Math 361

April 5, 2023

Quiz

Prove that if $\mathfrak{p}$ is a prime ideal in a number ring K of degree n, then

1. $\mathfrak{p}$ contains a *unique* rational prime p, and
2. $N(\mathfrak{p}) = p^m$ for where $1 \leq m \leq n$.

You may use the fact that the number of an ideal is an element of the ideal.

Final projects

- Choose final project by Wednesday of next week.

Final projects

- Choose final project by Wednesday of next week.
- When will the presentations occur? How long?

Today

- Lattices in $\mathbb{R}^n$.
- Minkowski's lattice point theorem.

Lattices

K a number field of degree n.

Motivation:

Lattices

K a number field of degree n.

Motivation:

- $\mathcal{F} =$ multiplicative group of nonzero fractional ideals.

Lattices

K a number field of degree n.

Motivation:

- $\mathcal{F} =$ multiplicative group of nonzero fractional ideals.
- $\mathcal{P} =$ nonzero principal fractional ideals.

Lattices

K a number field of degree n.

Motivation:

- $\mathcal{F}$ = multiplicative group of nonzero fractional ideals.
- $\mathcal{P}$ = nonzero principal fractional ideals.
- Class group of K (or $\mathfrak{O}_K$): $\mathcal{H} := \mathcal{F}/\mathcal{P}$.

Lattices

K a number field of degree n.

Motivation:

- $\mathcal{F} =$ multiplicative group of nonzero fractional ideals.
- $\mathcal{P} =$ nonzero principal fractional ideals.
- Class group of K (or $\mathfrak{O}_K$): $\mathcal{H} := \mathcal{F}/\mathcal{P}$.
- *Class number* $h = |\mathcal{H}|$.

Lattices

K a number field of degree n.

Motivation:

- $\mathcal{F} =$ multiplicative group of nonzero fractional ideals.
- $\mathcal{P} =$ nonzero principal fractional ideals.
- Class group of K (or $\mathfrak{O}_K$): $\mathcal{H} := \mathcal{F}/\mathcal{P}$.
- *Class number* $h = |\mathcal{H}|$.
- We will see $h = 1$ if and only if $\mathfrak{O}_K$ is a PID.

Lattices

K a number field of degree n.

Motivation:

- $\mathcal{F}$ = multiplicative group of nonzero fractional ideals.
- $\mathcal{P}$ = nonzero principal fractional ideals.
- Class group of K (or $\mathfrak{O}_K$): $\mathcal{H} := \mathcal{F}/\mathcal{P}$.
- *Class number* $h = |\mathcal{H}|$.
- We will see $h = 1$ if and only if $\mathfrak{O}_K$ is a PID.
- **Next goal:** Prove h is finite.

Lattices

Definition. A subset $L \subset \mathbb{R}^n$ is a *rank m lattice in* $\mathbb{R}^n$ if

Lattices

Definition. A subset $L \subset \mathbb{R}^n$ is a *rank m lattice in $\mathbb{R}^n$* if

$$L = \mathrm{Span}_{\mathbb{Z}}\{v_1, \ldots, v_m\}$$

for some set $\{v_1, \ldots, v_m\}$ of linearly independent vectors in $\mathbb{R}^n$.

Lattices

Definition. A subset $L \subset \mathbb{R}^n$ is a *rank m lattice in $\mathbb{R}^n$* if

$$L = \mathrm{Span}_{\mathbb{Z}}\{v_1, \ldots, v_m\}$$

for some set $\{v_1, \ldots, v_m\}$ of linearly independent vectors in $\mathbb{R}^n$.

A subset of $\mathbb{R}^n$ is *discrete* if its intersection with each compact subset of $\mathbb{R}^n$ is finite. Equivalently, the subset has no accumulation points.

Lattices

Definition. A subset $L \subset \mathbb{R}^n$ is a *rank m lattice in $\mathbb{R}^n$* if

$$L = \mathrm{Span}_{\mathbb{Z}}\{v_1, \ldots, v_m\}$$

for some set $\{v_1, \ldots, v_m\}$ of linearly independent vectors in $\mathbb{R}^n$.

A subset of $\mathbb{R}^n$ is *discrete* if its intersection with each compact subset of $\mathbb{R}^n$ is finite. Equivalently, the subset has no accumulation points.

