Week 2

1. Siegel's Lemma

2. Introduction to Diophantine approximation - Thue

**Lemma**

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

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

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

$$\max_{i=1}^{M} |x_i| \leq \left\lfloor \left( \frac{BM}{\sqrt{M}} \right)^{1/N} \right\rfloor.$$

**Proof**

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

$$T := \{ x \in \mathbb{Z}^N \mid 0 \leq x_i \leq k, \ i = 1, \ldots, N \}.$$

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

$$b \tilde{S}^+ \leq y_m \leq b \tilde{S}.$$
Let $T' = \{y \in \mathbb{Z}^m \mid b^T y \geq k b^T S y, 5 \leq k \leq m\}$. Writing $B_{m+1} = \text{max} |A_{m+1}|$, we have $S_{m+1} \leq NB_{m+1} \Rightarrow$ conclude $T'$ has at most $T (Nk B_{m+1})$ elements. Choose $b$ so $T$ has more elements than $T'$

$$T (Nk B_{m+1}) < (b+1)^N, \quad \text{(A)}$$

If we choose $b$ to be integer part of $\frac{1}{N} (NB_{m+1})^{\frac{1}{m}}$, and use $N k B_{m+1} < (NB_{m+1})^{\frac{1}{m}}$ then easily verify (A) is satisfied.

Now by Pigeon-hole, $\exists \ x^1, x^2 \in J$ with $A x^1 = A x^2$. The point $x^1 - x^2$ is a solution of $A x = 0$ in integers, with max. norm.

2.9.2

Consider $R = \text{field}$, $d(k) = d_k$, $k \in \mathbb{C}$, $1 \leq 1$ usual absolute value on $\mathbb{C}$. Let $A, N, C_{1,2}$, $0 \leq M < N$. Then $C_1$ the constants $C_1$, $C_2$ such that for any non-zero $N \times N$ matrix $A$ with entries $A_{nm} \in \mathbb{C}$, there is $x \in \mathbb{C}^N$ \{ for $A \cdot x = 0 \}$ and $H_1 (x) = C_1 C_G (A_{nm})$ with $G$ ranging.

$$H_1 (x) = C_1 C_G (A_{nm})$$
over the embeddings of $k$ into $G$

If \( \{x_j : j \in J \} \) was a $2$-basis of $U_k$. Then
\[
\alpha_{mn} = \frac{1}{2} \sum_{j \in J} \alpha_{mn} w_j, \quad \alpha_{mn} \in \mathbb{Z}.
\]

Using \( x_n = \sum_{b \in B} x_{n(b)} w_b \), we get
\[
(a - \frac{1}{2})_{mn} = \sum_{n=1}^{10} \sum_{b \in B} \alpha_{mn} w_b x_{n(b)} = \sum_{n=1}^{10} \sum_{b \in B} \alpha_{mn} b_{n(b)}^2
\]

Where \( w_j w_b = \frac{1}{2} b_{j b} \). Let \( A' \) be the \((Na) \times (Na)\) matrix \( A' = \left( \sum_{n=1}^{10} \sum_{b \in B} \alpha_{mn} b_{n(b)}^2 \right) \).

with rows indexed by \( (m, b) \), columns indexed by \( (n, b) \), and let \( \tilde{\gamma} \in \mathbb{R} \) not be the vector \( (X_b) \).

Then by Siegel's lemma \( -\tilde{\gamma} \) is a solution \( \tilde{y} \) of \( A\tilde{y} = 0 \) with
\[
H(\tilde{y}) = \left( N\tilde{\gamma}^2 \max |\alpha_{mn}| \max |b_{n(b)}| \right)^\frac{1}{2}.
\]

Let \( \delta \) be ranging over all $cl: \mathbb{H} \to \mathbb{Q}$ different embeddings of $k$ into $G$. By conjugating with all \( \delta \) & using \( I(k_{\delta}) \) is an invertible \( cl-k\)-matrix because square of \( cl \) is discriminant) Hence
\[
\max \left\{ \frac{1}{d} \right\} \leq C \max \left\{ \delta \left( \frac{d}{a_n} \right) \right\}
\]

for a suitable constant \( C \). Then \( x_n = \sum_{k=1}^{\infty} x_{n_k} \) yields

\[
H(x) \leq C H(g)
\]

and

\[
\text{using } G := G_1 \text{ we are done.}
\]

Aside: If you are interested

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

Then (Bambah, Vaaler). Let \( A \) be \( M \times N \)

matrix of rank \( M \) with entries in \( K \)

where \( K \) is field, \( \text{deg} (K) = d \). Discriminant \( D_K \).

