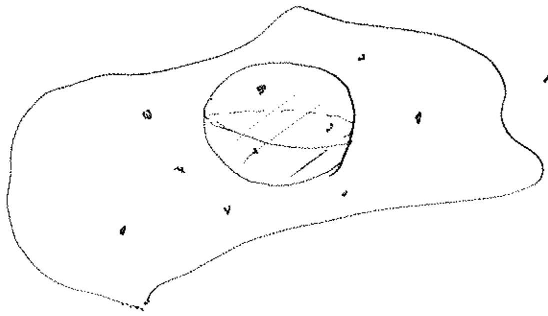
Lecture 1

Some problems in number theory

(I) Counting integral solutions

$$\{f_1(x_1, \dots x_d) = \dots = f_N(x_1, \dots x_d) = 0.\} = X$$
$$f_1, \dots f_N \in \mathbb{Z}[x_1, \dots x_d]$$

Let $\quad N_T(X) = \#\{x \in X \cap \mathbb{Z}^d : \|x\| < T\}$.



X

<u>Conj</u> (Chambert-Loir – Tschinkel)
For a general class of varieties,
$$N_T(X) \sim c\,T^a (\log T)^b \text{ as } T \to \infty$$
for $c > 0$, $a \in \mathbb{Q}^+$, $b \in \mathbb{N}_0$.

(II) Oppenheim Conj. (1929)

$Q(x,y,z) = x^2 + y^2 + \alpha z^2$ (more generally, a quadratic form $Q(x) = \sum_{i,j} a_{ij} x_i x_j$)

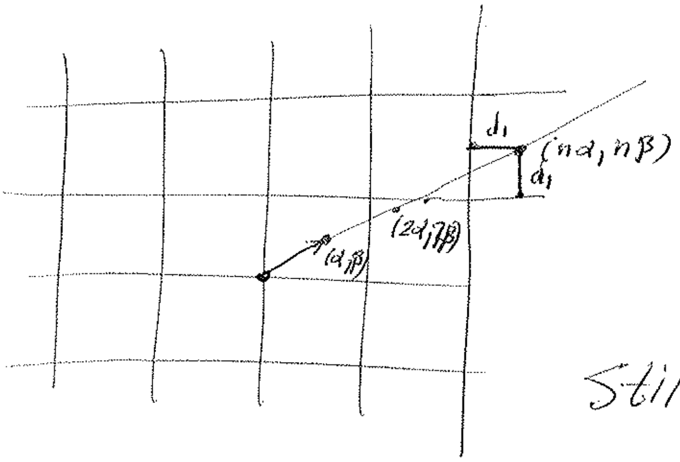
For $t \in \mathbb{R}$,
$$t \approx Q(x,y,z), \quad x, y, z \in \mathbb{Z}$$

<u>Thm</u> (Margulis, 1987) If $\alpha \notin \mathbb{Q}$, $\alpha < 0$.
$$Q(\mathbb{Z}^3) \text{ is dense in } \mathbb{R}.$$

(III) Littlewood conjecture ('1930)

$\alpha, \beta \in \mathbb{R}$.

$$\liminf_{n \to \infty} n \cdot d(n\alpha, \mathbb{Z}) \cdot d(n\beta, \mathbb{Z}) = 0.$$



$n \cdot d_1 \cdot d_2 \approx 0$.

Still open!

(IV) Diophantine approximation

$\overline{\alpha} \in \mathbb{R}^d$, Approximate α by rational vectors

$$\overline{\alpha} \approx \frac{\overline{p}}{q}$$

$\psi : \mathbb{R}^+ \to \mathbb{R}^+$, non-increasing,

α is called ψ-approximable if

$\exists$ infinitely many $q \in \mathbb{Z}$ such that

$$\left\| \overline{\alpha} - \frac{\overline{p}}{q} \right\|^d \leq \frac{\psi(|q|)}{|q|^d} \text{ for some } \overline{p} \in \mathbb{Z}^d!$$

Thm (Khintchine - Groshev)

Typicall α's are ψ-approximable

$$\Updownarrow$$

$$\sum_{\ell \geq 1} \psi(\ell) = \infty.$$

$\alpha \in \mathbb{R}^d$ is called <u>badly</u> ~~*~~<u>approximable</u>

if $\exists c > 0$: $\|q \cdot \alpha - p\|^d \cdot |q| \geq c$

for all $p \in \mathbb{Z}^d$, $q \in \mathbb{Z}^+$.

$\rightarrow$ $BA \subset \mathbb{R}^d$ is a complicated fractal set.