Theorem. An additive subgroup $L \subset \mathbb{R}^n$ is a lattice if and only if it is discrete.

Lattices

Definition. A subset $L \subset \mathbb{R}^n$ is a *rank m lattice in $\mathbb{R}^n$* if

$$L = \mathrm{Span}_{\mathbb{Z}}\{v_1, \ldots, v_m\}$$

for some set $\{v_1, \ldots, v_m\}$ of linearly independent vectors in $\mathbb{R}^n$.

A subset of $\mathbb{R}^n$ is *discrete* if its intersection with each compact subset of $\mathbb{R}^n$ is finite. Equivalently, the subset has no accumulation points.

Theorem. An additive subgroup $L \subset \mathbb{R}^n$ is a lattice if and only if it is discrete.

Proof. Theorem 6.1. $\square$

Lattices

Definition. A *fundamental domain* for a rank n lattice L in $\mathbb{R}^n$ is a set of the form

$$F = \left\{ \sum_{i=1}^{n} a_i v_i : 0 \leq a_i < 1 \text{ for } i = 1, \ldots n \right\}.$$

where $L = \mathrm{Span}_{\mathbb{Z}}\{v_1, \ldots, v_n\}$.

Lattices

Definition. A *fundamental domain* for a rank n lattice L in $\mathbb{R}^n$ is a set of the form

$$F = \left\{\sum_{i=1}^{n} a_i v_i : 0 \leq a_i < 1 \text{ for } i = 1, \ldots n\right\}.$$

where $L = \mathrm{Span}_{\mathbb{Z}}\{v_1, \ldots, v_n\}$.

- $\mathrm{vol}(F) = |\det(v_1, \ldots, v_n)|$.

Lattices

Definition. A *fundamental domain* for a rank n lattice L in $\mathbb{R}^n$ is a set of the form

$$F = \{\sum_{i=1}^n a_i v_i : 0 \le a_i < 1 \text{ for } i = 1, \dots n\}.$$

where $L = \mathrm{Span}_{\mathbb{Z}}\{v_1, \dots, v_n\}$.

- $\mathrm{vol}(F) = |\det(v_1, \dots, v_n)|$.
- For each $x \in \mathbb{R}^n$, there exists a unique ℓ such that $x \in \ell + F$.

Example

$L = \mathbb{Z} \subset \mathbb{R}$.

Example

$L = \mathbb{Z} \subset \mathbb{R}$.

Fundamental domain $F = [0, 1)$.

Example

$L = \mathbb{Z} \subset \mathbb{R}$.

Fundamental domain $F = [0, 1)$.

Homeomorphism:

$$\mathbb{R}/\mathbb{Z} \to S^1$$
$$x \to e^{2\pi i x}.$$

Example

$K = \mathbb{Q}(\sqrt{2})$ with number ring $\mathbb{Z}[1, \sqrt{2}]$.

Example

$K = \mathbb{Q}(\sqrt{2})$ with number ring $\mathbb{Z}[1, \sqrt{2}]$.

Embeddings of K into $\mathbb{C}$: $\sigma_1(a + b\sqrt{2}) = a + b\sqrt{2}$ and $\sigma_2(a + \sqrt{2}) = a - b\sqrt{2}$.

Example

$K = \mathbb{Q}(\sqrt{2})$ with number ring $\mathbb{Z}[1, \sqrt{2}]$.

Embeddings of K into $\mathbb{C}$: $\sigma_1(a + b\sqrt{2}) = a + b\sqrt{2}$ and $\sigma_2(a + \sqrt{2}) = a - b\sqrt{2}$.

Consider the homomorphism

$$\begin{aligned} K &\to \mathbb{R}^2 \\ x &\mapsto (\sigma_1(x), \sigma_2(x)). \end{aligned}$$

Example

$K = \mathbb{Q}(\sqrt{2})$ with number ring $\mathbb{Z}[1, \sqrt{2}]$.

Embeddings of K into $\mathbb{C}$: $\sigma_1(a + b\sqrt{2}) = a + b\sqrt{2}$ and $\sigma_2(a + \sqrt{2}) = a - b\sqrt{2}$.

