambda \leq \mu_1 \cdot \mu_2 \cdots \mu_n$.

5°. With every convex centrally symmetric convex body K we associate what is called the *gauge function* $f_K : \mathbb{R}^n \longrightarrow \mathbb{R}$: $f_K(x) = \min\big\{\mu : x \in \mu K\big\}$. Prove that $f_K(x) = f_K(-x)$ and $f_K(x+y) \leq f_K(x) + f_K(y)$. If K is closed then f_K is continuous. If K contains 0 as its interior point then $f_K(x) = 0$ if and only if $x = 0$.

(12.2) Theorem [Minkowski's Second Theorem]. *Let $\Lambda \subset \mathbb{R}^n$ be a lattice and $K \subset \mathbb{R}^n$ be a convex centrally symmetric body. Let $\mu_1, \ldots, \mu_n$ be the successive minima of K. Then*

$$\mu_1 \cdots \mu_n \cdot \mathrm{vol}\ K \leq 2^n \det \Lambda.$$

Proof. Let $u_1, \ldots, u_n \in \Lambda$ be the lattice vectors from Definition 12.1. So for $\mu \leq \mu_k$ every point $K \cap \Lambda$ is a linear combination of $u_1, \ldots, u_k$. Let $L_k \subset \mathbb{R}^n$ be the linear subspace generated by $u_1, \ldots, u_k$. In particular, $L_0 = \{0\}$ and $L_n = \mathbb{R}^n$. We shall construct a transformation $\Phi : K \longrightarrow \mathbb{R}^n$ which has the following property:

$$\Phi(x) = \mu_1\phi_1(x) + (\mu_2 - \mu_1)\phi_2(x) + \ldots + (\mu_i - \mu_{i-1})\phi_i(x) + \ldots + (\mu_n - \mu_{n-1})\phi_n(x),$$

where ϕ_i are continuous functions, $\phi_i(x) \in K \cap (x + L_{i-1})$ for every i. If $x = \sum_{i=1}^{n} \lambda_i u_i$ then ϕ_i depends on $\lambda_i, \lambda_{i+1}, \ldots, \lambda_n$ only. In particular, $\phi_1(\lambda_1, \ldots, \lambda_n) = x$ and $\phi_n(x)$ depends on λ_n only.

Suppose that such a Φ exists, we will show that the theorem follows at once.

First, we observe that for every $y \in \Phi(K)$ there exists a unique $x \in K$ such that $\Phi(x) = y$. Indeed, let $y = \sum_{i=1}^{n} \beta_i u_i$. Then

$$\beta_n = \mu_1\lambda_n + (\mu_2 - \mu_1)\lambda_n + \ldots + (\mu_n - \mu_{n-1})\lambda_n = \mu_n\lambda_n,$$

from which we find the coefficient λ_n in front of u_n in the expansion of x. Similarly,

$$\beta_{n-1} = \mu_1\lambda_{n-1} + (\mu_2 - \mu_1)\lambda_{n-1} + \ldots + (\mu_{n-1} - \mu_{n-2})\lambda_{n-1} + \psi(\lambda_n),$$

where $\psi(\lambda_n)$ is the coefficient in front u_{n-1} of $\phi_n(\lambda_n)$. Continuing this process we get

$$\beta_k = \mu_k\lambda_k + \psi_k(\lambda_{k+1}, \ldots, \lambda_n), \tag{12.2.1}$$

where ψ_k are continuous functions.

Next, we observe that the vol $\Phi(K) = \mu_1 \ldots \mu_n \cdot \mathrm{vol}\, K$. This follows from the equations (12.2.1). If ψ_k were smooth, then Jacobian of this transformation is the determinant of a triangular matrix with $\mu_1, \ldots, \mu_n$ on the main diagonal. If ψ_k are continuous, we can approximate them by smooth functions.

Assume now, that contrary to the statement of the Theorem we have $\mu_1 \cdots \mu_n \cdot \mathrm{vol}\, K > 2^n \det \Lambda$. Then vol $\Phi(K^\circ) > 2^n \det \Lambda$, where K° is the interior of K. Then vol $\frac{1}{2}\Phi(K^\circ) > \det \Lambda$ and by the Blichfeldt's Theorem (Theorem 7.1) we get that there are two points $y^1, y^2 \in \Phi(K^\circ)$ such that $u = \frac{1}{2}(y^1 - y^2) \in \Lambda \setminus \{0\}$. Let x^1 be the preimage of y^1 and x^2 be the preimage of y^2. Since Φ is injective, x^1 and x^2 should be different. Let k be the largest index where the coefficients of x^1 and x^2 in front of u_k are different. So we get

$$u = \frac{1}{2}\Big(\Phi(x^1) - \Phi(x^2)\Big) = \mu_1 \cdot \frac{1}{2}\Big(\phi_1(x^1) - \phi(x^2)\Big)$$

$$+(\mu_2 - \mu_1) \cdot \frac{1}{2}\Big(\phi_2(x^1) - \phi(x^2)\Big) + \ldots + (\mu_k - \mu_{k-1}) \cdot \frac{1}{2}\Big(\phi_k(x^1) - \phi_k(x^2)\Big).$$

Since $\phi_i(x^1), \phi_i(x^2) \in K^\circ$ and K° and K° is convex and centrally symmetric, we have that $\frac{1}{2}\big(\phi_i(x^1) - \phi_i(x^2)\big) \in K^\circ$ and since K° is convex we have that $u \in \mu_k K^\circ$. But then from (12.2.2) it follows that the coefficients of y^1 and y^2 in front of u_k are different, meaning that u is linearly independent of $u_1, \ldots, u_{k-1}$. This contradicts the definition of μ_k.

It remains to construct Φ, that is the functions ϕ_i. Let us choose $\phi_i(x)$ to be the center of gravity of $x + L_{i-1} \cap K$, where the center of gravity of a convex body B is given by the integral

$$\frac{1}{\text{vol } B} \int_B x \, dx.$$

□

Monday, February 5

---

13. Reduced Bases

We are looking for an "almost orthogonal" basis $u_1, \ldots, u_n$ of a lattice $\Lambda \subset \mathbb{R}^n$ such that $\|u_1\| \cdots \|u_n\| \leq C(n) \det \Lambda$, where $C(n)$ is a constant depending on the dimension of the lattice alone. Such bases are called *reduced*.

PROBLEMS

1. Let $\Lambda \subset \mathbb{R}^2$ be a lattice. Then there is a basis u_1, u_2 of Λ such that the angle α between u_1 and u_2 is in the interval $60° \leq \alpha \leq 90°$. So one can choose $C(2) = \dfrac{2}{\sqrt{3}}$. Furthermore, $C(2)$ can not be made smaller.

2. Let us construct a basis $u_1, \ldots, u_n$ of $\Lambda \subset \mathbb{R}^n$ in the following way: u_1 is a shortest non-zero vector in Λ, u_k is a shortest vector in Λ such that $u_1, \ldots, u_{k-1}, u_k$ are primitive (see Definition 6.1). Prove that $\|u_1\| \cdots \|u_n\| \leq C(n) \det \Lambda$.

Remark: Such a basis is called *Minkowski reduced* basis. One can prove that $C(n) \leq \left(\frac{4}{\pi}\right)^{\frac{n}{2}} \Gamma\left(\frac{n+1}{2}\right) \left(\frac{3}{2}\right)^{\frac{(n-1)(n-2)}{2}}$.

3. Let us construct a basis $u_1, \ldots, u_n$ of $\Lambda \subset \mathbb{R}^n$ in the following way: u_1 is a shortest non-zero vector in Λ, u_k is a vector with the shortest projection onto the orthogonal complement of $u_1, \ldots, u_{k-1}$ and such that $u_1, \ldots, u_k$ are primitive. Prove that $\|u_1\| \cdots \|u_n\| \leq C(n) \det \Lambda$.

This is so-called *Korkin - Zolotarev reduced* basis, see, for example, J.C. Lagarias, Point lattices, in: *Handbook of Combinatorics*, **vol.** 1,2, 919–966.

(13.1) Gram - Schmidt Orthogonalization. Let $u_1, \ldots, u_n$ be linearly independent vectors in $\mathbb{R}^n$. Let us define $w_1, \ldots, w_n \in \mathbb{R}^n$ recursively:

$$w_1 = u_1, \quad w_k = u_k - \sum_{i=1}^{k-1} \frac{\langle u_k, w_j \rangle}{\langle w_j, w_j \rangle} w_j \quad \text{for } k = 2, \ldots, n.$$

PROBLEMS.

1°. Make sure that $w_1, \ldots, w_n$ are non-zero pairwise orthogonal vectors and that $|u_1 \wedge \ldots \wedge u_n| = |w_1 \wedge \ldots \wedge w_n| = \|w_1\| \cdots \|w_n\|$.

2°. We have $u_k = w_k + \sum_{i=1}^{k-1} \alpha_i w_i$, where α_i are reals.

3°. Let $u_1, \ldots, u_n$ be linearly independent, m be a real number and $j < i$. Then $u_1, \ldots, u_{i-1}, u_i - m u_j, u_{i+1}, \ldots, u_n$ are linearly independent and their Gram - Schmidt orthogonalization is the same as of $u_1, \ldots, u_n$.

4°. If α is a real number and m is an integer, nearest to α then $|\alpha - m| \leq 0.5$.

5°. Let $u_1, \ldots, u_n$ be a set of linearly independent vectors and $u_1, \ldots, u_{i-1}, u_i', u_{i+1}', \ldots, u_n$ be a new set obtained by interchanging u_i and u_{i+1} so that $u_i' = u_{i+1}$ and $u_{i+1}' = u_i$. If $w_1, \ldots, w_n$ is the Gram - Schmidt orthogonalization of the first set and $w_1', \ldots, w_n'$ is the Gram - Schmidt orthogonalization of the second set then $w_1' = w_1', \ldots, w_{i-1}' = w_{i-1}, w_{i+2}' = w_{i+2}, \ldots, w_n' = w_n$.

(13.2) Definition. Let $u_1, \ldots, u_n$ be a basis of a lattice $\Lambda \subset \mathbb{R}^n$ and $w_1, \ldots, w_n$ be its Gram - Schmidt orthogonalization. For a vector u by $u(i)$ we denote its orthogonal projection onto the linear subspace orthogonal to $w_1, \ldots, w_{i-1}$ (that is, generated by $w_i, w_{i+1}, \ldots, w_n$). So $u_i(i) = w_i$. We say that the basis $u_1, \ldots, u_n$ is *reduced* or *LLL-reduced* or *A.K. Lenstra - H.W. Lenstra Jr. - L. Lovász reduced* if and only if

(13.2.1) in the decomposition $u_i = w_i + \sum_{j=1}^{i-1} \alpha_{ij} w_j$ one has $|\alpha_{ij}| \leq 0.5$ for every i;

(13.2.2) $\|u_i(i)\|^2 = \|w_i\|^2 \leq \dfrac{4}{3}\|u_{i+1}(i)\|^2$ for $1 \leq i < n$.

(13.3) Algorithm. Let us start with some basis $u_1, \ldots, u_n$ of the lattice. Then we compute its Gram-Schmidt orthogonalization $w_1, \ldots, w_n$. The algorithm consists of the two major alternating steps.

Step 1. We make sure that (13.2.1) is satisfied. If some $|\alpha_{ij}| > 0.5$ we choose a pair (i, j) with the largest j, let m_{ij} to be the integer closest to α_{ij} and modify the basis to $u_1, \ldots, u_{i-1}, u_i' = u_i - m_{ij} u_j, u_{i+1}, \ldots, u_n$. Then the new basis has the same Gram - Schmidt orthogonalization (see Problem 3 in Section 13.1). Furthermore, the coefficient in the expansion of u_i' with respect to $w_1, \ldots, w_n$ is $\alpha_{ij}' = \alpha_{ij} - m_{ij}$, so $|\alpha_{ij}'| \leq 0.5$. Repeating this procedure again and again, at most $\binom{n}{2}$ times we make sure that (13.2.1) is satisfied for all pairs $i > j$.

Step 2. Suppose that there is some i such that (13.2.2) is not satisfied. Then we interchange $u_i' = u_{i+1}, u_{i+1}' = u_i$. Then $u_i'(i) = u_{i+1}(i)$ and $u_{i+1}'(i) = u_i(i)$ so (13.2.2) now holds for $i, i+1$.

Now, we perform Steps 1 or 2 as long as it is possible. If neither of them is possible we have a reduced basis. We have to establish that the algorithm terminates (and, in fact, in polynomial time). To see that, consider the quantity

$$D(u_1, \ldots, u_n) = \prod_{i=1}^{n} \|w_i\|^{n-i},$$

where $w_1, \ldots, w_n$ is the Gram - Schmidt orthogonalization of the current basis $u_1, \ldots, u_n$. Step 1 doesn't change $D(u_1, \ldots, u_n)$ as it doesn't change $w_1, \ldots, w_n$. Step 2 changes w_i and w_{i+1} only (cf. Problem 5 of Section 13.1). Thus we have

$$\frac{D(u_1, \ldots, u_{i-1}, u_i', u_{i+1}', u_{i+2}, \ldots, u_n)}{D(u_1, \ldots, u_{i-1}, u_i, u_{i+1}, u_{i+2}, \ldots, u_n)} = \frac{\|w_i'\|^{n-i}\|w_{i+1}'\|^{n-i-1}}{\|w_i\|^{n-i}\|w_{i+1}\|^{n-i-1}}.$$

We claim that $\dfrac{\|w_i'\|}{\|w_i\|} < \dfrac{\sqrt{3}}{2}$ and $\dfrac{\|w_{i+1}'\|}{\|w_{i+1}\|} < \dfrac{2}{\sqrt{3}}$. Indeed, $w_i' = u_{i+1}(i)$ and the first inequality follows since the condition (13.2.2) is violated. Let H be the orthogonal complement to the linear subspace generated by $u_1, \ldots, u_{i-1}$. Then w_i is the orthogonal projection of u_i onto H and $u_{i+1}(i)$ is the orthogonal projection of u_{i+1} onto H. Then w_{i+1} is the orthogonal complement of $u_{i+1}(i)$ to the projection onto w_i and w_{i+1}' is the orthogonal complement of w_i to the projection onto $u_{i+1}(i)$. So $\|w_{i+1}'\| = \|w_i\| \sin\phi$ and $\|w_{i+1}\| = \|u_{i+1}(i)\| \sin\phi$, where ϕ is the angle between w_i and $u_{i+1}(i)$. So the second inequality is proved. Finally,

$$\frac{D(u_1, \ldots, u_{i-1}, u_i', u_{i+1}', u_{i+2}, \ldots, u_n)}{D(u_1, \ldots, u_{i-1}, u_i, u_{i+1}, u_{i+2}, \ldots, u_n)} \leq \frac{\sqrt{3}}{2}.$$

Thus to make sure that the algorithm stops we have to bound $D(u_1, \ldots, u_n)$ from below. Indeed, let

$$\lambda = \min\big\{\|u\| : u \notin \Lambda \setminus \{0\}\big\}.$$

Let Λ_k be the k-dimensional lattice generated by $u_1, \ldots, u_k$. Then by the Minkowski's First Theorem we have $\det \Lambda \geq \left(\dfrac{\lambda}{\sqrt{k}}\right)^k$, so $\det \Lambda_k$ is bounded from below. On the other hand, $\|w_1\| \cdots \|w_k\| = \det \Lambda_k$. Hence $D(u_1, \ldots, u_n)$ is bounded from below.

In fact, the above algorithm stops in *polynomial time*. The algorithm is constructed in A.K. Lenstra, H.W. Lenstra Jr. and L. Lovász, Factoring polynomials with rational coefficients, *Mathematische Annalen*, **261** (1982), 515–534.

(13.4) Lemma. *Let $u_1, \ldots, u_n$ be a basis of Λ and $w_1, \ldots, w_n$ be its Gram - Schmidt orthogonalization. Then*

$$\min\big\{\|u\| : u \in \Lambda \setminus \{0\}\big\} \geq \min\big\{\|w_1\|, \ldots, \|w_n\|\big\}.$$

Proof. Let $u \in \Lambda$ be a non-zero lattice vector and let $u = \sum_{i=1}^{k} \lambda_i u_i$, where $\lambda_k \neq 0$ and λ_i are integers. Let us substitute $u_i = w_i + \sum_{j=1}^{i-1} \alpha_j w_j$ (see Problem 2 above). Then we get

$$u = \sum_{i=1}^{k} \beta_i w_i, \quad \text{where } \beta_k \text{ is a non} - \text{zero integer }.$$

Then $\|u\|^2 = \beta_1^2 \|w_1\|^2 + \ldots + \beta_k^2 \|w_k\|^2 \geq \|w_k\|^2$ and the proof follows. □

(13.5) Theorem. *Let $u_1, \ldots, u_n$ be a reduced basis of a lattice $\Lambda \subset \mathbb{R}^n$. Then*

(13.5.1) $$\|u_1\| \leq 2^{\frac{(n-1)}{2}} \min\Big\{\|u\| : u \in \Lambda \setminus \{0\}\Big\},$$

(13.5.2) $$\|u_1\| \leq 2^{\frac{(n-1)}{4}} \Big(\det \Lambda\Big)^{\frac{1}{n}},$$

(13.5.3) $$\|u_1\| \cdots \|u_n\| \leq 2^{\frac{1}{2}\binom{n}{2}} \det \Lambda.$$

Proof. Let $w_1, \ldots, w_n$ be the Gram - Schmidt orthogonalization of $u_1, \ldots, u_n$. Then by (13.3.2) and (13.3.1)

$$\|w_i\|^2 \leq \frac{4}{3} \|u_{i+1}(i)\|^2 = \frac{4}{3} \|w_{i+1} + \alpha_{i+1,i} w_i\|^2 =$$

$$\frac{4}{3} \|w_{i+1}\|^2 + \frac{4}{3} \alpha_{i+1,i}^2 \|w_i\|^2 \leq \frac{4}{3} \|w_{i+1}\|^2 + \frac{1}{3} \|w_i\|^2$$

and we get that

$$\|w_{i+1}\|^2 \geq \frac{1}{2} \|w_i\|^2 \quad \text{and, therefore } \|w_i\|^2 \geq 2^{1-i} \|w_1\|^2 = 2^{1-i} \|u_1\|.$$

Lemma 3.2 implies (13.5.1). Also

$$\|u_1\|^{2n} \leq 2^{\binom{n}{2}} \prod_{i=1}^{n} \|w_i\|^2 = 2^{\binom{n}{2}} \Big(\det \Lambda\Big)^2$$

and (13.5.2) follows. Finally,

$$\|u_k\|^2 = \|w_k\|^2 + \Big\| \sum_{i=1}^{k-1} \alpha_{ki} w_i \Big\|^2 \leq \|w_k\|^2 + \frac{1}{4} \sum_{i=1}^{k-1} \|w_i\|^2 \leq 2^{k-1} \|w_k\|^2.$$

From this we get (13.5.3). □

Wednesday, February 7

---

14. Shortest Vector

(14.1) Definition. Let $\Lambda \subset \mathbb{R}^n$ be a lattice. We denote

$$\lambda(\Lambda) = \min\bigl\{\|u\| : u \in \Lambda \setminus \{0\}\bigr\}.$$

PROBLEMS.

1°. Here is another way to prove that $D(u_1, \ldots, u_n)$ decreases by at least a factor of $\frac{2}{\sqrt{3}}$ when the Step 2 in the Algorithm 13.3 is performed. Note that

$$D(u_1, \ldots, u_n) = \prod_{k=1}^{n-1} \prod_{i=1}^{k} \|w_i\|.$$

Now $\prod_{i=1}^{k} \|w_i\| = \det \Lambda_k$, where Λ_k is the sublattice generated by $u_1, \ldots, u_k$. If we interchange u_i and u_{i+1} then $\prod_{i=1}^{k} \|w_i\|$ does not change for $k < i$ and for $k \geq i+1$, whereas for $k = i$ it gets multiplied by $\frac{\sqrt{3}}{2}$ or a smaller number.

2. Let Λ be a lattice and let $\Lambda_0 \subset \Lambda$ be its sublattice. Then

$$\lambda(\Lambda) \leq \lambda(\Lambda_0) \leq |\Lambda : \Lambda_0| \cdot \lambda(\Lambda_0).$$

3*. Here is a modification of the LLL-reduced basis due to Schnorr, so called k-reduced basis. Let us fix k. Condition (13.2.1) remains the same whereas Condition (13.2.2) should be replaced by the condition

$$\|w_i\| \leq \frac{4}{3}\lambda(\Lambda_k),$$

where Λ_k is the lattice generated by $u_i(i), u_{i+1}(i), \ldots, u_{i+k}(i)$, where $u_j(i)$ is the orthogonal complement of u_j to the linear subspace generated by $u_1, \ldots, u_{i-1}$.

a) Show that the original condition (13.2.2) is the above condition with $k = 2$,

b) Let $u_1, \ldots, u_n$ be a k-reduced basis of a lattice Λ. Then $\|u_1\| \leq c(k)(k+1)^{\frac{n}{k}} \lambda(\Lambda)$, $\|u_1\| \leq c(k)(k+1)^{\frac{n}{2k}} \bigl(\det \Lambda\bigr)^{\frac{1}{n}}$ and $\|u_1\| \cdots \|u_n\| \leq c^n(k)(k+1)^{\frac{n^2}{2k}} \det \Lambda$.

4. Let $\alpha_1, \ldots, \alpha_n$ be real numbers. Consider the map $\phi_t : \mathbb{Z}^n \longrightarrow \mathbb{R}^{n+1}$, $(m_1, \ldots, m_n) \longmapsto \bigl(m_1, \ldots, m_n, t(\alpha_1 m_1 + \ldots + \alpha_n m_n)\bigr)$, where $t > 0$ is a real number. Let $\Lambda_t = \phi_t(\mathbb{Z}^n)$. Then Λ_t is a lattice in the n-dimensional linear span of Λ_t and

$$\lim_{t \longrightarrow +\infty} \lambda(\Lambda_t)$$

$$= \begin{cases} < \infty & \text{if } m_1\alpha_1 + \ldots + m_n\alpha_n = 0 \text{ for some } (m_1, \ldots, m_n) \neq 0; \\ \infty & \text{otherwise.} \end{cases}$$

This observation was used to find linear dependencies with small integer coefficients between given rational numbers.

5. Let α be a real number and $\alpha_i = \alpha^{i-1}$ for $i = 1, \ldots, n$ and let Λ_t be a lattice constructed as in Problem 4 above. Then

$$\lim_{t \longrightarrow +\infty} \lambda(\Lambda_t)$$

$$= \begin{cases} < \infty & \text{if } \alpha \text{ is an algebraic number of degree } \leq n; \\ \infty & \text{otherwise.} \end{cases}$$

6*. Using Problem 5, construct an efficient (that is, polynomial time) algorithm for the following problems:

a) Given a primitive polynomial with integer coefficients $p(x)$ (that is, the greatest common divisor of the coefficients of p is 1), a root α of p (so that $p(\alpha) = 0$) and an open interval (β, γ)containing α and no other roots of p, compute the minimal integer polynomial f such that $f(\alpha) = 0$.

b) Given a primitive integer polynomial p, compute a decomposition of p into the product of integer irreducible polynomials.

7. Let $u_1, \ldots, u_n$ be a basis of a lattice $\Lambda \subset \mathbb{R}^n$ such that

$$\|u_1\| \cdots \|u_n\| \leq C|u_1 \wedge \ldots \wedge u_n|.$$

Then

$$\lambda(\Lambda) = \min\Big\{ \Big\| \sum_{i=1}^{n} \alpha_i u_i \Big\| : |\alpha_i| \leq C \quad \text{for all } i \Big\}.$$

It follows, in particular, that a shortest non-zero vector in a lattice of a fixed dimension can be computed in polynomial time.

8*. Is there a polynomial time algorithm which for any given lattice $\Lambda \subset \mathbb{R}^n$ computes a non-zero vector $u \in \Lambda$ such that $\|u\| \leq p(n)\lambda(\Lambda)$, where p is a polynomial.

Actually, the problem of finding a shortest vector in a given lattice is not known to be NP-hard.

Friday, February 9

---

15. Shortest Vector, Continued

The following remarkable result provides a "weak converse" of Lemma 13.4, see J.C. Lagarias, H.W. Lenstra Jr. and C.-P. Schnorr, Korkin-Zolotarev bases and successive minima of a lattice and its reciprocal lattice, *Combinatorica*, **10**(1990), 333–348.

(15.1) Lemma. *Let $\Lambda \subset \mathbb{R}^n$ be a lattice. Then there exists a basis $u_1, \ldots, u_n$ of Λ such that if $w_1, \ldots, w_n$ its Gram - Schmidt orthogonalization, then*

$$\min\{\|w_1\|, \ldots, \|w_n\|\} \geq \frac{1}{n} \min\{\|u\| : u \in \Lambda \setminus \{0\}\}.$$

Sketch of proof. Let Λ^* be the dual lattice to Λ. Then by the Minkowski First Theorem (see also Problem 2 of Section 7.3) applied to Λ and Λ^*, there is a vector $c_1 \in \Lambda$ and a vector $d_1 \in \Lambda^*$ such that $\|c_1\| \leq \sqrt{n}\left(\det \Lambda\right)^{\frac{1}{n}}$ and $\|d_1\| \leq \sqrt{n}\left(\det \Lambda^*\right)^{\frac{1}{n}}$. Since $\left(\det \Lambda\right)\left(\det \Lambda^*\right) = 1$ we get that $\|c_1\| \cdot \|d_1\| \leq n$. Now we construct a sequence $c_1, \ldots, c_n \in \Lambda$ and a sequence of pairwise orthogonal $d_1, \ldots, d_n \in \mathbb{R}^n$ as follows: if $d_1, \ldots, d_k$ are chosen, we consider the $(n-k)$-dimensional lattice $\Lambda_k = \{x \in \Lambda : \langle x, d_i \rangle = 0 \text{ for } i = 1, \ldots, d_k\}$. In the linear span of Λ_k we consider the dual lattice Λ_k^* and choose a vector $c_{k+1} \in \Lambda_k$ and $d_{k+1} \in \Lambda_k^*$ so that $\|c_{k+1}\|\|d_{k+1}\| \leq n$. Now it is seen that

$$\min\left\{\|c_1\|, \ldots, \|c_n\|\right\} \leq n \min\left\{\frac{1}{\|d_1\|}, \ldots, \frac{1}{\|d_n\|}\right\}.$$

Furthermore, the vectors $w_1 = d_n/\|d_n\|^2, w_2 = d_{n-1}/\|d_{n-1}\|^2, \ldots, w_n = d_1/\|d_1\|^2$ is the Gram - Schmidt orthogonalization of a basis of Λ. □

Some more problems.

PROBLEMS.

1. Let $\{\Lambda_m \subset \mathbb{R}^n\}$ be a sequence of n-dimensional lattices and $\Lambda \subset \mathbb{R}^n$ be yet another lattice. We say that Λ_m *converges* to Λ (notation: $\Lambda_m \longrightarrow \Lambda$ or $\lim_{m \longrightarrow +\infty} \Lambda_m = \Lambda$) if and only if the following conditions are satisfied:

- if $x_m \in \Lambda_m$ and $\lim_{m \longrightarrow +\infty} x_m = x$ then $x \in \Lambda$;
- for every $x \in \Lambda$ there is a sequence $x_m \in \Lambda_m$ such that $\lim_{m \longrightarrow +\infty} x_m = x$.

Prove the *Mahler's Compactness Theorem*: Let $\{\Lambda_t \subset \mathbb{R}^n, t \in T\}$ be a family of lattices in $\mathbb{R}^n$. Suppose that there is an upper bound $\det \Lambda_t \leq D$ for some D and all t and there is a lower bound $\lambda(\Lambda_t) \geq \delta$, for some $\delta > 0$ and all t, where $\lambda(\Lambda)$ is the smallest length of a non-zero lattice vector. Then there is a lattice Λ and a sequence $\{\Lambda_m = \Lambda_{t_m}\}$ such that $\lim_{m \longrightarrow +\infty} \Lambda_m = \Lambda$.

Hint: Consider a limit basis of an LLL-reduced bases in Λ_t.

2. Prove that for every dimension n there exists a lattice $\Lambda \subset \mathbb{R}^n$ with the largest packing density $\sigma(\Lambda)$ (cf. Problem 20 of Section 10).

3. Consider the Minkowski - Hlawka Theorem (Theorem 9.2). Prove that if the set M is closed and contains the origin as its interior point then the theorem remains true even if M is unbounded.

16. Nearest Lattice Point

(16.1) Definitions. Let $\Lambda \subset \mathbb{R}^n$ be a lattice and $x \in \mathbb{R}^n$ be a point. The number $\min\{\|u-x\| : u \in \Lambda\}$ is called the *minimal distance* from x to Λ and is denoted $\operatorname{dist}(x, \Lambda)$. For a real number α by $\{\{\alpha\}\}$ we denote the distance of α to the nearest integer.

PROBLEM.
1°. The minimal distance $\operatorname{dist}(x, \Lambda)$ exists.
2°. We have $0 \leq \{\{\alpha\}\} \leq 0.5$ for all α and $\alpha \longmapsto \{\{\alpha\}\}$ is a continuous function.
3°. We have $|x| \geq \{\{x\}\}$ for any x.

(16.2) Lemma. *Let $\Lambda \subset \mathbb{R}^n$ be a lattice, Λ^* be its dual and $x \in \mathbb{R}^n$. Then*

$$\operatorname{dist}(x, \Lambda) \geq \max\Bigl\{ \frac{\{\{\langle x, u^* \rangle\}\}}{\|u^*\|} : \ u^* \in \Lambda^* \setminus \{0\} \Bigr\}.$$

Proof. Let $u \in \Lambda$ be the point closest to x, so $\operatorname{dist}(x, \Lambda) = \|x-u\|$. Let us choose any non-zero $u^* \in \Lambda^*$. Then

$$\|x-u\| \geq \frac{|\langle x-u, u^* \rangle|}{\|u^*\|} \geq \frac{\{\{\langle x-u, u^* \rangle\}\}}{\|u^*\|} = \frac{\{\{\langle x, u^* \rangle\}\}}{\|u^*\|},$$

so the lemma is proven. □

(16.3) Theorem. *Let $\Lambda \subset \mathbb{R}^n$ be a lattice and let $x \in \mathbb{R}^n$ be a point. Let $u_1, \ldots, u_n$ be a basis of Λ and $u_1^*, \ldots, u_n^*$ be the corresponding dual basis of Λ^*. Suppose that $\|u_1\| \cdots \|u_n\| \leq C\|u_1 \wedge \ldots \wedge u_n\|$. Then*

$$\operatorname{dist}(x, \Lambda) \leq nC \max\Bigl\{ \frac{\{\{\langle x, u_i^* \rangle\}\}}{\|u_i^*\|} : i = 1, \ldots, n \Bigr\}.$$

Proof. Let $x = \alpha_1 u_1 + \ldots + \alpha_n u_n$, where $\alpha_i \in \mathbb{R}$. Let m_i be the integer, nearest to α_i, so $|\alpha_i - m_i| = \{\{\alpha_i\}\}$. Let $u = m_1 u_1 + \ldots + m_n u_n \in \Lambda$. We claim that the distance $\|u - x\|$ satisfies the above inequality. Indeed, we have $\alpha_i = \langle x, u_i^* \rangle$ and hence

$$\|u-x\| = \Bigl| \sum_{i=1}^n \{\{\alpha_i\}\} \|u_i\| \Bigr| \leq \max\Bigl\{ \frac{\{\{\langle x, u_i^* \rangle\}\}}{\|u_i^*\|} i = 1, \ldots, n \Bigr\} \cdot \sum_{i=1}^n \|u_i\| \|u_i^*\|.$$

Our goal is to prove that

$$\sum_{i=1}^n \|u_i^*\| \|u_i\| \leq nC.$$

Let v_i be the orthogonal complement of u_i to the space generated by

$u_1, \ldots, u_{i-1}, u_{i+1}, \ldots, u_{n-1}$. Then

$$\frac{1}{C}\|u_1\|\cdots\|u_n\| \leq |u_1 \wedge \ldots \wedge u_n| = \frac{1}{C}\|v_i\| \cdot |u_1 \wedge \ldots \wedge u_{i-1} \wedge u_{i+1} \wedge \ldots \wedge u_n|$$

$$\leq \frac{1}{C}\|v_i\| \cdot \|u_1\|\cdots\|u_{i-1}\|\|u_{i+1}\|\cdots\|u_n\|.$$

Hence $\|v_i\| \geq C^{-1}\|u_i\|$. Now, since u_i^* is orthogonal to $u_1, \ldots, u_{i-1}, u_{i+1}, \ldots, u_n$, we have $1 = \langle u_i, u_i^* \rangle = \langle u_i^*, v_i \rangle = \|u_i^*\|\|v_i\| \geq C^{-1}\|u_i^*\|\|u_i\|$, so $\|u_i\|\|u_i^*\| \leq C$. □

(16.4) Corollary. *There exists a constant $f(n)$ such that*

$$\operatorname{dist}(x, \Lambda) \leq f(n) \max\Big\{\frac{\{\{\langle x, u^* \rangle\}\}}{\|u^*\|} : u^* \in \Lambda^* \setminus \{0\}\Big\}$$

for any n-dimensional lattice Λ.