<u>Thm</u> (Roth) If $\alpha \in \mathbb{R}$ is an algebraic number (i.e., a root of $p(x) \in \mathbb{Z}[x]$),

then $\forall \varepsilon > 0$ $\exists c(\varepsilon) > 0$:

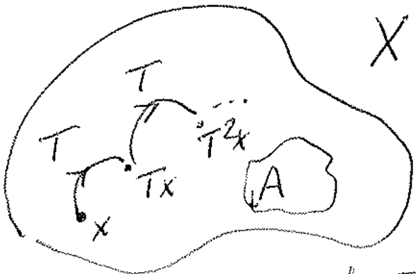
$$\left|\alpha - \frac{p}{q}\right| \geq \frac{c(\varepsilon)}{q^{2+\varepsilon}}.$$

<u>Problems in dynamical systems.</u>

<u>a dynamical system</u>: X - space, equipped with topology.

$T: X \to X$

X



$\{x, Tx, T^2x, \ldots\}$ - orbit

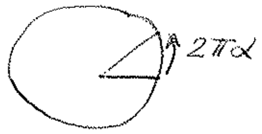
1) what is the closure $\{x, Tx, \ldots\}$?

2) what is the distribution of $\{x, Tx, \ldots\}$?

Fix $A \subset X$, $\displaystyle \frac{\#\{i = 0, \ldots n : T^i x \in A\}}{n+1} \xrightarrow[n \to \infty]{} ?$

Two examples: $X = S^1 = \{z \in \mathbb{C} : |z| = 1\}$.

1) $T_\alpha : S^1 \to S^1 : z \mapsto e^{2\pi i \alpha} z$



2) $D_k : S^1 \to S^1 : z \mapsto z^k,\ k \in \mathbb{N},\ k \geq 2.$

(I) Mixing of dynamical systems

$$\varphi_1, \varphi_2 : X \to \mathbb{C}, \quad T : X \to X$$

$T : X \to X$ is called <u>mixing</u> if

$$\underbrace{\int_X \varphi_1(T^n x)\,\overline{\varphi_2(x)}\,dx}_{\langle \varphi_1 \circ T^n, \varphi_2 \rangle} \xrightarrow[n\to\infty]{} \int_X \varphi_1 \int \overline{\varphi_2}.$$

($\varphi_1 \circ T^n$ and φ_2 are "asymptotically independent")

Prop. D_k is mixing.

$\varphi_1 = z^{m_1}$, $\varphi_2 = z^{m_2}$, (Fourier analysis)

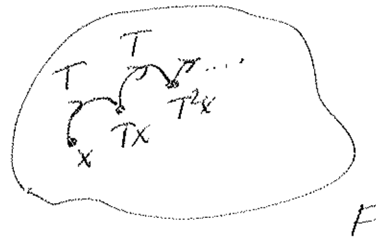
$$\langle \varphi_1 \circ T^n, \varphi_2 \rangle = \int_{S^1} z^{nm_1 - m_2}\,dz = \begin{cases} 1, & nm_1 - m_2 = 0 \\ 0, & nm_1 - m_2 \neq 0 \end{cases} = \begin{cases} 1, & m_1, m_2 = 0 \\ 0, & m_1, m_2 \neq 0 \text{ and } n \gg 0. \end{cases}$$

$$\| \qquad \int \varphi_1 \cdot \int \varphi_2$$

$\langle \varphi_1 \circ T^n, \varphi_2 \rangle \to \int \varphi_1 \cdot \int \overline{\varphi_2}$
for characters, linear combinations of characters, and the closure of linear combinations.
In particular, for $\varphi_1, \varphi_2 \in C(S^1)$.

(II) Density and distribution of orbits

$$\frac{\#\{n=0,\dots N:\ T^n x\in A\}}{N+1}\xrightarrow[N\to\infty]{} ?$$



For interval $A\subset S^1$, $\alpha\notin\mathbb{Q}$, $x\in S^1$

Prop. $\frac{\#\{n=\overline{0,N}\ :\ T_\alpha^n x\in A\}}{N+1}\to \text{length}(A)$.

⌈ Need to show that $\frac{1}{N+1}\sum_{n=0}^{N}\chi_A(T_\alpha^n z)\to\int_{S^1}\chi_A$ (χ_A - char. function)

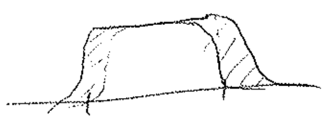
$$\frac{1}{N+1}\sum_{n=0}^{N}\left(e^{2\pi i\alpha}z\right)^m = z^m\cdot\frac{1}{N+1}\sum_{n=0}^{N}\left(e^{2\pi i\alpha m}\right)^n=\underbrace{\frac{\left(e^{2\pi i\alpha m}\right)^{N+1}-1}{e^{2\pi i\alpha m}-1}}_{\frac{z^m}{N+1}}.$$

$$\hookrightarrow\begin{cases}1, & m=0\\ 0, & m\neq 0.\end{cases}$$

$$\frac{1}{N+1}\sum_{n=0}^{N}\varphi(T^n z)\to\int_{S^1}\varphi$$

hold for characters and, hence, for linear combinations, which is dense in $C(S^1)$.

