Geometry of Numbers, lecture 10

We proved last time:

Let $G = SL_n(\mathbb{R})$, $\Gamma = SL_n(\mathbb{Z})$, so $\mathcal{X}_n = G/\Gamma$

$m_{\mathcal{X}_n}$ the G-inv. measure on $\mathcal{X}_n$

We proved: $m_{\mathcal{X}_n}(\mathcal{X}_n) < \infty$

We normalize $m_{\mathcal{X}_n}$ so that $m_{\mathcal{X}_n}(\mathcal{X}_n) = 1$.

This is the Haar-Siegel measure on $\mathcal{X}_n$.

For $f \in L^1(\mathbb{R}^n, \mathrm{Vol})$ define

$$\hat{f}^p : \mathcal{X}_n \to \mathbb{R}, \quad \hat{f}^p(L) = \sum_{\substack{v \in L \\ v \text{ primitive}}} f(v)$$

We proved: $\exists c_n > 0 \ \forall f \in L^1(\mathbb{R}^n, \mathrm{Vol})$,

$$c_n \int_{\mathcal{X}_n} \hat{f}^p \, dm_{\mathcal{X}_n} = \int_{\mathbb{R}^n} f \, d\mathrm{Vol}. \quad \text{(SSF1)}$$

Today we show:

For $f \in L^1(\mathbb{R}^n, \mathrm{Vol})$, define $\hat{f}(L) = \sum_{v \in L \smallsetminus \{0\}} f(v)$

Then: ① $\hat{f} \in L^1(\mathcal{X}_n, m_{\mathcal{X}_n})$

② $\forall f \in L^1(\mathbb{R}^n, \mathrm{Vol})$

$$\int_{\mathbb{R}^n} f \, d\mathrm{Vol} = \int_{\mathcal{X}_n} \hat{f} \, dm_{\mathcal{X}_n} \qquad (\mathrm{SSF2})$$

③ $c_n = \sum_{j=1}^{\infty} \frac{1}{j^n} = \zeta(n)$

$\uparrow$

Riemann ~~zeta~~ function, converges for $n > 1$.

Proof: By writing $f = f^+ - f^-$, $f^+, f^- \geq 0$

$\left(|f| = f^+ + f^- \right)$, $(\hat{f})^+ = (f^+)^\wedge$, $(\hat{f})^- = (f^-)^\wedge$.

(because the formula for $\hat{f}$ maps non-negative functions to non-negative functions), We may assume $f \geq 0$.

For $t > 0$, define $f_t(x) = f(tx)$

Then $\int_{\mathbb{R}^n} f_t \, dVol = \int_{\mathbb{R}^n} f(tx) \, dVol(x)$

$$= \frac{1}{t^n} \int_{\mathbb{R}^n} f(y) \, dVol(y)$$

$y = tx$

$dVol(y) = t^n dVol(x)$

Every $v \in L \setminus \{0\}$ can be written uniquely as

$j v_0$, where $j \in \mathbb{N}$, $v_0 \in L$ is primitive.

Write $j = j(v)$, $v_0 = v_0(v)$, and decompose

$$\hat{f}(L) = \sum_{v \in L \setminus \{0\}} f(v) = \sum_{j=1}^{\infty} \sum_{j(v)=j} f(v) =$$

$$= \sum_{j=1}^{\infty} \sum_{v_0 \in L \text{ primitive}} f(j v_0) = \sum_{j=1}^{\infty} \hat{f}_j^{P}(L_0)$$

So by monotone convergence theorem:

$$\int_{\mathcal{X}_n} \hat{f}(L)\, dm_{\mathcal{X}_n}(L) = \sum_{j=1}^{\infty} \int_{\mathcal{X}_n} \hat{f}_j^{\,p}(L)\, dm_{\mathcal{X}_n}(L)$$

