Week 2

① Siegel's lemma
② Introduction to Diophantine approximation — Thue

(2.9.1)
Lemma Let a_{ij}, $i=1,\dots,M$, $j=1,\dots,N$ be rational integers not all 0, bounded by B and suppose that $N>M$. Then the homogeneous linear system

$$a_{11}x_1+a_{12}x_2+\dots+a_{1N}x_N=0$$
$$a_{21}x_1+a_{22}x_2+\dots+a_{2N}x_N=0$$
$$\text{— — — — — —}$$
$$a_{M1}x_1+a_{M2}x_2+\dots+a_{MN}x_N=0$$

has a solution $x_1,\dots,x_N$ in rational integers not all 0, bounded by

$$\max_i |x_i| \le \left\lfloor (NB)^{\frac{M}{N-M}} \right\rfloor .$$

Pf Denote by A the $M\times N$ matrix (a_{ij}).
We may assume no row is identically 0.
For a positive int k, consider the set

$$T := \{\vec{x}\in\mathbb{Z}^N \mid 0\le x_i\le k,\ i=1,\dots,N\}$$

Denote by S_m^+ sum of positive entries in the m th row of A, and similarly by S_m^- the sum of negative entries. Then for $\vec{x}\in T$ and $\vec{y}:=A\vec{x}$ we have

$$k S_m^- \le y_m \le k S_m^+$$

Let $T' := \{ y \in \mathbb{Z}^M \mid k S_m^- \le y_m \le k S_m^+, m = 1, \dots, M \}$

writing $B_m := \max_n |a_{mn}|$, we have $S_m^+ - S_m^- \le N B_m$. $\Rightarrow$ conclude T' has at most $\prod_m (N k B_m + 1)$ elements. choose k so T has more elements than T'

$$\prod_m (N k B_m + 1) < (k+1)^N \quad (A)$$

If we choose k to be integer part of $\prod_m (N B_m)^{\frac{1}{N-M}}$, and use $N k B_m + 1 < N B_m (k+1)$

Then easily verify (A) is satisfied.
Now by pigeon-hole, $\exists\, x', x'' \in T$ with $A\vec{x}' = A\vec{x}''$. The point $\vec{x} := \vec{x}' - \vec{x}''$ is a solution of $A\vec{x} = 0$ in integers, with $\max_n |x_n| \le k$.

2.9.2
Cor K # field, $\deg(K) = d$, $K \subset \mathbb{C}$, $|\cdot|$ usual absolute value on $\mathbb{C}$. Let $M, N \in \mathbb{Z}$, $0 < M < N$. Then $\exists$ +ve constants C_1, C_2 such that for any non-zero $M \times N$ matrix A with entries $a_{mn} \in \mathcal{O}_K$ there is $\vec{x} \in \mathcal{O}_K^N \setminus \{\vec{0}\}$ with $A \cdot \vec{x} = \vec{0}$ and

$$H(\vec{x}) \le C_1 (C_2 N B)^{\frac{M}{N-M}}.$$

where $B := \sup_{\sigma, m, n} |\sigma(a_{mn})|$ with σ ranging over the embeddings of K into $\mathbb{C}$.

Pf $\{w_1, \dots, w_d\}$ $\mathbb{Z}$-basis of $\mathcal{O}_K$. Then

$$a_{mn} = \sum_{j=1}^{d} a_{mn}^{(j)} w_j, \quad a_{mn}^{(j)} \in \mathbb{Z}.$$

Using $x_n = \sum_{k=1}^{d} x_n^{(k)} w_k$, we get

$$(A \cdot \vec{x})_m = \sum_{n=1}^{N} \sum_{j,k=1}^{d} a_{mn}^{(j)} w_j w_k x_n^{(k)} = \sum_{\ell=1}^{d} \sum_{n=1}^{N} \sum_{j,k=1} a_{mn}^{(j)} b_{jk}^{(\ell)} x_n^{(k)} w_\ell.$$

Where $w_j w_k = \sum_{\ell=1}^{d} b_{jk}^{(\ell)} w_\ell$. Let A' be the $(Md) \times (Nd)$ matrix

$$A' := \left(\sum_{j=1}^{d} a_{mn}^{(j)} b_{jk}^{(\ell)} \right).$$

with rows indexed by (m, ℓ), columns indexed by (n, k), and let $\vec{y} \in \mathbb{Z}^{Nd}$ be the vector $(x_n^{(k)})$