It follows that if $u_1, \ldots, u_n$ is the LLL-reduced basis then we have $C = 2^{O(n^2)}$ (see (13.5.3)), so we can choose $f(n) = 2^{O(n^2)}$. □

However, this estimate can be significantly improved.

PROBLEMS.

1. If $u_1, \ldots, u_n$ is an LLL-reduced basis then

$$\operatorname{dist}(x, \Lambda) \leq \Big(\frac{3}{\sqrt{2}}\Big)^n \cdot \max\Big\{\frac{\{\{\langle x, u_i^* \}\}}{\|u_i^*\|}\Big\},$$

so we can choose $f(n) = 2^{O(n)}$. However, this estimate can be significantly improved.

2* Let $\Lambda \subset \mathbb{R}^n$ be a lattice. Then

$$\operatorname{dist}(x, \Lambda) \leq (6n^2 + 1) \max\Big\{\frac{\{\{\langle u^*, x \rangle\}\}}{\|u^*\|} : u^* \in \Lambda^* \setminus \{0\}\Big\},$$

so we can choose $f(n) = (6n^2 + 1)$, see J. Håstad, Dual vectors and lower bounds for the nearest lattice point problem, *Combinatorica*, **8**(1988), 75–81.

3*. The estimate $f(n) = 2^{O(n)}$ from Problem 1 can be achieved efficiently, that is, in polynomial time, whereas the estimate from Problem 2 is essentially non-constructive. Can you obtain an efficient polynomial bound for $f(n)$?

4. Let $\theta_1, \ldots, \theta_n$ be real numbers such that $m_1\theta_1 + \ldots + m_n\theta_n + m_{n+1} = 0$ for integer $m_1, \ldots, m_n, m_{n+1}$ implies $m_1 = \ldots = m_n = m_{n+1} = 0$. Then for any real vector $a = (a_1, \ldots, a_n)$ and for any $\epsilon > 0$ there exists a positive integer m such that $\{\{a_i - m\theta_i\}\} < \epsilon$ for $i = 1, \ldots, n$ (Kronecker's Theorem).

Hint: Let t be a very big number. Consider the lattice $\Lambda_t \subset \mathbb{R}^{n+1}$ generated by the vectors $u_1 = (\theta_1, \ldots, \theta_n, t^{-1})$, $u_2 = (1, 0, \ldots, 0)$, $u_3 = (0, 1, \ldots, 0), \ldots$, $u_{n+1} =$

$(0, \ldots, 1, 0)$. The dual lattice Λ_t^* has the basis $u_1^* = (0, \ldots, t)$, $u_2^* = (1, 0, \ldots, -t\theta_1)$, $u_3^* = (0, 1, 0 \ldots, 0, -t\theta_2)$, $\ldots$, $u_{n+1}^* = (0, \ldots, 1, -t\theta_n)$. Then $\lambda(\Lambda_t) \longrightarrow +\infty$ as $t \longrightarrow +\infty$. Therefore, by Corollary 16.4 $\operatorname{dist}(a, \Lambda_t) \longrightarrow 0$ as $t \longrightarrow +\infty$.

5°. The nearest point $u \in \mathbb{Z}^n$ to a given point $x \in \mathbb{R}^n$ is obtained as follows: round the i-th coordinate of x to the nearest integer.

6. This is how to find the nearest point $u \in D_n$ (see (10.2.3)) to a given point $x \in \mathbb{R}^n$. First, round all the coordinates of x to the nearest integer and get a point, say, $f(x) \in \mathbb{Z}^n$. Then do the same but the worst coordinate of x (furthest from integer) round the wrong way and get a point, say, $g(x)$. Choose from $f(x)$ and $g(x)$ the one that has an even sum of the coordinates.

7. This is how to construct the nearest point $u \in A_n$ (see (10.2.2)) to a given point $x \in \mathbb{R}^{n+1}$. First, compute $s = x_1 + \ldots + x_{n+1}$. Then modify $x_i := x_i - s/(n+1)$ for $i = 1, \ldots, n+1$. Then round every coordinate of x_i to the nearest integer and get a vector, say, $f(x)$. Compute $\Delta =$ sum of the coordinates of $f(x)$. Let $\delta(x) = x - f(x)$. Let $x_{i_0}, x_{i_1}, \ldots, x_{i_n}$ be the coordinates of x in order of increasing value of $\delta_i(x)$. If $\Delta = 0$ then $f(x)$ is the nearest to x. If $\Delta < 0$ then the nearest point is obtained by subtracting 1 from $f(x)_{i_0}, \ldots, f(x)_{i_{\Delta-1}}$. If $\Delta > 0$ then the nearest point is obtained by adding 1 to the coordinates $f(x)_{i_n}, f(x)_{i_{n-1}}, \ldots, f(x)_{i_n - \Delta+1}$.

Monday, February 12

---

17. Flatness Theorems

(17.1) Lemma. *Let $\Lambda \subset \mathbb{R}^n$ be a lattice, $x \in \mathbb{R}^n$ be a point and $B \subset \mathbb{R}^n$ be a ball. Suppose further that $B \cap \Lambda = \emptyset$. Then there exists a non-zero $u^* \in \Lambda^*$ such that*

$$\max\Bigl\{\langle u^*, x\rangle : x \in B\Bigr\} - \min\Bigl\{\langle u^*, x\rangle : x \in B\Bigr\} \leq f(n),$$

where $f(n) = 2^{O(n^2)}$ is a number depending on n only.

Proof. Let $x \in \mathbb{R}^n$ be the center of B and R be its radius. Then $\operatorname{dist}(x, \Lambda) \geq R$. Let $u_1, \ldots, u_n$ be a LLL-reduced basis of Λ and $u_1^*, \ldots, u_n^*$ be the corresponding dual basis of Λ^*. Let us choose u^* to be the vector u_i^* with the smallest norm. We use Theorem 16.3:

$$R \leq \operatorname{dist}(x, \Lambda) \leq 2^{O(n^2)} \max\Bigl\{\frac{\{\{\langle x, u_i^*\rangle\}\}}{\|u_i^*\|} \ : \ i = 1, \ldots, n\Bigr\}$$

$$\leq 2^{O(n^2)} \max\Bigl\{\frac{1}{\|u_i^*\|} \ : \ i = 1, \ldots, n\Bigr\} \leq 2^{O(n^2)} \frac{1}{\|u^*\|}.$$

Now, the maximal value of $\langle x, u^* \rangle$ on B is attained at $x + R\dfrac{u^*}{\|u^*\|}$ and is equal to $\langle x, u^* \rangle + R\|u^*\|$. The minimal value of $\langle x, u^* \rangle$ on B is attained at $x - R\dfrac{u^*}{\|u^*\|}$ and is equal to $\langle x, u^* \rangle - R\|u^*\|$. So the difference max − min is $2R\|u^*\| \leq 2^{O(n^2)}$. □

PROBLEMS.

1. Actually, one can choose $f(n) = 2^{O(n)}$ (cf. Problem 1, Section 16.4).

2^*. Actually, one can choose $f(n) = O(n^2)$ (cf. Problem 2, Section 16.4).

(17.2) Definition. Let $B \subset \mathbb{R}^n$ be a ball and $T : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ be a non-degenerate linear operator. The image $E = T(B)$ is called an *ellipsoid.*

PROBLEMS.

1°. Let $B = \{x : \|x - x_0\| \leq R\}$ be a ball in $\mathbb{R}^n$ and T be a non-degenerate linear operator. Let $E = T(B)$. Then $E = \big\{x : \langle x - y_0, Q(x - y_0) \rangle \leq R\big\}$, where $Q = T^{-1}(T^{-1})^*$ and $y_0 = T(x_0)$.

2°. Every ellipsoid $E \subset \mathbb{R}^n$ can be defined as $E = \big\{x : \langle x - y_0, Q(x - y_0) \rangle \leq R\big\}$ for some point $y_0 \in \mathbb{R}^n$ and some positive definite symmetric matrix Q.

3°. Let $\Lambda_1 \subset \mathbb{R}^n$ be a lattice, T be a linear non-degenerate operator and $\Lambda = T(\Lambda_1)$. Then Λ is a lattice and $\Lambda^* = (T^*)^{-1}\Lambda_1^*$, where T^* is the conjugate operator.

(17.3) Lemma. *Let $\Lambda \subset \mathbb{R}^n$ and $E \subset \mathbb{R}^n$ be an ellipsoid such that $E \cap \Lambda = \emptyset$. Then there exists a non-zero vector $u^* \in \Lambda^*$ such that*

$$\max\big\{\langle x, u^* \rangle : \ x \in E\big\} - \min\big\{\langle x, u^* \rangle : \ x \in E\big\} \leq f(n),$$

where $f(n) = 2^{O(n^2)}$ is a number depending on n only.

Proof. Let $B \subset \mathbb{R}^n$ be a ball and T be a non-degenerate linear operator on $\mathbb{R}^n$ such that $T(B) = E$. Let $\Lambda_1 = T^{-1}(\Lambda)$ be the preimage of Λ, so $T(\Lambda_1) = \Lambda$. Then Λ_1 is a lattice and $\Lambda^* = (T^*)^{-1}(\Lambda_1^*)$. By Lemma 17.1 there exists a vector, say $v^* \in \Lambda_1^*$ such that

$$\max\big\{\langle x, v^* \rangle : x \in B\big\} - \min\big\{\langle x, v^* \rangle : x \in B\big\} \leq f(n).$$

Let $u^* = (T^*)^{-1}v^* \in \Lambda^*$. Then for every $x \in E$ there exists an $y \in B$ such that $x = Ty$ and we have $\langle x, u^* \rangle = \langle Ty, (T^*)^{-1}v^* \rangle = \langle y, v^* \rangle$ and the proof follows by Lemma 17.1 □

PROBLEMS.

1. Actually, one can choose $f(n) = 2^{O(n)}$ (cf. Problem 1, Section 17.1).

2^*. Actually, one can choose $f(n) = O(n^2)$ (cf. Problem 2, Section 17.1).

(17.4) Theorem. *Let $K \subset \mathbb{R}^n$ be a convex compact set with non-empty interior. Then there exist two concentric ellipsoids E_1 and E_2 such that $E_1 \subset K \subset E_2$ and E_1 is obtained from E_2 by shrinking it n times towards its center.*

We don't prove this result as it has nothing to do with lattice properties. However, this is how one can prove it.

PROBLEMS.

1. Prove that one can choose for E_1 the ellipsoid of the largest volume contained in K.

Hint: Without loss of generality we can assume that E_1 is the unit ball B. We have to prove that K is contained in the ball of radius n. Suppose that it is not, so there is a point $x \in K$ with the distance larger than n from the origin. Since K is convex it must contain a cone over B with the vertex x. Now, we can stretch B a little bit in the direction of x so that we get an ellipsoid of a larger volume which fits in the cone.

2. Prove that one can choose for E_2 the ellipsoid of the smallest volume containing K.

3. For every convex compact set K with a non-empty interior there exists unique ellipsoid of the largest volume contained in K.

4. For every convex compact set K with a non-empty interior there exists unique ellipsoid of the smallest volume containing K.

5. Let $K \subset \mathbb{R}^n$ be a centrally symmetric (about the origin, say) compact convex set with non-empty interior. Then there exists an ellipsoid E_1 such that $E_1 \subset K \subset \sqrt{n}E_1$.

(17.5) Theorem. *Let $\Lambda \subset \mathbb{R}^n$ be a lattice and $K \subset \mathbb{R}^n$ be a convex compact set such that $K \cap \Lambda = \emptyset$. Then there exists a non-zero $u^* \in \Lambda^*$ such that*

$$\max\big\{\langle u^*, x\rangle : x \in K\big\} - \min\big\{\langle u^*, x\rangle : x \in K\big\} \leq f(n),$$

where $f(n) = 2^{O(n^2)}$ is a number depending on n only.

Proof. Let us construct a pair of ellipsoids $E_1 \subset K \subset E_2$ as in Theorem 17.4 above. Since E_1 does not contain a lattice point, by Lemma 17.3 there exists an $u^* \in \Lambda^*$ such that

$$\max\big\{\langle u^*, x\rangle : x \in E_1\big\} - \min\big\{\langle u^*, x\rangle : x \in E_1\big\} \leq f(n).$$

By Theorem 17.4 it follows that

$$\max\big\{\langle u^*, x\rangle : x \in E_2\big\} - \min\big\{\langle u^*, x\rangle : x \in E_2\big\} \leq nf(n).$$

Since $K \subset E_2$, the proof follows. □

PROBLEMS.

1. One can choose $f(n) = 2^{O(n)}$ (cf. Problem 1, Section 17.3).

2*. In fact, one can choose $f(n) = O(n^3)$ (cf. Problem 2, Section 17.3).

3*. In fact, one can choose $f(n) = O(n^2)$

See R. Kannan and L. Lovász, Covering minima and lattice-point-free convex bodies, *Annals of Mathematics. Second Series*, **128**(1988), 577–602.

4^*. Can we choose $f(n) = O(n)$?

Remark: This is an open problem. It is known though that for centrally symmetric bodies one can choose $f(n) = O(n \log n)$, see W. Banaszczyk, Inequalities for convex bodies and polar reciprocal lattices in $\mathbb{R}^n$. II. Application of K-convexity, *Discrete & Computational Geometry*, **16**(1996), 305–311.

5. We definitely can not choose $f(n) = O(1)$.

6^*. We can choose $f(3) = 1$, see H. Scarf, Integral polyhedra in three space, *Mathematics of Operations Research*, **10**(1985), 403–438.

(17.6) H.W. Lenstra's algorithm for integer programming. Roughly speaking, this algorithm addresses the following problem: given a lattice $\Lambda \subset \mathbb{R}^n$ (say, by its basis), and a convex body $K \subset \mathbb{R}^n$ (say, a polyhedron given by the list of linear inequalities), decide whether $K \cap \Lambda = \emptyset$, and if not, construct a lattice point in K.

The algorithm proceeds as follows: construct concentric ellipsoids $E_1 \subset K \subset E_2$, where E_1 obtained from E_2 by shrinking it towards its center by, say, $n\sqrt{n}$ times (it is not known if we can make factor n from Theorem 17.4 efficiently, but $n\sqrt{n}$ we can make). Apply a linear transform T that maps E_1 onto the unit ball B and let $\Lambda_1 = T(\Lambda)$. Construct an LLL-reduced basis $u_1, \ldots, u_n$ of Λ_1 and let $u_1^*, \ldots, u_n^*$ be the dual basis. Choose v^* to be u_i^* with the smallest norm. Let $u^* = (T^*)^{-1} v^*$. Note that $u^* \in \Lambda^*$. Compute $M = \max\{\langle u^*, x\rangle : x \in K\}$ and $m = \min\{\langle u^*, x\rangle : x \in K\}$. Note that $M - m \leq f(n)$. For every integer i in the interval $[m, M]$ let $K_i = \{x \in K : \langle u^*, x\rangle = i\}$. Note that if there is a point in $K \cap \Lambda$ then there is a point in $K_i \cap \Lambda$ for some i. Thus we reduced one n-dimensional problem to $f(n)$ $(n-1)$-dimensional problems. Proceed as above until we get a bunch of 0-dimensional problems which we can solve trivially. This algorithm has a polynomial time complexity provided the dimension n is fixed.

PROBLEM

1°. Make sure that the algorithm is correct.

General references are L. Lovász, *An Algorithmic Theory of Numbers, Graphs and Convexity*, SIAM, Philadelphia, PA, 1986 and M. Grötschel, L. Lovász and A. Schrijver, *Geometric Algorithms and Combinatorial Optimization*, 2nd ed, Springer-Verlag, New York, 1993.

Wednesday, February 14

---

18. Polytopes

(18.1) Definitions. Let $x_1, \ldots, x_m \in \mathbb{R}^n$ be a finite set of points from $\mathbb{R}^n$ and let $\lambda_1, \ldots, \lambda_n$ be non-negative numbers such that $\lambda_1 + \ldots + \lambda_m = 1$. A point

$$x = \sum_{i=1}^{m} \lambda_i x_i$$

is called a *convex combination* of $x_1, \ldots, x_m$ (of course, there are many of them). Let $X = \{x_1, \ldots, x_m\} \subset \mathbb{R}^n$ be a finite set of points. The set

$$P = \Big\{x = \sum_{i=1}^{m} \lambda_i x_i, \ \sum_{i=1}^{m} \lambda_i = 1 \text{ and } \lambda_i \geq 0 \text{ for } i = 1, \ldots, m\Big\}$$

of all convex combinations of $x_1, \ldots, x_m$ is a *polytope*. In this case we write

$$P = \operatorname{conv}\{x_1, \ldots, x_m\}.$$

Suppose that $m = n + 1$ and the points $x_1, \ldots, x_{n+1}$ are *affinely independent*, that is do not belong to the same hyperplane in $\mathbb{R}^{n+1}$. In other words, $\lambda_1 x_1 + \ldots + \lambda_{n+1} x_{n+1} = 0$ and $\lambda_1 + \ldots + \lambda_{n+1} = 0$ imply $\lambda_1 = \ldots = \lambda_{n+1} = 0$. The polytope $\Delta = \operatorname{conv}\{x_1, \ldots, x_{n+1}\}$ is called *simplex* with the vertices $x_1, \ldots, x_{n+1}$.

Let $f : \mathbb{R}^n \longrightarrow \mathbb{R}$ be a non-zero linear function and $\alpha \in \mathbb{R}$ be a number. The set $H = \{x \in \mathbb{R}^n : f(x) = \alpha\}$ is called a *hyperplane*. The set $H^- = \{x \in \mathbb{R}^n : f(x) \leq \alpha\}$ is called a *halfspace*. An intersection of finitely many halfspaces is called a *polyhedron*. If $K \subset \mathbb{R}^n$ is a convex body, H^- is a halfspace bounded by a hyperplane H and $K \subset H^-$ then the intersection $K \cap H$ is called a *face* of K. The dimension of the smallest affine subspace containing a face is called the *dimension* of the face. A zero-dimensional face of a polyhedron is called *vertex*. A face F of K such that $\dim F = \dim K - 1$ is called a *facet* of K.

PROBLEM.

1°. Polytopes are convex, closed and compact.

2°. Polyhedra are convex and closed.

3°. Let $\Delta_1, \Delta_2 \subset \mathbb{R}^n$ be two simplices in $\mathbb{R}^n$. Then there exists a non-degenerate affine transformation T (a composition of a translation and a non-degenerate linear transform) such that $T(\Delta_1) = \Delta_2$.

4°. Face of a convex set is convex.

5°. A face of a polyhedron is a polyhedron.

Here is the main structural result about polytopes.

(18.2) Theorem [Weyl - Minkowski Theorem]. *Every polytope is a polyhedron. Every bounded polyhedron is a polytope.*

We don't prove it but this is a way to do it.

PROBLEMS.

1. Let $K \subset \mathbb{R}^n$ be a closed convex set and $x \notin K$ be a point. Then there exists a hyperplane that separates x from K. That is, there exists a linear function $f : \mathbb{R}^n \longrightarrow \mathbb{R}$ such that for any $y \in K$ we have $f(y) < f(x)$.

2. Let $K \subset \mathbb{R}^n$ be a convex compact set. A point $x \in K$ is called *extreme* if it is not a midpoint of any interval $[z, y] \subset K$. Prove that K is the convex hull of the set of its extreme points.

Hint: It suffices to prove that every convex compact set has an extreme point. Call a convex subset $A \subset K$ extreme if for any interval $[y, z]$ whose midpoint is in A we must have both endpoints y and z in A. Prove that the smallest (under inclusion) extreme set is a point (use Problem 1).

3. Prove that a polyhedron P has only finitely many extreme points: they are intersection of the hyperplanes that define P.

4. Prove that every bounded polyhedron is a polytope.

5. Let $K \subset \mathbb{R}^n$ be a closed convex set such that $0 \in K$. Let us define the *polar* $K^* = \big\{x \in \mathbb{R}^n : \langle x, y\rangle \leq 1 \text{ for every } y \in K\big\}$. Prove that $(K^*)^* = K$.

Hint: Use Problem 1.

6. Prove that the polar to a polyhedron is a polytope and the polar to a polytope is a polyhedron.

7. Using Problems 4,5 and 6 prove that every polytope is a polyhedron.

(18.3) Various Results.

(18.3.1) Every polyhedron (polytope) has finitely many faces.

(18.3.2) Every face of a polytope is the intersection of the facets that contain this face.

(18.3.3) Every polytope is the convex hull of its vertices.

(18.3.4) Every face of a polytope is the convex hull of the vertices that belong to the face.

(18.3.5) Let P be a polyhedron and $x \in P$. Then x belongs to the relative interior of a face of P.

Again, we don't prove these results but they follow from the Weyl - Minkowski Theorem.

(18.4) Definitions. Let $P \subset \mathbb{R}^n$ be an n-dimensional polytope. A representation $P = \bigcup_{i=1}^m P_i$, where P_i are polytopes is called a *dissection* if and only if the interiors of P_i are pairwise disjoint. A dissection is called *subdivision* if and only if the intersection $P_i \cap P_j$ is the common face of P_i and P_j for any pair $i \neq j$. A subdivision is called *triangulation*, if every P_i is a simplex and every vertex of every P_i is a vertex of P.

(18.5) Theorem. *Every polytope $P \subset \mathbb{R}^n$ possesses a triangulation.*

Again, we don't prove this theorem. But the following seems to be the most efficient way to construct a triangulation.

PROBLEMS.

1. Let $P \subset \mathbb{R}^n$ be a polytope with the vertices $v_1, \ldots, v_m$. Let us consider $\mathbb{R}^n$ as a hyperplane $\{x = (x_1, \ldots, x_{n+1}) : x_{n+1} = 0\}$ in $\mathbb{R}^{n+1}$. Now, let us move up every vertex $v_i = (v_i, 0)$ "slightly": $(v_i, 0) \longmapsto (v_i, t_i)$, where $t_i > 0$ are "generic". Let $P_t = \operatorname{conv}\{(v_i, t_i) : i = 1, \ldots, m\}$ be the polytope in $\mathbb{R}^{n+1}$. If $t_1, \ldots, t_m$ are sufficiently generic, then every facet of P_t is an n-dimensional simplex (in its affine hull). The "lower part" of P_t projects onto P and the facets of that part give rise to a triangulation of P.

2. The triangulation constructed above possesses an interesting extremal property. Namely:

Let $P \subset \mathbb{R}^n$ be an n-dimensional polytope with m vertices and $P = \bigcup_{i \in I} \Delta_i$ be a triangulation (call it $\mathcal{D}$). Let us construct an m-dimensional vector $u_{\mathcal{D}}$ as follows: the i-the coordinate of $u_{\mathcal{D}}$ is the sum of the volumes of simplices of the triangulation containing the i-th vertex of P. Let Π be the convex hull of all vectors $u_{\mathcal{D}}$ in $\mathbb{R}^m$, where $\mathcal{D}$ ranges over all triangulations (so-called "secondary polytope"). The vector $u_{\mathcal{D}}$ is a vertex of Π if and only if $\mathcal{D}$ obtained as in Problem 1 above.

19. Valuations

(19.1) Definitions. Let $\mathcal{K}$ be a class of all convex compact sets in $\mathbb{R}^n$. A complex-valued function $\nu : \mathcal{K} \longrightarrow \mathbb{C}$ is called *valuation* if and only if for any $K_1, \ldots, K_m \in \mathcal{K}$ we have the "inclusion - exclusion" principle

$$\nu(K_1 \cup \ldots \cup K_m) = \sum_{i=1}^{m} \nu(K_i) - \sum_{1 \leq i_1 < i_2 \leq m} \nu(K_{i_1} \cap K_{i_2}) + \ldots +$$

$$(-1)^{s-1} \sum_{1 \leq i_1 < i_2 \ldots < i_s \leq m} \nu(K_{i_1} \cap K_{i_2} \cap \ldots \cap K_{i_s}) + \ldots + (-1)^{m-1} \nu(K_1 \cap \ldots \cap K_m),$$

whenever $K_1 \cup \ldots K_m$ is convex. Sometimes we call ν a valuation even if ν is defined on the class $\mathcal{P}$ of all polytopes. A valuation is called *simple* provided $\nu(K) = 0$ if $\dim K < n$.

Let $\Lambda \subset \mathbb{R}^n$ be a lattice. A valuation ν is called *lattice-invariant* if and only if $\nu(K) = \nu(K + u)$ for any $u \in \Lambda$. □

PROBLEMS.

1°. Let $\nu(K) = \operatorname{vol} K$. Then ν is a lattice invariant (with respect to any lattice) simple valuation.

2°. Let $\nu(K) = |K \cap \Lambda|$. Then ν is a lattice invariant valuation (although not necessarily simple).

3°. Let $\Lambda \subset \mathbb{R}^n$ be a lattice, Λ^* be the dual lattice. For $u^* \in \Lambda^*$ let

$$\nu_{u^*}(K) = \int_K \exp\{2\pi i \langle u^*, x \rangle\} \, dx.$$

Then $\nu_{u^*}(K)$ is a Λ-invariant simple valuation.

4°. Let $\Lambda \subset \mathbb{R}^n$ be a lattice and $P \subset \mathbb{R}^n$ be a polytope. For a point $u \in \Lambda$ let us define the *angle* $\alpha(u, P)$ as follows: let $B_r(u)$ be the ball of radius r centered at u and let

$$\alpha(u, P) = \lim_{r \longrightarrow 0} \frac{\operatorname{vol}\bigl(B_r(u) \cap P\bigr)}{\operatorname{vol}\bigl(B_r\bigr)} \quad \text{and} \quad \nu(P) = \sum_{u \in \Lambda} \alpha(u, P)$$

(note that $\alpha(u, P) = 0$ provided $u \notin P$, so the sum is well-defined). Then $\nu(P)$ is a Λ-invariant simple valuation.

5^*. Suppose we have a function $\nu : \mathcal{P} \longrightarrow \mathbb{C}$ (recall that $\mathcal{P}$ is the class of all polytopes in $\mathbb{R}^n$) such that $\nu(P_1 \cup P_2) = \nu(P_1) + \nu(P_2) - \nu(P_1 \cap P_2)$, whenever $P_1 \cup P_2$ is convex. Then ν is a valuation.

6^*. Suppose that we have a function $\nu : \mathcal{P} \longrightarrow \mathbb{C}$ such that for every $P \in \mathcal{P}$ and for every affine hyperplane H and $P^+ = P \cap H^+$ and $P^- = P \cap H^-$, where H^+ and H^- are closed halfspaces bounded by H, we have $\nu(P) = \nu(P^+) + \nu(P^-) - \nu(P_0)$, where $P_0 = P \cap H$. Then ν is a valuation.

It is not known whether the result of Problem 5 can be extended on class $\mathcal{K}$. It is known that the analogue of the result of Problem 6 is false for class $\mathcal{K}$.

See G.T. Sallee, Polytopes, valuations, and the Euler relation, *Canad. J. Math.* **20**(1968), 1412–1424; P. McMullen, *Valuations and dissections*, in: *Handbook of Convex Geometry*, North-Holland, Amsterdam, 1993, 933–988 and P. McMullen and R. Schneider, Valuations on convex bodies, in: *Convexity and its Applications*, Birkhäuser, Boston, 1983, 170–247.

Friday, February 16

---

20. Ehrhart Polynomial of a Simple Valuation

(20.1) Definition. Let $\Lambda \subset \mathbb{R}^n$ be a lattice and $P \subset \mathbb{R}^n$ be a polytope. We call P a *lattice* polytope if and only if every vertex of P is a lattice point. For a positive integer m by $mP = \{mx : x \in P\}$ we denote the dilatation (m times) of P.

PROBLEMS.

1. Let $P \subset \mathbb{R}^2$ be a polygon with the vertices in $\mathbb{Z}^2$. Using the Pick formula, prove that the number of integer points in mP is a polynomial in m of degree 2 with the constant term 1 and the highest coefficient equal to the area of P.

2. Let $P \subset \mathbb{R}^2$ be a polygon with the vertices in $\mathbb{Z}^2$. Let ν be the valuation of Problem 4, Section 19.1, that is, we count every integer point in P with the weight equal to the angle $\alpha(x, P)$. Prove that $\nu(P) =$ area of P.

3°. We have $m(P_1 \cap P_2) = mP_1 \cap mP_2$, $m(P_1 \cup P_2) = mP_1 \cup mP_2$.

(20.2) Theorem [McMullen]. *Let $\Lambda \subset \mathbb{R}^n$ be a lattice, $P \subset \mathbb{R}^n$ be a lattice polytope and ν be a lattice invariant simple valuation. Then $\nu(mP)$ is a polynomial in m of degree at most n with zero constant term. Furthermore, if $\nu : \mathcal{P} \longrightarrow \mathbb{R}$ takes non-negative values on all lattice polytopes then $\nu(mP) = \sum_{k=1}^{n} a_k \binom{m}{k}$, where a_k are non-negative coefficients (depending, of course, on P).*

Proof. Let $\mathcal{D}$ be a triangulation of P, so $P = \bigcup_{i \in I} \Delta_i$, where Δ_i are lattice simplices with pairwise disjoint interiors. Therefore

$$\nu(mP) = \nu\Big(\bigcup_{i \in I}(m\Delta_i)\Big) = \sum_{i \in I} \nu(m\Delta_i).$$

So it is enough to prove the theorem for a lattice simplex Δ. The general idea of the proof is the following: we construct a finite family of lattice polytopes, say $T_s : s \in S$ such that for every positive integer m the simplex $m\Delta$ can be dissected into the union of lattice polytopes such that:

- every polytope of the dissection is a lattice translation $T_s + u, u \in \Lambda$ of some T_s;

- the number of polytopes in the dissection which are lattice translates of a given T_s is a polynomial $p_s(m) = \binom{m}{r}$ for some $0 < r \leq n$.

If we can do this, then the theorem will be proven since

$$\nu(m\Delta) = \sum_{s \in S} p_s(m)\nu(T_s)$$

(we use that ν is simple and lattice invariant).

To construct this dissection, let us assume for a moment that Δ is the simplex with the vertices $v_0 = (0, 0, \ldots, 0)$, $v_1 = (1, 0, \ldots, 0)$, $v_2 = (1, 1, 0 \ldots, 0), \ldots, v_n = (1, \ldots, 1)$ and that $\mathbb{Z}^n$ is a sublattice of Λ. In other words, Δ is given by the system of linear inequalities $1 \geq x_1 \geq x_2 \geq \ldots \geq x_n \geq 0$. So $m\Delta$ is defined by the chain of linear inequalities $m \geq x_1 \geq x_2 \geq \ldots \geq x_n \geq 0$. Let $k = (k_1, \ldots, k_n) \in \mathbb{Z}^n$ be an integer vector and $I_k = \{x : \ k_i \leq x_i \leq k_i + 1, \ i = 1, \ldots, n\}$ be the translation $I_0 + k$ of the unit cube $0 \leq x_i \leq 1$. The cubes I_k tile $\mathbb{R}^n$, therefore $\{m\Delta \cap I_k : k \in \mathbb{Z}^n\}$ is a dissection of $m\Delta$. Let us describe the polytope $P(k, m) = (m\Delta \cap I_k)$. Let $x \in P(k, m)$. So we must have $m \geq x_1 \geq x_2 \geq \ldots \geq x_n \geq 0$ and $k_i \leq x_i \leq k_i + 1$ for $i = 1, \ldots, n$. There are three different cases:

a) $k_i \leq k_{i+1} - 1$. Then we must have $k_i + 1 \geq x_i \geq x_{i+1} \geq k_{i+1}$, so $k_i + 1 = k_{i+1}$ and $x_i = x_{i+1}$, thus $P(k, m)$ is at most $(n-1)$-dimensional and doesn't matter since ν is a simple valuation;

b) $k_i = k_{i+1}$. Then we must have $k_i + 1 \geq x_i \geq x_{i+1} \geq k_{i+1}$.

c) $k_i \geq k_{i+1} + 1$. Then for any $k_i \leq x_i \leq k_i + 1$ and any $k_{i+1} \leq x_{i+1} \leq k_{i+1} + 1$ we will have $x_i \geq x_{i+1}$ automatically.

