Notes for Math 669

Yiwei Fu, Instructor: Alexander Barvinok

FA 2022

Contents

Office hours:

Chapter 1

Introduction to Lattices

1.1 Definition

Definition 1.1.1. A lattice $\Lambda \subset V$ is a discrete additive group.

1.2 Lattice and Its Basis

Last time: $L \in V$ is a subspace if $L = \operatorname{span}(L \cap \Lambda)$

Theorem 1.2.1. *If L is a lattice subspace, $L \neq V$, then $\exists u \in L \setminus \Lambda$ such that $d(u, L) \leq d(x, L)$ for all $x \in L \setminus \Lambda$.*

Say $L \in \operatorname{span}\{u_1, \ldots, u_m\}$ linearly independent vectors, $\Pi = \{\}$ There is $u \in \Lambda \setminus L$ such that $\operatorname{dist}(u, \Pi) \leq \operatorname{dist}(x, \Pi)$ for all $x \in \Lambda \setminus L$.

Proof. Take $\rho > 0$ large enough. Consider $\Pi_\rho = \{y, d(y, \Pi) \leq \rho\}$. It contains points from $\Lambda \setminus L$, choose the one in $\Pi_\rho \cap (\Lambda \setminus L)$ closet to Π. ■

<u>CLAIM</u> $u \in \Lambda \setminus L$ is what we need. Why? Pick any $x \in \Lambda \setminus L$. Let $y \in L$ be the closest to x.

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

$$y = \sum_{i=1}^{m} d_i u_i$$

Let $w = \sum_{i=1}^{m} \lfloor \alpha_i \rfloor u_i \in \Lambda \setminus L, y - w = \sum_{i=1}^{m} \{\alpha_i\} u_i \in \Pi$.

Theorem 1.2.2. *Every lattice has a basis.*

Proof. By induction on $n = \dim V$.

Base case: for $n = 1$, we have $V = \mathbb{R}$.

Let $u > 0$ be the lattice vector closet to 0, among all positive vectors in Λ.

Then u is a basis of Λ. Pick any $v \in \Lambda$. Assume $v > 0$ WLOG. Then $v = \alpha u$ for $\alpha > 0$. If $\alpha \in \mathbb{Z}$ then we are done. If not, consider $w = \alpha u - \lfloor \alpha \rfloor u = \{\alpha\} u$, this is closer to 0 than u, a contradiction.

Induction hypothesis: suppose any lattice of dimension $n - 1$ has a basis.

Induction step: pick a lattice hyperplane H (lattice subspace with $\dim = n - 1$). Then $\Lambda_1 = H \cap \Lambda$ has a basis $u_1, \ldots, u_{n-1}$. Pick u_n such that $u_n \notin H$ and $\operatorname{dist}(u_n, H)$ is the smallest. We claim that $u_1, \ldots, u_{n-1}, u_n$ is a basis of Λ.

Let $u \in \Lambda$, $u = \sum_{i=1}^{n} \alpha_i u_i$ with $\alpha_i \in \mathbb{R}$. If $\alpha_n = 0$ then $u \in \Lambda_1$, then $\alpha_1, \ldots, \alpha_{n-1} \in \mathbb{Z}$. Suppose $\alpha_n \neq 0$. Consider $w = u - \lfloor \alpha_n \rfloor u_n$. $w \in \Lambda$ and $w = \{\alpha_n\} u_n + \sum_{i=1}^{n-1} \alpha_i u_i$. So

$$\operatorname{dist}(w, H) = \operatorname{dist}(\{\alpha_n\} u_n, H) = \{\alpha_n\} \operatorname{dist}(u_n, H)$$

If $\{\alpha_n\} > 0$ then $0 < \operatorname{dist}(w, H) < \operatorname{dist}(u_n, H)$, a contradiction.

So $\{\alpha_n\} = 0 \implies \alpha_n \in \mathbb{Z}$. Then $w = \sum_{i=1}^{n-1} \alpha_i u_i \implies \alpha_1, \ldots, \alpha_{n-1} \in \mathbb{Z}$.

So we have constructed a basis for lattice of dimension n, thus finishing the proof. ■

This is called A.N.Korkin(e)-Zolotarev(öff) basis.

<u>Exercise</u> Suppose $u_1, \ldots, u_n \in V$ is a basis of subspace. The integer combinations form a lattice.

<u>Exercise</u> Suppose a 2-dimensional lattice. Then there exists a lattice basis u, v such that the angle α between u, v satisfies $\frac{\pi}{3} \leq \alpha \leq \frac{\pi}{2}$.

<u>Exercise</u> If Λ is a lattice and L is a lattice subspace. The orthogonal projection $\mathrm{PR} : V \to L^{\perp}$. Then $\mathrm{PR}(\Lambda) \subset L^{\perp}$ is a lattice.

Definition 1.2.1. Suppose $u_1, \ldots, u_n$ be a basis of Λ.