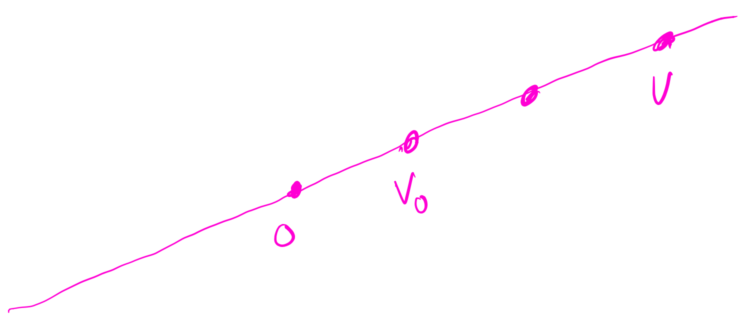
$$\underset{\uparrow \atop (\text{SSF1})}{=} \frac{1}{c_n} \sum_{j=1}^{\infty} \int_{\mathbb{R}^n} f_j \, d\mathrm{Vol} = \frac{\sum_{j=1}^{\infty} \frac{1}{j^n}}{c_n} \int_{\mathbb{R}^n} f \, d\mathrm{Vol}$$

$$= c_n' \int_{\mathbb{R}^n} f \, d\mathrm{Vol}, \quad \text{where } c_n' = \frac{\zeta(n)}{c_n} > 0$$

this proves 1, and also shows that

2 and 3 follow from $c_n' = 1$.

<u>primitive</u>: $\mathrm{span}_{\mathbb{R}}(v) \cap L = \mathrm{span}_{\mathbb{Z}}(v)$.



For each $R \in \mathbb{N}$ let $B_R = [-R,R]^n$

$= B(0,R)$ in L_∞ norm

$$f_R = \frac{\mathbb{1}_B}{\mathrm{Vol}(B_R)} = \frac{\mathbb{1}_B}{(2R)^n}$$

$$\hat{f}_R(L) = \frac{\hat{\mathbb{1}}_{B_R}(L)}{\mathrm{Vol}(B_R)} = \frac{\#(B_R \cap L) - 1}{\mathrm{Vol}(B_R)} \xrightarrow[R\to\infty]{} 1$$

<u>Claim:</u> there is $g \in L^1(\mathcal{X}_n, m_{\mathcal{X}_n})$ s.t.

$\forall L \in \mathcal{X}_n, \forall R \quad \hat{f}_R(L) \leq g(L)$.

Assuming claim, by dominated convergence,

$$1 = \int_{\mathcal{X}_n} 1 \cdot dm_{\mathcal{X}_n} = \lim_{R\to\infty} \int \hat{f}_R(L)\, dm_{\mathcal{X}_n}(L)$$

$$= c_n' \lim_{R\to\infty} \frac{1}{\mathrm{Vol}(B_R)} \int_{\mathbb{R}^n} \mathbb{1}_{B_R}\, d\mathrm{Vol}$$

$$= C_n' \cdot \lim_{R\to\infty} \frac{\mathrm{Vol}(B_R)}{\mathrm{Vol}(B_R)} = C_n'.$$

To prove the claim, we will show that $\forall L \in \mathcal{X}_n$

$$(*) \quad \#(L \cap B_R) \leq \alpha \, \#(L \cap B_1) \cdot \mathrm{Vol}(B_R)$$

Assuming $(*)$,

$$\hat{f}_R(L) = \frac{\#(L\cap B_R) - 1}{\mathrm{Vol}(B_R)} \leq \frac{\#(L\cap B_R)}{\mathrm{Vol}(B_R)}$$

$$\underset{(*)}{\leq} \frac{\#(L\cap B_1)\cdot \cancel{\mathrm{Vol}(B_R)}}{\cancel{\mathrm{Vol}(B_R)}} = \hat{\mathbb{1}}_{B_1}(L) + 1$$

Note $\hat{\mathbb{1}}_{B_1}(L) \in L^1(\mathcal{X}_n, m_{\mathcal{X}_n})$ by 1

and constant functions are in $L^1(\mathcal{X}_n, m_{\mathcal{X}_n})$

because $m_{\mathcal{X}_n}(\mathcal{X}_n) < \infty$, so can take

$g(L) = \hat{\mathbb{1}}_{B_1}(L) + 1$.