Consider the homomorphism

$$\begin{aligned} K &\to \mathbb{R}^2 \\ x &\mapsto (\sigma_1(x), \sigma_2(x)). \end{aligned}$$

Image of $\mathbb{Z}[\sqrt{2}]$ in $\mathbb{R}^2$ is a lattice with generators $(\sigma_1(1), \sigma_2(1)) = (1, 1)$ and $(\sigma_1(\sqrt{2}), \sigma_2(\sqrt{2})) = (\sqrt{2}, -\sqrt{2})$.

Example

$K = \mathbb{Q}(\sqrt{2})$ with number ring $\mathbb{Z}[1, \sqrt{2}]$.

Embeddings of K into $\mathbb{C}$: $\sigma_1(a + b\sqrt{2}) = a + b\sqrt{2}$ and $\sigma_2(a + \sqrt{2}) = a - b\sqrt{2}$.

Consider the homomorphism

$$\begin{aligned} K &\to \mathbb{R}^2 \\ x &\mapsto (\sigma_1(x), \sigma_2(x)). \end{aligned}$$

Image of $\mathbb{Z}[\sqrt{2}]$ in $\mathbb{R}^2$ is a lattice with generators $(\sigma_1(1), \sigma_2(1)) = (1, 1)$ and $(\sigma_1(\sqrt{2}), \sigma_2(\sqrt{2})) = (\sqrt{2}, -\sqrt{2})$.

Fundamental domain corresponding to these generators has volume

Example

$K = \mathbb{Q}(\sqrt{2})$ with number ring $\mathbb{Z}[1, \sqrt{2}]$.

Embeddings of K into $\mathbb{C}$: $\sigma_1(a + b\sqrt{2}) = a + b\sqrt{2}$ and $\sigma_2(a + \sqrt{2}) = a - b\sqrt{2}$.

Consider the homomorphism

$$\begin{aligned} K &\to \mathbb{R}^2 \\ x &\mapsto (\sigma_1(x), \sigma_2(x)). \end{aligned}$$

Image of $\mathbb{Z}[\sqrt{2}]$ in $\mathbb{R}^2$ is a lattice with generators $(\sigma_1(1), \sigma_2(1)) = (1, 1)$ and $(\sigma_1(\sqrt{2}), \sigma_2(\sqrt{2})) = (\sqrt{2}, -\sqrt{2})$.

Fundamental domain corresponding to these generators has volume

$$\left| \det \begin{pmatrix} 1 & \sqrt{2} \\ 1 & -\sqrt{2} \end{pmatrix} \right| = 2\sqrt{2}.$$

Tori

Definition. The n-torus is the topological space

$$T^n = \underbrace{S^1 \times \cdots \times S^1}_{n \text{ times}}$$

with the product topology.

Tori

Definition. The n-torus is the topological space

$$T^n = \underbrace{S^1 \times \cdots \times S^1}_{n \text{ times}}$$

with the product topology.

Proposition. Let L be a rank m lattice in $\mathbb{R}^n$ with generators $v_1, \ldots, v_m$.

Tori

Definition. The n-torus is the topological space

$$T^n = \underbrace{S^1 \times \cdots \times S^1}_{n \text{ times}}$$

with the product topology.

Proposition. Let L be a rank m lattice in $\mathbb{R}^n$ with generators $v_1, \ldots, v_m$. Complete $v_1, \ldots, v_m$ to a basis $v_1, \ldots, v_n$ for $\mathbb{R}^n$.

Tori

Definition. The n-torus is the topological space

$$T^n = \underbrace{S^1 \times \cdots \times S^1}_{n \text{ times}}$$

with the product topology.

Proposition. Let L be a rank m lattice in $\mathbb{R}^n$ with generators $v_1, \ldots, v_m$. Complete $v_1, \ldots, v_m$ to a basis $v_1, \ldots, v_n$ for $\mathbb{R}^n$. Homeomorphism

$$\begin{aligned} \phi\colon \mathbb{R}^n/L &\to T^m \times \mathbb{R}^{n-m} \\ \sum_{i=1}^n a_i v_i &\mapsto \left(e^{2\pi i a_1}, \ldots, e^{2\pi i a_m}, a_{m+1}, \ldots, a_n\right). \end{aligned}$$

The mapping ϕ is a bijection when restricted to a fundamental domain.