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

is the *fundamental parallelepiped* of a fundamental parallelepiped of Λ.

Theorem 1.2.3. *The volume of a fundamental parallelepiped* Π *doesn't depend on* Π. *The volume* *is called the determinant of* Λ*. Furthermore, if* $B_r = \{x : \|x\| \le r\}$*, then*

$$\lim_{r\to\infty} = \frac{|B_r \cap \Lambda|}{\operatorname{vol} B_r} = \frac{1}{\det \Lambda}.$$

We start with a lemma:

Lemma 1.2.1. *Let* Π *be a fundamental parallelepiped of* $\Lambda \subset V$*. Then every vector* $x \in V$ *is uniquely written as* $x = u + y$ *where* $u \in \Lambda, y \in \Pi$*.*

Proof. Existence: Π is the fundamental parallelepiped for $u_1, \dots, u_n$. If $x = \sum_{i=1}^n \alpha_i u_i$ then $u = \sum_{i=1}^n \lfloor \alpha_i \rfloor u_i$ and $y = \sum_{i=1}^n \{\alpha_i\} u_i$

Uniqueness: suppose $x = u_1 + y_1 = u_2 + y_2$ then $u_1 - u_2 = y_2 - y_1$. Since $u_1 - u_2 \in \Lambda$ we have $y_2 - y_1 = \sum_{i=1}^n (\alpha_i - \beta_i)\mathbf{u}_i$. We have $(\alpha_i - \beta_i) \in \mathbb{Z}$. Since $-1 < \alpha_i - \beta_i < 1$, it has to be 0. ■

A geometry interpretation is that we can cover the whole space with fundamental parallelepipeds without overlaps.

Proof of theorem. Let

$$X_r = \bigcup_{u \in B_r \cap \Lambda} (\Pi + u)$$

Then $\operatorname{vol} X_r = |B_r \cap \Lambda| \operatorname{vol} \Pi$.

Say, $\Pi \subset B_a$ for some $a > 0$. Then $X_r \subset B_{r+a}$. Look at B_{r-a}. It is covered by $\Pi + u : u \in \Lambda$. We should have $\|u\| \le r$. Hence $B_{r-a} \subset X_r$.

So we have

$$\left(\frac{r-a}{a}\right)^n = \frac{\operatorname{vol} B_{r-a}}{\operatorname{vol} B_r} \le \frac{\operatorname{vol} X_r}{\operatorname{vol} B_r} \le \frac{\operatorname{vol} B_{r+a}}{B_r} = \left(\frac{r+a}{a}\right)^n$$

This goes to 1 when $r \to \infty$. ■

REMARK/EXERCISE The same holds for balls not centered in the origin:

$$B_r(x_0) = \{x : \|x - x_0\| \le r\}.$$

EXERCISE Suppose a lattice $\Lambda \subset V$ and $u \in \Lambda$. The Voronoi (G.F. Voronoi, 1868-1908) region is defined by

$$\Phi_u = \{x \in V : \|x - u\| \le \|x - v\|, \forall v \in \Lambda\}.$$

Show that Φ is convex (bounded by at most 2^n affine hyperplanes) and $\operatorname{vol}\Phi = \det\Lambda$.

<u>Exercise</u> $(\det\Lambda)(\det\Lambda^*) = 1$

1.3 Sublattice

Definition 1.3.1. Suppose $\Lambda \subset V$ is a lattice, and $\Lambda_0 \subset \Lambda, \Lambda_0 \subset V$ is also a lattice. Λ_0 is then called a sublattice of Λ.

Remark. We have $\operatorname{rank}\Lambda_0 = \operatorname{rank}\Lambda$.

Example 1.3.1. $D_n \subset \mathbb{Z}^n$.

Λ is an Abelian group and $\Lambda_0 \subset \Lambda$ is a subgroup. Look at the quotient Λ/Λ_0 and cosets $\{u+\Lambda_0\}$. The index of Λ_0 in $\Lambda|\Lambda/\Lambda_0| =$ the number of cosets.

Theorem 1.3.1. *1. Let Π be a fundamental parallelepiped of Λ_0 Then $|\Lambda/\Lambda_0| = |\Pi\cap\Lambda|$.*

2. $|\Lambda/\Lambda_0| = \dfrac{\det\Lambda_0}{\det\Lambda}$.

Proof. 1. By Lemma 1.2.1, every coset has a unique representation in Π.