Proof of $(*)$: if $\#(L \cap B_1) = k$, then for any $z \in \mathbb{R}^n$, $B_{\frac{1}{2}} + z$ contains at most k points, because $\{x_1, \dots, x_\ell\} \subset B_{\frac{1}{2}} + z$

x_i distinct $\Longrightarrow \{x_j - x_1 : j = 1, \dots, \ell\} \subset B_1$ distinct, so $\ell \leq k$

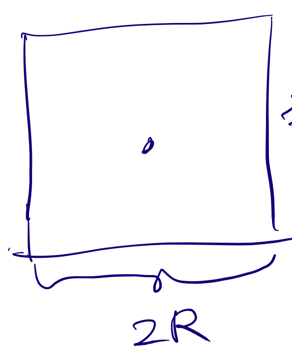
Cover $B_R = [-R, R]^n$ by $(2R)^n$ translates of $B_{\frac{1}{2}} = [-\frac{1}{2}, \frac{1}{2}]^n$. So

$$\#(B_R \cap L) \leq (2R)^n \cdot \#(B_1 \cap L) \leq \alpha \#(B_1 \cap L) \cdot \mathrm{Vol}(B_R)$$

$B_1 = [-1, 1]^n$

$\#(B_1 \cap L) = k$

$\#((z + [0,1]^n) \cap L) \leq k$



$\#(B_R \cap L) \leq k (2R)^n$

$= k \,\mathrm{Vol}(B_R)$

$= \#(B_1 \cap L) \mathrm{Vol}(B_R)$

Recall: We used (SSF2) to show that there is $L \in \mathcal{X}_n$ such that $L \cap B(0, r_{eff}) = \{0\}$ where $r_{eff} > 0$ is chosen so that $Vol(B(0, r_{eff})) = 1$

Euclidean ball

or in other words, $\lambda_1(L) \geq \frac{r_{eff}}{2}$.

Suppose by contradiction that for all $L \in \mathcal{X}_n$

$L \cap B(0, r_{eff}) \neq \{0\}$.

Since $v \in L \cap B(0,r) \Rightarrow -v \in L \cap B(0,r)$

this implies that $\widehat{\mathbb{1}}_{B(0,r_{eff})}(L) \geq 2$

for all $L \in \mathcal{X}_n$. But

$2\zeta(n) > vol(B(0,r))$

$$1 \underset{(SSF1)}{=} Vol(B(0, r_{\cancel{eff}})) = \int_{\mathbb{R}^n} \mathbb{1}_{B(0, r_{\cancel{eff}})} \, dVol$$

$$\underset{(SSF2)}{=} \zeta(n) \int_{\mathcal{X}_n} \widehat{\mathbb{1}}_{B(0, r_{eff})}(L) \, dm_{\mathcal{X}_n}(L) \geq 2\zeta(n) \int_{\mathcal{X}_n} dm_{\mathcal{X}_n} = 2\zeta(n)$$

Trivial improvement: If $\mathrm{Vol}(B(0,r)) < 2\zeta(n)$ then $\exists L \in \mathcal{X}_n$ s.t. $L \cap B(0,r) = \{0\}$.

Define $\Delta_n = \sup\left\{ \mathrm{Vol}(B(0,r)) : \begin{array}{l} \exists L \in \mathcal{X}_n \text{ s.t.} \\ L \cap B(0,r) = \{0\} \end{array} \right\}$

$B(0,r)$ is defined using Euclidean metric.

In terms of previous notations, $\Delta_n = 2^n \delta_n$

δ_n is optimal lattice packing density.

We just showed $\Delta_n \geq 2\zeta(n)$

Best known lower bound is $\Delta_n \geq cn$ for some c.

(due to: Rogers '47, Schmidt '58, Ball '92, Krivelevich-Litsyn-Vardy '04, Venkatesh '13)

Best upper bound: $\Delta_n \leq \beta^n$, $\beta \approx 1.33 > 1$.

<u>Conj (Venkatesh)</u> $\exists\, c, r > 0$ s.t. $\Delta_n \leq cn^r$.

Thm (Venkatesh '13, Vance '11) $\exists c>0$

$\exists n_j \nearrow \infty$ s.t. $\Delta_{n_j} \geq \frac{1}{2} n_j \log\log n_j$.

Prop: When defining Δ_n, could define

$B(0,r)$ using any norm which comes from an inner product on $\mathbb{R}^n$.

