Lecture 1:

Algebraic groups & Arithmetic subgroups

Do you know?

1.) Haar measure?
2.) p-adic numbers?
3.) Adeles
4.) Class group of a number field

Topics to cover

1.) Reduction theory of arithmetic groups
2.) Adeles, Ideles over a number field
3.) Analytic cont. of Dedekind zeta function.

Reduction theory:

1.) Consider $G = SL_n(\mathbb{R})$

$$= \{ A \in GL_n(\mathbb{R}) \mid \det A = 1 \}$$

$$\Gamma = SL_n(\mathbb{Z})$$

$\Gamma \leq G$ is discrete

G acts on the space G/Γ

G/Γ has the quotient topology.

Thm: (Haar) ?? $\exists$ a measure μ on G/Γ s.t. for $A \subseteq G/\Gamma$ "nice"

$$\mu(A) = \mu(gA) \quad \text{"left-invariance"}$$

This is unique upto scaling!

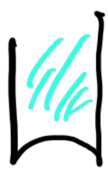
Def: This measure on G/Γ is called the left G-invariant Haar measure

Thm: (Siegel) WRT the above Haar measure

$$\mu(G/\Gamma) < \infty$$

For $n=2$, $SO(2)\backslash SL_2(\mathbb{R})/SL_2(\mathbb{Z})$

$\simeq \quad \mathbb{H}/SL_2(\mathbb{Z})$



← a mount of space is finite.

hyperbolic metric $\frac{dx\,dy}{y^2}$ $\quad$ vol $\overset{?}{=} 3/\pi$

How to prove?

Need to find some $\Sigma \subseteq G$ s.t. $\mathrm{vol}(\Sigma) < \infty$

$$\Sigma \cdot \Gamma = G$$

So $\Sigma \longrightarrow G/\Gamma$ is surjective

Reduction theory is showing that Σ exists.

2.) One can also ask this question for

$G(\mathbb{R}) = Sp(2n, \mathbb{R})$ $\qquad \Gamma = Sp(2n, \mathbb{Z})$

$= O_{p,q}(\mathbb{R})$ $\qquad$ "suitable"

3.) Let K be a number field

<u>Def:</u> A number field is the ring $K = \frac{\mathbb{Q}[x]}{\langle f(x) \rangle}$

for some $f \in \mathbb{Q}[x]$ that is irreducible.

irreducible $\Rightarrow$ K is a field.

<u>Rmk:</u> Number field is a $\mathbb{Q}$-vector space
it is also a field

Given a number field, one is interested in $\mathcal{O}_K \subseteq K$ "ring of integers"

where $\mathcal{O}_K = \{ x \in K \mid \exists$ a monic polynomial g in $\mathbb{Z}[x]$ s.t. $g(x) = 0 \}$

Exercise: Read / Ask ChatGPT: Why is $\mathcal{O}_K$ a ring?

<u>Fact:</u> $\mathcal{O}_K$ is a f.g. $\mathbb{Z}$-module.

Consider $\mathcal{O}_K^\times$ = group of units

$= \{ x \in \mathcal{O}_K \mid x^{-1} \in \mathcal{O}_K \}$, $x \neq 0$

Consider

$$K \otimes \mathbb{R} \approx \frac{\mathbb{Q}[x]}{\langle f(x) \rangle} \otimes \mathbb{R} \simeq \frac{\mathbb{R}[x]}{\langle f(x) \rangle}$$

Over $\mathbb{R}$, f splits into r_1 linear factors, r_2 quadratic factor $\Big\}$ irredu. over $\mathbb{R}$

$$f(x) = \underbrace{f_1(x) \cdots f_{r_1}(x)}_{\text{real roots}} \underbrace{f_{r_1+1}(x) \cdots f_{r_2}(x)}_{\text{complex roots}}$$

for $\quad i = 1, \dots r_1 \qquad \frac{\mathbb{R}[x]}{\langle f_i(x) \rangle} \cong \mathbb{R}$

$i = r_1 + 1, \dots r_2 \qquad \frac{\mathbb{R}[x]}{\langle f_i(x) \rangle} \cong \mathbb{C}$

complex embeddings

So $\quad K \otimes \mathbb{R} \cong \underbrace{\mathbb{R}^{r_1}}_{\text{real embeddings}} \oplus \mathbb{C}^{r_2}$ as $\mathbb{R}$-algebras

Now consider $\quad N : K \otimes \mathbb{R} \to \mathbb{R}_{>0}$

$$\mathbb{R}^{r_1} \oplus \mathbb{C}^{r_2}$$

$$x \mapsto \prod_{i=1}^{r_1} |x_i| \prod_{i=1+r_1}^{r_2} |x_i|^2$$

Observe that in $K \otimes \mathbb{R}$

$$N(x,y) = N(x) N(y)$$

Now consider the group

$$(K \otimes \mathbb{R})^{(1)} = \{ x \in K \otimes \mathbb{R} \mid N(x) = 1 \}$$