Finally, we must have $m \geq k_1 + 1$ (otherwise the polytope $P(k,m)$ is at most $(n-1)$-dimensional. So if the polytope $P(k,m)$ has a non-empty interior, we must have

$$m > k_1 \geq k_2 \geq \ldots \geq k_n \geq 0.$$

Let $q_i = k_i - k_{i+1}$, $q_0 = m - k_1$ and $q_n = k_n$. Thus $q_0, q_1, \ldots, q_n$ are non-negative integers such that $q_0 + \ldots + q_n = m$ and $q_0 > 0$. Furthermore, from such a sequence $q = (q_0, \ldots, q_n)$ we can reconstruct $k : k_i = q_i + q_{i+1} + \ldots + q_n$. Let us describe $P(k,m)$. Whenever we have an interval of zeros $q_i = q_{i+1} = \ldots = q_j = 0$ we must have the inequality $k_i + 1 \geq x_i \geq x_{i+1} \geq \ldots \geq x_j \geq k_i$. Whenever $q_l > 0$ for $n > l > 0$ we can choose x_l arbitrarily between $k_l + 1$ and k_l. So this $P(k,m)$ is an integer shift of the polytope T_s given by the inequalities $1 \geq x_i \geq x_{i+1} \geq \ldots \geq x_j \geq 0$ for every interval of zeros $q_i = q_{i+1} = \ldots = q_j = 0$ and $1 \geq x_l \geq 0$ for every $q_l > 0 : n > l > 0$. Thus T_s are encoded by subsets of s of $\{1, \ldots, n\}$, where q has zero value. The number of translates of T_s that participate in the dissection of Δ is the number of solutions of the equation $q_0 + q_{i_1} + \ldots + q_{i_r} + q_n = m$, where all q-s are positive integers except possibly q_n which is non-negative. The number of solutions is $\binom{m}{r+1}$.

Now, if Δ is an arbitrary lattice simplex, we translate so that one of its vertices, say v_0, is 0. Next, we let $\Lambda_0 \subset \Lambda$ to be the lattice generated by the other n vertices, say $u_1, \ldots, u_n$ as a basis. Applying a transformation $u_i \longmapsto v_i$ we map Λ_0 onto $\mathbb{Z}^n$ and we are in the above situation. $\square$

The proof is found in P. McMullen, Valuations and Euler-type relations on certain classes of convex polytopes, *Proc. London Math. Soc. (3)*, **35**(1977), 113–135.

Monday, February 19

---

21. Euler Characteristic as a Valuation

We adopt a bit more general view on valuations.

(21.1) Definitions. Let $K \subset \mathbb{R}^n$ be a compact convex body. We denote by

$$\chi_K : \mathbb{R}^n \longrightarrow \mathbb{R}, \quad \chi_K(x) = \begin{cases} 1 & \text{if } x \in K, \\ 0 & \text{if } x \notin K, \end{cases}$$

the characteristic function of K. By $\mathbb{Z}(\mathcal{K})$ we denote the set of all finite integer combinations of χ_K, where K are convex compact sets. So, a typical $f \in \mathbb{Z}(\mathcal{K})$ is of the form

$$f = \sum_{i \in I} m_i \chi_{K_i},$$

where $m_i \in \mathbb{Z}$ and I is finite. Thus $\mathbb{Z}(\mathcal{K})$ is a $\mathbb{Z}$-module. A function $\nu : \mathbb{Z}(\mathcal{K}) \longrightarrow \mathbb{R}, \mathbb{C}$ is called a *valuation*, if it is linear, that is $\nu(m_1 f_1 + m_2 f_2) = m_1 \nu(f_1) + m_2 \nu(f_2)$ for any $m_1, m_2 \in \mathbb{Z}$ and any $f_1, f_2 \in \mathbb{Z}(\mathcal{K})$. We call $\mathbb{Z}(\mathcal{K})$ the *Convex Algebra* or the *Convex Ring.* If we want to show explicitly the dimension of the ambient space, we write $\mathbb{Z}(\mathcal{K}_n)$ instead.

PROBLEMS.

1°. The functions χ_K, where K are convex compacts do *not* constitute a basis of $\mathbb{Z}(\mathcal{K})$.

2°. If $f, g \in \mathbb{Z}(\mathcal{K})$ then $fg \in \mathbb{Z}(\mathcal{K})$.

3°. Let $K, K_1, \ldots, K_m$ be convex compact sets such that $K = \bigcup_{i=1}^{m} K_i$. For a subset $I \subset \{1, \ldots, m\}$ let $K_I = \bigcap_{i \in I} K_i$ (we let $K_I = K$ for $I = \emptyset$). Prove that

$$\sum_{I \subset \{1, \ldots, n\}} (-1)^{|I|} \chi_{K_I} = 0.$$

4°. If $\nu : \mathbb{Z}(\mathcal{K}) \longrightarrow \mathbb{R}$ is a valuation, then letting $\nu_1(K) = \nu(\chi_K)$ we get a valuation in the sense of Definition 19.1.

5. Actually, the converse of Problem 4 is also true.

6°. Let $\Lambda \subset \mathbb{R}^n$ be a lattice, and $w : \Lambda \longrightarrow \mathbb{R}$ be a weight on the lattice points. There exists a valuation $\nu : \mathbb{Z}(\mathcal{K}) \longrightarrow \mathbb{R}$ such that for any convex compact set K we have

$$\nu(\chi_K) = \sum_{x \in \Lambda \cap K} w(x).$$

7°. There exists a valuation ν on $\mathbb{Z}(\mathcal{K})$ such that for any convex compact set K we have

$$\nu(\chi_K) = \operatorname{vol} K.$$

(21.2) Theorem. *There exists a unique valuation $\mu : \mathbb{Z}(\mathcal{K}) \longrightarrow \mathbb{R}$ such that $\mu(\chi_K) = 1$ for every non-empty convex compact set K.*

Proof. It is immediate that if μ exists then it must be unique. Indeed, let $f \in \mathbb{Z}(\mathcal{K})$, so $f = \sum_{i \in I} m_i \chi_{K_i}$, where K_i are non-empty convex compact sets and we must have $\mu(f) = \sum_{i \in I} m_i$. Let us prove the existence. We prove this by induction on the dimension n. For $n = 0$ the result is obvious. Suppose that the valuation μ (call it μ_{n-1}) exists in the dimension $n-1$. Let us choose a non-zero linear function $l : \mathbb{R}^n \longrightarrow \mathbb{R}$ and for $\alpha \in \mathbb{R}$ let $H^\alpha = \{x \in \mathbb{R}^n : l(x) = \alpha\}$ be a hyperplane. Hence in every hyperplane H^α there is a valuation μ_{n-1}. Let us define the valuation $\mu = \mu_n$ on the Convex Algebra of $\mathbb{R}^n$. Let us choose $f \in \mathbb{Z}(\mathcal{K}_n)$. For every hyperplane H^α we have the restriction f^α of f onto H^α and a value $\mu_{n-1}(f^\alpha)$. Let us call $\alpha \in \mathbb{R}$ *regular* for f if and only if $\mu_{n-1}(f^\alpha) = \mu_{n-1}(f^{\alpha+\epsilon})$ for all sufficiently small $\epsilon > 0$. Otherwise we call α a *critical* value for f. We claim that for any f there are only finitely many critical values. Indeed, let $f = \sum_{i \in I} m_i \chi_{K_i}$, where $K_i \subset \mathbb{R}^n$ are non-empty convex sets. Let $\alpha_i = \max\{l(x) : x \in K_i\}$. We claim that unless $\alpha = \alpha_i$ for some i, α is a regular value for f. Indeed, let $K_i^\alpha = K_i \cap H^\alpha$. Then $f^\alpha = \sum_{i \in I} m_i \chi_{K_i^\alpha}$ and we must have

$$\mu_{n-1}(f^\alpha) = \sum_{i : K_i^\alpha \neq \emptyset} m_i.$$

So if $\alpha \neq \alpha_i$ for any i then $K_i^\alpha \neq \emptyset$ if and only if $K_i^{\alpha+\epsilon} \neq \emptyset$ for any sufficiently small $\epsilon > 0$. Now we are ready to define $\mu_n(f)$. Let

$$\mu_n(f) = \sum_{\alpha \in \mathbb{R}} \lim_{\epsilon \longrightarrow +0} \Big(\mu_{n-1}(f^\alpha) - \mu_{n-1}(f^{\alpha+\epsilon}) \Big). \tag{21.2.1}$$

Since the set of critical values for every f is finite, the above sum contains only finitely many summands. By the induction conjecture it follows that μ_n is a valuation on $\mathbb{Z}(\mathcal{K}_n)$. Now, let us make sure that $\mu_n(f) = 1$, where $f = \chi_K$ is the characteristic function of a non-empty convex compact set. Then $\alpha_0 = \max\{l(x) : x \in K\}$ is the only critical value for f. Furthermore, by the induction conjecture we have $\mu_{n-1}(\chi_{K^\alpha}) = 0$ if $\alpha > \alpha_0$ or $\alpha < \min\{l(x) : x \in K\}$. Otherwise K^α is non-empty convex and we must have $\mu_{n-1}(\chi_{K^\alpha}) = 1$. If $\alpha < \alpha_0$ then $K^{\alpha+\epsilon}$ is not empty for all sufficiently small $\epsilon > 0$. If $\alpha = \alpha_0$ then K^α is not empty, but $K^{\alpha+\epsilon}$ is empty for any $\epsilon > 0$. Thus

$$\lim_{\epsilon \longrightarrow +0} \Big(\mu_{n-1}(f^\alpha) - \mu_{n-1}(f^{\alpha+\epsilon}) \Big) = \begin{cases} 1 & \text{if } \alpha = \alpha_0, \\ 0 & \text{otherwise.} \end{cases}$$

The proof now follows by (21.2.1). □

The valuation μ is called the *Euler characteristic*.

PROBLEMS.

1. Let $P \subset \mathbb{R}^n$ be a convex polytope and P° be its relative interior. Then $\chi_{P^\circ} \in \mathbb{Z}(\mathcal{K})$.

2.

a) Let I be an open interval in $\mathbb{R}^n$. Then $\chi_I \in \mathbb{Z}(\mathcal{K})$ and $\mu(\chi_I) = -1$;

b) Let Δ be a triangle in $\mathbb{R}^n$ and Δ° be its relative interior. Then $\chi_{\Delta^\circ} \in \mathbb{Z}(\mathcal{K})$ and $\mu(\chi_{\Delta^\circ}) = 1$.

c*. Let $P \subset \mathbb{R}^n$ be a k-dimensional polytope and P° be its relative interior. Then $\mu(\chi_{P^\circ}) = (-1)^k$.

22. Support Function as a Valuation

(22.1) Definition. Let $K \subset \mathbb{R}^n$ be a convex compact set. Let us define

$$h_K : \mathbb{R}^n \longrightarrow \mathbb{R}, \quad h_K(c) = \max\{\langle c, x\rangle : x \in K\}.$$

Then h_K is called the *support function* of K.

PROBLEMS.

1°. For a convex compact set K and a non-negative α let $\alpha K = \{\alpha x : x \in K\}$. Then $h_{\alpha K} = \alpha h_K$.

2. Let K_1 and K_2 be two convex compact sets such that $h_{K_1} = h_{K_2}$. Then $K_1 = K_2$.

Hint: Suppose there is a point x, which is in K_1, say, but not in K_2. Construct a hyperplane which separates x from K_2. Use the normal vector of this hyperplane to find c such that $h_{K_1}(c) > h_{K_2}(c)$.

(22.2) Theorem. *Let us choose a $c \in \mathbb{R}^n$. There exists a valuation $h_c : \mathbb{Z}(\mathcal{K}) \longrightarrow \mathbb{R}$ such that $h_c(\chi_K) = h_K(c)$ for any non-empty convex set $K \subset \mathbb{R}^n$.*

Proof. If $c = 0$ then h_c is the zero valuation. So we can assume that $c \neq 0$. For $\alpha \in \mathbb{R}$ let $H^\alpha = \{\langle c, x\rangle = \alpha\}$. For $f \in \mathbb{Z}(\mathcal{K})$ let

$$h_c(f) = \sum_{\alpha \in \mathbb{R}} \alpha \lim_{\epsilon \longrightarrow +0} \Big(\mu(f \cdot \chi_{H^\alpha}) - \mu(f \cdot \chi_{H^{\alpha+\epsilon}})\Big), \tag{22.2.1}$$

where "$\cdot$" denotes the usual point-wise multiplication of functions (cf. Problem 2, Section 21.1). If $K \subset \mathbb{R}^n$ is a convex compact set and $\alpha \neq h_K(c)$ then either $H^\alpha \cap K = \emptyset$ and $H^{\alpha+\epsilon} \cap K = \emptyset$ for all sufficiently small $\epsilon > 0$ or $H^\alpha \cap K \neq \emptyset$ and $H^{\alpha+\epsilon} \cap K \neq \emptyset$ for all sufficiently small $\epsilon > 0$. If $\alpha = h_K(c)$ then $H^\alpha \cap K \neq \emptyset$ but $H^{\alpha+\epsilon} \cap K = \emptyset$ for any $\epsilon > 0$. So $h_c(\chi_K) = h_K(c)$. Similarly, for an $f = \sum_{i \in I} m_i \chi_{K_i} \in \mathbb{Z}(\mathcal{K})$ the expression (22.2.1) has only finitely many non-zero summands and thus well-defined. It is easy to see now that h_c is linear and hence a valuation. □

PROBLEMS.

1°. Let $K_1, K_2 \subset \mathbb{R}^n$ be convex compact sets such that $K_1 \cup K_2$ is convex. Prove that

$$h_{K_1 \cup K_2} + h_{K_1 \cap K_2} = h_{K_1} + h_{K_2}.$$

Hint: $\chi_{K_1 \cup K_2} = \chi_{K_1} + \chi_{K_2} - \chi_{K_1 \cap K_2}$ by the inclusion - exclusion.

2. Let $\Lambda \subset \mathbb{R}^n$ be a lattice, $P_1, P_2 \subset \mathbb{R}^n$ be lattice polytopes such that $P_1 \cup P_2$ is convex. Then $P_1 \cap P_2$ is a lattice polytope.

Hint: Use Problem 1 to show that $h_{K_1 \cap K_2}(u^*) \in \mathbb{Z}$ for any $u^* \in \Lambda^*$.

23. New Valuations from Old

(23.1) Lemma. *Let $\mathcal{A} : \mathbb{Z}(\mathcal{K}_n) \longrightarrow \mathbb{Z}(\mathcal{K}_m)$ be a linear transform (a homomorphism of $\mathbb{Z}$-modules). Suppose that $\phi : \mathbb{Z}(\mathcal{K}_m) \longrightarrow \mathbb{R}$ is a valuation on $\mathbb{Z}(\mathcal{K}_m)$. Then the composition $\nu = \phi \circ \mathcal{A} : \nu(f) = \phi(\mathcal{A}(f))$ is a valuation on $\mathbb{Z}(\mathcal{K}_n)$.*

Proof. Obvious. □

(23.2) Theorem. *Let $A : \mathbb{R}^n \longrightarrow \mathbb{R}^m$ be an affine transformation (that is, a composition of a linear transform and a translation). Then there exists a linear transform $\mathcal{A} : \mathbb{Z}(\mathcal{K}_n) \longrightarrow \mathbb{Z}(\mathcal{K}_m)$ such that $\mathcal{A}(\chi_K) = \chi_{A(K)}$ for any non-empty compact set K.*

Proof. Let us define $T(x, y) : \mathbb{R}^n \times \mathbb{R}^m \longrightarrow \mathbb{R}$ by the formula

$$T(x,y) = \begin{cases} 1 & \text{if } A(x) = y, \\ 0 & \text{otherwise.} \end{cases}$$

Now for $f \in \mathbb{Z}(\mathcal{K}_n),\ f : \mathbb{R}^n \longrightarrow \mathbb{R}$ we let $\mathcal{A}(f) : \mathbb{R}^m \longrightarrow \mathbb{R}$ as follows

$$\mathcal{A}(f)(y) = \mu_x\big(f(x) \cdot T(x,y)\big), \tag{23.2.1}$$

where μ_x denotes the Euler characteristic in $\mathbb{Z}(\mathcal{K}_n)$. Let us check that (23.2.1) sends every χ_K to $\chi_{A(K)}$. Indeed, if $f = \chi_K$ then

$$f(x)T(x,y) = \begin{cases} 1 & \text{if } x \in K \text{ and } A(x) = y, \\ 0 & \text{otherwise.} \end{cases}$$

Therefore for every $y \in \mathbb{R}^m$ we have $f(x)T(x,y) = \chi_{K \cap A^{-1}(y)}$. Since A is affine, $K \cap A^{-1}(y)$ is the intersection of a convex compact K and an affine subspace $x : A(x) = y$. So this intersection is either empty or a convex compact set in $\mathbb{R}^n$. Thus $f(x)T(x,y) \in \mathbb{Z}(\mathcal{K}_n)$ for every y and the Euler characteristic μ_x is well-defined. So

$$\mathcal{A}(f)(y) = \begin{cases} 1 & \text{if } A(x) = y \text{ for some } x \in K, \\ 0 & \text{otherwise.} \end{cases}$$

Hence $\mathcal{A}(\chi_K) = \chi_{A(K)}$. Now it is seen that (23.2.1) is linear, so $\mathcal{A}$ is defined on $\mathbb{Z}(\mathcal{K}_n)$ and satisfies the required property. □

PROBLEMS.

1. Let $G_s(\mathbb{R}^n)$ denote the set of all (linear) s-dimensional subspaces L in $\mathbb{R}^n$ (Grassman manifold). The orthogonal group $O(n)$ acts on $G_s(\mathbb{R}^n)$ transitively, so there exists an invariant probability measure, say dL on $G_s(\mathbb{R}^n)$. Let $K \subset \mathbb{R}^n$ be a convex compact

set. Let us denote by $K|L$ the orthogonal projection of K onto L and let vol_s be the s-dimensional volume in L. Finally, let

$$V_s(K) = \int_{G_s(\mathbb{R}^n)} \mathrm{vol}_s(K|L)\ dL.$$

Prove that

a) $V_s(K)$ is a valuation, that is satisfies the inclusion - exclusion property (see Section 19.1). It can be extended to a linear function of $\mathbb{Z}(\mathcal{K}_n)$ as well.

b) $V_s(\alpha K) = \alpha^s V_s(K)$ for $\alpha \geq 0$.

c) $V_s(K') = V_s(K)$ if K' is obtained from K by a translation and rotation.

d) V_s is *monotone*, that is $V_s(K') \leq V_s(K)$ whenever $K' \subset K$.

Remark: Up to a factor $const(s,n)$ the valuation $V_s(K)$ is the famous s-th *quermass-integral.* So $V_0(K)$ is the Euler characteristic and $V_n(K)$ is the volume.

2* [Hadwiger]. Every valuation which satisfies a)-d) is a non-negative linear combination of the quermassintegrals $V_s(K)$. A valuation which satisfies a)-c) and continuous in the Hausdorff metric is a linear combination the quermassintegrals $V_s(K)$.

See D. Klain and G.-C. Rota, *Introduction to Geometric Probability*, preprint (1996), to appear.

3°. Let us consider the projection $p : \mathbb{R}^n \longrightarrow \mathbb{R}^s$ which maps the lattice $\mathbb{Z}^n$ onto the lattice $\mathbb{Z}^s$. For a compact convex body $K \subset \mathbb{R}^n$ let $\nu(K) = |p(K) \cap \mathbb{Z}^s|$ be the number of integer points in the projection of K. Then $\nu(K)$ is a valuation.

(23.3) Definition. Let $K_1, K_2 \subset \mathbb{R}^n$ be convex compact sets. Let $K = \{x + y : x \in K_1, y \in K_2\}$. The set K is called the *Minkowski sum* of K_1 and K_2 and denoted $K = K_1 + K_2$.

PROBLEMS.

1°. If K_1, K_2 are convex compact then $K = K_1 + K_2$ is convex compact.

2°. $\alpha K + \beta K = (\alpha + \beta) K$ for non-negative α, β and convex K.

3°. Let us consider the linear map $A : \mathbb{R}^n \times \mathbb{R}^n \longrightarrow \mathbb{R} :\ (x,y) \longmapsto x + y$ and the product $K_1 \times K_2 \subset \mathbb{R}^n$. Then $K_1 + K_2 = A(K_1 \times K_2)$.

4°. $h_{K_1+K_2} = h_{K_1} + h_{K_2}$, where h is the support function and K_1, K_2 are convex.

(23.4) Theorem. *Let us fix $Q \in \mathcal{K}_n$. Suppose that ν is a valuation on $\mathbb{Z}(\mathcal{K}_n)$. Then there is a valuation ν_Q on $\mathbb{Z}(\mathcal{K}_n)$ such that $\nu_Q(\chi_K) = \nu(\chi_{K+Q})$ for every compact convex set K.*

Proof. Let us consider the product $\mathbb{R}^{2n} = \mathbb{R}^n \times \mathbb{R}^n$ and the linear map $A : \mathbb{R}^n \times \mathbb{R}^n \longrightarrow \mathbb{R}^n : (x,y) \longmapsto x + y$. By Theorem 22.2 this linear map induces a linear map $\mathcal{A} : \mathbb{Z}(\mathcal{K}_{2n}) \longrightarrow \mathbb{Z}(\mathcal{K}_n)$ such that $\mathcal{A}(\chi_K) = \chi_{A(K)}$. Consider a linear map: $\mathcal{Q} : \mathbb{Z}(\mathcal{K}_n) \longrightarrow \mathbb{Z}(\mathcal{K}_{2n})$ which sends $f : \mathbb{R}^n \longrightarrow \mathbb{R}$ to $f \times \chi_Q : \mathbb{R}^n \times \mathbb{R}^n \longrightarrow \mathbb{R}$: $f \times \chi_Q(x,y) = f(x) \cdot \chi_Q(y)$. Then the composition $\mathcal{A}(\mathcal{Q})$ is a linear map which sends χ_K to χ_{Q+K}. The result follows by Lemma 23.1. $\square$

PROBLEMS.

1. Suppose that K_1, K_2 and $K = K_1 \cup K_2$ are convex. Then $(K_1 \cap K_2) + (K_1 \cup K_2) = K_1 + K_2$.

Hint: Use Problem 2 in Section 22.2, Problem 2 in Section 22.1 and Problem 4, Section 23.3.

2. A function $\nu : \mathcal{K} \longrightarrow \mathbb{R}$ is called *Minkowski additive* if $\nu(K_1+K_2) = \nu(K_1)+\nu(K_2)$. Prove that a Minkowski additive function satisfies the inclusion - exclusion property (cf. Section 19.1).

Hint: Use Theorem 22.2 and Problem 4 from Section 23.3.

3. Prove that there exists a bilinear map (convolution) $\star : \mathbb{Z}(\mathcal{K}) \times \mathbb{Z}(\mathcal{K}) \longrightarrow \mathbb{Z}(\mathcal{K})$ such that $\chi_{K_1} \star \chi_{K_2} = \chi_{K_1+K_2}$. Prove that $\chi_{\{0\}}$ is the unit for this convolution.

4^*. Let $P \subset \mathbb{R}^n$ be an n-dimensional polytope. Then

$$\sum_{F \subset P} (-1)^{\dim F} h_F = -h_{-P},$$

where the sum is taken over all faces (including P but excluding the empty face).

5. Using Problem 3 prove that

$$-P + \sum_{\dim F \text{ even}} F = \sum_{\dim F \text{ odd}} F.$$

Remark: This result can be interpreted as follows: the indicator function χ_P of every polytope has its "inverse" $-\chi_{-P^\circ}$ under the convolution $\star$ from Problem 3, so that $\chi_P \star (-\chi_{-P^\circ}) = \chi_{\{0\}}$, where $^\circ$ denotes the relative interior of P.

6°. Let $Q \subset \mathbb{R}^n$ be a convex set and $\Lambda \subset \mathbb{R}^n$ be a lattice. The function $\nu(K) = |(K+Q) \cap \Lambda|$, the number of lattice points in $K+Q$ is a valuation.

(23.5) Hadwiger's Transform. Let us choose a non-zero vector $c \in \mathbb{R}^n$. For a convex compact set K let $\alpha = h_K(c) = \max\{\langle c, x \rangle : x \in K\}$. Finally, let $K_c = K \cap H_\alpha$, where $H^\alpha = \{x \in \mathbb{R}^n : \langle c, x \rangle = \alpha\}$. Thus K_c is the set of points on K where the maximum value of $\langle c, x \rangle$ is attained.

PROBLEM.

1°. K_c is convex.

(23.5.1) Theorem. *For any $c \neq 0$ there is a linear transformation $\mathcal{A}_c : \mathbb{Z}(\mathcal{K}) \longrightarrow \mathbb{Z}(\mathcal{K})$ such that $\mathcal{A}_c(\chi_K) = \chi_{K_c}$ for any convex compact K.*

Proof. We define

$$\mathcal{A}_c(f) = \sum_{\alpha \in \mathbb{R}} \Big(\lim_{\epsilon \longrightarrow +0} (\mu(f^\alpha) - \mu(f^{\alpha+\epsilon})) \Big) f^\alpha,$$

where f^α is the restriction of f onto the hyperplane $H^\alpha = \{x : \langle x, c \rangle = \alpha\}$. The proof is similar to that of Theorem 22.2. $\square$

(23.5.2) Corollary. *Suppose that on every hyperplane $H^\alpha = \{x : \langle x, c\rangle = \alpha\}$ there is a valuation ν_α. For every convex compact K let $\nu(K) = \nu_\alpha K_c$, where $\alpha = h_K(c)$. Then ν is a valuation.*

Proof. Follows by Theorem 23.5.1 and Lemma 23.1. □

Friday, February 23

---

24. Decomposition of a Simple Valuation

(24.1) Notation, Definitions and General Agreements. Here is the situation: we have a lattice $\Lambda \subset \mathbb{R}^n$ and a simple lattice invariant valuation ν. Let $H \subset \mathbb{R}^n$ be a lattice hyperplane, so $\Lambda_1 = \Lambda \cap H$ is a lattice in H. We may consider Λ_1-invariant simple valuations ν_H in H. Furthermore, if $H + a$ is a translation of H, we may still consider Λ_1-invariant lattice valuations in $H + a$. For a unit vector c let $H_c = \{x \in \mathbb{R}^n : \langle c, x\rangle = 0\}$ be a hyperplane in $\mathbb{R}^n$. If H_c happens to be a lattice hyperplane and we choose a certain Λ_1-invariant valuation ν_c on H_c we agree to choose just the same valuation on every lattice translate $H_c + u$, where $u \in \Lambda$ and we also agree that $\nu_c = \nu_{-c}$. If H_c is *not* a lattice hyperplane, we just agree that the only valuation ν_H we may consider there is a trivial valuation $\nu_H \equiv 0$. Recall that if c is a unit vector, $P \subset \mathbb{R}^n$ is a convex polytope and $\alpha = \max\{\langle c, x\rangle : x \in P\}$ then we denote $P_c = \{x \in P : \langle c, x\rangle = \alpha\}$. We say that a function $\kappa(c)$ on the unit vectors $c \in \mathbb{R}^n$ is *odd* if and only if $\kappa(-c) = -\kappa(c)$. Finally, all our valuations are defined on all lattice polytopes and only on lattice polytopes!

(24.2) Theorem [McMullen]. *Let ν be a simple lattice invariant valuation on $\mathbb{R}^n$. Then there exist*

- *a number a*
- *a simple lattice-invariant valuation ν_c on H_c for every unit vector $c \in \mathbb{R}^n$;*
- *an odd function $\kappa(c)$ on unit vectors $c \in \mathbb{R}^n$*

such that for every lattice polytope P we have

$$\nu(P) = a \cdot \mathrm{vol}(P) + \sum_c \kappa(c)\nu_c(P_c).$$

Since ν_c is required to be simple, $\nu_c(P_c) = 0$ unless P_c is a facet of P. Thus the sum contains only finitely many non-zero terms and well -defined.

It is best to prove Theorem 24.2 together with yet another fact:

(24.3) Lemma [McMullen]. *Let $u_1, \dots, u_n$ be a basis of Λ and $\mathbb{R}^{n-1}$ be the linear hull of $u_1, \dots, u_{n-1}$. Let $I = [0, u_n]$ be the interval with the endpoints 0 and u_n. Suppose that there is a simple lattice invariant valuation ν_0 in $\mathbb{R}^{n-1}$. Then there is a simple lattice invariant valuation ν_1 in $\mathbb{R}^n$ such that $\nu_1(Q+mI) = m\nu_0(Q)$ for any non-negative integer m and any lattice polytope $Q \subset \mathbb{R}^{n-1}$. Furthermore, $\nu_1(P) = a\cdot \mathrm{vol}(P) + \sum_c \kappa(c)\nu_{1,c}(P_c)$, where the sum is taken over all unit vectors c in $\mathbb{R}^{n-1}$.*

Proof. We prove Theorem 24.2 and Lemma 24.3 by induction on n using the following scheme:

Step 1. Theorem 24.2 and Lemma 24.3 for $n = 0$.

Step 2. Theorem 24.2 for $n-1$ and Lemma 24.3 for $n-1$ implies Lemma 24.3 for n.

Step 3. Lemma 24.3 for $n-1$ implies Theorem 24.3 for n.

Let's make the first step. If $n = 0$ then every polytope is a point and $\nu(\cdot) = a$ is the only valuation. There is nothing to prove in Lemma 24.3.

Let's make the second step. If ν_0 is a valuation in $\mathbb{R}^{n-1}$ then there is a decomposition

$$\nu_0(Q) = a_0 \cdot \mathrm{vol}(Q) + \sum_c \kappa(c)\nu_{0,c}(Q_c),$$

where c ranges over all unit vectors in $\mathbb{R}^{n-1}$ and Q is a lattice polytope in $\mathbb{R}^{n-1}$. Note, that $\nu_{0,c}$ is a valuation on the hyperplane in $H_c \subset \mathbb{R}^{n-1}$ with the unit normal vector c. The induction conjecture for Lemma 24.3 implies that $\nu_{0,c}$ can be extended to a valuation $\nu_{1,c}$ on the hyperplane $H_c \oplus \mathbb{R}u_n$. The polytope $Q+I$ is a prism with the base Q, so there exists a such that $a \cdot \mathrm{vol}(Q+I) = a_0 \cdot \mathrm{vol}Q$, so we can extend ν_0 to ν_1 as follows

$$\nu_1(P) = a \cdot \mathrm{vol}(P) + \sum_c \kappa(c)\nu_{1,c}(P_c),$$

where the sum is taken over all unit vectors c in $\mathbb{R}^n$, orthogonal to u_n. This as a valuation as follows by Corollary 23.5.2.

Let's make the third step. Let ν be a valuation in $\mathbb{R}^n$. Choose a valuation ν_0 on $\mathbb{R}^{n-1}$ as follows: $\nu_0(Q) = \nu(Q+I)$. Then ν_0 is a valuation (cf. Theorem 23.4), and it is obviously lattice invariant. Moreover, it is simple since if Q is not full-dimensional, then $Q+I$ is not full-dimensional and ν is simple. Therefore by Lemma 24.3 there is a lifting ν_1 of ν_0 onto $\mathbb{R}^n$. Let $\nu' = \nu - \nu_1$. Then ν' is simple and lattice invariant. Furthermore, $\nu'(Q+mI) = 0$ for any positive integer m and any lattice polytope $Q \subset \mathbb{R}^{n-1}$. Now it is time to define ν_c. If H_c is not a lattice subspace, we of course let $\nu_c = 0$. If it is a lattice subspace, we do the following: take a lattice polytope $F \subset H_c$. Translate it, if necessary, so that it belongs to the "upper halfspace" of $\mathbb{R}^n$ with a positive u_n coordinate. Project it down to $\mathbb{R}^{n-1}$ via u_n and get, say F'. Take $\overline{F}$ to be the convex hull of F and F' and let $\nu_c(F) = \nu'(\overline{F})$. If we choose a different translation of F then $\overline{F}$ will be different by a cylinder $(Q + mI)$, so we get the same value of $\nu'(\overline{F})$. This shows that ν_c is well-defined and that ν_c is lattice invariant. Let us prove that

$$\nu'(P) = \sum_c \kappa(c)\nu'_c(P_c),$$

where

$$\kappa(c) = \begin{cases} 1 & \text{if } \langle u_n, c\rangle > 0, \\ -1 & \text{if } \langle c, u_n\rangle < 0, \end{cases}$$

and the sum extends over all c such that $\langle c, u_n\rangle \neq 0$. This follows since P can be represented as the corresponding signed sum of $\overline{F}$ for facets F of P (up to a set of dimension at most $n-1$) Since $\nu = \nu_1 + \nu'$ the proof follows by Lemma 24.3. $\square$

The proof is found in P. McMullen, Lattice invariant valuations on rational polytopes, *Archiv der Mathematik*, **31** (1978/79), 509–516.