Pf Let $\langle x,y\rangle$ be some inner product on $\mathbb{R}^n$

i.e. $\langle x,y\rangle = x^t A y$ where A is a pos definite

symmetric matrix; as we saw (lecture 6)

there is $E \in GL_n(\mathbb{R})$ such that $A = E^t E$.

And then: for a given

$\{0\} = L \cap B_{\langle \cdot,\cdot \rangle}(0,r) \iff \forall x \in L \setminus \{0\}$,

$$\underset{\substack{\| \\ (Ex,Ex)}}{x^t E^t E x} = \langle x, x\rangle \geq r^2 \iff \forall y \in E^{-1} L \setminus \{0\}$$

$y = Ex$ $\quad (y,y) \geq r^2$

(where (x,y) is standard inner product $(x,y)=x^t y$)

$$\iff E^{-1}L \cap B_{(\cdot,\cdot)}(0,r) = \{0\}.$$

Main idea: Instead of analyzing random lattices w.r.t. $m_{\mathcal{X}_n}$, use a smaller group $H < SL_n(\mathbb{R})$ and get a space of lattices strictly contained in $\mathcal{X}_n$, which is an H-orbit, is equipped with an H-inv. probability measure, and such that lattices in this space contain $\geq n$ shortest vectors of equal length.

Reminder: Last week, we used $H = U = \left\{ \left(\begin{array}{c|c} 1 & x \\ \hline 0 & \\ \vdots & A \\ 0 & \end{array} \right) : \begin{array}{l} x \in \mathbb{R}^{n-1} \\ A \in SL_{n-1}(\mathbb{R}) \end{array} \right\}$

$= \mathrm{Stab}_{SL_n(\mathbb{R})}(e_1)$

We saw $U_{\mathbb{Z}}$ is a lattice in U

(i.e. there is a U-inv. measure $m_{U/U_{\mathbb{Z}}}$ on $U/U_{\mathbb{Z}}$ which is finite), and

$$U/U_{\mathbb{Z}} \cong U\cdot\mathbb{Z}^n = \left\{\begin{array}{l}\text{lattices in } \mathcal{X}_n \text{ containing}\\ e_1 \text{ as a primitive vector}\end{array}\right\} \subset \mathcal{X}_n.$$

Some elementary number theory.

Let $\zeta_n = e^{\frac{2\pi i}{n}} = \left(\cos\frac{2\pi}{n}, \sin\frac{2\pi}{n}\right)$,

primitive n^{th} root of unity, i.e. $\zeta_n^n = 1$,

$\zeta_n^j \neq 1$ for $j = 1, \dots, n-1$.

Let $\mathbb{K} = \mathbb{Q}(\zeta_n)$ (cyclotomic field extension)

(note $\mathbb{K}$ depends on n).

<u>Lemma</u>: $\deg(\mathbb{K}/\mathbb{Q}) = \phi(n)$

$= \#\{1 \leq k \leq n : \gcd(k,n) = 1\}$ Euler totient fn.

In particular, $\exists c > 0$ and infinitely many n, for which $\deg(\mathbb{K}/\mathbb{Q}) \leq \dfrac{cn}{\log\log n}$

<u>Sketch of proof</u>: Let $f \in \mathbb{Z}[X]$ be the minimal polynomial of ζ_n.

ζ_n is a root of $X^n - 1 = 0$.

$$X^n - 1 = (X-1)(X^{n-1} + X^{n-2} + \cdots + X + 1)$$

If $j \in \mathbb{N}$ then $(\zeta_n^j)^n = (\zeta_n^n)^j = 1^j = 1$

So ζ_n^j is also a root of $X^n - 1$.

If $\gcd(n,j) = d > 1$

$$X^n - 1 = (X^d - 1)(X^{n-d} + X^{n-2d} + \cdots + X^d + 1)$$

$$X^n - 1 = \prod_{j=0}^{n-1} (X - \zeta_n^j)$$

One can show (Gauss, Kummer, Dirichlet)

$$\prod_{\substack{j=0 \\ \gcd(n,j)=1}}^{n-1} (X - \zeta_n^j)$$ has integer coefficients and is irreducible.