Then by Siegel's Lemma — $\exists$ $\neq 0$ int solution $\vec{y}$ of $A' \cdot \vec{y} = 0$ with

$$H(\vec{y}) \leq \left(Nd^2 \max_{m,n,j} |a_{mn}^{(j)}| \max_{j,k,\ell} |b_{jk}^{(\ell)}|\right)^{\frac{M}{N-M}}$$

Let σ be ranging over $d = [K : \mathbb{Q}]$ different embeddings of K into $\mathbb{C}$. By conjugating with all σs & using $(\sigma(w_j))$ is an invertible $d \times d$-matrix (because square of det is discriminant) Hence

$$\max_j |a_{mn}^{(j)}| \le C_2' \max_\sigma |\sigma(a_{mn})|$$

for a suitable constant C_2'. Then $x_n = \sum_{k\ge 1}^{d} x_n^{(k)} w_k$ yields $H(\vec{x}) \le C_1 H(\vec{y})$ and

using $C_2 := C_2' d^2 \max_{j,k} |b_{jk}^{(l)}|$ we are done.

Aside: If you are interested

Here is an improved bound for Siegel's Lemma specific for a given number field of degree d.

(2.4.4) Thm (Bombieri, Vaaler). Let A be $M \times N$ matrix of rank M with entries in K where K # field, $\deg(K) = d$, Discriminant $D_{K/\mathbb{Q}}$

Then the K-vector space of solutions of $A\vec{x} = 0$ has basis $\vec{x}_1, \ldots, \vec{x}_{N-M}$, contained in $\mathcal{O}_K^N$.

Such that $$\prod_{l\ge 1}^{N-M} H(\vec{x}_l) \le |D_{K/\mathbb{Q}}|^{\frac{N-M}{2d}} H_{Ar}(A)$$

we have not talked about H_{Ar} yet — but rest assured & we'll do it after proof of Roth's thm).

Rmk $H(\vec{x})$ is multiplicative homogeneous ht, so we consider $\vec{x}$ as a pt in $\mathbb{P}^{N-1}(K)$

so no deep information contained in the statement we can choose our solutions in $\mathcal{O}_K^N$. because $\lambda\cdot\vec{x}$ doesn't change ht for $\forall\lambda\in K$

Rmk $H_{Ar}(A)$ is multiplicative Arakelov Ht of the line $\Lambda^M W$ in the projective space $\mathbb{P}(\Lambda^M K^N)$. Difference with usual ht consists only in using the L^2-local ht. instead of L^∞-local ht. at the archimedean places.

Let $W \subseteq K^N$ subspace spanned by rows of A

Def $H_{Ar}^{row}(A) := H_{Ar}(W) = H_{Ar}(\Lambda^R W)$.

where $\Lambda^R W$ viewed as a pt of projective space $\mathbb{P}(\Lambda^R K^N)$.

Cor Let A as $M\times N$ / K of rank R. Then $\exists$ a basis $\vec{x}_1, \ldots, x_{N-R}$ of $\ker(A)$, contained in $\mathcal{O}_K^N$, such that

$$\prod_{\ell=1}^{N-R} H(\vec{x}_\ell) \leq |D_{K/\mathbb{Q}}|^{\frac{N-R}{2d}} H_{Ar}^{row}(A)$$

Rmk If A_m is the mth row of A, then

$$H^{new}_{Ar}(A) \le \prod_m H_{Ar}(A_m)$$

where m ranges over R linearly independent rows of A. denote by $H(A)$ "multiplicative ht of matrix A" as a point $\mathbb{P}_K^{NM-1}$

so $H_{Ar}(A_m) \le \sqrt{N}\, H(A)$ gives

Cor
$$\prod_{l=1}^{N-R} H(\vec{x}_l) \le |D_{K/\mathbb{Q}}|^{\frac{N-R}{2d}} (\sqrt{N}\, H(A))^R.$$

In particular, $\exists \ne 0$ solution $\vec{x} \in \mathcal{O}_K^N$ of $A\vec{x} = 0$ with

$$H(\vec{x}) \le |D_{K/\mathbb{Q}}|^{\frac{1}{2d}} (\sqrt{N} H(A))^{\frac{R}{N-R}}$$

Now for $\forall v \in M_K$, v archimedean, let S_v be non-empty, convex, symmetric, open subset of K_v^N. (By symmetric we mean $S_v = -S_v$).