Monday, February 26

---

25. Frames

(25.1) Definitions. A set of k pairwise orthogonal unit vectors $c_1, \ldots, c_k$ in $\mathbb{R}^n$ is called a *k-frame*. Given a polytope $P \subset \mathbb{R}^n$ and a frame $C = \{c_1, \ldots, c_k\}$, we define a face P_C of P as follows:

If $k = 0$ and $C = \emptyset$ we let $P_C = P$. Next, we define P_1. Consider $\alpha_1 = \max\{\langle c_1, x\rangle : x \in P\}$ and let $P_1 = \{x \in P : \langle c_1, x\rangle = \alpha_1\}$. Next, we consider $\alpha_2 = \max\{\langle c_2, x\rangle : x \in P_1\}$ and let $P_2 = \{x \in P_1 : \langle c_2, x\rangle = \alpha_2\}$. Proceeding as above we get $\alpha_i = \max\{\langle c_i, x\rangle : x \in P_{i-1}\}$ and $P_i = \{x \in P_{i-1} : \langle c_i, x\rangle = \alpha_i\}$. Finally, we let $P_C = P_k$.

We say that C is *proper* for P if $\dim P_i = n - i$ for $i = 0, \ldots, k$.

We call k the *size* of the frame C and denote $|C| = k$.

A function κ on k-frames $C = (c_1, \ldots, c_k)$ is called *odd* if and only if $\kappa(\epsilon_1 c_1, \ldots, \epsilon_k c_k) = \epsilon_1 \cdots \epsilon_k \kappa_(c_1, \ldots, c_k)$, where $\epsilon_i \in \{-1, 1\}$.

PROBLEMS.

1°. Let us choose a k-frame $C = \{c_1, \ldots, c_k\}$. The transformation $P \longmapsto P_C$ can be extended to a linear transform of the convex ring $\mathbb{Z}(\mathcal{K})$.

2°. We have $\dim(P_C) \leq n - |C|$.

(25.2) Theorem [McMullen]. *Let $\Lambda \subset \mathbb{R}^n$ be a lattice and ν be a simple lattice - invariant valuation. Then for any $k = 0, \ldots, n$ there is an odd function κ on the set of all k-frames C such that for any lattice polytope P one has*

$$\nu(P) = \sum_{k=0}^{n} \sum_{|C|=k} \kappa(C)\mathrm{vol}_{n-k}(P_C),$$

where vol_{n-k} *is the* $(n-k)$*-dimensional volume on affine subspaces in* $\mathbb{R}^n$ *and the inner sum is taken over frames* C *of size* k *that are proper for* P*.*

Proof. Follows by recursive application of Theorem 24.2. First, we get a decomposition

$$\nu(P) = a \cdot \mathrm{vol}\ P + \sum_c \kappa(c)\nu_c(P_c),$$

where $\nu_c = \nu_{-c}$ are simple valuations on the hyperplanes $H = \{\langle c, x\rangle = \alpha\}$ and $\kappa(-c) = -\kappa(c)$. Since ν_c is simple we can restrict our sum on the normal vectors to the facets of P. Now we apply Theorem 24.2 to the valuations ν_c, getting a decomposition

$$\nu(P) = a \cdot \mathrm{vol}\ P + \sum_c \kappa(c) a_c \mathrm{vol}_{n-1}(P_c) + \sum_{C=(c_1,c_2)} \kappa(c_1)\kappa(c_2)\nu_{c_1,c_2},$$

where $a_c = a_{-c}$, the last sum is taken over pairs of orthogonal unit vectors and ν_{c_1,c_2} are simple valuations on the subspaces $H = \{x : \langle x, c_1\rangle = \langle x, c_2\rangle = 0\}$. Proceeding as above we end up with the decomposition claimed by the theorem. □

PROBLEMS.

1. Let $C = (c_1, \ldots, c_k)$ be a k-frame. For $\epsilon = (\epsilon_1, \ldots, \epsilon_k)$, where $\epsilon_i \in \{-1, 1\}$ we define $\epsilon C = (\epsilon_1 c_1, \ldots, \epsilon_k c_k)$. Prove that

$$\sum_{\epsilon \in \{-1,1\}^n} \mathrm{vol}_{n-k}(P_{\epsilon C}) = 0,$$

unless ϵC is proper for P for some $\epsilon \in \{-1, 1\}^n$.

So, formally speaking, we can consider the sum in Theorem 25.2 taken over all frames C. The non-proper frames will cancel each other.

2. The *Hadwiger functional* ϕ_C is a function on polytopes $P \subset \mathbb{R}^n$:

$$\phi_C(P) = \sum_{\epsilon \in \{-1,1\}^k} \epsilon_1 \cdots \epsilon_k \mathrm{vol}_{n-k}(P_{\epsilon C}).$$

a°) Make sure that ϕ_C is a valuation;

b*). From our proof of Theorem 24.2 deduce that ϕ_C separate P up to a translation: if $\phi_C(P_1) = \phi_C(P_2)$ for any frame C then P_1 is a translation of P_2 in $\mathbb{R}^n$.

26. Reciprocity

Now we can say some more about the Ehrhart polynomial of a simple valuation.

(26.1) Theorem. *Let $\Lambda \subset \mathbb{R}^n$ be a lattice and ν be a simple lattice-invariant valuation. Let P be a lattice polytope and $-P = \{-x : x \in P\}$. Let*

$$\nu(mP) = \sum_{k=0}^{n} a_k(P)m^k, \quad \nu(-mP) = \sum_{k=0}^{n} a_k(-P)m^k$$

be the Ehrhart polynomials of the polytopes P and $-P$ and the valuation ν. Then

$$a_k(-P) = (-1)^{n-k} a_k(P).$$

Proof. Theorem 25.2 implies that

$$a_k(P) = \sum_{|C|=n-k} \kappa(C)\mathrm{vol}_k(P_C) \quad \text{and} \quad a_k(-P) = \sum_{|C|=n-k} \kappa(C)\mathrm{vol}_k\big((-P)_C\big),$$

where the sum is taken over all $(n-k)$-frames C which are proper for P (for the first sum) or for $-P$ (for the second sum) and κ is an odd function on $(n-k)$-frames. For a frame $C = (c_1, \ldots, c_{n-k})$ let $-C = (-c_1, \ldots, -c_{n-k})$. Now if C is proper for P then $-C$ is proper for $-P$ and $\kappa(-C) = (-1)^{n-k}\kappa(C)$. The proof now follows since $\mathrm{vol}_k(P_C) = \mathrm{vol}_k\big((-P)_C\big)$. □

(26.2) Corollary. *Suppose that $\nu(P) = \nu(-P)$ for any lattice polytope P. Then in the Ehrhart polynomial*

$$\nu(mP) = \sum_{k=1}^{n} a_k(P)m^k$$

we have $a_k(P) = 0$ provided $(n-k)$ is odd.

Proof. Since $\nu(P) = \nu(-P)$ for every P (and thus for the dilatation mP), the Ehrhart polynomials of $\nu(P)$ and $\nu(-P)$ must coincide. Thus $a_k(P) = a_k(-P)$. The proof follows by Theorem 26.1. □

PROBLEMS.

Here we sketch an alternative (a bit more geometric) proof of Theorem 26.1, found in P. McMullen, Valuations and Euler-type relations on certain classes of convex polytopes, *Proc. London Math. Soc. (3)*, **35**(1977), 113–135.

Let $L_1, \ldots, L_s \subset \mathbb{R}^n$ be independent linear subspaces (so $L_i \cap L_j = \{0\}$ for $i \neq j$). Let us choose $Q_i \subset L_i$. The Minkowski sum $P = Q_1 + \ldots + Q_s$ is called an *s-cylinder*. Let us fix a lattice $\Lambda \subset \mathbb{R}^n$. A valuation ϕ is called *homogeneous* of degree r if $\phi(mP) = m^r\phi(P)$. All valuations below are simple, lattice-invariant and defined on all lattice polytopes in $\mathbb{R}^n$.

1. Draw a picture of the dissection of the tetrahedron 3Δ, where Δ is a 3-dimensional tetrahedron from the proof of Theorem 20.2

2. Make sure that the dissection of mP from the proof of Theorem 20.2 contains $d(P)\binom{m}{s}$ s-cylinders.

3. Let ν be a simple lattice-invariant valuation in $\mathbb{R}^n$ and $L_1, \ldots, L_s$ are independent lattice subspaces so that $\Lambda_i = L_i \cap \Lambda$ are lattices in L_i and $\Lambda = \Lambda_1 + \ldots + \Lambda_s$. Let $K_i \subset L_i$ and $\overline{\nu}(K_1, \ldots, K_s) = \nu(K_1 + \ldots + K_s)$. Then $\overline{\nu}$ is a simple Λ_i-invariant valuation in every K_i.

4. Prove that the k-th coefficient $a_k(P)$ of the Ehrhart polynomial $\nu(mP)$ is a simple lattice-invariant valuation. Besides, $a_k(P)$ is homogeneous of degree k: $a_k(mP) = m^k a_k(P)$ for any integer m.

5. If ϕ is a homogeneous simple lattice-invariant valuation of degree r and P is an s-cylinder for some $s > r$ then $\phi(P) = 0$.

Hint: Suppose that $P = Q_1 + \ldots + Q_s$. Consider $\nu(mP) = \overline{\nu}(mQ_1, \ldots, mQ_s)$ (see Problem 3). Use Theorem 20.2.

6. A homogeneous simple lattice invariant valuation of degree r is completely determined by its values on r-cylinders.

Hint: Use Problem 5 and Problem 2.

7. Suppose that $L_1, \ldots, L_r$ are independent and $L_1 + \ldots + L_r = \mathbb{R}^n$. Suppose that ϕ is homogeneous of degree r. Then $\phi(Q_1 + \ldots + Q_r)$ is linear in each Q_i.

8. If ϕ is simple lattice-invariant and linear then $\phi(-P) = (-1)^{(n-1)}\phi(P)$.

Hint: Use induction on the dimension.

9. If ϕ is homogeneous simple of degree r and lattice-invariant then $\phi(-P) = (-1)^{(n-r)}\phi(P)$.

(26.3) Counting Lattice Points. Let us fix a lattice $\Lambda \subset \mathbb{R}^n$. Consider the valuation ν from Problem 4, Section 19.1. Namely, given an integer polytope P, we assign to every $u \in \mathbb{Z}^n$ a weight

$$\alpha(u, P) = \lim_{r \longrightarrow 0} \frac{\operatorname{vol}\big(B_r(u) \cap P\big)}{\operatorname{vol}\big(B_r(u)\big)},$$

where $B_r(u)$ is the ball of radius r centered at u and let

$$\nu(P) = \sum_{x \in \Lambda} \alpha(u, P).$$

Then $\nu(P)$ is a simple lattice-invariant valuation and besides $\nu(-P) = \nu(P)$. Theorems 20.2 and 26.1 imply that for the Ehrhart polynomial

$$\nu(mP) = \sum_{k=0}^{n} a_k(P) m^k$$

one has:

$a_0(P) = 0$,

$a_k(P) = 0$ provided $n - k$ is odd,

one has $\nu(mP) = \sum_{s=1}^{n} b_s(P)\binom{m}{s}$ for some non-negative coefficients $b_s(P)$, $a_n(P) = \mathrm{vol}(P)/(\det \Lambda)$.

PROBLEMS.

1. Prove the last expression for $a_n(P)$ (cf. Problem 6, Section 2.5).
2. Prove that $b_s(P)$ are valuations.

Wednesday, February 28

---

27. Counting Lattice Points

We denote by ρ the valuation of Section 26.3. That is

$$\rho(P) = \sum_{u \in \Lambda} \alpha(u, P),$$

where

$$\alpha(u, P) = \lim_{r \longrightarrow 0} \frac{\mathrm{vol}(B_r(u) \cap P)}{\mathrm{vol}(B_r(u))}$$

is the angle of P at u.

(27.1) More about Symmetry. Suppose that $P \subset \mathbb{R}^n$ is a polytope. We say that P is centrally symmetric with respect to $z \in \mathbb{R}^n$ if and only if $P = \{2z - x : x \in P\}$ (this is just the usual definition despite its strange appearance).

PROBLEMS.

1°. Let us fix a lattice $\Lambda \subset \mathbb{R}^n$ and let $P \subset \mathbb{R}^n$ be a lattice polytope. If P is centrally symmetric with respect to z then $2z \in \Lambda$.

2°. Let ν be a simple Λ-invariant valuation and $P \subset \mathbb{R}^n$ be a lattice polytope. Let $P_1 = 2P$. Suppose that $p(m) = \nu(mP)$ is the Ehrhart polynomial of P and $p_1(m) = \nu(mP_1)$ is the Ehrhart polynomial of P_1. Prove that $p_1(m) = p(2m)$.

3. Let $P \subset \mathbb{R}^n$ be a lattice polytope and ν be a simple lattice-invariant valuation. Suppose that P is centrally symmetric and that every facet of P is centrally symmetric. Then $\nu(P) = a \cdot \mathrm{vol}(P)$, for some constant a depending on ν and Λ alone and independent of P.

(27.1.1) Lemma. *Let $\Lambda \subset \mathbb{R}^n$ be a lattice and ν be a simple lattice-invariant valuation. Then there exists a constant $a = a(\Lambda, \nu)$ such that for every lattice polytope P whose every facet is centrally symmetric we have*

$$\nu(P) + \nu(-P) = 2a \cdot \mathrm{vol}(P).$$

Proof. We use Theorem 24.2. We get

$$\nu(P) = a \cdot \mathrm{vol}(P) + \sum_c \kappa(c)\nu_c(P_c), \quad \nu(-P) = a \cdot \mathrm{vol}(-P) + \sum_c \kappa(c)\nu_c((-P)_c).$$

Now $\nu_c(P_c) = 0$ unless P_c is a facet of P. If P_c is a facet of P then $(-P)_{-c}$ is a facet of $(-P)$. Since these facets are centrally symmetric, the translation which maps the center of symmetry of P_c to the center of symmetry of $(-P)_{-c}$ also maps P_c onto $(-P)_c$ and hence is a lattice translation (in other words: if z is the center of P_c then $-z$ is the center of $(-P)_{-c}$. A translation $x \longmapsto x + 2z$ is the lattice translation that maps $-z$ to z. If $x \in (-P)_{-c}$ then $-2z - x \in (-P)_{-c}$ and hence $2z + x \in P_c$). Since ν_c is lattice invariant we get that $\nu_c(P_c) = \nu_{-c}(P_{-c})$ and since $\kappa(c) = -\kappa(-c)$ we get the desired cancelation when we add $\nu(P)$ to $\nu(-P)$. □

(27.1.2) Corollary. *Consider the valuation ρ. For a lattice polytope P whose facets are centrally symmetric one has*

$$\rho(P) = \frac{\mathrm{vol}(P)}{\det \Lambda}.$$

Proof. Since $\rho(P) = \rho(-P)$ it follows by Lemma 27.1.1 that $\rho(P) = a \cdot \mathrm{vol}(P)$. Now it is almost obvious that

$$\lim_{m \longrightarrow +\infty} \frac{\rho(mP)}{m^n} = \frac{\mathrm{vol}(P)}{\det \Lambda}$$

(cf. Problem 1, Section 26.3 and Problem 6, Section 2.5). The proof follows. □

This Corollary may be considered as a higher-dimensional generalization of the Pick formula (in dimension 2 facets of every polytope are centrally symmetric). There are several interesting classes of polytopes whose facets are centrally symmetric: zonotopes (take the Minkowski sum of finitely many integer intervals in $\mathbb{R}^n$), parallelohedra (polytopes whose lattice translates tile the space), etc.

(27.2) An Illustration: Exponential Valuations. Let us fix a lattice $\Lambda \subset \mathbb{R}^n$ and let Λ^* be the dual lattice. Let us choose $l \in \Lambda^*$ and let

$$\rho^l(K) = \int_K \exp\{2\pi i \langle l, x \rangle\} \, dx,$$

where dx is the usual Lebesgue measure and K is a convex body.

PROBLEM.

1°. Prove that ρ^l is a lattice-invariant simple valuation.

(27.2.1) Theorem. *Let $P \subset \mathbb{R}^n$ be a polytope. Then $\rho^l(P) = \mathrm{vol}(P)$ if $l = 0$ and*

$$\rho^l(P) = \frac{1}{2\pi i \|l\|^2} \sum_c \langle l, c \rangle \rho^l_c(P_c), \quad \textit{where} \quad \rho^l_c(P_c) = \int_{P_c} \exp\{2\pi i \langle l, y \rangle\} dy;$$

the sum is taken over all unit vectors c and dy is the Lebesgue measure in the hyperplane $\langle c, x\rangle = \alpha$ that contains P_c.

Proof. The first assertion is obvious, the second is just the Stokes' formula $\displaystyle\int_{\partial P} \omega = \int_P d\omega$ applied to P and the form $\omega = \exp\{2\pi i \langle l, x\rangle\} dx_1 \wedge \ldots \wedge dx_{n-1}$, where $dx_1 \wedge \ldots \wedge dx_{n-1}$ is the $(n-1)$-dimensional volume form on the hyperplane $\langle l, x\rangle = 0$. $\square$

The valuations ρ^l constitute kind of a "Fourier expansion" for the valuation ρ. Indeed, let

$$\theta_t(x) = t^{\frac{n}{2}} \sum_{u \in \Lambda} \exp\{-\pi t \|x - u\|^2\}.$$

Then

$$\lim_{t \longrightarrow +\infty} \int_P \theta_t(x)\ dx = \rho(P).$$

On the other hand,

$$\theta_t(x) = \frac{1}{\det \Lambda} \sum_{l \in \Lambda^*} \exp\{-\pi \|l\|^2/t\} \exp\{2\pi i \langle l, x\rangle\}$$

(modularity relation). Therefore

$$\rho(P) = \lim_{t \longrightarrow +\infty} \frac{1}{\det \Lambda} \sum_{l \in \Lambda} \exp\{-\|l\|^2/t\} \rho^l(P). \tag{27.2.2}$$

PROBLEMS.

1. Consider the Ehrhart polynomial p of P of the valuation ρ^l. If deg $p \geq k$ then l is orthogonal to some k-dimensional face of P.

2. Deduce Corollary 27.1.2 from the representation (27.2.2) and Theorem 27.2.1.

Hint: If P has centrally symmetric facets then Theorem (27.2.1) implies that $\rho^l(P) = 0$ provided $l \neq 0$. Now use (27.2.2).

3*. Prove Theorem 24.2 for $\nu = \rho$ using Theorem 27.2.1 and (27.2.2)

4. Prove that for the valuation $\nu = \rho^l$ one can choose $\kappa(C)$, $C = (c_1, \ldots, c_k)$ in Theorem 25.2 to be polynomial in $c_1, \ldots, c_k$.

5*. What can we get for $\kappa(C)$ for the valuation $\nu = \rho$ from (27.2.2) and Problem 4?

(27.3) Lattice Points in the Polytopes with "Moving Walls". We say that the polytopes P and Q in $\mathbb{R}^n$ are *strongly combinatorially isomorphic* if and only if dim $P_C =$ dim Q_C for every frame C. In other words, the polytope Q can be obtained from P by moving its facets parallel to themselves so that we don't acquire new faces and don't lose any old face. Let us denote by $\mathcal{C}(P)$ the set of all polytopes that are strongly combinatorially isomorphic to P. The faces of every $Q \in \mathcal{P}$ are in one-to-one correspondence with the faces of P. For the polytopes from $\mathcal{C}(P)$, Theorem 25.2 has especially simple form.

(27.3.1) Theorem. *Let us fix a lattice $\Lambda \subset \mathbb{R}^n$, a simple lattice-invariant valuation ν and a lattice polytope P. Then to every face F of P one can assign a number a_F such that for any lattice polytope $Q \in \mathcal{C}(P)$ one has*

$$\nu(Q) = \sum_F a_F \cdot \operatorname{vol} F,$$

where the sum is taken over all faces F of Q, vol *denotes the volume of a face in its affine hull and a_F is the coefficient assigned to the corresponding face of P.*

Proof. Follows by Theorem 25.2 and the above definition.

PROBLEMS.

1. Let us fix a lattice $\Lambda \subset \mathbb{R}^n$ and a simple lattice-invariant valuation ν. Let $P = \{x : \langle c_i, x\rangle \leq \alpha_i,\ i = 1, \ldots, m\}$ be an n-dimensional polytope. For $h = (h_1, \ldots, h_m)$ let $P_h = \{x : \langle c_i, x\rangle \leq \alpha_i + h_i,\ i = 1, \ldots, m\}$. Then there exists a polynomial $p(h_1, \ldots, h_m)$ such that

$$\nu(P_h) = p(h_1, \ldots, h_m)$$

whenever P_h is a lattice polytope strongly combinatorially isomorphic to P.

Hint: Prove that the volumes of faces of P_h are polynomials in $h = (h_1, \ldots, h_m)$.

2. Deduce the existence of the Ehrhart polynomial from Problem 1.

Friday, March 1

---

28. Rational Polytopes

(28.1) Definitions. Let $P \subset \mathbb{R}^n$ be a polytope. We say that P is *rational* if and only its vertices are points with rational coordinates. In other words, for some positive integer m the polytope mP is integral. Generally, if we consider a lattice $\Lambda \subset \mathbb{R}^n$ other than $\mathbb{Z}^n$, we call a polytope $P \subset \mathbb{R}^n$ rational, if mP is a lattice polytope for some positive integer m. Alternatively, the vertices of P belong to $\mathbb{Q}\Lambda$, where $\mathbb{Q}\Lambda$ is the set of all finite linear combinations of points from Λ with rational coefficients.

PROBLEMS.

1°. If P is a rational polytope then every face of P is a rational polytope.

2. Let $P \subset \mathbb{R}^n$ be a rational polytope and ν be a simple lattice-invariant valuation. Let us choose a positive integer d such that $Q = dP$ is a lattice polytope. Consider the Ehrhart polynomial

$$\nu(mQ) = \sum_{k=1}^{n} a_k(Q) m^k \quad \text{and let} \quad a_k(P) = \frac{a_k(Q)}{d^k}.$$

a) Prove that $a_k(P)$ doesn't depend on a choice of d;

b) Prove that $a_k(P)$ is a valuation defined on the set of all rational polytopes;

c) Prove that $a_k(P)$ is homogeneous of degree k, that is $a_k(mP) = m^k a_k(P)$ for any positive integer m.

First, we need a generalization of Theorem 24.2 for the case of rational polytopes, see P. McMullen, Lattice invariant valuations on rational polytopes, *Archiv der Mathematik*, **31** (1978/79), 509–516.

(28.2) Theorem. *Let $\Lambda \subset \mathbb{R}^n$ be a lattice and ν be a simple lattice-invariant valuation. Then there exist a number a, an odd function $\kappa(c)$ on the unit vectors c in $\mathbb{R}^n$ and for every unit vector $c \in \mathbb{R}^n$ one can define a family of simple valuations ν_c on the hyperplanes $H_\alpha = \{x \in \mathbb{R}^n : \langle x, c\rangle = \alpha\}$ such that*

a) $\nu_c \equiv 0$ if $H_0 = \{x \in \mathbb{R}^n : \langle c, x\rangle = 0\}$ is not a lattice hyperplane;

b) if H_0 is a lattice hyperplane, $Q_1 \subset H_{\alpha_1}$, $Q_2 \subset H_{\alpha_2}$ and Q_2 is a lattice translation of Q_1 then $\nu_c(Q_1) = \nu_c(Q_2)$;

c) for every rational polytope P we have

$$\nu(P) = a \cdot \mathrm{vol}\,(P) + \sum_c \kappa(c)\nu_c(P_c),$$

where the sum is taken over all unit vectors c.

Proof. The proof is literally the same as in Theorem 24.2.

Now we want to generalize Theorem 25.2. The function $\kappa(C)$ should be defined in a more tricky way: it is a function $\kappa(C, A)$, where $C = (c_1, \ldots, c_k)$ is a k-frame and A is an $(n-k)$-dimensional affine subspace orthogonal to every $c_i : i = 1, \ldots, k$. If C is a k-frame and $P \subset \mathbb{R}^n$ is a polytope for which C is proper, by A_C we denote the (necessarily $(n-k)$-dimensional) affine hull of P_C.

(28.3) Theorem. *Let $\Lambda \subset \mathbb{R}^n$ be a lattice and and ν be a simple lattice-invariant valuation. For every $k = 0, 1, \ldots, n$ there exists a function $\kappa(C, A)$ such that*

a) $\kappa(C, A)$ is odd as a function of C, that is

$$\kappa\bigl(\epsilon_1 c_1, \ldots, \epsilon_k c_k; A\bigr) = \epsilon_1 \cdots \epsilon_k \kappa\bigl(c_1, \ldots, c_k; A\bigr) \quad \text{where } \epsilon_i \in \{-1, 1\};$$

b) $\kappa(C, A)$ is lattice-invariant as a function of A, that is

$$\kappa(C, A+u) = \kappa(C, A) \quad \text{for any } u \in \Lambda;$$

c) For every rational polytope P we have

$$\nu(P) = \sum_{k=0}^{n} \sum_{|C|=k} \kappa(C, A_C)\mathrm{vol}_{n-k}(P_C),$$

where the inner sum is taken over all k-frames C that are proper for P and A_C is the affine hull of P_C.

Proof. We apply Theorem 28.2 recursively, first to P, then to its facets, and so forth. On the first step we get the decomposition

$$\nu(P) = a \cdot \text{vol } P + \sum_c \kappa(c)\nu_c(P_c),$$

where the summands for which P_c is not a facet are obviously zero (as ν_c is simple). Now we apply Theorem 28.2 to every facet P_c. Since P_c is not necessarily a lattice polytope, the valuation ν_c depends on the Λ-translation class of the hyperplane A_c containing P_c. In particular, the coefficient in front of $\text{vol}_{n-1}(P_c)$ depends not only on c but also on the translation class of A_c. This is how we arrive to the function $\kappa(C, A)$ of two arguments. So, for a given k-frame $C = (c_1, \ldots, c_k)$ and $(n-k)$-dimensional affine subspace A we let $\kappa(C, A) = a(A)\kappa(c_1)\cdots\kappa(c_k)$, where κ is the function from Theorem 28.2 and the constant $a(A)$ is defined as follows: we consider the sequence of valuations $\nu, \nu_1, \ldots, \nu_k$ where ν_i is the valuation on the $(n-i)$-dimensional affine subspace containing A and orthogonal to $c_1, \ldots, c_i$ obtained from ν_{i-1} by Theorem 28.2; finally $a(A)$ is the coefficient of the volume term from Theorem 28.2 for $\nu = \nu_k$. □

Now we can establish a "quasi-polynomial" behavior of $\nu(mP)$ for a rational polytope P.

(28.4) Definition. Let $P \subset \mathbb{R}^n$ be a rational n-dimensional polytope. We define the *r-index* of P (denoted $\text{ind}_r(P)$) as the smallest positive integer m such that for each r-dimensional face F of P, the affine hull of F contains a lattice point.

PROBLEMS.
1°. $\text{ind}_n(P) = 1$.
2. $\text{ind}_i(P)$ divides $\text{ind}_j(P)$ for $i > j$.

(28.5) Theorem. *Let $\Lambda \subset \mathbb{R}^n$ be a lattice and ν be a simple lattice-invariant valuation. Let $P \subset \mathbb{R}^n$ be a rational polytope. Then for positive integers m*

(28.5.1) $$\nu(mP) = \sum_{r=0}^{n} \nu_r(P, m)m^n,$$

where $\nu_r(P, m)$ is a periodic function of m with whose period divides $\text{ind}_r(P)$ that is,

(28.5.2) $$\nu_r(P, m + \text{ind}_r(P)) = \nu_r(P, m).$$

Furthermore, by the periodicity (28.5.2) $\nu_r(P, m)$ can be defined for negative integers m. Then we must have

(28.5.3). $$\nu_r(-P, -m) = (-1)^{n-r}\nu_r(P, m) \quad \textit{(reciprocity)}$$

Proof. We use 28.3. Indeed, let

$$\nu_r(P, m) = \sum_{|C|=n-r} \kappa(C, mA_C)\mathrm{vol}_r(P_C),$$

where as usual $mA = \{mx : x \in A\}$. Then (28.5.1) is satisfied since vol_r is homogeneous of degree r. Now if $\mathrm{ind}_r(P) = d$, say, then dA_C contains a lattice point and hence $(m+d)A_C = mA_C + dA_C$ is a lattice translation of mA_C. Hence by Theorem 28.3 we must have $\kappa(C, mA_C) = \kappa(C, (m+d)A_C)$ and (28.5.2) is proven. Let $d = \mathrm{ind}_r(P)$ as above and $s = -m \mod d$, $d > s \geq 0$. We have to prove that $\nu_r(-P, s) = (-1)^{n-r}\nu_r(P, d-s)$. Indeed, if $(-P)_{-C} = -(P_C)$, and, therefore the affine span $(-A)_{-C}$ of $(-P)_{-C}$ is $-A_C$. Now we observe that $-sA_C$ is a lattice translation of $(d-s)A_C$, since dA_C contains a lattice point. Therefore $\kappa(-C, (-A)_{-C}) = (-1)^{n-r}\kappa(C, A_C)$ and (28.5.3) follows. □

PROBLEMS.

1. Generalize Corollary 27.1.2 for rational polytopes.
2. Generalize Theorem 27.3.1 for rational polytopes.
3. Prove that $\nu_r(P, m)$ are *quasi-homogeneous*, that is $\nu_r(kP, m) = k^r\nu_r(P, km)$ for every positive integer k.
4. Let $\Lambda \subset \mathbb{R}^n$ be a lattice and ν be a simple lattice-invariant valuation in $\mathbb{R}^n$. Let us choose a rational vector $t \in \mathbb{R}^n$. Prove that for a rational polytope P

$$\nu(mP + t) = \sum_{r=0}^{n} \nu_r(P, m; t)m^r,$$

where $\nu_r(P, m; t)$ is a periodic function in m with a period $\mathrm{ind}_r(P)$.
Furthermore, $\nu_r(-P, -m, -t) = (-1)^{n-r}\nu_r(P, m, t)$ once ν_r defined for negative values of m by periodicity.

Hint: Consider $\nu^t = \nu(P + t)$. Prove that ν^t is simple lattice invariant valuation.

Monday, March 11

---

29. Solutions to Some Problems from the First Set

Wednesday, March 13

---

30. Cones and Angles

(30.1) Definitions. Let $c_1, \ldots, c_m \in \mathbb{R}^n$ be some vectors. A *cone* or *polyhedral cone* is the set of points:

$$K = \big\{x \in \mathbb{R}^n : \langle c_i, x \rangle \leq 0, \text{ for } i = 1, \ldots, m\big\}.$$

The *conic hull* of some vectors $c_1, \ldots, c_m$ is the set of all their linear combinations with non-negative coefficients:

$$\operatorname{co}\{c_1, \ldots, c_m\} = \Big\{\sum_{i=1}^{m} \lambda_i c_i : \lambda_i \geq 0 \text{ for } i = 1, \ldots, m\Big\}.$$

PROBLEMS.

1°. A cone K is a polyhedron and every face of K is a cone.

2°. A cone K is a closed convex set in $\mathbb{R}^n$ such that for any $x \in K$ and any $\lambda \geq 0$ one has $\lambda x \in K$.

3°. The conic hull K of a finite set of vectors is a closed convex set in $\mathbb{R}^n$ such that for any $x \in K$ and any $\lambda \geq 0$ one has $\lambda x \in K$.

(30.2) Theorem [Weyl - Minkowski Theorem]. *Every cone in $\mathbb{R}^n$ is a conic hull of finitely many vectors. The conic hull of finitely many vectors in $\mathbb{R}^n$ is a cone.*

We don't prove this but there is a proof following the line sketched in Problems 1-7, Section 18.2.

(30.3) Definition. Let $K \subset \mathbb{R}^n$ be a cone. The set

$$K^* = \big\{x \in \mathbb{R}^n : \langle x, y \rangle \leq 0\big\}$$

is called the *polar* of K.

PROBLEMS.

1. Prove that $\{0\}^* = \mathbb{R}^n$ and that $(\mathbb{R}^n)^* = \{0\}$.

2°. If $K = \operatorname{co}\{c_1, \ldots, c_m\}$ then $K^* = \{x : \langle c_i, x \rangle \leq 0 : i = 1, \ldots, m\}$.

3. If $K = \{x : \langle c_i, x \rangle \leq 0 : \ i = 1, \ldots, m\}$ is a cone then $K^* = \operatorname{co}\{c_1, \ldots, c_m\}$.

Hint: The inclusion $\operatorname{co}\{c_1, \ldots, c_m\} \subset K^*$ is immediate. To prove the opposite inclusion, use a separation theorem (a point which does not belong to a closed convex set in $\mathbb{R}^n$ can be separated from this set by a hyperplane).

4. Prove that $(K^*)^* = K$.

5*. Let us associate with every cone K its indicator function

$$\chi_K : \mathbb{R}^n \longrightarrow \mathbb{R}, \quad \chi_K(x) = \begin{cases} 1, & \text{if } x \in K, \\ 0, & \text{if } x \notin K. \end{cases}$$

Prove that if we have an identity

$$\sum_{i=1}^{m} a_i \chi_{K_i} \quad \text{for some integers } a_i$$

then we have the identity

$$\sum_{i=1}^{m} a_i \chi_{(K_i^*)} = 0.$$

6. Let $K \subset \mathbb{R}^n$ be a cone. Then

$$K^* = \Big\{ x \in \mathbb{R}^n : \|x\| \leq \|x - y\| \text{ for every } y \in K \Big\}.$$

In other words, the polar cone K^* is the set of points which closer to the origin than to any other point in K.