<u>Lemma</u>: $\quad x \in \mathcal{O}_K^\times \;,\quad N(x) = 1$

"Proof": $\quad x \cdot x^{-1} = 1, \quad$ To check

$N(x)\, N(x^{-1}) = 1, \quad x \in \mathcal{O}_K,$

$N(x)\, N(x)^{-1} = 1, \quad N(x) \in \mathbb{Z}$

$\boxed{//}$

So in fact $\quad \mathcal{O}_K^\times \subseteq (K \otimes \mathbb{R})^{(1)}$

$\Rightarrow$ One can consider

$$(K \otimes \mathbb{R})^{(1)} / \mathcal{O}_K^\times$$

Thm (Dirichlet's unit theorem)

$$\mathrm{vol}\left((K \otimes \mathbb{R})^{(1)} / \mathcal{O}_K^\times \right) < \infty$$

"to explore"

For $K = \mathbb{Q}(\sqrt{2})$ this is related to the solution Pell's equation.

Def: Ideals are subrings $I \subseteq \mathcal{O}_K$ s.t. $\mathcal{O}_K \cdot I \subseteq I$

4.) Class group of K

$$Cl(K) = \{\text{All ideals of } \mathcal{O}_K\} / \sim$$

$I_1 \sim I_2$ iff $\exists\ x \in K^{\times}$ s.t. $x I_1 = I_2$

Fact: Class-set of a # field is a finite set.

All these examples generalize to the theorem of Borel-Harish Chandra (1962)

Eg 1.) will follow today from BHC (maybe 2)

(3, 4) will follow tomorrow

Def: A linear alg. group G is a subgroup of $SL_n(\mathbb{C})$ for some n given as a zero-set of some polynomials in $\{X_{ij}\}_{1 \le i,j \le n}$, the matrix coeffs of $SL_n(\mathbb{C})$

$G \subseteq SL_n(\mathbb{C})$ is an R-group if the polynomials are in $R[\{X_{ij}\}]$

Eg: $GL_n \subseteq SL_{n+1}(\mathbb{C})$, $g \mapsto \begin{bmatrix} g & 0_{n\times 1} \\ 0_{1\times n} & (\det(g))^{-1} \end{bmatrix}$

Def: Morphisms of alg. groups G, H are

$f: G \to H$ s.t. each entry of $y = f(x)$ is a polynomial in entries of x.

" R "-morphisms if entries have R-coeff.

Def: $\chi: G \xrightarrow{\mathbb{Q}\text{-morphism}} GL_1$ is called $\mathbb{Q}$-character

$X(G) =$ group of $\mathbb{Q}$-characters

Def: $G(\mathbb{R}) = G \cap SL_n(\mathbb{R})$, $G(\mathbb{Z}) = G \cap SL_n(\mathbb{Z})$

Lemma: Let G be an alg. $\mathbb{Q}$-group

Let $\chi: G \to GL_1$ be a $\mathbb{Q}$-char.

Then $\chi(G(\mathbb{Z})) = \{\pm 1\}$

"Proof":

$$\chi(G(\mathbb{Z})) \leq GL_1(\mathbb{Q})$$

$$= \left\{ \begin{bmatrix} t & \\ & t^{-1} \end{bmatrix}, t \in \mathbb{Q} \right\}$$

$t =$ rat. polynomial of entries of $g \in G(\mathbb{Z})$

$\in \frac{1}{N}\mathbb{Z}$ for some $N \in \mathbb{Z}$

$\blacksquare$

Claim: Rational characters obstruct $G(\mathbb{R})/G(\mathbb{Z})$ from having finite volume.

Eg: **Lemma:** $GL_n(\mathbb{R})/GL_n(\mathbb{Z})$ has inf. volume

"Proof" Consider $|\det| : GL_n(\mathbb{R}) \to \mathbb{R}$

$$|\det| : GL_n(\mathbb{R})/GL_n(\mathbb{Z}) \to \mathbb{R}_{>0}$$

Suppose $\mathrm{vol}(GL_n(\mathbb{R})/GL_n(\mathbb{Z})) < \infty$

This would imply $\mathrm{vol}(\mathbb{R}_{>0}) < \infty$

$\Rightarrow\Leftarrow$

Ex:

Thm: (Borel-Harish Chandra)

"$\mathbb{Q}$-Characters are the only obstructions"

Suppose G is an alg. $\mathbb{Q}$-group

s.t. $X(G^{\circ}) = \{1\}$

G° is the identity comp in Zariski topo. or identity component $G(\mathbb{C})$

then 1.) $G(\mathbb{R})/G(\mathbb{Z})$ has finite Haar measure

2.) $G(\mathbb{A})/G(\mathbb{Q})$ has finite Haar measure.