Finally, approximate χ_A by continuous functions. ⌋



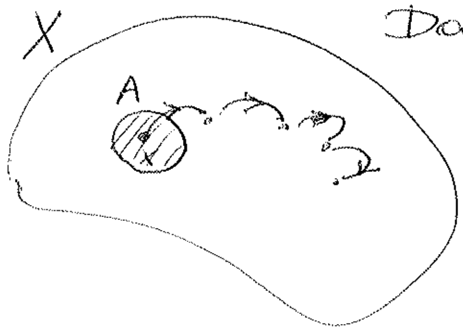
$\{x, D_k x, D_k^2 x, \dots\}$ is dense in S^1 for typical $x\in S^1$. However, there are many complicated orbits.

(III) Thm. (Furstenberg), p, q - primes, $p \neq q$.

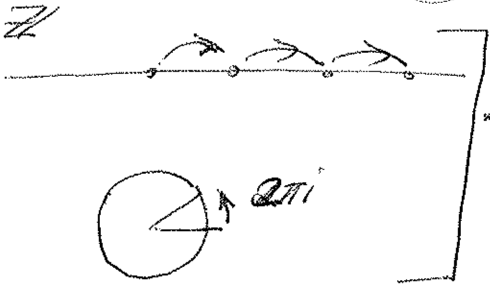
For every $z \notin e^{2\pi i \mathbb{Q}}$,

$$\{ D_p^i \cdot D_q^j \cdot z : \ i, j \geq 0 \} = S^1.$$

(IV) Recurence.



Does $T^n z$ comes back to a nbhd of z?



T_α preserves lengths of intervals

$\downarrow$

concept of measure

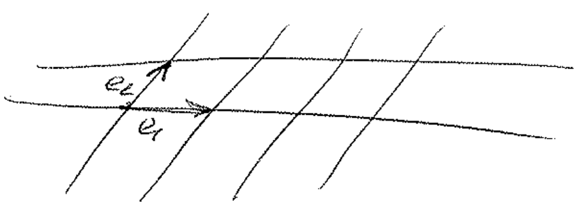
$\downarrow$

Poincare Recurence Thm.

Space of lattices.

Lattice: $\{e_1, \dots e_d\}$ - basis of $\mathbb{R}^d$.

$L = \mathbb{Z}e_1 + \dots + \mathbb{Z}e_d$.



$\mathcal{B}_d$ = the set of bases in $\mathbb{R}^d$.

$(e_1, \dots e_d) \sim (e_1', \dots e_d')$
if $\mathbb{Z}e_1 + \dots + \mathbb{Z}e_d = \mathbb{Z}e_1' + \dots + \mathbb{Z}e_d'$.

Space of lattices $\mathcal{L}_d = \mathcal{B}_d / \sim$

Aside: $\mathcal{L}_d$ = the moduli space of flat d-dim. tori
g $O_d(\mathbb{R})$
[orthogonal group]
(i.e., it parametrizes ~~i~~isomorphism classes of tori up to isometry).

Compare with the moduli space of surfaces.

$G = GL(d,\mathbb{R}) = \{g \in M_d(\mathbb{R}) : \det(g) \neq 0\}$.

the group G acts on $\mathcal{B}_d$: $(e_i) \xrightarrow{g} (ge_i)$

$$\mathrm{Stab}_G((e_i)) = \{e\}.$$

$$GL(d,\mathbb{R}) \simeq \mathcal{B}_d.$$

If $(e_i) \sim (e_i')$, then $\exists g, g' \in GL(d, \cancel{\mathbb{R}})$, (with coefficients in $\mathbb{Z}$) such that $(ge_i) = (e_i')$ and $(g'e_i') = (e_i)$.
Then $g' = g^{-1}$.

$$\Gamma = GL(d,\mathbb{Z}) = \{g \in GL(d,\mathbb{R}) : g, g^{-1} \in M_d(\mathbb{Z})\}$$
$$= \{g \in M_d(\mathbb{Z}) : \det(g) = \pm 1\}$$

$$(e_i) \sim (e_i') \iff \Gamma(e_i) = \Gamma(e_i').$$

$$\mathcal{L}_d = \mathcal{B}_d/\sim \;\simeq GL_d(\mathbb{R})/GL_d(\mathbb{Z}).$$

The space $\mathcal{L}_d \simeq GL_d(\mathbb{R})/GL_d(\mathbb{Z})$
and actions of subgroups of $GL_d(\mathbb{R})$ on $\mathcal{L}_d$ is the subject of this course.