We can measure cones.

(30.4) Definition. Let $K \subset \mathbb{R}^n$ be a cone. We define its *measure* or *angle* $\alpha(K)$ as follows

$$\alpha(K) = \int_K e^{-\pi \|x\|^2} \, dx,$$

or, equivalently

$$\alpha(K) = \frac{\operatorname{vol}(K \cap B_r(0))}{\operatorname{vol} B_r(0)},$$

where $B_r(0)$ is the ball of radius r centered in the origin (please make sure that these two definitions are equivalent).

PROBLEMS.

1°. Make sure that $\alpha(\mathbb{R}^n) = 1$, $\alpha(\{0\}) = 0$, $\alpha(\text{halfspace}) = 1/2$.

2°. Make sure that α is a valuation, that is, if $K = \bigcup_{i=1}^{m} K_i$, where K and K_i are cones then

$$\alpha(K) = \sum_{i=1}^{m} \alpha(K_i) - \sum_{i_1 < i_2} \alpha(K_{i_1} \cap K_{i_2}) + \ldots + (-1)^{s-1} \sum_{i_1 < i_2 < \ldots < i_s} \alpha(K_{i_1} \cap \ldots \cap K_{i_s}) +$$

$$\ldots + (-1)^{m-1} (K_1 \cap \ldots \cap K_m).$$

(30.5) Lemma. *Let $K_1 \subset \mathbb{R}^{n_1}$ and $K_2 \subset \mathbb{R}^{n_2}$ be cones. Let $\mathbb{R}^n = \mathbb{R}^{n_1 + n_2} = \mathbb{R}^{n_1} \times \mathbb{R}^{n_2} = \{(x, y) : x \in \mathbb{R}^{n_1}, y \in \mathbb{R}^{n_2}\}$ and let $K = \{(x, y) : x \in K_1, y \in K_2\}$. Then $K \subset \mathbb{R}^n$ is a cone and $\alpha(K) = \alpha(K_1)\alpha(K_2)$.*

Proof. Well, if $K_1 = \{x_1 \in \mathbb{R}^{n_1} : \langle c_i^1, x_1 \rangle \leq 0 : i = 1, \ldots, m_1\}$ and $K_2 = \{x_2 \in \mathbb{R}^{n_2} : \langle c_i^2, x_2 \rangle \leq 0 : i = 1, \ldots, m_2\}$ then $K = \{(x, y) : \langle (x, y), (c_i^1, 0) \rangle \leq 0 : \quad i = 1, \ldots, m_1 \quad \text{and} \quad \langle (x, y), (0, c_i^2) \rangle \leq 0 \ i = 1, \ldots, m_2\}$ is a cone.

Now

$$\alpha(K) = \int_K e^{-\pi \|x\|^2} \, dx = \int_K e^{-\pi \|x_1\|^2} e^{-\pi \|x_2\|^2} \, dx_1 dx_2$$
$$= \int_{K_1} e^{-\pi \|x_1\| 2} \, dx_1 \int_{K_2} e^{-\pi \|x_2\|^2} \, dx_2 = \alpha(K_1)\alpha(K_2).$$

PROBLEM.

1°. If $K_1 = \text{co}\{c_i^1, i = 1, \ldots, m_1\}$ and $K_2 = \text{co}\{c_i^2, i = 1, \ldots, m_2\}$ then $K_1 \times K_2 = \text{co}\{(c_i^1, c_j^2), i = 1, \ldots, m_1; j = 1, \ldots, m_2\}$. □

(30.6) Definition. Let P be a polyhedron and $F \subset P$ be a face. We define the *interior angle* $\beta(F, K)$ as follows: Suppose that dim $F = k$. Choose a point in the relative interior of F, say p. Consider the $(n - k)$-dimensional subspace L orthogonal to F and passing through the point p. Make p the origin of L. Suppose that the polyhedron P is defined by the inequalities $P = \{x \in \mathbb{R}^n : \langle c_i, x \rangle \leq \alpha_i, i = 1, \ldots, m\}$. Let us choose the inequalities that become equalities on p, say, the first k. So "locally", in a neighborhood of p, P coincides with a cone $K(p) = \{x : \langle c_i, x - p \rangle \leq 0, i = 1, \ldots, k\}$. Hence $K_F = L \cap K(p)$ is a cone in L and we let $\beta(F, K) = \alpha(K_F)$. We define the *exterior angle* $\gamma(F, K)$ as $\alpha(K_F^*)$ in L.

Now is the main result of this section.

(30.7) Theorem. *Let $K \subset \mathbb{R}^n$ be a cone. Then*

$$\sum_F \beta(\{0\}, F)\gamma(F, K) = 1,$$

where the sum is taken over all faces F of K.

Proof. Let $K^* \subset \mathbb{R}^n$ be the polar of K. For a face $F \subset K$ let us define

$$\hat{F} = \big\{x \in K^* : \langle x, y \rangle = 0 \text{ for each } y \in F\big\}.$$

First, we observe that $\alpha(\hat{F}) = \gamma(F, K)$. Next, we observe that F and $\hat{F}$ belong to a pair of orthogonal subspaces of complementary dimensions, so there is a cone $F \times \hat{F}$ such that

$$\alpha(F \times \hat{F}) = \alpha(F)\alpha(\hat{F}) = \beta(\{0\}, F)\gamma(F, K)$$

(cf. Lemma 30.5). Finally, we observe that cones $F \times \hat{F}$ dissect the whole space $\mathbb{R}^n$ as F ranges over all faces of K. To see that, let us consider the "nearest point" map

$$N : \mathbb{R}^n \longrightarrow K, \quad x \longmapsto y,$$

where $y \in K$ is the nearest point in K for y. For every point $x \in \mathbb{R}^n$ there exists unique face F of K such that $N(x)$ is in the relative interior of K. Then the set of such x-s is just $F \times \hat{F}$ (cf. Problem 6, Section 30.3). Therefore we get

$$1 = \sum_F \alpha(F \times \hat{F}) = \sum_F \beta(\{0\}, F)\gamma(F, K).$$

$\square$

Friday, March 15

---

31. Ehrhart Polynomial of the Counting Valuation

We start with a problem.

PROBLEM

1°. Let $P \subset \mathbb{R}^n$ be a polytope and $c \in \mathbb{R}^n$ be a vector. Then there exists a vertex v of P such that $\langle c, v\rangle \geq \langle c, x\rangle$ for every $x \in P$. In other words, the maximal value of a linear function on a polytope is attained at a vertex of the polytope.

Hint: Use the fact that P is the set of convex combinations of its vertices, that is for every $x \in P$ there exist numbers $\{\lambda_v\}$, v is a vertex such that $\sum_v \lambda_v = 1$, $\lambda_v \geq 0$ and $x = \sum_v \lambda_v v$.

(31.1) Theorem. *Let $P \subset \mathbb{R}^n$ be a polytope and V be the set of its vertices. Then*

$$\sum_{v \in V} \gamma(v, P) = 1.$$

Proof. For every $v \in V$ let us consider the cone

$$K^v = \Big\{c \in \mathbb{R}^n : \langle c, v - u\rangle \geq 0 \text{ for every } u \in V\Big\}.$$

In other words, K^v is the set of vectors $c \in \mathbb{R}^n$ such that the linear function $\langle c, x\rangle$ attains its maximum at v. It is clear that K^v is a cone and we claim that $\alpha(K^v) = \gamma(v, P)$. Indeed, it follows that K^v is the polar to the cone K_v from Definition 30.6. Now, every point $c \in \mathbb{R}^n$ belongs to some cone K^v and the intersection $K^v \cap K^u$ is at most $(n-1)$-dimensional, since is contained in the hyperplane $\langle c, u\rangle = \langle c, v\rangle$. So K^v constitute a dissection of $\mathbb{R}^n$. Therefore

$$1 = \sum_{v \in V} \alpha(K^v) = \sum_{v \in V} \gamma(v, P)$$

and the proof follows. $\square$

PROBLEMS.

1. Let $P \subset \mathbb{R}^n$ be a polytope with the vertex set V. The point

$$s(P) = \sum_{v \in V} \gamma(v, P) v$$

is called the *Steiner point* of P.

a°). Prove that $s(P) \in P$.

b) Prove that $s(P_1 + P_2) = s(P_1) + s(P_2)$, where "+" denotes the Minkowski sum and that $s(\alpha P) = \alpha s(P)$ for $\alpha \in \mathbb{R}$.

c°. Prove that $s(T(P)) = T(s(P))$, where T is a rigid motion (a composition of translations and rotations).

d) Problem 2 from Section 23.4 implies that $s(P)$ satisfies the inclusion-exclusion property: if $P_1, \ldots, P_m \subset \mathbb{R}^n$ are convex polytopes such that $P = P_1 \cup \ldots \cup P_m$ is a convex polytope then

$$s(P) = \sum_{i=1}^{m} s(P_i) - \sum_{1 \leq i_1 < i_2 \leq m} s(P_{i_1} \cap P_{i_2}) + \ldots + (-1)^{m-1} s(P_1 \cap \ldots \cap P_m).$$

2*. Suppose there is a function $P \longmapsto s(P) \in \mathbb{R}^n$ such that a)-c) are satisfied. Is it true that $s(P)$ is a Steiner point of P?

Remark: It is true that if the map $P \longmapsto s(P)$ is continuous (in the Hausdorff metric) and satisfies c) and d) then $s(P)$ is the Steiner point.

3. Apart from $\alpha(K)$ there are some other interesting and bizarre ways to measure cones. Some of them proved to be quite useful:

A function $f : \mathbb{R} \longrightarrow \mathbb{R}$ is called *additive* if and only if $f(a + b) = f(a) + f(b)$ for every $a, b \in \mathbb{R}$.

a) Prove that a continuous additive function is linear: $f(a) = ca$ for some constant c and all $a \in \mathbb{R}$;

b) Prove that there exists an additive function f, not identically zero, such that $f(1) = 0$.

This is how the famous *Dehn invariant* is constructed: let us choose an additive function f such that $f(1) = 0$. Let $P \subset \mathbb{R}^3$ be a polytope. Let

$$D_f(P) = \sum_{l} \|l\| \cdot f(\beta(l, P)),$$

where the sum is taken over all edges l of P.

c) Prove that every D_f is a simple valuation on polytopes in $\mathbb{R}^3$ which is invariant under rigid motions;

d) Prove that if the P_1 and P_2 are *equidissectable*, that is P_1 can be cut into finitely many polytopal pieces that can be reassembled into P_2 (by applying rigid motions to the pieces) then $D_f(P_1) = D_f(P_2)$;

e) Let T be a regular tetrahedron in $\mathbb{R}^3$ and C be a regular cube in $\mathbb{R}^3$ such that $\mathrm{vol}\, T = \mathrm{vol}\, C$. Prove that there exists a Dehn invariant D_f such that $D_f(C) \neq D_f(T)$. In particular, C and T are not equidissectable.

Remark: This is a solution of the third Hilbert problem.

f) Prove that if two convex polygons in $\mathbb{R}^2$ have equal areas then they are equidissectable.

Now the main result of this section.

(31.2) Theorem. *Let us fix a lattice $\Lambda \subset \mathbb{R}^n$. Let $P \subset \mathbb{R}^n$ be a lattice polytope. As usual, for $m \in \mathbb{N}$ we denote $mP = \{mx : x \in P\}$. Let $p(m) = |mP \cap \Lambda|$ be the number of lattice points in mP. Then*

$$p(m) = \sum_{k=0}^{n} e_k(P) m^k$$

is a polynomial in m such that

(31.2.1)
$$e_n(P) = \frac{\mathrm{vol}_n P}{\det \Lambda};$$

(31.2.2)
$$e_{n-1}(P) = \frac{1}{2} \sum_F \frac{\mathrm{vol}_{n-1}(F)}{\det \Lambda_F},$$

where the sum is taken over all facets F of P and Λ_F is the $(n-1)$-dimensional lattice in the affine span of F;

(31.2.3)
$$e_0(P) = 1;$$

(31.2.4)
$$p(m) = \sum_{k=0}^{n} g_k(P) \binom{m}{k}$$

for some non-negative $g_k(P)$.

Proof. Let us consider a face F of P. In the affine hull of F we consider the valuation ρ (see Section 27). In other words, if a lattice point $u \in \Lambda$ belongs to a relative interior of a face $G \subset F$ we count it with the weight $\beta(F, G)$. Now we claim that

$$|P \cap \Lambda| = \sum_F \gamma(F, P)\rho(F),$$

where the sum is taken over all faces F of P. Let us choose an $u \in P$. Suppose that u belongs to the relative interior of a face F of P. Then the total weight we assign to u is $\sum_G \beta(F, G)\gamma(G, P)$, where the sum is taken over all faces G that contain F. Theorem 30.7 implies that

$$\sum_G \beta(F, G)\gamma(G, P) = 1.$$

Therefore every point is counted with weight 1. If we apply a dilatation, we observe that $\gamma(mG, mP)$ does not change and $\rho(mF)$ behaves polynomially (see Theorem 20.2). So $p(m)$ is indeed a polynomial. Now $e_n(P)$ is the highest coefficient of $\rho(mP)$ which is $(\mathrm{vol}_n P)/\det \Lambda$ (see Problem 1, Section 26.3), so (31.2.1) is proven. Since ρ is a simple centrally-symmetric valuation, the next coefficient in $\rho(mP)$ is 0 (see Section 26.3). So $e_{n-1}(P)$ comes from the highest coefficients of $\rho(mF)$ for the facets of P. Noting that $\gamma(F, P) = 1/2$ for every facet, we get (31.2.2). Now, the constant term of $\rho(mF)$ is 0 (see Theorem 20.2) unless F is 0-dimensional (that is, a vertex), when $\rho(mF) \equiv 1$. Thus by Theorem 31.1.1

$$e_0(P) = \sum_v \gamma(v, P) = 1$$

and (31.2.3) is proven. Finally, (31.2.4) follows by Theorem 20.2 and the fact that $\gamma(F, P) \geq 0$. □

If instead of Theorem 20.2 we use Theorem 28.5 we get the following

(31.3) Theorem. *Let $\Lambda \subset \mathbb{R}^n$ be a lattice and $P \subset \mathbb{R}^n$ be a rational polytope. Let $p(m) = |mP \cap \Lambda|$* for $m \in \mathbb{N}$. *Then $p(m)$ is a quasi-polynomial, that is*

$$p(m) = \sum_{k=0}^{n} e_k(P, m),$$

where $e_k(P, m)$ is a periodic function of m, so

$$e_k(P, m + \mathrm{ind}_k(P)) = e_k(P, m),$$

where $\mathrm{ind}_k P$ is the smallest natural number d such that the affine hull of each k-dimensional face of dP contains a lattice point.

PROBLEM.

1°. Prove Theorem 31.3.

If we use Theorem 27.3.1 we get the following.

(31.4) Theorem. *Let us fix a lattice Λ and a lattice polytope P. Then to every face F of P one can assign a number a_F such that for every lattice polytope Q strongly combinatorially isomorphic to P one has*

$$|Q \cap \Lambda| = \sum_F a_F \cdot \mathrm{vol}\, F,$$

where the sum is taken over all faces F of Q, vol *denotes the volume of a face in its affine hull and a_F is the coefficient assigned to the corresponding face of P.*

PROBLEM.

1°. Prove Theorem 31.4.

Monday, March 18

---

32. Polytopal Subdivisions

First, some problems for the previous section.

PROBLEMS.

1°. Let $\Lambda \subset \mathbb{R}^n$ be a lattice and $P \subset \mathbb{R}^n$ be a lattice polytope. Consider the Ehrhart polynomial $p(m) = |\Lambda \cap mP|$. This polynomial has rational coefficients and the two highest coefficients are positive.

2. Show that there exists an integer tetrahedron $P \subset \mathbb{R}^n$ whose Ehrhart polynomial $|\mathbb{Z}^3 \cap mP|$ has a negative coefficient $e_1(P)$.

Hint: Consider a tetrahedron with the vertices $(0, 0, 0)$, $(1, 0, 0)$, $(0, 1, 0)$, and $(1, 1, k)$, where k is a positive integer. Its Ehrhart polynomial is

$$\frac{k}{6}m^3 + m^2 + \frac{12-k}{6}m + 1,$$

so for $k \geq 13$ the coefficient in front of m is negative.

3. a) If a plane triangle $T \subset \mathbb{R}^2$ with integral vertices has no other integral points then the area of T is $1/2$;

b) For any v there exists a tetrahedron $T \subset \mathbb{R}^3$ with integral vertices which contains no other integral points and whose volume is greater than v.

c*) For any $k \geq 1$ and n there exists a number $f(k, n)$ such that the volume of every polytope P with vertices in $\mathbb{Z}^n$, containing precisely k integer points in its interior is at most $f(k, n)$. As Problem b) states this is no longer true for $k = 0$.

Remark: One can choose $f(k, n) = k(7(k + 1))^{2^{n+1}}$, see J.C. Lagarias and G. Ziegler, Bounds for lattice polytopes containing a fixed number of interior points in a sublattice, *Canad. J. Math.*, **43**(1991), 1022–1035.

(32.1) Definitions. A *polytopal subdivision* P is a finite set $\{P_i : i = 1, \ldots, m\}$ of polytopes $P_i \subset \mathbb{R}^n$ such that the intersection $P_i \cap P_j$ is either empty or a proper face of P_i and P_j for any two P_i and P_j. For a subdivision P we denote $|P| = \bigcup_{i=1}^{m} P_i$. The largest of dim P_i is called the *dimension* of P. A face of a polytope P_i from the subdivision is called a *face* of the subdivision. The number of k-dimensional faces of a subdivision P is denoted $f_k(P)$. A *hollow polytope* ∂P is a polytopal subdivision that is the union of all proper faces of a polytope $P \subset \mathbb{R}^n$.

We identify subsets $X \subset \mathbb{R}^n$ with their indicator functions

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

PROBLEMS.

1°. Let P be a polytopal subdivision. Then the indicator function $\chi_{|P|}$ of $|P|$ belongs to the Convex Ring $\mathbb{Z}(\mathcal{K})$.

2. Let us fix a lattice $\Lambda \subset \mathbb{R}^n$ and let P be a polytopal subdivision such that every polytope P_i is a lattice polytope. For $m \in \mathbb{N}$ we let $m|P| = \{mx : x \in |P|\}$ and $p(m) = \operatorname{card}\{m|P| \cap \Lambda\}$. Then $p(m)$ is a polynomial in m whose coefficient in front of m^n is equal to vol $|P|$ and the constant term is $\mu(|P|)$, the Euler characteristic of $|P|$.

(32.2) Lemma. *Let P be a d-dimensional polytope. Then $\mu(|\partial P|) = 1 + (-1)^{d-1}$.*

Proof. We prove by induction on d. If $d = 1$ then P is an interval and ∂P is a subdivision consisting of two points (the endpoints of the interval), so the formula is obviously correct. Suppose that $d > 1$ and $P \subset \mathbb{R}^n$. We use the formula of Theorem 21.2 for Euler characteristic. Let us choose a linear function $l : \mathbb{R}^n \longrightarrow \mathbb{R}$ such that for any $\alpha \in \mathbb{R}$ the intersection of P with the hyperplane $H^\alpha = \{x \in P : l(x) = \alpha\}$ is either empty (if $\alpha > \max\{l(x) : x \in P\}$ or $\alpha < \min\{l(x) : x \in P\}$), or a point (if $\alpha = \max\{l(x) : x \in P\}$ or $\alpha = \min\{l(x) : x \in P\}$), or a $(d-1)$-dimensional polytope $P^\alpha = P \cap H^\alpha$ (if $\min\{l(x) : x \in P\} < \alpha < \max\{l(x) : x \in P\}$). Now we are going to use the formula from Theorem 21.2:

$$\mu(|\partial P|) = \sum_{\alpha \in \mathbb{R}} \lim_{\epsilon \longrightarrow +0} \Big(\mu\big(|\partial P| \cap H^\alpha\big) - \mu\big(|\partial P| \cap H^{\alpha+\epsilon}\big) \Big).$$

But there are only two possible values for α corresponding to non-zero summands. If $\alpha = \max\{l(x) : x \in P\}$ then the summand is $1 - 0 = 1$. If $\alpha = \min\{l(x) : x \in P\}$ then the summand is $1 - 1 - (-1)^{d-2} = (-1)^{d-1}$ (induction conjecture). Therefore $\mu(|\partial P|) = 1 + (-1)^d$. □

We are going to prove the following main result:

(32.3) Theorem. *Let P be a polytopal subdivision in $\mathbb{R}^n$ of dimension d. Then*

$$\mu(|P|) = \sum_{k=0}^{d} (-1)^k f_k(P).$$

Proof. We use induction on d If $d = 0$ then P consists of several points in $\mathbb{R}^n$ and the result is obvious.

Suppose that $d > 0$. Now we use induction on the number m of polytopes in the subdivision. If $m = 1$ then the faces of P are the faces of some d-dimensional polytope $|P|$. There is one face of dimension d (the polytope itself) and faces of dimensions $\leq d-1$ constituting the hollow polytope ∂P. The subdivision ∂P is $(d-1)$-dimensional, so we can use the induction conjecture and get

$$\mu(|\partial P|) = \sum_{k=0}^{d-1}(-1)^k f_k(\partial P).$$

Lemma 32.2 implies that

$$\sum_{k=0}^{d-1}(-1)^k f_k(\partial P) = 1 + (-1)^{d-1}.$$

Since

$$f_k(P) = \begin{cases} f_k(\partial P) & \text{for } k < d, \\ 1 & \text{for } k = d. \end{cases}$$

we get

$$\sum_{k=0}^{d}(-1)^k f_k(P) = 1 = \mu(P).$$

Suppose that $m > 1$, so the subdivision P consists of at most d-dimensional polytopes $P_1, \ldots, P_m$. Let us consider the subdivision Q consisting of $P_1, \ldots, P_{m-1}$ and let $Q \cap P_m$ be the subdivision $P_i \cap P_m$, $i = 1, \ldots, m-1$. Then

$$\mu(|P|) = \mu(|Q|) + \mu(P_m) - \mu(|Q \cap P_m|) = \mu(|Q|) + 1 - \mu(|Q \cap P_m|).$$

Now, since Q contains $m-1$ polytope, and since $Q \cap P_m$ consists of at most $(d-1)$-dimensional polytopes applying the induction conjecture we get

$$\mu(|Q|) = \sum_{k=0}^{d}(-1)^k f_k(Q), \quad \mu(|Q \cap P_m|) = \sum_{k=0}^{d}(-1)^k f_k(Q \cap P_m).$$

Now the faces of P are of the two kinds: some of them belong to Q (class I) and others don't (class II). Faces of class II are the faces of P_m that do not belong to $Q \cap P_m$. So by the result for P_m (case $m = 1$) we get

$$\sum_{F \text{ in class II}} (-1)^{\dim F} = 1 - \sum_{k=0}^{d}(-1)^k f_k(Q \cap P_m) = 1 - \mu(|Q \cap P_m|).$$

Finally,

$$\mu(|P|) = \sum_{k=0}^{d}(-1)^k f_k(Q) + \sum_{F \text{ in class II}} (-1)^{\dim F} = \sum_{k=0}^{d}(-1)^k f_k(P)$$

and the proof follows. $\square$

PROBLEMS.

1°. In particular, we get the *Euler - Poincaré formula*: if P is an n-dimensional polytope then $\sum_{k=0}^{n}(-1)^k f_k(P) = 1$.

2. Let P be a 3-dimensional polytope. We define the *curvature* $\kappa(v)$ at every vertex v as follows: let $F_1, \ldots, F_m$ be the facets of P containing v. We define $\kappa(v) = 1-$ sum of angles of F_i at v (normalized in such a way that the complete angle is 1). Prove the Gauss-Bonnet formula

$$\sum_v \kappa(v) = 2,$$

where the sum is taken over all vertices of P.

(32.4) Corollary. *Let $K \subset \mathbb{R}^n$ be a polyhedral cone with vertex 0. Then*

$$\sum_F (-1)^{\dim F} = 0,$$

where the sum is taken over all (non-empty) faces of K, unless $K = \{0\}$ when the sum is 1.

Proof. Let $H \subset \mathbb{R}^n$ be a hyperplane such that $H \cap K = \{0\}$. Suppose that H_+ is the halfspace that contains K. Let us choose a non-zero $u \in H_+$ and let $P = K \cap (H + u)$. Then there is the one-to-one correspondence between k-dimensional faces F of K and $(k-1)$-dimensional faces $F \cap (H + u)$ of P. Now we apply Theorem 32.3. $\square$

(32.5) Corollary. *Let $P \subset \mathbb{R}^n$ be a polyhedron and $H \subset G$ be its non-empty faces. Then*

$$(-1)^{\dim G} \sum_{H \subset F \subset G} (-1)^{\dim F} F = \begin{cases} 1 & \text{if } H = G, \\ 0 & \text{if } H \neq G. \end{cases}$$

Proof. Consider a section of P by a subspace orthogonal to H and passing through an interior point o of H. In the neighborhood of o we get a cone in the section whose faces are in one-to-one correspondence with the faces F. Now we apply Corollary 32.4. $\square$

Wednesday, March 20

---

33. Some Identities for Angles

PROBLEMS.

1°. Let K be a cone and $H \subset G$ be its faces. Then

$$\sum_F \beta(H, F)\gamma(F, G) = 1,$$

where the sum is taken over all faces F that contain H and contained in G.

Hint: Suppose that $\dim F = k$. Consider an $(n-k)$-dimensional subspace orthogonal to F and passing through an interior point of F. The intersection locally is a cone whose faces are in one-to-one correspondence with the faces F. Now apply Theorem 30.7.

2°. Let $K \subset \mathbb{R}^n$ be a cone with vertex 0 and such that $K \neq \{0\}$. Then

$$\sum_F (-1)^{\dim F - \dim K} \chi_F = \chi_{K^\circ},$$

where the sum is taken over all faces of K, χ_F is the indicator function of F and K° is the (relative) interior of K.

Hint: Take a point $p \in K$ and prove that unless it is in the relative interior of K the summands χ_F for F containing p annihilate each other; use Corollary 32.4.

3°. Consider the space $\mathbb{Z}(\mathcal{C})$ of all functions on $\mathbb{R}^n$ which are linear combinations with integer coefficients of the indicator functions of the cones in $\mathbb{R}^n$, cf. Convex Ring, Section 21. Let us define $J(x, y)$ on $\mathbb{R}^n \times \mathbb{R}^n$

$$J(x, y) = \begin{cases} 1 & \text{if } \langle x, y \rangle = 1, \\ 0 & \text{otherwise,} \end{cases}$$

and for an $f \in \mathbb{Z}(\mathcal{C})$ let $T(f) \in \mathbb{Z}(\mathcal{K})$ be the function on $\mathbb{R}^n$ defined as follows

$$T(f)(y) = \mu_x\Big(J(x, y) f(x)\Big),$$

where μ_x is the Euler characteristic of a function in x. Prove that T is a linear operator on $\mathbb{Z}(\mathcal{C})$ such that

$$T(\chi_K) = 1 - \chi_{K^*},$$

where K^* is the polar to K.

4°. Let K be a cone with vertex 0, $K \neq 0$. Then

$$(-1)^{\dim K} \chi_{-(K^*)^\circ} = \sum_F (-1)^{\dim F - \dim K} \chi_{F^*},$$

where the sum is taken over all non-empty faces F of K.

Hint: Take the identity of Problem 2. Apply the operator T to both sides of the identity.

5°. Let K be a cone. Prove a theorem of Sommerville:

$$\sum_F (-1)^{\dim K - \dim F} \beta(F, K) = \beta(0, K),$$

where the sum is taken over all faces of F of K. In particular, for $k=3$ we get a famous formula: the area of a spherical n-gon is $\frac{1}{2}\Big($ the sum of its angles $-\frac{(n-2)}{2}\Big)$. Note, that $(n-2)/2$ is the sum of angles of the plane n-gon.

Hint: Take the identity of Problem 4 for K^*. Now integrate this identity against the density $e^{-\pi\|x\|^2}$.

6°. Let $K \subset \mathbb{R}^n$, $K \neq \{0\}$ be a cone and let H, G be a pair of its faces such that $H \subset G$. Then

$$\sum_F (-1)^{\dim\, G - \dim\, F} \beta(H,F)\gamma(F,G) = \begin{cases} 1 & \text{if } H = G, \\ 0 & \text{if } H \neq G. \end{cases}$$

where the sum is taken over all faces F of K that contain H and contained in G.

Hint: Let us consider square matrices whose entries are indexed by pairs H, G of faces of K. In particular, we consider the following three matrices B and C and U:

$$B_{H,G} = \begin{cases} \beta(H,G) & \text{if } H \text{ is a face of } G, \\ 0 & \text{if } H \text{ is not a face of } G; \end{cases}$$

$$C_{H,G} = \begin{cases} \gamma(H,G) & \text{if } H \text{ is a face of } G, \\ 0 & \text{if } H \text{ is not a face of } G; \end{cases}$$

$$U_{H,G} = \begin{cases} 1 & \text{if } H \text{ is a face of } G, \\ 0 & \text{if } H \text{ is not a face of } G. \end{cases}$$

Problem 1 implies that $BC = U$. Therefore $U^{-1}BC = I$, there I is the identity matrix (provided U^{-1} exists). Corollary 32.5 implies now that U^{-1} exists and has the following structure

$$U^{-1}_{H,G} = \begin{cases} (-1)^{\dim\, G - \dim\, H} & \text{if } H \text{ is a face of } G, \\ 0 & \text{if } H \text{ is not a face of } G. \end{cases}$$

Now using Problem 5 prove that

$$(U^{-1}B)_{H,G} = (-1)^{\dim\, G - \dim\, H} \beta(H,G).$$

Now we get what we wanted.

The identities and their proofs are found in P. McMullen, Non-linear angle-sum relations for polyhedral cones and polytopes, *Math. Proc. Cambridge Philos. Soc.*, **78**(1975), 247–261.

Friday, March 22

---

34. Reciprocity for the Counting Valuation

(34.1) Theorem. *Let $\Lambda \subset \mathbb{R}^n$ be a lattice and let $P \subset \mathbb{R}^n$ be a lattice polytope such that $\dim P = d$. Let $p(m) = |mP \cap \Lambda|$ be the Ehrhart polynomial of P. Then $p(-m) = (-1)^d |mP^\circ \cap \Lambda|$ where m is a positive integer and P° is the relative interior of P.*

Proof. From the proof of Theorem 31.2 we can write $p(m) = \sum_F \rho(mF)\gamma(F, P)$, where ρ is the simple valuation from Section 27 and $\gamma(F, P)$ is the exterior angle of P at the face F. By the reciprocity for ρ (see Section 26) we get $\rho(-mF) = (-1)^{\dim F}\rho(mF)$, so

$$p(-m) = \sum_F (-1)^{\dim F}\rho(mF)\gamma(F, P).$$

Let us consider a point $u \in \Lambda$. Suppose this point belongs to the relative interior of a face H of P. Then it belongs to every face F containing H and the total weight of u is

$$\sum_{H \subset F} (-1)^{\dim F}\beta(H, F)\gamma(F, P) = \begin{cases} (-1)^{\dim P} & \text{if } H = P, \\ 0 & \text{if } H \neq P \end{cases}$$

by Problem 6, Section 33. □

PROBLEM.

1. Let P be a d-dimensional rational polytope. For $m \in \mathbb{N}$ we have

$$p(m) = \sum_{k=0}^{n} e_k(P, m) m^k,$$

where $e_k(P, m)$ is a periodic function of m (see Theorem 31.3). Therefore, by periodicity, we can define $e_k(P, m)$ for negative integers m and hence we can define $p(m)$ for negative integers m. Then $p(-m) = (-1)^d |mP^\circ \cap \Lambda|$.

Here is an application of the Ehrhart polynomial and reciprocity.

(34.2) Definitions. A *magic square* of size r and weight m is a non-negative integer $r \times r$ matrix x_{ij} such that $\sum_{i=1}^{r} x_{ij} = m$ for every j and $\sum_{j=1}^{r} x_{ij} = m$ for every i. The *Birkhoff Polytope* P_r is the set of $r \times r$ matrices (x_{ij}) (considered as points in $\mathbb{R}^{r^2}$) such that

$$\sum_{i=1}^{r} x_{ij} = 1 \ j = 1, \ldots, r; \quad \sum_{j=1}^{r} x_{ij} = 1 \ i = 1, \ldots, r; \quad x_{ij} \geq 0 \quad i, j = 1, \ldots, r$$

(such matrices are called *doubly stochastic*). Let σ be a permutation of the set $\{1, \ldots, r\}$. The *permutation matrix* x^σ is defined as follows:

$$x^\sigma_{ij} = \begin{cases} 1 & \text{if } \sigma(i) = j, \\ 0 & \text{if } \sigma(i) \neq j. \end{cases}$$

PROBLEM.