Examples

Consider the examples

- $L = \mathrm{Span}_{\mathbb{Z}}\{(1,0),(0,1)\}$,

Examples

Consider the examples

- $L = \mathrm{Span}_{\mathbb{Z}}\{(1,0),(0,1)\}$, and
- $L' = \mathrm{Span}_{\mathbb{Z}}\{(1,0)\}$ in $\mathbb{R}^2$

Volume

Definition. Let $L \subset \mathbb{R}^n$ be a rank n lattice, and consider the mapping $\pi : \mathbb{R}^n \to \mathbb{R}^n/L \xrightarrow{\phi} T^n$.

Volume

Definition. Let $L \subset \mathbb{R}^n$ be a rank n lattice, and consider the mapping $\pi : \mathbb{R}^n \to \mathbb{R}^n/L \xrightarrow{\phi} T^n$.

The *volume* of $Y \subseteq T^n$ is

$$\mathrm{vol}(Y) = \mathrm{vol}(\pi^{-1}(Y) \cap F)$$

where F is a fundamental domain for L.

Volume

Definition. Let $L \subset \mathbb{R}^n$ be a rank n lattice, and consider the mapping $\pi : \mathbb{R}^n \to \mathbb{R}^n/L \xrightarrow{\phi} T^n$.

The *volume* of $Y \subseteq T^n$ is

$$\mathrm{vol}(Y) = \mathrm{vol}(\pi^{-1}(Y) \cap F)$$

where F is a fundamental domain for L.

Proposition. Let $X \subset \mathbb{R}^n$ be a bounded such that $\mathrm{vol}(X)$ exists. With notation as in the above definition, suppose that π restricted to X is injective.

Volume

Definition. Let $L \subset \mathbb{R}^n$ be a rank n lattice, and consider the mapping $\pi : \mathbb{R}^n \to \mathbb{R}^n/L \xrightarrow{\phi} T^n$.

The *volume* of $Y \subseteq T^n$ is

$$\mathrm{vol}(Y) = \mathrm{vol}(\pi^{-1}(Y) \cap F)$$

where F is a fundamental domain for L.

Proposition. Let $X \subset \mathbb{R}^n$ be a bounded such that $\mathrm{vol}(X)$ exists. With notation as in the above definition, suppose that π restricted to X is injective. Then $\mathrm{vol}(X) = \mathrm{vol}(\pi(X))$.

Volume

Definition. Let $L \subset \mathbb{R}^n$ be a rank n lattice, and consider the mapping $\pi : \mathbb{R}^n \to \mathbb{R}^n/L \xrightarrow{\phi} T^n$.

The *volume* of $Y \subseteq T^n$ is

$$\mathrm{vol}(Y) = \mathrm{vol}(\pi^{-1}(Y) \cap F)$$

where F is a fundamental domain for L.

Proposition. Let $X \subset \mathbb{R}^n$ be a bounded such that $\mathrm{vol}(X)$ exists. With notation as in the above definition, suppose that π restricted to X is injective. Then $\mathrm{vol}(X) = \mathrm{vol}(\pi(X))$.

Proof. See Theorem 6.7 and the accompanying Figure 6.6. $\square$

Convexity

Definition. Let $X \subseteq \mathbb{R}^n$. Then X is *convex* if it contains the line segment joining each pair of points in X.

Convexity

Definition. Let $X \subseteq \mathbb{R}^n$. Then X is *convex* if it contains the line segment joining each pair of points in X. In other words, if $x, y \in X$, then $\lambda x + (1 - \lambda)y \in X$ for $\lambda \in [0, 1]$.

Convexity

Definition. Let $X \subseteq \mathbb{R}^n$. Then X is *convex* if it contains the line segment joining each pair of points in X. In other words, if $x, y \in X$, then $\lambda x + (1 - \lambda)y \in X$ for $\lambda \in [0, 1]$.

Example. If $P = \{p_1, \ldots, p_k\} \subset \mathbb{R}^n$, the smallest convex set containing P is

Convexity

Definition. Let $X \subseteq \mathbb{R}^n$. Then X is *convex* if it contains the line segment joining each pair of points in X. In other words, if $x, y \in X$, then $\lambda x + (1-\lambda)y \in X$ for $\lambda \in [0,1]$.