2. Let $B_r = \{x : \|x\| \le r\}$. Then

$$\lim_{r\to\infty} = \frac{|B_r\cap\Lambda|}{\operatorname{vol}B_r} = \frac{1}{\det\Lambda}.$$

Let $S \subset \Lambda$ be the set of coset representatives. Then $|S| = |\Lambda/\Lambda_0|$. Then $\Lambda = \bigcup_{u\in S}(u+\Lambda_0)$. Hence

$$\lim_{r\to\infty}\frac{|B_r\cap(u+\Lambda_0)|}{\operatorname{vol}B_r} = \frac{1}{\det\Lambda_0}. \implies \frac{1}{\det\Lambda} = |S|\frac{1}{\Lambda_0}$$

∎

<u>Exercise</u>

1. $\det\mathbb{Z}^n = 1$
2. $\det D_n = 2$.
3. $\det D_n^+ = 1$. (n even)
4. $\det A_n = \sqrt{n+1}$. $\det E_8 = 1, \det E_7 = \sqrt{2}, \det E_6 = \sqrt{3}$.
5. If $a_1,\ldots,a_n$ are coprime integers not all 0.

$$\Lambda = \{(x_1,\ldots,x_n)\in\mathbb{Z}^n : a_1x_1+\ldots+a_nx_n = 0\} \text{ has } \det\Lambda = \sqrt{a_1^2+\ldots+a_n^2}.$$

Corollary 1.3.1. *If $u_1, \ldots, u_n \in \Lambda$ are linearly independent and*

$$\operatorname{vol}\left\{\sum_{i+1}^{n} \alpha_i u_i : 0 \leq \alpha_i < 1\right\} = \det \Lambda$$

then $u - 1, \ldots, u_n$ is a basis.

Proof. Look at

$$\Lambda_0 = \left\{\sum_{i=1}^{n} m_i u_i : m_i \in \mathbb{Z}\right\}, |\Lambda/\Lambda_0| = 1 \implies \Lambda = \Lambda_0$$

■

Counting integer points. Suppose $\Lambda = \mathbb{Z}^n$.

Pick n linearly independent vectors $u_1, \ldots, u_n \in \Lambda$. Consider

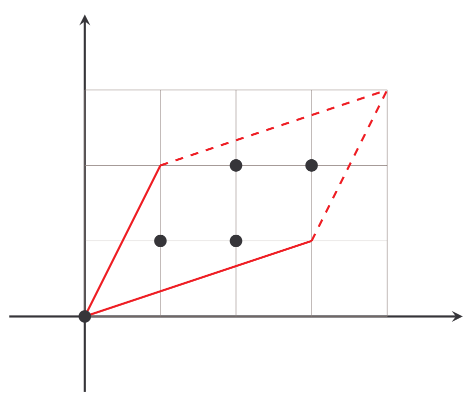
$$\Pi = \left\{\sum_{i=1}^{n} \alpha_i u_i : 0 \leq \alpha_i < 1\right\}.$$

Then

$$|\Pi \cap \mathbb{Z}^n| = ?$$

Suppose $\Lambda_0 = \{\sum_{i=1}^{n} m_i u_i : m_i \in \mathbb{Z}\}$. Then $\det \Lambda_0 = \operatorname{vol} \Pi$.

Suppose $n = 2$, $u_1 = (3, 1), u_2 = (1, 2)$. Then $\operatorname{vol} \Pi = 5$. We can see that the parallelogram contains 5 integer points.



The case for $n = 2$ is special.

Theorem 1.3.2 (Pick Formula (G.A. Pick, 1859-1942)). *If $P \subset \mathbb{R}^2$ is a convex polygon with* *integer vertices and non-empty interior. Then*

$$|P \cap \mathbb{Z}^2| = \text{ area of } P + \frac{1}{2}|\partial P \cap \mathbb{Z}^2| + 1$$

Proof. Left as exercise. Hint: do it for parallelograms (in any dimension) first, then do it for triangles (special case for $n = 2$), and then all polygons with integer vertices. ■

EXERCISE For $n = 2$, linearly independent vectors of $u, v \in \mathbb{Z}^2$ form a basis $\iff$ the triangle with vertices $0, u, v$ has no other integer points.

EXERCISE For $n = 3$, construct an example of linearly independent $u, v, w \in \mathbb{Z}^3$ such that the tetrahedron with vertices $0, u, v, w$ has no other integer points but $\{u, v, w\}$ is not a basis of $\mathbb{Z}^3$. In fact, you can have $|\mathbb{Z}^n/\Lambda|$ arbitrarily large.

EXERCISE Suppose $u_1, \ldots, u_k \in \mathbb{Z}^n$ are linearly independent vectors and $\Lambda = \mathbb{Z}^n \cap \operatorname{span}(u_1, \ldots, u_k)$. The $\{u_1, \ldots, u_k\}$ is a basis of Λ if and only if the great common divisor of all $k \times k$ minors of $\begin{bmatrix} u_1^T \\ u_2^T \\ \cdots \\ u_k^T \end{bmatrix}$ is 1.

Linear algebra (Smith normal form, will not use)

If $\Lambda_0 \subset \Lambda$ is a sublattice, then there is a basis $u_1, \ldots, u_n$ of Λ and a basis $v_1, \ldots, v_n$ of Λ_0 such that $v_i = m_i u_i$ for positive integer m_i and such that m_1 divides m_2 which divides $m_3, \ldots$.