Now for $v \in M_K$ NOT Archimedean. Let S_v be K_v-lattice in K_v^N. (Namely, a non-empty compact and open R_v submodule of K_v^N, assume $S_v = R_v^N$ for all but finitely-many v.

Def: $\Lambda := \{\vec{x} \in K^N \mid \vec{x} \in S_v$ for $\forall$ non-archimedean $v\}$.

is a K-lattice in K^N (f.g. as $\mathcal{O}_K$-module

Denote Λ_∞ to be $\mathrm{Im}(\Lambda)$ under canonical embedding $K^N \to E_\infty := \prod_{v|\infty} K_v^N$.

Λ_∞ is then an $\mathbb{R}$-lattice in E_∞.

So Λ_∞ is discrete subgroup of $\mathbb{R}$-vector space E_∞ & E_∞/Λ_∞ is compact.

Def nth successive minimum of the non-empty convex, symmetric open subset $S_\infty := \prod_{v|\infty} S_v$ of E_∞ w.r.t. Λ_∞ is

$\lambda_n := \inf\{t>0 \mid tS_\infty$ contains n K-linearly independent vectors of $\Lambda_\infty\}$.

Now Adelic Minkowski's second theorem

Thm Successive minima satisfy

$$(\lambda_1 \lambda_2 \cdots \lambda_N)^d \prod_{v \in M_K} \beta_v(S_v) \leq 2^{dN}.$$

Now let Q_v^N be the unit cube in K_v^N of volume 1 w.r.t. Haar measure β_v.

$$Q_v^N := \begin{cases} \max \|x_n\|_v \leq \frac{1}{2} & v \in \mathbb{R} \\ \max \|x_n\|_v < \frac{1}{2\pi} & v \text{ complex} \\ \max \|x_n\|_v \leq 1 & v \text{ non-archimedean} \end{cases}$$

Now A matrix rank M, entries in K

Set $S_v := \{\vec{y} \in K_v^M \mid A\vec{y} \in \mathcal{O}_v^N\}$.

If v archimedean, $S_v \neq \emptyset$, convex, symmetric, bounded open set of K_v^M, w.r.t. to injective map $\vec{x} \mapsto A\vec{x}$, $\mathrm{Im}(S_v)$ is a linear slice of $\mathcal{O}_v^N$.

2.9.5 Prop If v non-arch, then:

$$\beta_v(S_v) \geq \| \det(A^* A) \|_v^{-\frac{1}{2}}$$

v non-archi. where $A^* = \overline{A^t}$ is transpose conjugate of A. (β_v is Haar measure of v).

Prop Let v be non-archimedean place of K lying over prime p. Then

$$\beta_v(S_v) = |D_{K_v/\mathbb{Q}_p}|_p^{\frac{M}{2}} \left(\max_I \|\det(A_I)\|_v\right)^{-1}$$

where I ranges over all subsets of $\{1, \ldots, N\}$ of cardinality M and A_I is the $M \times M$ matrix formed by the ith rows of A with $i \in I$.

The above prop shows S_v is a R_v-lattice in K_v^M for $\forall$ non-archimedean v and $S_v = R_v^M$ for all but finitely-many v.

Now ready for main results.

29.18

Prop Let A be defined as before ($M \times N$, $r \cdot M$ entries in K). Then image of A has a basis $\vec{x}_1, \dots, \vec{x}_M$, with

$$\prod_{m=1}^{M} H(\vec{x}_m) \le \left(\frac{2}{\pi}\right)^{\frac{Ms}{d}} |D_{K/\mathbb{Q}}|^{\frac{M}{2d}} H_{Ar}(A).$$

where s is the # of complex places of K.

From this, we'll have relative version of Siegel's Lemma:

29.19

Thm Let K be a # field, $\deg(K) = d$, discriminant $D_{K/\mathbb{Q}}$. Let F be f.d. field extension of K of deg $r = [F:K]$. Let A be $M \times N$ matrix, entries in F, assume $rM < N$. Then $\exists$ $N - rM$ K-linearly independent vectors $\vec{x}_\ell \in \mathcal{O}_K^N$ such that

$$A\vec{x}_\ell = 0, \quad \ell = 1, 2, \dots, N - rM.$$

and
$$\prod_{\ell=1}^{N-rM} H(\vec{x}_\ell) \le |D_{K/\mathbb{Q}}|^{\frac{N-rM}{2d}} \prod_{i=1}^{M} H_{Ar}(A_i)^r$$

where A_i is the ith row of A.

Roth Theorem