1°. Permutation matrices are doubly stochastic and the number of $r \times r$ permutation matrices is $r!$.

(34.3) Theorem. *The Birkhoff polytope P_r is an $(r-1)^2$-dimensional polytope with the vertices x^σ, where σ are permutations of $\{1, \ldots, r\}$.*

Proof. Suppose that we have chosen non-negative $x_{ij} : i, j = 1, \ldots, r-1$ such that the sum in every row and every column is strictly less than 1. Then the only way we can append x to a doubly stochastic matrix is by letting

$$x_{ir} = 1 - \sum_{j=1}^{r-1} x_{ij}, \ i = 1, \ldots, r-1, \quad x_{rj} = 1 - \sum_{i=1}^{r-1} x_{ij}, \ i = 1, \ldots, r-1$$

and

$$x_{rr} = -r + 2 + \sum_{ij=1}^{r-1} x_{ij}$$

If the numbers $x_{ij}, \ i, j = 1, \ldots, r-1$ are close to $1/r$ then x_{ij} for $i = r$ or $j = r$ are close to $1/r$ and hence positive. Thus P_r is indeed $(r-1)^2$-dimensional. Next, we observe that $P_r \subset I_{r^2}$, where $I_{r^2} = \{0 \le x_{ij} \le 1\}$ is the unit cube in $\mathbb{R}^{r^2}$. Since x^σ is a vertex of I_{r^2}, it has to be a vertex of P_r. Now it remains to show that there are no other vertices of P_r. We use induction on r. If $r = 1$, the result is clear. Suppose that $r > 1$. Let y be a vertex of P_r. We claim that at least $(r-1)^2 = r^2 - 2r + 1$ entries of y are zeros. Otherwise, the intersection of a $(r-1)^2$ dimensional subspace

$$\sum_{i=1}^{r} x_{ij} = 1, \ j = 1, \ldots, r \quad \sum_{j=1}^{r} x_{ij} = 1, \ i = 1, \ldots, r$$

with the subspace $x_{ij} = 0$ provided $y_{ij} = 0$ is at least 1-dimensional, so y can't be a vertex of P_r. Now we say that y should have at least $(r-1)$ zeros in some row (otherwise, the total number of zeros is at most $r(r-2) = r^2 - 2r$ which is short by 1). Then the remaining non-zero element in that row should be 1 (y is doubly stochastic) and hence all other elements in this column have to be zero. Let's remove the row and the column. We get an $(r-1) \times (r-1)$ doubly stochastic matrix which has to be a vertex of P_{r-1}. Now we apply the induction conjecture. □

(34.4) Corollary. *Let $p_r(m)$ be the number of magic squares of size r and weight m. Then $p_r(m)$ is a polynomial in m of degree $(r-1)^2$ and with constant term 1. So we can define its values for negative m. Then*

$$p(-1) = \ldots = p(-r+1) = 0 \quad \text{and} \quad p_r(-m-r) = (-1)^{r-1} p(m).$$

Proof. We observe that $p_r(m) = |mP_r \cap \mathbb{Z}^{r^2}|$. Since by Theorem 33.3 P_r is a lattice polytope of dimension $(r-1)^2$, Theorem 31.2 implies that $p_r(m)$ is the Ehrhart polynomial of degree $(r-1)^2$ with constant term 1. Reciprocity (Theorem 34.1) implies that

$$p(-m) = (-1)^{(r-1)}|mP_r^\circ \cap \mathbb{Z}^{r^2}|.$$

On the other hand, $|mP^\circ \cap \mathbb{Z}^{r^2}|$ is the number of strictly positive magic squares of weight m which is equal to the number of magic squares of weight $(m-r)$ (subtract 1 from every entry). In particular, this number is 0 for $m < r$, so $p(-1) = \ldots = p(-r+1) = 0$ and $p(-m) = (-1)^{(r-1)}p(m-r)$ for $m \geq r$ which is what is required. $\square$

PROBLEM.

1. Find $p_3(m)$.

We discuss briefly Ehrhart polynomial of a general valuation, say, ϕ. Let $P \subset \mathbb{R}^n$ be a polytope and let P° be its relative interior then the indicator function χ_{P° is in the Convex Ring $\mathbb{Z}(\mathcal{K})$, for example, we can write

$$\chi_{P^\circ} = \sum_F (-1)^{\dim\, P - \dim\, F}\chi_F,$$

where the sum is taken over all non-empty faces F of P (cf. Problem 2, Section 33). Therefore we may define $\phi(P^\circ)$, letting for example

$$\phi(P^\circ) = \sum_F (-1)^{\dim\, P - \dim\, F}\phi(F).$$

(34.5) Theorem. *Let $\Lambda \subset \mathbb{R}^n$ be a lattice and ϕ be a lattice-invariant valuation. Let $P \subset \mathbb{R}^n$ be a polytope and $mP = \{mx : x \in P\}$ for a positive integer m. Then $p(m) = \phi(mP)$ is a polynomial in m (the Ehrhart polynomial of valuation ϕ).*

Furthermore, the following reciprocity holds: let us consider $p^\circ(m) = \phi(mP^\circ)$ and $p_-(m) = \phi(m(-P))$, where $-P = \{-x : x \in P\}$. It follows that p° and p_- are polynomials and we have

$$p^\circ(m) = (-1)^{\dim\, P}p_-(-m).$$

We don't prove this theorem, but this is how we could prove it if we wanted to, see P. McMullen, Valuations and Euler-type relations on certain classes of convex polytopes, *Proc. London Math. Soc. (3)*, **35**(1977), 113–135.

PROBLEMS.

1. Let ϕ be a lattice-invariant valuation. For a polytope P let us define

$$\psi(P) = \sum_F (-1)^{\dim\, P - \dim\, F}\beta(F, P)\phi(F),$$

where the sum is taken over all non-empty faces F of P and $\beta(F,P)$ is the interior angle of P at F measured in the affine hull of P. Let us choose a lattice subspace in $\mathbb{R}^n$ and let $\mathcal{A} = \{A\}$ be the set of all lattice translates of this subspace. Then ψ is a simple valuation on the polytopes whose affine hull belongs to some $A \in \mathcal{A}$.

2. We have

$$\phi(P) = \sum_F \gamma(F,P)\psi(F),$$

where the sum is taken over all non-empty faces F of P.

3. Deduce Theorem 34.5 from Problems 1,2, Theorem 20.2 and Theorem 26.1.

Monday, March 25

---

35. Some Additional Insight into Valuations

We start with problems.

PROBLEMS.

1. Let us consider the standard integer lattice $\mathbb{Z}^n \subset \mathbb{R}^n$ with the standard orthonormal basis $e_1, \ldots, e_n$. For a lattice polytope $P \subset \mathbb{R}^n$ and a point $u \in \mathbb{Z}^n$ let us define a number $\epsilon(u,P) = \sum_{i=1}^{n} \epsilon_i(u,P)$, where

$$\epsilon_i(u,P) = \begin{cases} 1 & \text{if } u + te_i \in P \text{ and } u - te_i \notin P \text{ for each sufficiently small } t > 0, \\ -1 & \text{if } u - te_i \in P \text{ and } u + te_i \notin P, \text{ for each sufficiently small } t > 0 \\ 0 & \text{otherwise.} \end{cases}$$

Finally, let $b(P) = \sum_{u \in \mathbb{Z}^n} \epsilon(u,P)$. Prove that $b(P)$ is a lattice-invariant valuation. It is called the *boundary characteristic* of P since $\epsilon(u,P) = 0$ unless u is on the boundary of P. Interpret the Ehrhart polynomial and the reciprocity for the valuation b.

2. Let $\Lambda \subset \mathbb{R}^n$ be a lattice and $P_1, \ldots, P_k \subset \mathbb{R}^n$ be lattice polytopes. Prove that $|\Lambda \cap (m_1P_1 + m_2P_2 + \ldots + m_kP_k)|$ is a polynomial in non-negative integers $m_1, \ldots, m_k$. Here "+" denotes the Minkowski addition.

Hint: Use Theorem 23.4. That is, for every fixed $m_1, \ldots, m_{k-1}$ and polytopes $P_1, \ldots, P_{k-1}$, the value

$$\phi(P) = |\Lambda \cap \big((m_1P_1 + m_2P_2 + \ldots + m_{k-1}P_{k_1}) + P\big)|$$

is a valuation on lattice polytopes P.

3. Let us consider $\mathbb{R}^k \subset \mathbb{R}^n$ and $\mathbb{Z}^k \subset \mathbb{Z}^n$ and let p be the orthogonal projection of $\mathbb{R}^n$ onto $\mathbb{R}^k$. For a lattice polytope P let $\phi(P) = |\mathbb{Z}^k \cap p(P)|$ - the number of lattice

points in the projection of P. Then $\phi(P)$ is a lattice-invariant valuation (see Theorem 23.2), so there exists the Ehrhart polynomial of ϕ. Interpret the reciprocity for ϕ.

(35.1) Definitions. Let $L \subset \mathbb{R}^n$ be a linear subspace. We define an Abelian group $\Sigma(L)$ as follows: consider the linear space $\mathbb{R}(\mathcal{C})$ of all finite linear combinations with real coefficients of the indicator functions of cones from L and the subspace $\mathbb{R}_0(\mathcal{C})$ generated by the indicator functions of the cones K with dim $K <$ dim L. Now let $\Sigma(L) = \mathbb{R}(\mathcal{K})/\mathbb{R}_0(\mathcal{K})$. Finally, let $\Sigma(\mathbb{R}^n) = \bigoplus_{L \subset \mathbb{R}^n} \Sigma(L)$, where the direct sum is taken over all linear subspaces L in $\mathbb{R}^n$. The linear space $\Sigma(\mathbb{R}^n)$ is called the *cone group*.

Let $P \subset \mathbb{R}^n$ be a polytope and $F \subset P$ be its face. The cone $n(F, P)$ generated by the outer normals of of the facets of P that contain F is called the *exterior cone* of P at F. Note, that its measure is the exterior angle $\gamma(F, P)$. Consider a map σ which maps a polytope P into an element of $\Sigma(\mathbb{R}^n)$:

$$\sigma(P) = \sum_F \Big(\text{vol } F\Big)\chi_{n(F,P)},$$

where

- the sum is taken over all faces F of P;
- vol F is the volume of F measured in the affine hull of F;
- $\chi_{n(F,P)}$ is the indicator function of the exterior cone $n(F, P)$ represented by its class in $\Sigma(\mathbb{R}^n)$.

Here is a very powerful result:

(35.2) Theorem [McMullen]. *The map σ can be extended to a linear map $\sigma : \mathbb{R}(\mathcal{P}) \longrightarrow \Sigma(\mathbb{R}^n)$, where $\mathbb{R}(\mathcal{P})$ is the space of all finite linear combinations with real coefficients of the indicator functions of polytopes $P \subset \mathbb{R}^n$. Furthermore, the kernel of σ is generated by the functions $\chi_P - \chi_{P+t}$, where $P + t$ is a translation of P for some $t \in \mathbb{R}^n$.*

See P. McMullen, The polytope algebra, *Advances in Mathematics*, **78** (1989), 76–130; P. McMullen, Separation in the polytope algebra, *Beiträge zur Algebra und Geometrie*, **34**(1993), 15–30 and P. McMullen, *Valuations and dissections*, in: *Handbook of Convex Geometry*, North-Holland, Amsterdam, 1993, 933–988.

(35.3) Corollary. *Let $\Lambda \subset \mathbb{R}^n$ be a lattice and ϕ is a lattice invariant valuation. Then there exists a function ψ on the cones in $\mathbb{R}^n$ such that for every lattice polytope P*

$$\phi(P) = \sum_F \Big(\text{ vol } F\Big)\psi\big(n(F, P)\big).$$

Sketch of proof. Actually, it follows by, say, Hahn-Banach Theorem from Theorem 35.2 (extension of a linear function from a subspace). $\square$

Wednesday, March 27

Review

Friday, March 29

36. Exponential Sums

(36.1) Definitions. Let $P \subset \mathbb{R}^n$ be a set and $\mathbb{Z}^n \subset \mathbb{R}^n$ be the standard integral lattice. We let

$$s(P, c) = \sum_{x \in \mathbb{Z}^n \cap P} \exp\big\{\langle c, x\rangle\big\} \quad \text{for } c \in \mathbb{R}^n.$$

We call $s(P, c)$ an *exponential sum* and consider it as a function of c whenever the series converges. If it is possible to define an analytic continuation of $s(P, c)$ for $c \in \mathbb{C}^n$, we will do that. A similar object

$$s_\Lambda(P, c) = \sum_{x \in \Lambda \cap P} \exp\big\{\langle c, x\rangle\big\}$$

can be considered for an arbitrary lattice $\Lambda \subset \mathbb{R}^n$.

Let $u_1, \ldots, u_k \in \mathbb{Z}^n$ be linearly independent integer vectors. The cone

$$K = \operatorname{co}\{u_1, \ldots, u_k\} = \Big\{\sum_{i=1}^{k} \alpha_i u_i : \alpha_i \geq 0, i = 1, \ldots, k\Big\}$$

is called a *simple rational cone*. If $u_1, \ldots, u_k$ is a primitive set of vectors, then K is called a *primitive* or *unimodular* cone.

PROBLEMS.

1°. Let $n = 1$ and $K = [0, +\infty)$. Then

$$s(K, c) = \sum_{m=0}^{\infty} e^{mc} = \frac{1}{1 - e^c}$$

(for $c < 0$ the series converges). Therefore we let $s(K, c) = (1 - e^c)^{-1}$ for any complex $c \neq 2\pi i k,\ k \in \mathbb{Z}$.

2°. Suppose that we have three sets $A, B, C \subset \mathbb{R}^n$ such that for any $x \in C \cap \mathbb{Z}^n$ there exists a unique pair $y \in A \cap \mathbb{Z}^n$ and $z \in B \cap \mathbb{Z}^n$ such that $x = y + z$. Then $s(C, c) = s(A, c)s(B, c)$.

3°. Let $\mathbb{R}^n_+ = \{x = (x_1, \ldots, x_n) : x_i \geq 0, i = 1, \ldots, k\}$. Then

$$s(\mathbb{R}^n_+, c) = \prod_{i=1}^{n} \frac{1}{1 - \exp\{c_i\}},$$

where $c = (c_1, \ldots, c_n)$.

(36.2) Theorem. *Let $u_1, \ldots, u_k \in \mathbb{Z}^n$ be linearly independent vectors and $K = co\{u_1, \ldots, u_k\}$. Then*

$$s(K, c) = \Big(\sum_{x \in \Pi \cap \mathbb{Z}^n} \exp\{\langle c, x\rangle\}\Big) \prod_{i=1}^{k} \frac{1}{1 - \exp\{\langle c, u_i\rangle\}}, \tag{36.2.1}$$

where

$$\Pi = \Big\{ \sum_{i=1}^{k} \alpha_i u_1 : \ 0 \leq \alpha_i < 1 \Big\}$$

is the semi-open parallelepiped generated by $u_1, \ldots, u_k$. In particular, if K is primitive then

$$s(K, c) = \prod_{i=1}^{k} \frac{1}{1 - \exp\{\langle c, u_i\rangle\}}. \tag{36.2.2}$$

Let K° be the relative interior of K. Then

$$s(K^\circ, c) = \Big(\sum_{x \in \overline{\Pi} \cap \mathbb{Z}^n} \exp\{\langle c, x\rangle\}\Big) \prod_{i=1}^{k} \frac{1}{1 - \exp\{\langle c, u_i\rangle\}}, \tag{36.2.3}$$

where

$$\overline{\Pi} = \Big\{ \sum_{i=1}^{k} \alpha_i u_1 : \ 0 < \alpha_i \leq 1 \Big\}$$

is yet another semi-open parallelepiped generated by $u_1, \ldots, u_k$. In particular, if K is primitive then

$$s(K^\circ, c) = \exp\{\langle c, u\rangle\} \prod_{i=1}^{k} \frac{1}{1 - \exp\{\langle c, u_i\rangle\}}, \quad \text{where } u = u_1 + \ldots + u_k \tag{36.2.4}$$

Finally, for a simple rational k-dimensional cone K we have

$$s(K^\circ, -c) = (-1)^k s(K, c) \quad (\text{reciprocity}). \tag{36.2.5}$$

Proof. Let $x \in K \cap \mathbb{Z}^n$. Then $x = \sum_{i=1}^{k} \alpha_i u_i$ for some non-negative α_i. Since $u_1, \ldots, u_k$ are linearly independent, the numbers $\alpha_1, \ldots, \alpha_k$ are uniquely determined. If $x \in K^\circ \cap \mathbb{Z}^n$ then all the α's are positive.

First, we discuss (36.2.1). Let $\alpha_i = [\alpha_i] + \{\alpha_i\}$, where $[\cdot]$ is the integer and $\{\cdot\}$ is the fractional part of a number. Then $x = y + m$, where

$$y = \sum_{i=1}^{k} \{\alpha_i\} u_i \in \Pi \cap \mathbb{Z}^n \quad \text{and} \quad m = \sum_{i=1}^{k} [\alpha_i] u_i \in M,$$

where M is the set of all non-negative integer combinations of $m_1 u_1 + \ldots + m_k u_k$ (cf. Proof of Lemma 2.4). Therefore, every point $x \in K \cap \mathbb{Z}^n$ can be represented in the form $x = y + m$, where $y \in \Pi \cap \mathbb{Z}^n$ and $m \in M$. Therefore, $s(K, c) = s(\Pi, c) \cdot s(M, c)$. However, $s(M, c)$ is just the sum of the multiple geometric series

$$\sum_{m \in M} \exp\{\langle c, m \rangle\} = \Big(\sum_{m_1=0}^{+\infty} \exp\{\langle c, m_1 u_1 \rangle\} \Big) \cdots \Big(\sum_{m_k=0}^{+\infty} \exp\{\langle c, m_k u_k \rangle\} \Big)$$

$$= \prod_{i=1}^{k} \frac{1}{1 - \exp\{\langle c, u_i \rangle\}}$$

and the formula for $s(K, c)$ follows. If K is primitive, then Π contains a single integral point, that is 0 (see Theorem 4.3), so we get (36.2.2).

Next, we deduce (36.2.3). Let $x \in K^\circ \cap \mathbb{Z}^n$, so $x = \sum_{i=1}^{k} \alpha_i u_i$ for $\alpha_i > 0$. Let $\alpha_i = \{\alpha_i\}^+ + [\alpha_i]^+$, where $\{\alpha\}^+ = \{\alpha\}$ unless α is an integer when we have $\{\alpha\}^+ = 1$. Then $x = y + m$ where

$$y = \sum_{i=1}^{k} \{\alpha_i\}^+ u_i \in \overline{\Pi} \cap \mathbb{Z}^n \quad \text{and} \quad m = \sum_{i=1}^{k} [\alpha_i]^+ u_i \in M,$$

where M is defined as above. Furthermore, every point $x \in K^\circ \cap \mathbb{Z}^n$ can be uniquely represented as a sum $y + m$. Therefore $s(K, c) = s(\overline{\Pi}, c) s(M, c)$ and the proof follows. Finally, we remark that if $x \in \Pi$ then $u - x \in \overline{\Pi}$ where $u = u_1 + \ldots + u_k$ and vice versa. Therefore if K is primitive then $\overline{\Pi} \cap \mathbb{Z}^n$ consists of a single point u and (36.2.4) is proven. Finally, $x \in \Pi \cap \mathbb{Z}^n \iff u - x \in \overline{\Pi} \cap \mathbb{Z}^n$ implies that

$$\exp\{\langle c, u \rangle\} s(\overline{\Pi}, -c) = s(\Pi, c)$$

and (36.2.5) follows. $\square$

PROBLEMS.

1. Let us consider the set of all intervals $P = [a, b]$, where $b \geq a$ and $b, a \in \mathbb{Z}$ (we allow $b = +\infty$ and $a = -\infty$. Let us agree that $s(\mathbb{R}^1, c) \equiv 0$. Prove that $P \longmapsto s(P, c)$ is a valuation, that is $s(P_1 \cup P_2, c) = s(P_1, c) + s(P_2, c) - s(P_1 \cap P_2, c)$, provided $P_1 \cup P_2$ is an interval.

2. Let $K \subset \mathbb{R}^3$ be a cone generated by the vectors $(1, 1, 1)$, $(1, -1, 1)$, $(-1, 1, 1)$ and $(-1, -1, 1)$ and K° be its interior. Prove that $s(K^\circ, -c) = -s(K, c)$.

Hint: Represent K as a union of two simple cones whose intersection is a simple cone. Use (36.2.5)

3. Let $K = \text{co}\{u_1, \ldots, u_m\}$, where $u_i \in \mathbb{Z}^n$. Suppose that 0 is the vertex of K. Prove that for every $c \in (K^*)^\circ$ the series

$$\sum_{x \in K \cap \mathbb{Z}^n} \exp\{\langle c, x \rangle\}$$

converges and defines a meromorphic function on $\mathbb{C}^n$.

Hint: Subdivide K into simple cones and use inclusion - exclusion.

Monday, April 1

---

37. Exponential Sums over Polyhedral Sets

First, we rephrase formula (36.2.1) of Theorem 36.2. Let $K \subset \mathbb{R}^n$, $K = \text{co}\{u_1, \ldots, u_k\}$, where $u_i \in \mathbb{Z}^n$. Then there exists a meromorphic function (ratio of two entire functions) $s(K, c)$ defined on $\mathbb{C}^n$ except a discrete set of the hyperplanes $\langle c, u_j \rangle = 2\pi i m$, $m \in \mathbb{Z}^n$ such that

$$s(K, c) = \sum_{x \in \mathbb{Z}^n \cap K} \exp\{\langle c, x \rangle\}$$

for those c where the series converges (that is, for c from the interior of the polar K^*).

A general form of $s(K, c)$ is

$$s(K, c) = \Big(\sum_{x \in \Pi \cap \mathbb{Z}^n} \exp\{\langle c, x \rangle\} \Big) \prod_{i=1}^{k} \frac{1}{1 - \exp\{\langle c, u_i \rangle\}},$$

where Π is the fundamental parallelepiped generated by $u_1, \ldots, u_k$. We observe the following thing. Let us make a substitution $q_i = \exp\{c_i\}$. Then $s(K, c)$ is a rational function in $q_1, \ldots, q_n$:

$$s(K, c) = \Big(\sum_{x \in \Pi \cap \mathbb{Z}^n} q_1^{x_1} \cdots q_n^{x_n} \Big) \prod_{i=1}^{k} \frac{1}{1 - q_1^{u_{i1}} \cdots q_n^{u_{in}}},$$

where u_{ij} is the j-th coordinate of u_i.

(37.1) Definition. Let $c_1, \ldots, c_m \in \mathbb{Z}^n$ be a finite set of integer vectors and $a_1, \ldots, a_m$ be a set of integers. The set

$$P = \Big\{ x \in \mathbb{R}^n : \langle c_i, x \rangle \leq a_i : \ i = 1, \ldots, m \Big\}$$

is called a *rational polyhedron.* The set

$$K = \Big\{ x \in \mathbb{R}^n : \langle c_i, x \rangle \leq 0 : \ i = 1, \ldots, m \Big\}$$

is called a *rational cone.* A rational cone K is called *pointed* if and only if 0 is a vertex of K. In other words, if there exists a vector $c \in \mathbb{R}^n$ such that $\langle c, x \rangle < 0$ for every $x \in K \setminus \{0\}$.

We need a version of Weyl - Minkowski Theorem.

(37.2) Theorem. *A set $K \subset \mathbb{R}^n$ is a rational cone if and only if*

$$K = \Big\{ \sum_{i=1}^{k} \alpha_i u_i : \ \alpha_i \geq 0 \Big\}$$

for some $u_1, \ldots, u_k \in \mathbb{Z}^n$. In this case we write $K = \operatorname{co}\{u_1, \ldots, u_k\}$.

PROBLEMS.

1°. Let $K \subset \mathbb{R}^n$ be a rational cone and $L \subset K$ be a linear subspace with $\dim L > 0$. Then K is not pointed.

2. Let $K \subset \mathbb{R}^n$ be a cone such that if $L \subset K$ is a linear subspace then $L = \{0\}$. Prove that K is pointed.

3. Prove Theorem 37.2.

4. Let $P \subset \mathbb{R}^n$ be a (non-empty) rational polyhedron and $L \subset P$ be an affine subspace. If P contains a vertex, then $\dim L = 0$.

(37.3) Theorem. *Let $K = \operatorname{co}\{u_1, \ldots, u_k\}$, $u_i \in \mathbb{Z}^n \setminus \{0\}$ be a pointed rational cone. Then the series*

$$\sum_{x \in K \cap \mathbb{Z}^n} \exp\{\langle c, x \rangle\}$$

converges for an open set of $c \subset \mathbb{R}^n$ and defines (by analytic continuation) a meromorphic function $s(K, c)$ which is defined in $\mathbb{C}^n$ except, possibly, a discrete set of the hyperplanes $\{\langle c, u_i \rangle = 2\pi i m, \ m \in \mathbb{Z}\}$. A general form of $s(K, c)$ is

$$s(K, c) = \sum_{I \subset \{1, \ldots, k\}} p_I(c) \cdot \prod_{i \in I} \frac{1}{1 - \exp\{\langle c, u_i \rangle\}},$$

where the sum is taken over subsets of $\{1, \ldots, c\}$ and $p_I(c)$ are exponential polynomials

$$p_I(c) = \sum_{x \in S_I} \exp\{\langle c, x \rangle\}$$

for some finite subsets $S_i \subset \mathbb{Z}^n$.

Furthermore, the substitution $q_i = \exp\{c_i\}$ transforms $p_I(c)$ into polynomials $p_I(q) = \sum_{x \in S_I} q_1^{x_1} \cdots q_n^{x_n}$ and $s(K,c)$ into a rational function:

$$s(K,c) = \sum_{I \subset \{1,\ldots,k\}} p_I(q) \prod_{i \in I} \frac{1}{1 - q_1^{u_{i1}} \cdots q_n^{u_{in}}}.$$

Proof. The idea of the proof is to triangulate the cone K into simple rational cones and use Theorem 36.2. Since K is a pointed cone, there exists $c \in \mathbb{R}^n$ such that $\langle c, x \rangle < 0$ for every $x \in K \setminus \{0\}$. The last condition is equivalent to $\langle c, u_i \rangle < 0$ for $i = 1, \ldots, k$ (please check that). Then the vectors c from a small neighborhood $U \subset \mathbb{R}^n$ have this property. We are going to prove that for $c \in U$ the series converges.

Let us choose a rational vector $c \in U$. Multiplying, if necessary, by a positive integer, we may assume that $c \in \mathbb{Z}^n$. Let us consider the hyperplane $H = \{x \in \mathbb{R}^n : \langle x, c \rangle = 1\}$. Then H intersects every ray $[0, u_i)$ in some rational point v_i, so the intersection $H \cap K$ is a polytope $P = \mathrm{conv}\{v_1, \ldots, v_k\}$ with rational vertices . Multiplying $H_1 = mH$ onto a sufficiently large positive number we get an integer polytope $P_1 = K \cap H_1$ with the vertices $w_i = mv_i$ such that $K = \mathrm{co}\{w_1, \ldots, w_k\}$. Let us triangulate P_1 (see Theorem 18.5). Every simplex $\Delta_I = \mathrm{conv}\{w_i : i \in I\}$ gives rise to a simple rational cone $K_I = \mathrm{co}\{w_i : i \in I\}$. Then by the inclusion-exclusion we define $s(K,c)$ as a combination of $s(K_I, c)$ and use Theorem 36.2, formula (36.2.1) and the remark in the beginning of this section. $\square$

(37.4) Theorem. *Let $P \subset \mathbb{R}^n$ be a rational polyhedron with a vertex, say, v. Then the series*

$$\sum_{x \in P \cap \mathbb{Z}^n} \exp\{\langle c, x \rangle\}$$

converges for c from an open subset in $\mathbb{R}^n$ and defines (by analytic continuation) a meromorphic function $s(P,c)$ which is defined in $\mathbb{C}^n$, except possibly a discrete set of hyperplanes $\langle c, u_i \rangle = 2\pi i m$, $m \in \mathbb{Z}$ ($\{u_i\}$ is a finite set of vectors from $\mathbb{Z}^n$). A general form of $s(P,c)$ is

$$s(P,c) = \sum_{I \subset \{1,\ldots,k\}} p_I(c) \cdot \prod_{i \in I} \frac{1}{1 - \exp\{\langle c, u_i \rangle\}},$$

where the sum is taken over subsets of $\{1, \ldots, c\}$ and $p_I(c)$ are exponential polynomials

$$p_I(c) = \sum_{x \in S_I} \exp\{\langle c, x \rangle\}$$

for some finite subsets $S_i \subset \mathbb{Z}^n$. Furthermore, if $P + u$ is a translation of P onto an integer vector $u \in \mathbb{Z}^n$ then

$$s(P + u, c) = \exp\{\langle c, u \rangle\} s(P, c).$$

Proof. Let

$$P = \Big\{x \in \mathbb{R}^n : \langle c_i, x\rangle \le a_i,\ i = 1, \ldots, k\Big\}.$$

We consider $\mathbb{R}^n$ as a hyperplane $x_{n+1} = 1$ in $\mathbb{R}^{n+1}$. Let us consider a rational cone $K \subset \mathbb{R}^{n+1}$:

$$K = \Big\{(x, x_{n+1}) : \langle c_i, x\rangle - a_i x_{n+1} \le 0,\ x_{n+1} \ge 0\Big\}.$$

We claim that K is a pointed cone. Indeed, if $\{tz\}$, $z = (y, \alpha) \in \mathbb{R}^{n+1}$ is a line in K then we have

$$t \cdot \langle c_i, y\rangle - t(\alpha a_i) \le 0, \quad t\alpha \ge 0$$

for every $t \in \mathbb{R}$. This implies that $\alpha = 0$ and hence

$$\langle c_i, y\rangle = 0, \quad i = 1, \ldots, k.$$

If $x \in P$ then $x + ty \subset P$ is a straight line contained in P which contradicts to the fact that P has a vertex (see Problem 4, Section 37.2). Therefore by Theorem 37.3 there exists a function $s(K, \bar{c})$, where $\bar{c} = (c, \tau):\ c \in \mathbb{C}^n, \tau \in \mathbb{C}$. Let us choose $\bar{c}$ for which

$$\sum_{x \in K \cap \mathbb{Z}^{n+1}} \exp\{\langle \bar{c}, x\rangle\}$$

converges. Since K contains points with arbitrarily large positive x_{n+1}, we must have $\tau < 0$. Denoting $P_m = \{x : \langle c_i, x\rangle - m a_i \le 0 :\ i = 1, \ldots, k\}$ we get

$$s(K, \bar{c}) = \sum_{k=0}^{\infty} e^{\tau k} \sum_{x \in P_m \cap \mathbb{Z}^n} \exp\{\langle c, x\rangle\} = \sum_{k=0}^{\infty} q^k \sum_{x \in P_m \cap \mathbb{Z}^n} \exp\{\langle c, x\rangle\},$$

where $q = e^{\tau}$. Theorem 37.3 implies that this series defines a meromorphic function, $s(K, (c, q))$. Furthermore, in the hyperplane $q = 0$ we have $s(K, (c, 0)) = s(K_0, c)$, where $K_0 = P_0 = \{x \in \mathbb{R}^n : \langle c_i, x\rangle \le 0 :\ i = 1, \ldots, k\}$. Now we let

$$s(P, c) = \frac{\partial}{\partial q} s(K, (c, q))\Big|_{q=0}.$$

It remains to prove that $s(P + u, c) = \exp\{\langle c, u\rangle\} s(P, c)$ for any lattice vector u. Indeed, let us choose an open set $U \subset \mathbb{R}^n$ for which the series

$$\sum_{x \in P \cap \mathbb{Z}^n} \exp\{\langle c, x\rangle\}$$

converges. Then the series

$$\sum_{x \in (P+u) \cap \mathbb{Z}^n} \exp\{\langle c, x\rangle\} = \sum_{x \in P \cap \mathbb{Z}^n} \exp\{\langle c, x + u\rangle\} = \exp\{\langle c, u\rangle\} \sum_{x \in P \cap \mathbb{Z}^n} \exp\{\langle c, x\rangle\}$$

obviously converges. So we have $s(P+u,c)=\exp\{\langle c,u\rangle\}s(P,c)$ on an open set $c \in U \subset \mathbb{R}^n$, so we must have $s(P+u,c)=\exp\{\langle c,u\rangle\}s(P,c)$ everywhere (since $s(P+u,c)$ and $s(P,c)$ are meromorphic). $\square$

Wednesday, April 3

---

38. Solutions to Some Problems from the Second Set

Friday, April 5

---

39. The Main Theorem for Exponential Sums

PROBLEM.