Example. If $P = \{p_1, \ldots, p_k\} \subset \mathbb{R}^n$, the smallest convex set containing P is

$$\mathrm{conv}(P) = \left\{ \sum_{i=1}^k \lambda_i p_i : \lambda_i \geq 0 \text{ and } \sum_{i=1}^k \lambda_i = 1 \right\}.$$

Convexity

Definition. Let $X \subseteq \mathbb{R}^n$. Then X is *convex* if it contains the line segment joining each pair of points in X. In other words, if $x, y \in X$, then $\lambda x + (1-\lambda)y \in X$ for $\lambda \in [0,1]$.

Example. If $P = \{p_1, \ldots, p_k\} \subset \mathbb{R}^n$, the smallest convex set containing P is

$$\mathrm{conv}(P) = \left\{ \sum_{i=1}^k \lambda_i p_i : \lambda_i \geq 0 \text{ and } \sum_{i=1}^k \lambda_i = 1 \right\}.$$

This set is called the *convex hull* of P.

Symmetry

Definition. Let $X \subseteq \mathbb{R}^n$. Then X is *centrally symmetric about the origin* if $x \in X$ implies $-x \in X$ for all $x \in X$.

Symmetry

Definition. Let $X \subseteq \mathbb{R}^n$. Then X is *centrally symmetric about the origin* if $x \in X$ implies $-x \in X$ for all $x \in X$.

We will use the abbreviation *symmetric* to mean centrally symmetric about the origin in the context of Minkowski's theorem.

Minkowski's Theorem

Warm-up. Consider the lattice $L = \mathrm{Span}_{\mathbb{Z}}\{(1, 0), (0, 1)\} \subset \mathbb{R}^2$.

Minkowski's Theorem

Warm-up. Consider the lattice $L = \mathrm{Span}_{\mathbb{Z}}\{(1,0),(0,1)\} \subset \mathbb{R}^2$.

What is the volume of the largest convex symmetric set $X \subset \mathbb{R}^2$ containing no nonzero lattice point?

Minkowski's Theorem

Warm-up. Consider the lattice $L = \mathrm{Span}_{\mathbb{Z}}\{(1,0),(0,1)\} \subset \mathbb{R}^2$.

What is the volume of the largest convex symmetric set $X \subset \mathbb{R}^2$ containing no nonzero lattice point?

What about the analogous question in $\mathbb{R}^3$?

Minkowski's theorem

Minkowski's Theorem. Let $L \subset \mathbb{R}^n$ be a rank n lattice, and let F be a fundamental domain for L.

Minkowski's theorem

Minkowski's Theorem. Let $L \subset \mathbb{R}^n$ be a rank n lattice, and let F be a fundamental domain for L.

Let $X \subset \mathbb{R}^n$ be bounded, convex, and symmetric.

Minkowski's theorem

Minkowski's Theorem. Let $L \subset \mathbb{R}^n$ be a rank n lattice, and let F be a fundamental domain for L.

Let $X \subset \mathbb{R}^n$ be bounded, convex, and symmetric. Suppose that

$$\mathrm{vol}(X) > 2^n \, \mathrm{vol}(F).$$

Minkowski's theorem

Minkowski's Theorem. Let $L \subset \mathbb{R}^n$ be a rank n lattice, and let F be a fundamental domain for L.

Let $X \subset \mathbb{R}^n$ be bounded, convex, and symmetric. Suppose that

$$\mathrm{vol}(X) > 2^n \,\mathrm{vol}(F).$$

Then X contains a nonzero lattice point.

Minkowski's theorem

Hypotheses: $X \subset \mathbb{R}^n$ bounded, convex, and symmetric,

Minkowski's theorem

Hypotheses: $X \subset \mathbb{R}^n$ bounded, convex, and symmetric, and $\mathrm{vol}(X) > 2^n \,\mathrm{vol}(F)$.

Minkowski's theorem

Hypotheses: $X \subset \mathbb{R}^n$ bounded, convex, and symmetric, and $\mathrm{vol}(X) > 2^n \mathrm{vol}(F)$.

Proof. Consider the lattice $2L$, whose fundamental domain has volume $2^n \mathrm{vol}(F)$.

Minkowski's theorem

Hypotheses: $X \subset \mathbb{R}^n$ bounded, convex, and symmetric, and $\mathrm{vol}(X) > 2^n \, \mathrm{vol}(F)$.