This is called the $n^{\underline{th}}$ cyclotomic polynomial.

This is therefore the minimal polynomial of ζ_n, and clearly has degree $\phi(n)$.

So $\deg(K/\mathbb{Q}) = \phi(n)$.

Suppose $p_1 < p_2 < p_3 < \cdots$ are the primes, then for $n = p_1 \cdots p_k$

$$\phi(n) = \phi(p_1 \cdots p_k) = (p_1 - 1) \cdots (p_k - 1)$$

$$= n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right) \sim c\,\frac{n}{\log\log n}$$

Mertens theorem 1874.

Prop: Let $m_n = 2\phi(n)$. There is $L_0 \in \mathcal{X}_{m_n}$ and a group $H \subset SL_{m_n}(\mathbb{R})$ such that:

① HL_0 is closed, $\Gamma = \mathrm{Stab}_H(L_0)$ is a lattice in H, so the measure $m_{H/\Gamma}$ (H-inv. measure on H/Γ, probability) induces an H-inv. measure supported on $HL_0 \subset \mathcal{X}_{m_n}$. (the notation $m_{H/\Gamma}$ to denote the measures on H/Γ and on HL_0).

② One has (SSF3) $\forall f \in L^1(\mathbb{R}^{m_n}; \mathrm{Vol})$

$$\int_{\mathbb{R}^{m_n}} f \, d\mathrm{Vol} = \int_{\mathcal{X}_n} \hat{f}(L) \, d_{H/\Gamma}(L)$$

(where $\hat{f}$ is as in (SSF2)).

③ $\exists$ an inner product $\langle \cdot, \cdot \rangle$, s.t. for each $L = hL_0$, for $h \in H$, has a group of order n acting on L, preserving

$\langle \cdot,\cdot \rangle$, such that nonzero vectors in L have orbits of size n.

Proof of Venkatesh thm, assuming Prop:

Let B be a ball of volume $< n$ in $\mathbb{R}^{m_n}$, w.r.t. the inner product $\langle \cdot,\cdot \rangle$ (in ③ of Prop).

Suppose by contradiction that for all $L \in \mathcal{X}_{m_n}$ $L \cap B \neq \{0\}$. For any $L \in \operatorname{supp} m_{H/\Gamma}$, can apply the group action in ③ to find $L \cap B$ contains at least n different nonzero points. So $\widehat{\mathbb{1}_B}(L) \geq n$, hence

$$n > \mathrm{Vol}(B) = \int_{\mathbb{R}^{m_n}} \mathbb{1}_B \, d\mathrm{Vol} =$$

$$\underset{(SSF3)}{=} \int_{\mathcal{X}_{m_n}} \widehat{\mathbb{1}}_B(L) \, dm_{H/\Gamma} \geq n \int_{H/\Gamma} dm_{H/\Gamma} = n$$

So $\Delta_{m_n} \geq n$, for all n. $m_n = 2\phi(n)$

$\Delta_{2\phi(k)} \geq k$

Choose $k_j \to \infty$ s.t. $n_j = 2\phi(k_j) \leq c \frac{j}{\log\log j}$

(by lemma)

$\Delta_{n_j} \geq j \geq \frac{1}{c} n_j \log\log j \geq \frac{1}{c} n_j \log\log n_j$.

We will $H = SL_2(\mathbb{K} \otimes_{\mathbb{Q}} \mathbb{R})$

We now explain these symbols.

We can think of $\mathbb{K}$ as a vector space over $\mathbb{Q}$,

of dimension $\deg(\mathbb{K}/\mathbb{Q}) = \phi(n)$.

If we take a basis $x_1, \dots, x_{\phi(n)}$ of $\mathbb{K}$ over $\mathbb{Q}$,

we consider a formal vector space over $\mathbb{R}$,

spanned by the x_i, and extend mult. by

linearity: $\left(\sum a_i x_i\right) \cdot \left(\sum b_j x_j\right) = \sum_{i,j} a_i b_j \underbrace{x_i x_j}_{\text{expressed as a}}$

$a_i, b_j \in \mathbb{R}$

lin. comb of the x_i.