Thm (Iwasawa decomposition)

$$GL(d,\mathbb{R}) = KB \quad \text{where}$$
$$K = O(d,\mathbb{R}) = \{g \in GL(d,\mathbb{R}) : {}^t g g = Id\}.$$
$$B = \text{upper triangular subgroup of } GL(\mathbb{R}).$$

Proof (review the Gramm-Schmidt orthonalization algorith)

Let (e_i) be the standard basis of $\mathbb{R}^d$ and $(e_i') = (g^{-1} e_i)$. By GS algorith, $\exists$ orthonormal basis (e_i'') obtained from (e_i') by $b \in B$

$e_i'' = b e_i'$. $\exists k \in O(d,\mathbb{R})$: $k e_i'' = e_i$

$$(k b e_i') = (g e_i') \Rightarrow g = kb.$$

Measures

$\mu : \{\text{subsets of } X\} \to \mathbb{R}^+ \cup \{\infty\}$.

such that

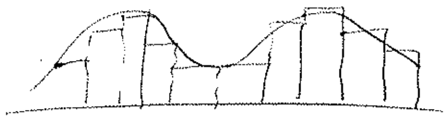
1) $\mu(\emptyset) = 0$

2) $\mu(\bigcup_{i \geq 1} A_i) = \sum_{i \geq 1} \mu(A_i)$

for $A_i \cap A_j = \emptyset$, $i \neq j$.

~~Rk.~~ In general, it is impossible to define consistently on all subsets, but only on a large family (called measurable sets).

$\mu : \{\text{functions on } X\} \to \mathbb{C}$.



$$\int_X f(x)\, d\mu(x).$$

ex. Lebesgue measure $\lambda : \{\text{measurable subsets of } X\} \to \mathbb{R}^+ \cup \{\infty\}$

$\hookrightarrow$ integration on $\mathbb{R}^d$

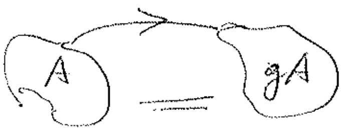
$$\lambda\left(\prod_{i=1}^{d} [a_i, b_i)\right) = \prod_{i=1}^{d} (b_i - a_i)$$

Haar measure

<u>Thm</u> $G = GL_d(\mathbb{R})$, $f : G \to \mathbb{R}$

$$\int_G f(g) \frac{\left(\prod_{i,j} dg_{ij}\right)}{\det(g)^d}$$

defines a measure which is invariant under left and right multiplication.



$g_0 \in G$, $g = g_0 h$,

$$\int_G f(g) \frac{\left(\prod_{i,j} dg_{ij}\right)}{\det(g)^d} = \int_G f(g_0 h)\, \mathrm{Jac}(h \mapsto g_0 h) \times \frac{\left(\prod_{i,j} dg_{ij}\right)}{\det(g_0)^d \det(h)^d}.$$

$$h = (h_1 \dots h_d)$$

$$g_0 h = (g_0 h_1, \dots g_0 h_d)$$

$$\mathrm{Jac}(h_i \longmapsto g_0 h_i) = \det(g_0)$$

$$\mathrm{Jac}(h \longmapsto g_0 h) = \det(g_0)^d$$

Measure on space of lattices

$G = GL_d(\mathbb{R})$, $\Gamma = GL_d(\mathbb{Z})$, $\mathcal{L} = G/\Gamma$. $\pi: G \to G/\Gamma$

$F \subset G$ is called <u>fundamental domain</u> if $\forall x \in G/\Gamma$: $|\pi^{-1}(x) \cap F| = 1$.

1) $G = F\Gamma$.

2) $F\gamma_1 \cap F\gamma_2 = \emptyset$ for $\gamma_1 \neq \gamma_2 \in \Gamma$.

$\mathbb{R}^2$ ~~[illegible]~~

$\downarrow$

$\mathbb{R}^2/\mathbb{Z}^2$

Define measure on G/Γ by

$$\bar{\mu}(A) = \mu(\pi^{-1}(A) \cap F)$$

<u>Lemma</u> $\bar{\mu}$ does not depend on a choice of fundamental domain.

$\ulcorner$
$$\mu(\pi^{-1}(A) \cap F) = \mu\Big(\bigcup_\gamma \pi^{-1}(A) \cap F \cap F'\gamma\Big)$$
$$= \mu\Big(\bigcup_\gamma \pi^{-1}(A) \cap F\gamma^{-1} \cap F'\Big) = \mu(\pi^{-1}(A) \cap F').$$
$\lrcorner$

<u>Lemma</u> $\bar{\mu}$ is G-invariant.

$\ulcorner$
$$\mu(\pi^{-1}(gA) \cap F) = \mu(\pi^{-1}(A) \cap \underline{g^{-1}F}) = \bar{\mu}(A)$$
$\uparrow$ fundamental domain
$\lrcorner$