1°. Let X be a set and $\mathcal{A}$ be a family of subsets $A \subset X$ closed under finite intersections: $A_1 \cap \ldots \cap A_m \in \mathcal{A}$ provided $A_1, \ldots, A_m \in \mathcal{A}$. Let $\nu : \mathcal{A} \longrightarrow G$ be a function with the values in an abelian group G such that the inclusion-exclusion is satisfied: if $A = \bigcup_{i=1}^{m} A_i$ then $\nu(A) = \sum_{i=1}^{m} \nu(A_i) - \sum_{1 \le i < j \le m} \nu(A_i \cap A_j) + \ldots + (-1)^{m-1}\nu(A_1 \cap \ldots \cap A_m)$ whenever $A, A_1, \ldots, A_m \in \mathcal{A}$. We agree that $\nu(\emptyset)=0$. Then ν can be extended to a finitely additive measure on the set of all finite unions $A = A_1 \cup \ldots \cup A_m$ simply by applying the above formula. Furthermore, ν can be extended to a linear function $\nu : \mathbb{Z}(\mathcal{A}) \longrightarrow G$ on the space $\mathbb{Z}(\mathcal{A})$ consisting of all finite linear combinations of the indicator functions χ_A with $A \in \mathcal{A}$.

(39.1) Theorem. *For every rational polyhedron $P \subset \mathbb{R}^n$ there exists a meromorphic function $s(P,c):\ c \in \mathbb{C}^n$ such that:*

(39.1.1)
$$s(P,c) = \sum_{x \in P \cap \mathbb{Z}^n} \exp\{\langle c,x\rangle\}$$

provided the series absolutely converges. In particular, if P is a polytope then $s(P,0)$ is the number $|P \cap \mathbb{Z}^n|$ of lattice points in P;

(39.1.2) *If $P_1, \ldots, P_m \subset \mathbb{R}^n$ are rational polyhedra and $P = \bigcup_{i=1}^{m} P_i$ is a rational polyhedron then $s(P,c) = \sum_{i=1}^{m} s(P_i,c) - \sum_{1 \le i<j \le m} s(P_i \cap P_j, c) + \ldots + (-1)^{m-1} s(P_1 \cap \ldots \cap P_m, c)$ (the valuation property);*

(39.1.3)
$$s(P+u,c) = \exp\{\langle c,u\rangle\}s(P,c),$$

where $P+u$ is a translation of P on a vector $u \in \mathbb{Z}^n$;
(39.1.4) *If P contains a straight line then $s(P,c)=0$.*

Proof. Theorem 37.4 states that for a rational polyhedron P with a vertex the series in (39.1.1) converges for each c from an open set $U \subset \mathbb{R}^n$ and defines a meromorphic function $s(P,c)$. Let us check (39.1.2) if P and $P_1,\ldots,P_m$ are rational polyhedra with vertices. Indeed, for every c from an open set $U \subset \mathbb{R}^n$ the series $\sum\limits_{x \in P \cap \mathbb{Z}^n} \exp\{\langle c,x\rangle\}$ converges (absolutely) and so does the corresponding series for every P_i and every intersection $P_{i_1} \cap \ldots \cap P_{i_k}$. Therefore, by the usual inclusion-exclusion argument (39.1.2) holds for each c from an open set in $\mathbb{R}^n$. Since $s(P,c)$ and $s(P_{i_1} \cap \ldots \cap P_{i_k}, c)$ are meromorphic, the formula (39.1.2) must hold for any $c \in \mathbb{C}^n$. Similarly, if $\sum\limits_{x \in P \cap \mathbb{Z}^n} \exp\{\langle c,x\rangle\}$ converges then the series

$$\sum_{x \in (P+u) \cap \mathbb{Z}^n} \exp\{\langle c,x\rangle\} = \sum_{x \in P \cap \mathbb{Z}^n} \exp\{\langle c,x+u\rangle\} = \exp\{\langle c,u\rangle\} \sum_{x \in P \cap \mathbb{Z}^n} \exp\{\langle c,x\rangle\}$$

also converges. So we have $s(P+u,c) = \exp\{\langle c,u\rangle\} s(P,c)$ for all c from an open set $U \subset \mathbb{R}^n$. Since $s(P,c)$ and $s(P+u,c)$ are both meromorphic, we must have (39.1.3) for any $c \in \mathbb{C}^n$. Now we are going to define $s(P,c)$ for a rational polyhedron P with a straight line. Let us represent $\mathbb{R}^n$ as a union of 2^n polyhedral cones $K_\epsilon = \{x=(x_1,\ldots,x_n) : \epsilon_i x_i \geq 0\}$, where $\epsilon = (\epsilon_1,\ldots,\epsilon_n)$ and $\epsilon_i \in \{-1,1\}$. Since $\bigcup K_\epsilon = \mathbb{R}^n$ we have $P = \bigcup_\epsilon (P \cap K_\epsilon)$. Since every cone K_ϵ does not contain a straight line, the polyhedron P_ϵ does not contain a straight line either, so P can be represented as a finite union of polyhedra without straight lines. Therefore by Problem 1 we can define $s(P,c)$ by the inclusion-exclusion (39.1.2) for any rational polyhedron P. Let's prove (39.1.3). If $P = \bigcup\limits_{i=1}^m P_i$ is a representation of a polyhedron P as a union of polyhedra without straight lines then $P+u = \bigcup\limits_{i=1}^m (P_i+u)$ is a similar representation of $P+u$. Since (39.1.3) holds for P_i it must hold for P.

It remains to prove (39.1.4). Suppose that P is a rational polyhedron, given by the inequalities, say $P = \{x : \langle c_i,x\rangle \leq a_i, i=1,\ldots,m\}$. If P contains a straight line, say $x+ty : y \neq 0, -\infty < t < \infty$ then we must have $\langle c_i,y\rangle = 0$ for $i=1,\ldots,m$. Therefore $L = \big\{x \in \mathbb{R}^n : \langle c_i,x\rangle = 0,\ i=1,\ldots,m\big\}$ is a non-zero linear subspace. Since $c_i \in \mathbb{Z}^n$, L is a lattice subspace (cf. Theorem 6.3), so it must contain a non-zero vector $u \in \mathbb{Z}^n$. Then $x \in P \Longrightarrow x+u \in P$. Therefore $P+u=P$ and $s(P,c) = \exp\{\langle c,u\rangle\} s(P,c)$. Since this holds for every c from an open dense set in $\mathbb{C}^n$ we may choose c such that $\langle c,u\rangle \neq 0$. Then we must have $s(P,c)=0$. $\square$

(39.2) Remark. Actually, we proved a little bit more. Let $\mathbb{Z}(\mathcal{P})$ be the space of all linear combinations of the characteristic functions χ_P for rational polyhedra P. Then there exists a linear function s taking its values in the space of meromorphic function on $\mathbb{C}^n$ such that (39.1.1)-(39.1.4) is satisfied (we substitute χ_P instead of P).

We are going to use this remark at some point.

Monday, April 8

---

40. Some Additional Discussion

Theorem 39.1 was proved by J. Lawrence, see J. Lawrence, Rational-function-valued valuations on polyhedra, in: *Discrete and Computational Geometry (New Brunswick, NJ, 1989/1990)*, 199–208, DIMACS Series in Discrete Mathematics and Theoretical Computer Science, **6**, Amer. Math. Soc., Providence, RI , 1991 and independently by A. Khovanskii and A. Pukhlikov, see A.G. Khovanskii and A.V. Pukhlikov, The Riemann-Roch theorem for integrals and sums of quasipolynomials on virtual polytopes, *Algebra i Analiz*, **4**(1992), no. 4, 188–216 (Russian), translated in *St. Petersburg Mathematical Journal*, **4**(1993), 789–812. We discuss the last step: extension $s(P,c)$ from rational polyhedra with vertices to arbitrary rational polyhedra and even to the *Algebra of Rational Polyhedra* $\mathbb{Z}(\mathcal{P}_{\mathbb{Q}})$ generated by the indicator functions of rational polyhedra $P \subset \mathbb{R}^n$, is some more details. Basically, we are going to prove the statement of Problem 1, Section 39 in this particular setting.

(40.1) Theorem. *Let $\mathbb{Z}(\mathcal{P}_{\mathbb{Q}})$ be the set of all finite integer combinations of the indicator functions χ_P of rational polyhedra $P \subset \mathbb{R}^n$. There exists a linear function $s : \mathbb{Z}(\mathcal{P}_{\mathbb{Q}}) \longrightarrow \Big\{$ meromorphic functions on $\mathbb{C}^n \Big\}$ such that $s(\chi_P) = s(P,c)$, where P is a rational polyhedron with a vertex.*

Proof. First, we prove the following: If $P_1, \ldots, P_m \subset \mathbb{R}^n$ are rational polyhedra with vertices then

$$\sum_{i=1}^m \alpha_i \chi_{P_i} = 0 \Longrightarrow \sum_{i=1}^m \alpha_i s(P_i, c) = 0. \tag{40.1.1}$$

We can exclude the cases of empty polyhedra P_i or $\alpha_i = 0$. Then every point of P_i must belong to some other polyhedron P_j. Let $X_i = \bigcup_{j \neq i} P_j$. Then we must have $P_i \subset X_i$ for $i = 1, \ldots, n$. For every non-empty subset $I \subset \{1, \ldots, m\}$ let $P_I = \bigcap_{i=1}^m P_i$. Using the inclusion-exclusion formula, we write

$$\chi_{X_i} = \sum_{I \subset \{1,\ldots,n\} \setminus \{i\}} (-1)^{|I|-1} \chi_{P_I}.$$

Multiplying both parts onto χ_{P_i} we get

$$\chi_{P_i} = \sum_{I \subset \{1,\ldots,n\} \setminus \{i\}} (-1)^{|I|-1} \chi_{P_{I \cup \{i\}}}.$$

Now, there exists a non-empty set U_i such that for every $c \in U_i$ the series $\sum_{x \in P_i \cap \mathbb{Z}^n} \exp\{\langle c, x \rangle\}$ converges to $s(P_i, c)$. Therefore the corresponding series converge for every $s(P_{I \cup \{i\}}, c)$ and we must have

$$\sum_{x \in P_i \cap \mathbb{Z}^n} \exp\{\langle c, x \rangle\} = \sum_{I \subset \{1,\ldots,n\} \setminus \{i\}} (-1)^{|I|-1} \sum_{x \in P_{I \cup \{i\}} \cap \mathbb{Z}^n} \exp\{\langle c, x \rangle\}$$

for every $c \in U_i$. Since P_I are rational polyhedra the series $\sum_{x \in P_{I \cup \{i\}} \cap \mathbb{Z}^n} \exp\{\langle c, x \rangle\}$ converges to $s(P_{I \cup \{i\}}, c)$ and by analytic continuation

$$s(P_i, c) = \sum_{I \subset \{1,\ldots,n\} \setminus \{i\}} (-1)^{|I|-1} s(P_{I \cup \{i\}}, c). \tag{40.1.2}$$

Furthermore, for every non-empty I there is some non-empty open set $U_I \subset \mathbb{R}^n$ such that

$$s(P_I, c) = \sum_{x \in P_I \cap \mathbb{Z}^n} \exp\{\langle c, x \rangle\}$$

for all $c \in U_I$. Multiplying the equation (40.1.1) by χ_{P_I} we get

$$\sum_{i=1}^{m} \alpha_i \chi_{P_{I \cup \{i\}}} = 0.$$

Now, since for $P_{I \cup \{i\}} \subset P_I$ for every i

$$s(P_{I \cup \{i\}}, c) = \sum_{x \in P_{I \cup \{i\}} \cap \mathbb{Z}^n} \exp\{\langle c, x \rangle\}$$

for all $c \in U_I$. Then

$$\sum_{i=1}^{m} \alpha_i \sum_{x \in P_{I \cup \{i\}} \cap \mathbb{Z}^n} \exp\{\langle c, x \rangle\} = 0$$

for all $c \in U_I$ and hence

$$\sum_{i=1}^{m} \alpha_i s(P_{I \cup \{i\}}, c) = 0. \tag{40.1.3}$$

Now by (40.1.2) and (40.1.3) we finally get (40.1.1). Identity (40.1.1) allows us to extend s by linearity by letting

$$s(f) = \sum_{i=1}^{n} \alpha_i s(P_i, c) \quad \text{for} \quad f = \sum_{i=1}^{n} \alpha_i \chi_{P_i}.$$

The final observation is that for any polyhedron P the indicator function χ_P is a finite linear combination of the indicator functions of χ_{P_i} with integer coefficients, where P_i are polyhedra with vertices (see construction of the cones K_ϵ in Theorem 39.1). □

There exists a continuous analogue of $s(P, c)$.

PROBLEM

1. With every polyhedron $P \subset \mathbb{R}^n$ (not necessarily rational) one can associate a meromorphic function $\sigma(P, c): \ c \in \mathbb{C}^n$ such that

a) $\sigma(P, c) = \int_P \exp\{\langle c, x\rangle\}\, dx$, whenever the integral converges. In particular, if P is a polytope, we get $\sigma(P, 0) = \text{vol}\, P$, so $\sigma(P, c)$ is an extension of the volume to unbounded polyhedra. If $K = \text{co}\{u_1, \ldots, u_n\}$ is a simple cone generated by linearly independent (not necessarily integral) vectors $u_1, \ldots, u_n$ then $\sigma(K, c) = |u_1 \wedge \ldots \wedge u_n| \prod_{i=1}^{n} \frac{1}{\langle -c, u_i\rangle}$;

b) $\sigma(P, c)$ satisfies the inclusion-exclusion principle, that is

$$\sigma(P, c) = \sum_{i=1}^{m} s(P_i, c) - \sum_{1 \leq i_1 < i_2 \leq m} s(P_{i_1} \cap P_{i_2}, c) + \ldots + (-1)^{m-1} s(P_1 \cap \ldots \cap P_m, c)$$

whenever $P = \bigcup_{i=1}^{m} P_i$ and $P_1, \ldots, P_m$ are polyhedra;

c) $\sigma(P + u, c) = \exp\{\langle c, u\rangle\} s(P, c)$ if $P + u$ is a translation of P by a vector $u \in \mathbb{R}^n$;

d) $\sigma(P, c) = 0$ if P contains a straight line;

e) Let $\mathbb{Z}(\mathcal{P})$ be the space of all finite linear combinations of χ_P with integer coefficients for polyhedra $P \subset \mathbb{R}^n$. Then there is a linear function $\sigma : \mathbb{Z}(\mathcal{P}) \longrightarrow \Big\{$ meromorphic functions on $\mathbb{C}^n \Big\}$, such that $\sigma(\chi_P) = s(P, c)$ for a polyhedron $P \subset \mathbb{R}^n$.

Hint: It is easy to prove the formula for simple cones as it reduces to the case $K = \mathbb{R}^n_+ = \{(x_1, \ldots, x_n) : x_i \geq 0, i = 1, \ldots, n\}$ by a non-degenerate linear transformation. It is then easy to extend $\sigma(K, c)$ to pointed cones by triangulating the cone K into simple cones. The main problem is to show that for any polyhedron P with a vertex the integral $\int_P \exp\{\langle c, x\rangle\}\, dx$ gives rise to a meromorphic function (our trick with representing P as a hyperplane section of a higher-dimensional cone doesn't seem to work here). We can do the following: find an open subset $U \subset \mathbb{R}^n$ such that $\int_P \exp\{\langle c, x\rangle\}\, dx$ converges for all

$c \in U$. Apply the Stokes formula to P and its facets $F_i : i = 1, \ldots, m$ with outer unit normals n_i to get

$$\int_P \exp\{\langle c, x\rangle\}\ dx = \frac{1}{\langle c, c\rangle} \sum_{i=1}^{m} \langle c, n_i\rangle \int_{F_i} \exp\{\langle c, x\rangle\}\ dy_i,$$

where dy_i is the Lebesgue measure on the affine hulls of the facets F_i. Proceed further with this decomposition, passing from facets to faces of codimension 2, 3 and so on, until we reach vertices. Obviously, we will end up with a meromorphic function.

Wednesday, April 10

---

41. Brion's Theorem

(41.1) Definitions. Let $K \subset \mathbb{R}^n$ be a cone an $p \in \mathbb{R}^n$ be a point. The translation $K_p = K + p$ is called a *cone with a vertex* p. Note that if K is a pointed cone, then the vertex of K_p is uniquely defined. Let $P \subset \mathbb{R}^n$ be a polyhedron and $v \in P$ be its vertex. Let us represent P as an intersection of halfspaces $P = \bigcap_{i=1}^{n} H_i^+$, where H_i^+ are closed halfspaces bounded by hyperplanes H_i. Let $K_v = \bigcap_{i: v \in H_i} H_i^+$. We call K_v the *cone of* P *at* v and denote sometimes by $\operatorname{cone}(P, v)$.

PROBLEMS.

1°. Prove that if K is a pointed cone then the vertex of $K + p$ is indeed determined uniquely.

2°. If P is a polyhedron and $v \in P$ its vertex then $\operatorname{cone}(P, v)$ is indeed a cone with vertex v.

3. Let $K \subset \mathbb{R}^n$ be a simple n-dimensional cone. Then K can be represented as the intersection of n closed halfspace in $\mathbb{R}^n$ with linearly independent normals to the boundary hyperplanes.

Hint: Use the Weyl - Minkowski Theorem, cf. Theorem 37.2.

4°. If $P \subset \mathbb{R}^n$ is a rational polyhedron which can be represented as the intersection of fewer than n halfspaces, then $s(P, c) = 0$.

Hint: If P is not empty then with every point it contains a straight line orthogonal to the normal vectors of the boundary hyperplanes.

(41.2) Lemma. *Let $K_p \subset \mathbb{R}^n$ be a simple rational n-dimensional cone with vertex p. Let $x \longmapsto 2p - x$ be the central symmetry with the center p and $-K_p^\circ$ denote the interior of the image of K (we call $-K_p^\circ$ the cone vertical to K_p). Then*

$$s(K_p, c) = (-1)^n s(-K_p^\circ, c)$$

(yet another reciprocity).

Proof. Let us represent K_p as an intersection of n closed halfspaces $K_p = \bigcap_{i=1}^{n} H_i^+$. Let H_i^- be the complementary open halfspaces, so $H_i^- = \mathbb{R}^n \setminus H_i^+$. Then $-K_p^\circ = \bigcap_{i=1}^{n} H_i^-$. For $\epsilon = (\epsilon_1, \ldots, \epsilon_n)$, where $\epsilon_i \in \{-, +\}$ let

$$K_p(\epsilon) = \bigcap_{i=1}^{n} H_i^{\epsilon_i} \quad \text{and} \quad \sigma(\epsilon) = |\{i : \epsilon_i = -\}|.$$

We are going to prove a more general statement, that is

$$s(K_p(\epsilon), c) = (-1)^{\sigma(\epsilon)} s(K, c).$$

We get our result when $\epsilon = (-, \ldots, -)$. We are going to use induction on $\sigma(\epsilon)$. If $\sigma(\epsilon) = 0$, the result is trivial. Suppose that $\sigma(\epsilon) \geq 1$ and let us choose an index j such that $\epsilon_j = -$. Consider $\overline{\epsilon} = (\overline{\epsilon_1}, \ldots, \overline{\epsilon_n})$, where $\overline{\epsilon_i} = \epsilon_i$ for $i \neq j$ and $\overline{\epsilon_j} = +$. Then $\sigma(\overline{\epsilon}) = \sigma(\epsilon) - 1$, so $s\big(K_p(\overline{\epsilon}), c\big) = (-1)^{\sigma(\epsilon)-1} s(K_p, c)$ by the induction conjecture. On the other hand,

$$K_p(\epsilon) = \bigcap_{i=1}^{n} H_i^{\epsilon_i} = \Big(\mathbb{R}^n \setminus H_j^+\Big) \bigcap \Big(\bigcap_{i \neq j} H_i^{\epsilon_i}\Big) = \Big(\mathbb{R}^n \bigcap \Big(\bigcap_{i \neq j} H_i^{\epsilon_i}\Big)\Big) \setminus \bigcap_{i=1}^{n} H_i^{\overline{\epsilon_i}}$$

$$= \Big(\bigcap_{i \neq j} H_i^{\epsilon_i}\Big) \setminus K_p(\overline{\epsilon}).$$

Therefore by Theorem 40.1 we have

$$s\big(K_p(\epsilon), c\big) = s\Big(\bigcap_{i \neq j} H_i^{\epsilon_i}, c\Big) - s\big(K_p(\overline{\epsilon}), c\big).$$

Now we claim that $s\Big(\bigcap_{i \neq j} H_i^{\epsilon_i}, c\Big) = 0$. Indeed, by representing $H_i^- = \mathbb{R}^n \setminus H_i^+$ we get the decomposition of the indicator function of the intersection into a linear combination of χ_P, where P is the intersection of at most $n-1$ halfspaces in $\mathbb{R}^n$. But any such a polyhedron, if non-empty, must contain a straight line (see Problem 4, Section 41.1) and we have $s(P, c) = 0$ by (39.1.4). So finally we get

$$s\big(K_p(\epsilon), c\big) = -s\big(K_p(\overline{\epsilon}), c\big) = (-1)^{\sigma(\epsilon)} s\big(K_p, c\big)$$

and the result follows.

(41.3) Lemma (Brion's Theorem for a simplex). *Let $\Delta \subset \mathbb{R}^n$ be a rational n-dimensional simplex with vertices $v_1, \ldots, v_{n+1}$. Let K_i be the cone of Δ at v_i. Then*

$$s(P, c) = \sum_{i=1}^{n+1} s(K_i, c).$$

Proof. Let us represent Δ as the intersection of $(n+1)$ closed halfspaces $\Delta = \bigcap_{i=1}^{n+1} H_i^+$. Then

$$s(\Delta, c) = s(\mathbb{R}^n, c) - s(\mathbb{R}^n \setminus \Delta, c) = -s\big(\mathbb{R}^n \setminus \Delta, c\big) = -s\big(\bigcup_{i=1}^{n+1} H_i^-, c\big),$$

where $H_i^- = \mathbb{R}^n \setminus H_i^+$. Furthermore by the inclusion-exclusion

$$s\big(\bigcup_{i=1}^{n+1} H_i^-, c\big) = \sum_{I \subset \{1, \ldots, n+1\}} (-1)^{|I|-1} s\big(\bigcap_{i \in I} H_i^-, c\big).$$

On the other hand, the indicator function of the intersection $\bigcap_{i \in I} H_i^-$ is a linear combination of the indicator functions of polyhedra which contain a straight line unless $|I| \geq n$. If $|I| = n+1$ then the intersection is empty. If, however $|I| = n$ then $\bigcap_{i \in I} H_i^- = -K_i^\circ$ for $i = \{1, \ldots, n\} \setminus I$, where $-K_i^\circ$ is the cone vertical to K_i. Therefore we get

$$s(\Delta, c) = \sum_{i=1}^{n+1} (-1)^n s(-K_i^\circ, c).$$

From Lemma 41.2 we get, however $s(-K_i^\circ, c) = (-1)^n s(K_i, c)$ and hence the result follows. $\square$

PROBLEMS.

1°. Let $\Delta \subset \mathbb{R}^n$ be a rational, not necessarily n-dimensional simplex. Then

$$s(\Delta, c) = \sum_{v \text{ is a vertex of } \Delta} s\big(\text{cone}(\Delta, v), c\big).$$

2°. Let $\Delta \subset \mathbb{R}^n$ be an n-dimensional rational simplex with the vertices $v_1, \ldots, v_{n+1}$. Let K_i be the cone of Δ at v_i. Then

$$s(\Delta^\circ, c) = \sum_{i=1}^{n+1} s(K_i^\circ, c),$$

where Δ° is the interior of Δ and K_i° is the interior of K_i.

3. Let $\Delta = \bigcap_{i=1}^{n+1} H_i^{\epsilon_i} \ : \ \epsilon_i \in \{-, 0, +\}$ be an intersection of $(n+1)$ hyperplanes (H_i^0) and halfspaces some of which are closed (H_i^+) and some are open (H_i^-). Let $k = |\{i : \epsilon_i = 0\}|$ be the number of hyperplanes. Suppose that all these hyperplanes and halfspaces are rational and that they are sufficiently generic so that $\dim \Delta = n - k$. For every vertex v of the closure $\overline{\Delta}$ let

$$K_v = \bigcap_{i:\ v \in \text{closure of } H_i^{\epsilon_i}} H_i^{\epsilon_i}.$$

Then

$$s(\Delta, v) = \sum_{v \text{ is a vertex of } \overline{\Delta}} s(K_v, c).$$

The following result was proven in M. Brion, Points entiers dans les polyèdres convexes, *Annales Scientifiques de l'École Normale Supérieure (4)*, **21**(1988), no. 4, 653–663;, see also M. Brion, Polyèdres et réseaux, *L'Enseignement Mathématique (2)*, **38**(1992), no. 1-2, 71–88.

(41.4) Theorem (Brion's Theorem, 1988.) *Let $P \subset \mathbb{R}^n$ be a rational polytope. Then*

$$s(P, c) = \sum_{v \text{ is a vertex of } P} s\big(\operatorname{cone}(P, v), c\big).$$

Proof. Let's triangulate P. Using the inclusion-exclusion, we express $s(P, c)$ as a linear combination of $s(\Delta, c)$:

$$s(P, c) = \sum_{\Delta} \epsilon_\Delta s(\Delta, c) \quad \epsilon_\Delta \in \{-1, 1\},$$

where Δ are the simplices of the triangulation. Now apply Lemma 41.3 and Problem 1 from Section 41.3 to every simplex of this triangulation:

$$s(\Delta, c) = \sum_{v \text{ is a vertex of } \Delta} s\big(\operatorname{cone}(\Delta, v), c\big).$$

Consider a vertex v of P. Then

$$\sum_{\Delta : v \in \Delta} \epsilon_\Delta s\big(\operatorname{cone}(\Delta, v), c\big) = s\big(\operatorname{cone}(P, v), c\big)$$

and the proof follows. $\square$

PROBLEM.

1 (Brion's Theorem, 1988). Prove that

$$s(P^\circ, c) = \sum_{v \text{ is a vertex of } P} s\big(\operatorname{cone}(P, v)^\circ, c\big),$$

where $^\circ$ denotes the relative interior.

Friday, April 12

---

42. Some Ramifications of Brion's Theorem

PROBLEMS.

1. Let $P \subset \mathbb{R}^n$ be a rational polyhedron. Then

$$s(P, c) = \sum_{v \text{ is a vertex of } P} s\big(\operatorname{cone}(P, v), c\big).$$

2. Let $P = \bigcap_{i=1}^{m} H_i^{\epsilon_i}$, where $\epsilon_i \in \{0, -, +\}$ and H_i^+ are closed halfspaces, H_i^- are open halfspaces and H^0 are hyperplanes. For a vertex v of the closure of P let $\operatorname{cone}(P, v) = \bigcap_{i: v \in \partial H_i^{\epsilon_i}} H_i^{\epsilon_i}$, where "$\partial$" stands for the boundary. Then

$$s(P, c) = \sum_{v \text{ is a vertex of } P} s\big(\operatorname{cone}(P, v), c\big).$$

3. Let $\sigma(P, c)$ be the function from Problem 1, Section 40.1. Then for any polyhedron $P \subset \mathbb{R}^n$ we have

$$\sigma(P, v) = \sum_{v \text{ is a vertex of } P} \sigma\big(\operatorname{cone}(P, v), c\big).$$

4. Let $\mathbb{Z}(\mathcal{P})$ be the $\mathbb{Z}$-module of all finite linear combinations with integer coefficients of the indicator functions of the polyhedra $P \subset \mathbb{R}^n$ and let $\mathbb{Z}(\mathcal{P}_1)$ be its submodule generated by the indicator function of polyhedra $P \subset \mathbb{R}^n$ that contain a straight line. Prove the following identity in the quotient module $\mathbb{Z}(\mathcal{P})/\mathbb{Z}(\mathcal{P}_1)$:

$$\chi_P = \sum_{v \text{ is a vertex of } P} \chi_{\operatorname{cone}(P,v)}$$

for any polyhedron $P \subset \mathbb{R}^n$.

5*. Let us fix k and consider the $\mathbb{Z}$-module $\mathbb{Z}(\mathcal{P}_k)$ generated by the indicator functions of polyhedra $P \subset \mathbb{R}^n$ that contain a k-dimensional affine space. Find an analogue of the identity from Problem 4 for the quotient $\mathbb{Z}(\mathcal{P})/\mathbb{Z}(\mathcal{P}_k)$.

Generally speaking, we have a *filtration* $\mathbb{Z} = \mathbb{Z}(\mathcal{P}_n) \subset \mathbb{Z}(\mathcal{P}_{n-1}) \subset \ldots \subset \mathbb{Z}(\mathcal{P}_k) \subset \mathbb{Z}(\mathcal{P}_{k-1}) \subset \ldots \subset \mathbb{Z}(\mathcal{P}_1) \subset \mathbb{Z}(\mathcal{P}_0) = \mathbb{Z}(\mathcal{P})$. Is there a "natural" isomorphism

$$\mathbb{Z}(\mathcal{P}) = \bigoplus_{k=1}^{n+1} \mathbb{Z}(\mathcal{P}_{k-1})/\mathbb{Z}(\mathcal{P}_k),$$

where we let $\mathbb{Z}(\mathcal{P}_{n+1}) = \{0\}$?

Hint: I suspect there is, or at least something close to it, cf. the identity of Problem 4, Section 33.

43. Totally Unimodular Polytopes

(43.1) Definition. Let $P \subset \mathbb{R}^n$ be a polytope. We say that P is *totally unimodular* if and only if the following conditions are satisfied:

- P is a lattice polytope, that is every vertex v of P is an integer point;
- for every vertex v of P the cone $K_v = \operatorname{cone}(P, v)$ of P at v is a translation of a unimodular cone $K_v - v$ (see Definition 36.1). So $K_v = v + \operatorname{co}\{u_1, \ldots, u_d\}$, where $u_1, \ldots, u_d \in \mathbb{Z}^n$ is a primitive set of vectors.

PROBLEM.

1. This is how a typical totally unimodular polytope arises:

Let A be $m \times n$ $(m > n)$ integer matrix such that every minor of A is either 0 or 1 or -1 (such a matrix is called *totally unimodular*). Suppose further that no linear combination of rows of A with non-negative coefficients is 0 (this makes sure that the set of solutions to the system $\{x \in \mathbb{R}^n : Ax \leq b\}$ of inequalities is bounded, that is a polytope).

a) Let $b \in \mathbb{Z}^n$ be an integer vector. Then $P_b = \{x \in \mathbb{R}^n : Ax \leq b\}$ is a lattice polytope (the inequalities are understood as component-wise inequalities).

b) Suppose P_b is an n-dimensional polytope and that on every vertex of P_b precisely n of the inequalities turn into equalities. Then P_b is a totally unimodular polytope.

Hint: Let $a_1, \ldots, a_n$ be the rows of A such that $\langle a_i, v\rangle = b_i$ for $i = 1, \ldots, n$. Since $a_1, \ldots, a_n$ are linearly independent and A is unimodular, we must have $|a_1 \wedge \ldots \wedge a_n| = 1$. Then $a_1, \ldots, a_n$ is a basis of $\mathbb{Z}^n$ and $\operatorname{cone}(P, v) = v + \operatorname{co}\{u_1, \ldots, u_n\}$, where $u_1, \ldots, u_n$ is the dual basis of $\mathbb{Z}^n : \langle u_i, a_j\rangle = \delta_{ij}$.

From the Brion's Theorem we get:

(43.2) Theorem. *Suppose that $P \subset \mathbb{R}^n$ is a totally unimodular polytope and* $\dim P = d$. *Let $v_1, \ldots, v_m$ be the vertices of P and let $u_{i1}, \ldots, u_{id} : i = 1, \ldots, m$ be the primitive set of vectors in $\mathbb{Z}^n$ such that* $\operatorname{cone}(P, v_i) = v_i + \operatorname{co}\{u_{i1}, \ldots, u_{id}\}$. *Then*

$$\sum_{x \in P \cap \mathbb{Z}^n} \exp\{\langle c, x\rangle\} = \sum_{i=1}^{m} \exp\langle c, v_i\rangle \prod_{j=1}^{d} \frac{1}{1 - \exp\{\langle c, u_{ij}\rangle\}}.$$

Proof. By Brion's Theorem 41.1 we have

$$s(P,c)=\sum_{i=1}^{m} s\big(\operatorname{cone}(P,v_i),c\big).$$

Since $\operatorname{cone}(P,v_i)=v_i+\operatorname{co}\{u_{i1},\ldots,u_{id}\}$ by 39.1.3 we have

$$s\big(\operatorname{cone}(P,v_i),c\big)=\exp\{\langle c,v_i\rangle\}s\big(\operatorname{co}\{u_{i1},\ldots,u_{id}\},c\big).$$

Since $u_{i1},\ldots,u_{id}$ are primitive, we use formula 36.2.2 for $s\big(\operatorname{co}\{u_{i1},\ldots,u_{id}\},c\big)$. □

(43.3) Definition. Let $x_1,\ldots,x_n$ be (complex) variables and t be yet another (complex) variable. Consider the function

$$f(t,x_1,\ldots,x_n)=\prod_{i=1}^{n}\frac{tx_i}{1-\exp\{-tx_i\}}.$$

It is easy to see that f is analytic in a neighborhood of the origin $x_1=\ldots=x_n=t=0$ and therefore there exists its Taylor series expansion in the origin. Let us group together all monomials that have degree k in t.

$$f(t,x_1,\ldots,x_n)=\sum_{k=0}^{+\infty}t^k\operatorname{td}_k(x_1,\ldots,x_n).$$

The polynomial $\operatorname{td}_k(x_1,\ldots,x_n)$ is called the k-th *Todd polynomial* in $x_1,\ldots,x_n$.