Such an extension is called extension of scalars.

$\mathbb{K} \otimes_{\mathbb{Q}} \mathbb{R}$ is an (associative) algebra over $\mathbb{R}$ (with unit). That is, a vector space over $\mathbb{R}$, equipped with $+$ (vector space addition) and $\cdot$, s.t.

$$\left.\begin{aligned} (x+y)z &= xz+yz \\ z(x+y) &= zx+zy \\ (xy)z &= x(yz) \end{aligned}\right\} \forall x,y,z$$

$$(ax)\cdot(by) = (ab)(xy) \quad \forall x,y \in \text{algebra},\ a,b \in \mathbb{R}$$

$$x\cdot 1 = 1\cdot x = x \quad \forall x.$$

This is almost a field, we give up on commutativity of mult. and of existence of a mult. inverse.

Here is a concrete way to think of $\mathbb{K} \otimes_{\mathbb{Q}} \mathbb{R}$.

Fix a basis for $\mathbb{K}/\mathbb{Q}$ as before.

Any element $x \in \mathbb{K}$ can be identified

with $\bar{A}(x) = \begin{pmatrix} a_1 \\ \vdots \\ a_{\phi(n)} \end{pmatrix}$, where $x = \sum a_i x_i$

$$\begin{aligned} y &\longmapsto xy \\ \mathbb{K} &\longrightarrow \mathbb{K} \end{aligned}$$

becomes a ($\mathbb{Q}$-) linear transformation

Let $A(x) \in M_{\phi(n)}(\mathbb{Q})$ be the corresponding matrix, w.r.t. the given basis.

$$A(x)\bar{A}(y) = \bar{A}(xy)$$

$$\begin{aligned} x &\longmapsto A(x) \\ \mathbb{K} &\longrightarrow M_{\phi(n)}(\mathbb{Q}) \end{aligned}$$

satisfies

$$A(x_1 x_2) = A(x_1)A(x_2)$$
$$A(x_1 + x_2) = A(x_1) + A(x_2)$$
$$A(\underline{1}) = \mathrm{Id}$$
$$A(x^{-1}) = A(x)^{-1}$$

We can think of $M_{\phi(n)}(\mathbb{Q})$ as a dense subset of $M_{\phi(n)}(\mathbb{R})$.

$$\mathbb{K} \cong \{A(x) : x \in \mathbb{K}\} \subset M_{\phi(n)}(\mathbb{Q}) \subset M_{\phi(n)}(\mathbb{R})$$

We can think of the closure of this embedding of $\mathbb{K}$ in $M_{\phi(n)}(\mathbb{R})$ as $\mathbb{K} \otimes_{\mathbb{Q}} \mathbb{R}$.

We can think of $H = SL_2(\mathbb{K} \otimes_{\mathbb{Q}} \mathbb{R})$ as

$2\phi(n) \times 2\phi(n) = m_n \times m_n$ real matrices, of determinant 1, of form

$$\left(\begin{array}{c|c} a & b \\ \hline c & d \end{array}\right), \text{ where } a, b, c, d \in \mathbb{K} \otimes_{\mathbb{Q}} \mathbb{R} \subset M_{\phi(n)}(\mathbb{R}).$$

Now we define L_0.

<u>Recall:</u> $z \in \mathbb{C}$ is called an algebraic integer if $\exists\, p \in \mathbb{Z}[X]$ s.t. $p(z) = 0$, p is monic (leading coefficient is 1). Algebraic integers form a ring. For any number field $\mathbb{K}$, can

look at $\mathcal{O}_{\mathbb{K}}$ = ring of integers in $\mathbb{K}$.

In case $\mathbb{K} = \mathbb{Q}(\zeta_n)$, $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta_n]$.

Let $L_0 = \bar{A}(\mathcal{O}_{\mathbb{K}}^2) = \left\{ \begin{pmatrix} \bar{A}(x) \\ \bar{A}(y) \end{pmatrix} : x, y \in \mathcal{O}_{\mathbb{K}} \right\}$.