Proof. Consider the lattice $2L$, whose fundamental domain has volume $2^n \, \mathrm{vol}(F)$. Since $\mathrm{vol}(X) > 2^n \, \mathrm{vol}(F)$, it follows that $\pi \colon \mathbb{R}^n \to \mathbb{R}^n/(2L)$ is not injective when restricted to X.

Minkowski's theorem

Hypotheses: $X \subset \mathbb{R}^n$ bounded, convex, and symmetric, and $\mathrm{vol}(X) > 2^n \mathrm{vol}(F)$.

Proof. Consider the lattice $2L$, whose fundamental domain has volume $2^n \mathrm{vol}(F)$. Since $\mathrm{vol}(X) > 2^n \mathrm{vol}(F)$, it follows that $\pi\colon \mathbb{R}^n \to \mathbb{R}^n/(2L)$ is not injective when restricted to X. Thus, there exist distinct $x, y \in X$ such that $\pi(x) = \pi(y)$.

Minkowski's theorem

Hypotheses: $X \subset \mathbb{R}^n$ bounded, convex, and symmetric, and $\mathrm{vol}(X) > 2^n \mathrm{vol}(F)$.

Proof. Consider the lattice $2L$, whose fundamental domain has volume $2^n \mathrm{vol}(F)$. Since $\mathrm{vol}(X) > 2^n \mathrm{vol}(F)$, it follows that $\pi\colon \mathbb{R}^n \to \mathbb{R}^n/(2L)$ is not injective when restricted to X. Thus, there exist distinct $x, y \in X$ such that $\pi(x) = \pi(y)$.
So $x - y \in 2L$, and thus

$$\frac{1}{2}(x - y) \in L.$$

Minkowski's theorem

Hypotheses: $X \subset \mathbb{R}^n$ bounded, convex, and symmetric, and $\mathrm{vol}(X) > 2^n \, \mathrm{vol}(F)$.

Proof. Consider the lattice $2L$, whose fundamental domain has volume $2^n \, \mathrm{vol}(F)$. Since $\mathrm{vol}(X) > 2^n \, \mathrm{vol}(F)$, it follows that $\pi \colon \mathbb{R}^n \to \mathbb{R}^n/(2L)$ is not injective when restricted to X. Thus, there exist distinct $x, y \in X$ such that $\pi(x) = \pi(y)$.
So $x - y \in 2L$, and thus

$$\frac{1}{2}(x - y) \in L.$$

Since X is symmetric, $-y \in X$.

Minkowski's theorem

Hypotheses: $X \subset \mathbb{R}^n$ bounded, convex, and symmetric, and $\mathrm{vol}(X) > 2^n \,\mathrm{vol}(F)$.

Proof. Consider the lattice $2L$, whose fundamental domain has volume $2^n \,\mathrm{vol}(F)$. Since $\mathrm{vol}(X) > 2^n \,\mathrm{vol}(F)$, it follows that $\pi\colon \mathbb{R}^n \to \mathbb{R}^n/(2L)$ is not injective when restricted to X. Thus, there exist distinct $x, y \in X$ such that $\pi(x) = \pi(y)$.
So $x - y \in 2L$, and thus

$$\frac{1}{2}(x - y) \in L.$$

Since X is symmetric, $-y \in X$. Since X is convex, it follows that

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

Minkowski's theorem

Hypotheses: $X \subset \mathbb{R}^n$ bounded, convex, and symmetric, and $\mathrm{vol}(X) > 2^n \mathrm{vol}(F)$.

Proof. Consider the lattice $2L$, whose fundamental domain has volume $2^n \mathrm{vol}(F)$. Since $\mathrm{vol}(X) > 2^n \mathrm{vol}(F)$, it follows that $\pi\colon \mathbb{R}^n \to \mathbb{R}^n/(2L)$ is not injective when restricted to X. Thus, there exist distinct $x, y \in X$ such that $\pi(x) = \pi(y)$.
So $x - y \in 2L$, and thus

$$\frac{1}{2}(x - y) \in L.$$

Since X is symmetric, $-y \in X$. Since X is convex, it follows that

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

Since $x \neq y$, we have $(x - y)/2$ is a nonzero lattice point in X. $\square$