PROBLEMS.

1°. Prove that $\operatorname{td}_k(x_1,\ldots,x_n)$ is a symmetric homogeneous polynomial of degree k with rational coefficients.

2°. Compute td_0, td_1, td_2 and td_3.

(43.4) Theorem. *Let $P\subset\mathbb{R}^n$ be a totally unimodular d-dimensional polytope with the vertices $v_1,\ldots,v_m$. Suppose that $\operatorname{cone}(P,v_i)=v_i+\operatorname{co}\{u_{i1},\ldots,u_{id}\}$, for some primitive vectors $u_{i1},\ldots,u_{id}\in\mathbb{Z}^n$. Let us choose $c\in\mathbb{R}^n$ such that $\langle c,u_{ij}\rangle\neq 0$ for any $i,j: i=1,\ldots,m, j=1,\ldots,d$. In other words, c in not orthogonal to any edge of P. Then*

$$|P\cap\mathbb{Z}^n|=\sum_{i=1}^{m}\frac{1}{x_{i1}\cdots x_{id}}\sum_{k=0}^{d}\frac{y_i^k}{k!}\operatorname{td}_{d-k}(x_{i1},\ldots,x_{id}),$$

where $y_i=\langle c,v_i\rangle$ and $x_{ij}=-\langle c,u_{ij}\rangle$.

Proof. Obviously,

$$|P\cap\mathbb{Z}^n|=\lim_{t\longrightarrow 0}\sum_{x\in P\cap\mathbb{Z}^n}\exp\{\langle tc,x\rangle\}.$$

By Theorem 43.2 the last limit is equal to

$$\lim_{t \longrightarrow 0} \sum_{i=1}^{m} \exp\{ty_i\} \prod_{j=1}^{d} \frac{1}{1-\exp\{-tx_{ij}\}}$$

$$\lim_{t \longrightarrow 0} \frac{1}{t^d} \sum_{i=1}^{m} \exp\{ty_i\} \frac{1}{x_{i1}\cdots x_{id}} \prod_{j=1}^{d} \frac{tx_{ij}}{1-\exp\{-tx_{ij}\}}.$$

On the other hand, the sum after $\dfrac{1}{t^d}$ is an analytic function in t. So the limit is the coefficient in front of t^d in the Taylor expansion of the function

$$\sum_{i=1}^{m} \exp\{ty_i\} \frac{1}{x_{i1}\cdots x_{id}} \prod_{j=1}^{d} \frac{tx_{ij}}{1-\exp\{-tx_{ij}\}}$$

and the result follows. □

PROBLEMS.

1. Prove the following continuous analogue of Theorem 43.2. Suppose that $P \subset \mathbb{R}^n$ is a simple n-dimensional polytope with the vertices $v_1, \ldots, v_m$. That is, every vertex belongs to exactly n facets, or, equivalently, n edges. Let $u_{i1}, \ldots, u_{in}$ be the vectors of the edges from v_i. Then

$$\int_P \exp\{\langle c, x\rangle\}\ dx = \sum_{i=1}^{m} \exp\{\langle c, v_i\rangle\} |u_{i1} \wedge \ldots \wedge u_{in}| \prod_{j=1}^{n} \frac{1}{\langle -c, u_{ij}\rangle}.$$

2. Prove the continuous analogue of Theorem 43.4, known as the Gramm formula: if P is the polytope as above and $c \in \mathbb{R}^n$ is a vector which is not orthogonal to any edge of P then

$$\text{vol}\ P = \sum_{i=1}^{m} \frac{y_i^n}{n!} |u_{i1} \wedge \ldots \wedge u_{in}| \prod_{j=1}^{n} \frac{1}{x_{ij}},$$

where $y_i = \langle c, v_i\rangle$ and $x_{ij} = \langle -c, u_{ij}\rangle$.

3* (A. Khovanskii, A. Pukhlikov, 1992). Let $P = \big\{x \in \mathbb{R}^n : \langle c_i, x\rangle \le a_i : i = 1, \ldots, m\big\}$ be an n-dimensional totally unimodular polytope. Suppose that every $a_i \in \mathbb{Z}^n$ is primitive. Let $h = (h_1, \ldots, h_m)$ and $P_h = \big\{x \in \mathbb{R}^n : \langle c_i, x\rangle \le a_i + h_i : i = 1, \ldots, m\big\}$. If $\|h\|$ is small enough then P_h has the same "shape" as P and vol P_h is a polynomial in h. Prove the formula for the coefficients of the Ehrhart polynomial of P:

$$e_{d-k}(P) = \text{td}_k\Big(\frac{\partial}{\partial h_1}, \ldots, \frac{\partial}{\partial h_m}\Big) \text{vol}(P_h)\Big|_{h=0}.$$

See A.G. Khovanskii and A.V. Pukhlikov, The Riemann-Roch theorem for integrals and sums of quasipolynomials on virtual polytopes, *Algebra i Analiz*, **4**(1992), no. 4, 188–216 (Russian), translated in *St. Petersburg Mathematical Journal*, **4**(1993), 789–812.

Monday, April 15

---

44. Counting Lattice Points in an Integer Polytope

We begin with some problems.

PROBLEMS

1°. Let $P \subset \mathbb{R}^n$ be a d-dimensional totally unimodular polytope and let us define y_i and x_{ij} as in Theorem 43.4 . Then the k-th coefficient $e_k(P)$ of the Ehrhart polynomial of P can be written as

$$e_k(P) = \sum_{i=1}^{m} \frac{y_i^k}{k!} \frac{1}{x_{i1} \cdots x_{id}} \mathrm{td}_{n-k}(x_{i1}, \ldots, x_{id}).$$

2^*. Let $P \subset \mathbb{R}^n$ be an integer polytope. Then there exists an integer m such that mP can be subdivided into totally unimodular simplices.

See G. Kempf, F. Knudsen, D. Mumford and B. Saint-Donat, *Toroidal embeddings. I.*, *Lecture Notes in Mathematics*, **339**, Springer-Verlag, Berlin, 1973.

3. Let $\Delta = \big\{(x_1, \ldots, x_n) : 1 \geq x_1 \geq x_2 \geq \ldots \geq x_n \geq 0\big\}$. Then Δ is totally unimodular and its volume is $n!$.

4. Let $S = \{s_1, \ldots, s_n\}$ be a partially ordered set. Let us construct a polytope $P_S \subset \mathbb{R}^n$: $P_S = \big\{0 \leq x_i \leq 1 \text{ and } x_i \leq x_j \Leftrightarrow s_i \leq s_j\big\}$. Every extension of S to a total order $s_{i_1} \leq s_{i_2} \leq \ldots \leq s_{i_n}$ gives rise to a simplex $\Delta \subset P_S$: $0 \leq x_{i_1} \leq \ldots \leq x_{i_n} \leq 1$. The simplices Δ form a triangulation of P_S. In particular, the number of linear extensions of S to a total order is $n!\mathrm{vol}\, P_S$.

(44.1) Brion's Theorem for an integer simplex. Suppose we are given an integer polytope $P \subset \mathbb{R}^n$ and we want to compute $|P \cap \mathbb{Z}^n|$, the number of lattice points in P. Since every polytope can be triangulated, to count integer points in a given integral simplex is a sufficiently general problem. Let $\Delta \subset \mathbb{R}^n$ be an n-dimensional lattice simplex with the vertices, say, $v_1, \ldots, v_{n+1} \in \mathbb{Z}^n$. Suppose that $\mathrm{cone}(\Delta, v_i) = v_i + \mathrm{co}\{u_{i1}, \ldots, u_{in}\}$, for some integer vectors $u_{ij} \in \mathbb{Z}^n$. Let $K_i = \mathrm{co}\{u_{i1}, \ldots, u_{in}\}$ and let $\Pi_i = \Big\{\sum_{j=1}^{n} \alpha_j u_{ij} : 0 \leq \alpha_j < 1\Big\}$ be the fundamental parallelepiped generated by $u_{i1}, \ldots, u_{in}$. Brion's Theorem (see Theorem 41.4) implies

$$\sum_{x \in \Delta \cap \mathbb{Z}^n} \exp\{\langle c, x\rangle\} = \sum_{i=1}^{n+1} s\big(\mathrm{cone}(\Delta, v_i), c\big).$$

On the other hand, by (39.1.3)

$$s(\Delta, v_i) = \exp\{\langle c, v_i\rangle\} s(K_i, c)$$

and by Theorem 36.2

$$s(K_i, c) = \sum_{y \in \Pi_i \cap \mathbb{Z}^n} \exp\{\langle c, y\rangle\} \prod_{j=1}^{n} \frac{1}{1 - \exp\{\langle c, u_{ij}\rangle\}}.$$

In principle, we could apply the trick of Theorem 43.4 to get an expression $|\Delta \cap \mathbb{Z}^n|$ as $\lim\limits_{t \longrightarrow} s(P, tc)$, where c is a vector such that $\langle c, u_{ij}\rangle \neq 0$, that is c is not orthogonal to any edge of Δ.

PROBLEMS.

1°. Prove the formula

$$|\Delta \cap \mathbb{Z}^n| = \sum_{i=1}^{n+1} \frac{1}{x_{i1} \cdots x_{in}} \sum_{k+l+m=n} \frac{1}{k!} \frac{1}{l!} \langle c, v_i\rangle^k \sum_{y \in \Pi_i \cap \mathbb{Z}^n} \langle c, y\rangle^l \mathrm{td}_m(x_{i1}, \ldots, x_{in}),$$

where $x_{ij} = \langle c, u_{ij}\rangle$.

2°. Prove that the k-th coefficient $e_k(\Delta)$ of the Ehrhart polynomial is

$$e_k(\Delta) = \sum_{i=1}^{n+1} \frac{\langle c, v_i\rangle^k}{k!} \frac{1}{x_{i1} \cdots x_{in}} \sum_{m+l=n-k} \frac{1}{l!} \sum_{y \in \Pi_i \cap \mathbb{Z}^n} \langle c, y\rangle^l \mathrm{td}_m(x_{i1}, \ldots, x_{in}),$$

where $x_{ij} = \langle c, u_{ij}\rangle$.

(44.2) Decomposition of a cone into primitive cones. The main trouble of using the formulas of Section 44.1 is that they contain summations over potentially large sets $\Pi_i \cap \mathbb{Z}^n$, and, therefore, are not computationally efficient (we say that they have the *exponential complexity*). Let us call $|\Pi \cap \mathbb{Z}^n| = |u_1 \wedge \ldots \wedge u_n|$ the *index* of K, denoted $\mathrm{ind}(K)$. If $\mathrm{ind}(K) = 1$ then K is primitive. We want to find simpler formulas for $s(K, c)$. The immediate idea is to triangulate K into primitive cones but this does not necessarily work.

PROBLEMS.

1. Let $K = \mathrm{co}\{u_1, \ldots, u_n\}$ where $u_i \in \mathbb{Z}^n$ are linearly independent vectors. Prove that K can be triangulated into primitive cones.

Hint: Consider the fundamental parallelepiped $\Pi = \left\{\sum_{i=1}^{n} \alpha_i u_i \ : \ 0 \leq \alpha_i < 1\right\}$. If $\Pi \cap \mathbb{Z}^n = \{0\}$ then K is primitive. Otherwise, there is an $w \in \Pi \cap \mathbb{Z}^n$, $w \neq 0$. Consider the triangulation of K onto $K_i = \mathrm{co}\{u_1, \ldots, u_{i-1}, w, u_{i+1}, \ldots, u_n\}$. Prove that $\mathrm{ind}(K_i) < \mathrm{ind}(K)$.

2. Consider the cone $K \subset \mathbb{R}^2$ generated by $u_1 = (1,0)$ and $u_2 = (1,n)$. Prove that $\operatorname{ind}(K) = n$ and that K can not be subdivided in fewer than n primitive cones.

3. Consider the cone K in Problem 2 above. Prove that

$$K = K_1 - K_2 + K_3, \quad \text{meaning that} \quad \chi_K = \chi_{K_1} - \chi_{K_2} + \chi_{K_3}$$

where $K_1 = \operatorname{co}\{(1,0),(0,1)\}$, $K_2 = \operatorname{co}\{(0,1),(1,n)\}$ and $K_3 = tu_2 : \ t \geq 0$ are primitive cones and χ is the characteristic function.

4. This is how a rational plane cone can be triangulated into primitive cones: let $K = \operatorname{co}\{u_1, u_2\}$, where $u_1, u_2 \in \mathbb{Z}^2$. Consider the convex hull of the set $\big\{(K \cap \mathbb{Z}^n) \setminus \{0\}\big\}$. It is a polyhedron with finitely many vertices, including u_1 and u_2. Draw a straight line through the origin and every integer point on the boundary "between" u_1 and u_2. You got a triangulation onto primitive cones.

Hint: Cf. Problem 4, Section 2.5.

The fact that we need $O\big(\operatorname{ind}(K)\big)$ cones in the worst case means that the triangulation has the *exponential complexity.* However, Problem 3 inspires some hope.

(44.3) Theorem [Barvinok, 1993]. *Let us fix dimension n. Then for every simple rational cone K one can construct $O\big((\log \operatorname{ind}(K))^{O(1)}\big)$ primitive cones $K_i : i \in I$ such that*

$$K = \sum_{i \in I} \epsilon_i K_i : \quad \epsilon_i \in \{-1, 1\},$$

where the identity is understood as the identity for the characteristic functions. In particular,

$$s(K,c) = \sum_{i \in I} \epsilon_i s(K_i, c).$$

As a corollary: for every fixed n there exists a polynomial time algorithm for counting integral points in polytopes $P \subset \mathbb{R}^n$.

The idea of the proof. Let us consider the parallelepiped

$$\overline{\Pi} = \Big\{\sum_{i=1}^{n} \alpha_i : |\alpha_i| \leq \big(\operatorname{ind}(K)\big)^{-\frac{1}{n}}\Big\}.$$

Then $\overline{\Pi}$ is centrally symmetric convex compact set and $\operatorname{vol} \overline{\Pi} = 2^n$. Minkowski's Theorem (see Theorem 7.2) implies that there is a non-zero integer point $w \in \overline{\Pi}$. Let $K_i = \operatorname{co}\{u_1, \ldots, u_{i-1}, w, u_{i+1}, \ldots, u_n\}$. Then $\operatorname{ind}(K_i) = |u_1 \wedge \ldots \wedge u_{i-1} \wedge w \wedge u_{i+1} \wedge \ldots \wedge u_n| = |\alpha_i||u_1 \wedge \ldots \wedge u_n| \leq \big(\operatorname{ind}(K)\big)^{\frac{n-1}{n}}$. Furthermore,

$$K = \sum_{i=1}^{n} \epsilon_i K_i + \text{combination of faces } F \text{ of } K_i,$$

where $\epsilon_i = 1$ if the hyperplane H generated by $u_1, \ldots, u_{i-1}, u_{i+1}, u_n$ does not separate u_i and w and $\epsilon_i = -1$ if H separates u_i and w. It is easy to see that $\operatorname{ind}(F) \leq \operatorname{ind}(K_i) \leq \big(\operatorname{ind}(K)\big)^{\frac{n-1}{n}}$ for every face F of K_i. Let us iterate this construction. On the m-th iteration we get const^m of cones whose indices are at most $\big(\operatorname{ind}(K)\big)^{\frac{n-1}{n}^m}$. Therefore, to get unimodular cones we need $m = \log\log\operatorname{ind}(K)$ iterations of the above procedure. Then the number of cones we get is a polynomial in $\log\operatorname{ind}(K)$.

We note that this decomposition can be constructed "efficiently", that is, in polynomial time. The main problem is to find the vector w, but here we can use Lenstra's algorithm (see (17.6)). So the general counting algorithm looks as follows: first, we triangulate the polytope P onto integral simplices Δ. Then, for every simplex Δ of the triangulation and every vertex v of Δ we represent the cone $\operatorname{cone}(\Delta, v)$ as a combination $\sum \epsilon_i K_i$ of primitive cones K_i. Then we choose a vector c which is not orthogonal to any edge $u_{i1}, \ldots, u_{id}$ of K_i. Next, for every piece $v + K_i$, $\dim K_i = d$ we compute the value

$$\epsilon_i \frac{1}{x_{i1} \cdots x_{id}} \sum_{k=0}^{d} \frac{\langle c, v\rangle}{k!} \operatorname{td}_{d-k}(x_{i1}, \ldots, x_{id}), \quad \text{where } x_{ij} = -\langle c, u_{ij}\rangle.$$

Finally, we take the sum of all these expressions and get $|P \cap \mathbb{Z}^n|$. $\square$

Complete proof see in A.I. Barvinok, A polynomial time algorithm for counting integral points in polyhedra when the dimension is fixed, *Mathematics of Operations Research*, **19**(1994), 769–779.

Wednesday, April 17

---

45. Dual Primitive Decomposition

Let $K \subset \mathbb{R}^n$ be a cone. We recall that

$$K^* = \Big\{x \in \mathbb{R}^n : \langle x, y\rangle \leq 0 \quad \text{for all} \quad y \in K\Big\}$$

is called the *polar* of K. Recall that K^* is a cone and that $(K^*)^* = K$, cf. Problem 4, Section 30.3.

Let $\mathbb{Z}(\mathcal{P})$ be the $\mathbb{Z}$-module generated by the characteristic functions of all polyhedra in $\mathbb{R}^n$. We would like to extend the Euler characteristic μ to a linear function on $\mathbb{Z}(\mathcal{P})$ (recall from Section 21 that μ is defined on $\mathbb{Z}(\mathcal{K})$, the $\mathbb{Z}$-module generated by the characteristic functions of convex compact sets). Let $I_m = \Big\{x \in \mathbb{R}^n : |x_i| \leq m, \ i = 1, \ldots, n\Big\}$ be a cube. It is easy to see that for any $f \in \mathbb{Z}(\mathcal{P})$ and any $m \in N$ one has $f \cdot \chi_{I_m} \in \mathbb{Z}(\mathcal{K})$, so we may define $\mu(f \cdot \chi_{I_m})$. Now let

$$\mu(f) = \lim_{m \longrightarrow +\infty} \mu\big(f \cdot \chi_{I_m}\big).$$

PROBLEM.

1°. Prove that μ is a well-defined linear function on $\mathbb{Z}(\mathcal{P})$ and that $\mu(\chi_P) = 1$, where $P \subset \mathbb{R}^n$ is a non-empty polyhedron.

(45.1) Theorem.

(45.1.1) *Suppose that*

$$\alpha_1 \chi_{K_1} + \ldots + \alpha_m \chi_{K_m} = 0,$$

where $K_1, \ldots, K_m \subset \mathbb{R}^n$ *are cones. Then*

$$\alpha_1 \chi_{K_1^*} + \ldots + \alpha_m \chi_{K_m^*} = 0.$$

(45.1.2) *Let* $K = \text{co}\{u_1, \ldots, u_n\}$ *be a primitive* n*-dimensional cone. Then* K^* *is a primitive* n*-dimensional cone.*

(45.1.3) *Suppose that a cone* $K \subset \mathbb{R}^n$ *is such that* $\dim K < n$. *Then the cone* K^* *contains a straight line.*

Proof. Let us prove (45.1.1). Applying the Euler characteristic μ we get $\alpha_1 + \ldots + \alpha_m = 0$. Now we follow Problem 3, Section 33. Let us define a function

$$J(x, y) = \begin{cases} 1 & \text{if } \langle x, y \rangle = 1; \\ 0 & \text{otherwise,} \end{cases}$$

and a linear map $T : \mathbb{Z}(\mathcal{C}) \longrightarrow \mathbb{Z}(\mathcal{C})$ by letting

$$T(f)(y) = \mu_x \Big(J(x, y) f(x) \Big),$$

where μ_x is the Euler characteristic of a function in x and $\mathbb{Z}(\mathcal{C})$ is the $\mathbb{Z}$-module generated by the characteristic functions of cones in $\mathbb{R}^n$. We claim $T(\chi_K) = 1 - \chi_{K^*}$. Indeed,

$$\mu_x \Big(J(x, y) \chi_K(x) \Big) = \mu\big(\chi_{K \cap H_y}\big),$$

where $H_y = \{x \in \mathbb{R}^n : \langle x, y \rangle = 1\}$. So the intersection $K \cap H_y$ is either empty (then the Euler characteristic is 0) or a non-empty polyhedron, then the Euler characteristic is 1. It is equal to 1 if and only if there is an $x \in K$ such that $\langle x, y \rangle = 1$. Since $x \in K \Leftrightarrow \lambda x \in K$ for $\lambda > 0$ we get that $T(\chi_K)(y) = 1$ if and only if for some $x \in K$ we have $\langle x, y \rangle > 0$, or in other words, $y \notin K^*$. So $T(\chi_K) = 1 - \chi_{K^*}$ and T is well-defined as a linear map on $\mathbb{Z}(\mathcal{C})$. Applying T to the first equation in (45.1.1) and taking into account that $\alpha_1 + \ldots + \alpha_m = 0$ we get the second equation.

To prove (45.1.2) we note that if $K = \text{co}\{u_1, \ldots, u_n\}$, where $\{u_i\}$ is a basis of $\mathbb{Z}^n$ then $K^* = \text{co}\{u_1^*, \ldots, u_n^*\}$, where $\{u_j^*\}$ is the dual basis: $\langle u_i, u_j^* \rangle = \delta_{ij}$.

Finally, (45.1.3) holds since if $\dim K < n$ then K is contained in a hyperplane $H \subset \mathbb{R}^n$ and then K^* contains the line l that is the orthogonal complement to H. $\square$

Theorem 45.1 suggests a “dual” way to represent a given rational cone as a linear combination of primitive cones. It is especially useful if the cone is given as an intersection of halfspaces. Indeed, suppose we want to get a decomposition of the cone $K = \{x \in \mathbb{R}^n : \langle a_i, x\rangle \leq 0\}$, where $a_1, \ldots, a_m \in \mathbb{Z}^n$. We observe that $K^* = \mathrm{co}\{a_1, \ldots, a_m\}$, see Problem 3, Section 30.3. So we triangulate K^* into simple cones, then decompose them into a linear combination of primitive cones K_i^* as in Section 44.2:

$$K^* = \sum_{i \in I} \epsilon_i K_i^*.$$

Then we write

$$K = \sum_{i \in I} \epsilon_i K_i,$$

where $K_i = (K_i^*)^*$. In the corresponding decomposition

$$s(K, c) = \sum_{i \in I} \epsilon_i s(K_i, c)$$

we ignore all K_i for which dim $K_i^* < n$ as those K_i contain a straight line. The remaining cones K_i are primitive by Theorem 45.1.

Friday, April 19

---

46. Solutions to Some Problems from the Third Set

Monday, April 22

---

47. Ehrhart Polynomial Revisited

(47.1) Lemma. *Let $K \subset \mathbb{R}^n$ be a rational cone and let $c \in \mathbb{C}^n$ be a regular point of $s(K, c)$. Then the function $f(t) = s(K, tc)$, $t \in \mathbb{C}$ has a pole at $t = 0$ of order at most n.*

Proof. If $K = \mathrm{co}\{u_1, \ldots, u_k\}$ is a simple rational cone then

$$t^k s(K, tc) = \sum_{x \in \Pi \cap \mathbb{Z}^n} \exp\{\langle tc, x\rangle\} \prod_{i=1}^{k} \frac{t^k}{1 - \exp\{t\langle c, u_i\rangle\}}$$

and we have seen (cf. Definition 43.3 and Theorem 43.4) that this expression is regular at $t = 0$. For an arbitrary rational cone K the result follows since K can be subdivided into simple cones. □

Let $P \subset \mathbb{R}^n$ be an n-dimensional integral polytope. For a vertex v of P let $K_v = \mathrm{cone}(P, v) - v$. So K_v is a translation of the cone of P at v to the origin. Let $a_{-k}(K_v, c)$ be the coefficient of t^{-k} in the Laurent expansion of $s(K_v, tc)$ at $t = 0$.

(47.2) Corollary. *Let $P \subset \mathbb{R}^n$ be an integer polytope. For $m \in \mathbb{N}$ the number $|mP \cap \mathbb{Z}^n|$ of integer points in mP is a polynomial in m (the Ehrhart polynomial of P) of degree at most n. The k-th coefficient $e_k(P)$ of this polynomial can be expressed as*

$$e_k(P) = \frac{1}{k!} \sum_{v \text{ is a vertex of } P} \langle c, v\rangle^k a_{-k}(K_v, c),$$

where $c \in \mathbb{R}^n$ is any vector which is not orthogonal to any edge of P.

We note that for any $m \in \mathbb{N}$ we have $\operatorname{cone}(P, v) - v = \operatorname{cone}(mP, mv) - mv$. Applying Brion's Theorem (see Theorem 41.4) we get

$$\sum_{mP \cap \mathbb{Z}^n} \exp\{t\langle c, x\rangle\} = \sum_{v \text{ is a vertex of } P} \exp\{\langle mv, ct\rangle\} s(K_v, tc).$$

Taking the limit as $t \longrightarrow 0$ we get

$$|mP \cap \mathbb{Z}^n| = \sum_{v \text{ is a vertex of } P} \sum_{k=0}^{n} \frac{\langle mv, c\rangle^k}{k!} a_{-k}(K_v, c).$$

The proof now follows. $\square$

To get the reciprocity for the Ehrhart polynomial we need a reciprocity for functions $s(K, c)$. We discussed it for simple rational cones in Theorem 36.2 and Lemma 41.2. For a general rational cone it can be obtained from triangulation but we prefer a more straightforward way.

PROBLEMS.

1. Let $P \subset \mathbb{R}^n$ be a polytope and let P° be its relative interior. Then $\mu(P^\circ) = (-1)^{\dim P}$, where μ is the Euler characteristic and as usual we identify a set with its characteristic function.

Hint: We have $\mu(P^\circ) = \mu(P) - \mu(|\partial P|)$, where $|\partial P|$ is the boundary of P. Now use Lemma 32.2.

2. Let $P \subset \mathbb{R}^n$ be an unbounded polyhedron with a vertex and let P° be its relative interior. Then $\mu(P^\circ) = 0$.

Hint: Let v be a vertex of P. Let $c \in \mathbb{R}^n$ be a vector such that the function $\langle c, x\rangle$ attains its maximum on P at v and $\inf\{\langle c, x\rangle : x \in P\} = -\infty$. We have $\mu(P^\circ) = \mu(P) - \mu(|\partial P|)$, where $|\partial P|$ is the boundary of P. Let us slice P and $|\partial P|$ into level sets of the function $\langle c, x\rangle$ and use the construction of Theorem 21.2.

(47.3) Theorem. *Let $K \subset \mathbb{R}^n$ be an n-dimensional pointed cone and let K° be its interior. Let $-K^\circ = \{-x : x \in K^\circ\}$ and let * denote the polar of a cone. Then*

$$\chi_{-K^\circ} = \sum_{F \subset K^*} (-1)^{\dim F} \chi_{F^*},$$

where the sum is taken over all non-empty faces F of K^*, including the cone K^* itself.

Proof. Let $\mathbb{Z}(\mathcal{C})$ be the $\mathbb{Z}$-module generated by the characteristic functions of cones. Consider the linear map $T : \mathbb{Z}(\mathcal{C}) \longrightarrow \mathbb{Z}(\mathcal{C})$ defined in Theorem 45.1, so $T(f)(y) = \mu_x\Big(J(x,y)f(x)\Big)$, where

$$J(x,y) = \begin{cases} 1 & \text{if } \langle x,y\rangle = 1, \\ 0 & \text{otherwise.} \end{cases}$$

Let $C \subset \mathbb{R}^n$ be a pointed n-dimensional cone and C° be its relative interior. We claim that

$$T\big(\chi_{C^\circ}\big) = (-1)^{\dim\, C-1}\chi_{(-C^*)^\circ}. \tag{47.3.1}$$

Indeed, let $f = T\big(\chi_{C^\circ}\big)$. Then $f(y) = \mu\big(C^\circ \cap H_y\big)$, where $H_y = \{x : \langle x,y\rangle = 1\}$ is a hyperplane. From Problems 1 and 2, Section 47.1 it follows that $f(y) \neq 0$ if and only if $C^\circ \cap H_y$ is non-empty and bounded. Then $f(y) = (-1)^{\dim\, C-1}$ and we must have $y \in -(C^*)^\circ$. So (47.3.1) is proven. Now Corollary 32.5 implies that

$$C^\circ = \sum_{F \subset C} (-1)^{\dim\, F - \dim\, C}, \tag{47.3.2}$$

where the sum is taken over all non-empty faces F of C. Now let us apply (47.3.2) to $C = K^*$ and then apply the transformation T and (47.3.1). This gives us the desired identity. $\square$

PROBLEM.

1. Let P be a polytope and $F \neq P$ be a non-empty face of P. Let us define $\operatorname{cone}(P,F)$ as follows: suppose that $P = \bigcap_{i=1}^{m} H_i^+$, where H_i^+ are closed halfspaces bounded by hyperplanes H_i, then $\operatorname{cone}(P,F) = \bigcap_{i: F \subset H_i} H_i^+$. Prove that

$$\chi_P = (-1)^{\dim\, P} + \sum_{F \neq P} (-1)^{\dim\, F}\chi_{\operatorname{cone}(P,F)},$$

where the sum is taken over all non-empty faces F of P such that $F \neq P$.

Remark: This is a generalization of the identity

$$P = \sum_{v \text{ is a vertex of } P} \operatorname{cone}(P,v) \quad \text{modulo polyhedra with straight lines,}$$

the underlying identity for Brion's Theorem.

(47.4) Corollary. *Let $K \subset \mathbb{R}^n$ be a rational cone and K° be its relative interior. Then*

$$s(K^\circ, c) = (-1)^{\dim\, K} s(K, -c).$$

Proof. Without loss of generality we assume that K is pointed and $\dim K = n$. Consider the decomposition of Theorem 47.3. Then F^* contains a straight line unless $F = K^*$ and then $F^* = K$. Since $s(P, c) = 0$ if P contains a straight line we get that $s(-K^\circ, c) = (-1)^n s(K, c)$. Since $s(-K^\circ, c) = s(K^\circ, -c)$, the proof follows. □

PROBLEM

1. Deduce the reciprocity law for the Ehrhart polynomial (see Theorem 34.1) from Corollary 47.4.

48. Beyond Polyhedra

To count lattice points in a convex body which is not a polyhedron generally is a very difficult problem. Here's one example, suggested by R. Kannan.

(48.1) Theorem (Jacobi's formula). *For a positive integer n the number of integer solutions to the equation $x_1^2 + x_2^2 + x_3^2 + x_4^2 = n$ is*

$$8 \sum_{d|n,\ d \not\equiv 0 \pmod 4} d,$$

where the sum is taken over all divisors of n that are not divisible by 4.

See D. Mumford, *Tata lectures on theta*, Boston, Birkhäuser, 1983. Suppose one can efficiently count integer points in a 4-dimensional ball
$B_n = \{(x_1, x_2, x_3, x_4) : x_1^2 + x_2^2 + x_3^2 + x_4^2 \leq n\}$. Then one can crack the famous RSA cryptosystem. That cryptosystem is based on the presumption that given a number n which is a product of two large primes p and q, it is difficult to compute the decomposition $n = pq$. Now, if we can count integer points in a ball, we can compute the number $|B_n \cap \mathbb{Z}^4| - |B_{n-1} \cap \mathbb{Z}^4|$, that is the number of integer solutions to the equation $x_1^2 + x_2^2 + x_3^2 + x_4^2 = n$. On the other hand, by Theorem 48.1 this number is just $8(1 + p + q + pq) = 8(1 + p + q + n)$. If we know the product $pq = n$ and the sum $p + q$ we can find p and q.

PROBLEMS.

1*. Suppose we can count integer points in a given 4-dimensional ball. Is it possible then to construct an algorithm for factorization of a given number into the product of primes?

2*. Suppose we have an algorithm for counting integer points in a 2-dimensional disc $\{(x, y) : x^2 + y^2 \leq n\}$. Is it possible to construct an algorithm for the primality testing problem (given a number, decide if it is prime).

3*. What is the complexity status of the counting problem in, say, 4-dimensional ball?

Remark: It is not known to be NP-hard or $\#P$-complete.