ζ_n acts on $\mathbb{R}^{m_n}$ by multiplying each factor:

$$\zeta_n \cdot v = \left(\begin{array}{c|c} A(\zeta_n) & 0 \\ \hline 0 & A(\zeta_n) \end{array} \right) v$$

Since A is a field embedding

$$A(\zeta_n^n) = A(\zeta_n)^n = Id.$$

Let $\langle \cdot , \cdot \rangle$ be an inner product on $\mathbb{R}^{m_n}$, invariant under the action of ζ_n, for instance $\langle x, y \rangle = \sum_{j=0}^{n-1} (\zeta_n^j x, \zeta_n^j y)$.

<u>Prop</u>: Each $L \in HL_0$ is inv. under the action of ζ_n, moreover ζ_n acts on nonzero

elements of L with trivial stabilizers,

or in other words, for any $x \in L \setminus \{0\}$,

the vectors $x, \zeta_n x, \dots, \zeta_n^{n-1} x$ are distinct (and have the same length w.r.t. $\langle \cdot, \cdot \rangle$).

Remark this Prop. proves ③ of preceding Prop.

Pf: Note

$$\zeta_n \begin{pmatrix} \bar{A}(x) \\ \bar{A}(y) \end{pmatrix} = \left(\begin{array}{c|c} A(\zeta_n) & 0 \\ \hline 0 & A(\zeta_n) \end{array}\right) \begin{pmatrix} \bar{A}(x) \\ \bar{A}(y) \end{pmatrix} =$$

$$= \begin{pmatrix} A(\zeta_n) \bar{A}(x) \\ A(\zeta_n) \bar{A}(y) \end{pmatrix} = \begin{pmatrix} \bar{A}(\zeta_n x) \\ \bar{A}(\zeta_n y) \end{pmatrix}$$

If $L = L_0$, i.e. $h = \{e\}$, then

$$\zeta_n \cdot L_0 = \left\{ \zeta_n \begin{pmatrix} \bar{A}(x) \\ \bar{A}(y) \end{pmatrix} : x, y \in \mathcal{O}_K \right\}$$

$$= \left\{ \begin{pmatrix} \bar{A}(\zeta_n x) \\ \bar{A}(\zeta_n y) \end{pmatrix} : x, y \in \mathcal{O}_K \right\} = L_0 .$$

$$\zeta_n \in \mathcal{O}_{\mathbb{K}} \Rightarrow \zeta_n \mathcal{O}_{\mathbb{K}} \subset \mathcal{O}_{\mathbb{K}}$$

and $\zeta_n^{-1} \in \mathcal{O}_{\mathbb{K}} \Rightarrow \mathcal{O}_{\mathbb{K}} \subset \zeta_n \mathcal{O}_{\mathbb{K}}$

$$\Rightarrow \zeta_n \mathcal{O}_{\mathbb{K}} = \mathcal{O}_{\mathbb{K}}$$

Now for $h \in H$, $L = hL_0$, we can write

$h = \left(\begin{array}{c|c} a & b \\ \hline c & d \end{array}\right)$ $\quad a, b, c, d \in \mathbb{K} \otimes_{\mathbb{Q}} \mathbb{R}$ (thought of as matrices in $M_{\phi(n)}(\mathbb{R})$)

$A(\zeta_n) a = a A(\zeta_n)$ and similarly for b, c, d.

$$\begin{pmatrix} A(\zeta_n) & 0 \\ 0 & A(\zeta_n) \end{pmatrix} h = h \left(\begin{array}{c|c} A(\zeta_n) & 0 \\ \hline 0 & A(\zeta_n) \end{array}\right)$$

So $L = hL_0 = h\zeta_n L_0 = \zeta_n h L_0 = \zeta_n L$.

If, for some $v \in L$, $\zeta_n^j v = v$, $v \neq 0$,

then for $h^{-1}v = \begin{pmatrix} x \\ y \end{pmatrix} \in L_0$ we would also

have $\zeta_n^j h^{-1} v = h^{-1} v$, i.e.

$\zeta_n^j x = x$, $\zeta_n^j y = y$

x, y are not both 0, so multiplying by

x^{-1} or y^{-1} we get $\zeta_n^j = 1$ so j is a

power of n. So ζ_n acts on $L \setminus \{0\}$

without nontrivial stabilizers.