Then the \( K \)-vector space of solutions of \( Ax = 0 \)

has basis \( x_1, \ldots, x_{N-M} \) contained in \( U_K \)

such that

\[
\sum_{k=1}^{N-M} H(x_k) \leq D_K^2 \text{ Har}(A)
\]

we have not talked about \( \text{Har} \) yet — but

rest assured & we'll do it after proof of

Roth's thm).

Pipe \( H(x) \) is multiplicative homogeneous at

so we consider \( x \) as a pt in \( \mathbb{R}^\mathbb{N} \).
so no deep information contained in the statement we can choose our solutions in $O(K)$ because $A \cdot \bar{x}$ doesn't change it for $A \cdot x$

**Prop.** $Har(A)$ is multiplicative. And below $H_{\bar{t}}$ of the line $A^M W$ in the projective space $\mathbb{P}(A^M K^N)$. Difference with usual $H_{\bar{t}}$ consists only in using the $L^2$-local $H_{\bar{t}}$ instead of $L^\infty$-local $H_{\bar{t}}$ at the archimedean places.

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

**Def.** $Har(A) := Har(W) = Har(A^R W)$.

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

**Cor.** Let $A$ as $M \times N / R$ of rank $R$. Then $\exists$ a basis $x_1, \ldots, x_{\min\{M, N\}}$ of $\ker(A)$, contained in $O(K)$, such that

$$\frac{N \cdot R}{2^\alpha} \left| H_{\bar{t}}(x_i) \right| < \frac{1}{10K^2} \sqrt{N \cdot R} Har(A)$$

$\bar{t}$ is the $m$th row of $A$, then
\[ H_{\text{AR}}(A) = \frac{1}{n} H_{\text{AR}}(A^n) \]

where \( n \) ranges over the linearly independent rows of \( A \). denote by \( H(A) \) the multiplicative subset of \( \text{cont}(A)^n \) as a point \( p_{\text{AR}} \in \mathbb{A}^1 \).

so \( H_{\text{AR}}(A^n) = \frac{1}{n} H(A) \) gives

\[
\text{Con} \quad \frac{\mathbf{U}, R}{\mathbf{1}} H(x^n) \leq \frac{1}{D_{\mathbf{R}^n}} \left( \frac{UR}{2n} \right)^{\frac{1}{2n}} (\frac{H(A)}{R})^R.
\]

In particular, \( \exists \) solution \( x \in \mathbb{C}^{n \times n} \) of

\[
\mathbf{Ax} = 0 \quad \text{with}
\]

\[
H(x) \leq \left( \frac{1}{D_{\mathbf{R}^n}} \right)^{\frac{1}{2n}} (\frac{H(A)}{R})^R.
\]

Now for \( A \in \mathbb{M}_{n \times n} \), \( \nu \) archimedean let \( S_\nu \) be non-empty, convex, symmetric \& open subset of \( \mathbb{K}^n \). (By symmetric, we mean \( S_\nu = -S_\nu \)).

Now for \( \nu \in \mathbb{M}_{n \times n} \) NOT archimedean. let \( S_\nu \) be \( \mathbb{K}^n \)- lattice in \( \mathbb{K}^n \). (Namely, a non-empty compact and open \( \mathbb{K}^n \) submonad of \( \mathbb{K}^n \), assume \( S_\nu - R \nu \) for all but finitely many \( \nu \).

def: \( \Delta = \{ x \in \mathbb{G}_{\text{K}}^{n \times n} | x \in S_\nu \text{ for a non-archimedean } \nu \} \).

is a \( \mathbb{K}^n \)- lattice in \( \mathbb{K}^n \) (f.g. as \( \mathbb{K}^n \)-module).
Denote $\Lambda_{\infty}$ to be $\text{Im}(\Delta)$ under canonical embedding $K^N \to E_\infty := \bigoplus_{n \geq 1} K^n$.

$\Lambda_{\infty}$ is then an $R$-sublattice in $E_\infty$, so $\Lambda_{\infty}$ is discrete, $R$-subgroup of $R$-vector space $E_\infty$ and $E_\infty/\Lambda_{\infty}$ is compact.

Def $n$th successive minimum of the non-empty, convex, symmetric open subset $S_0$ := $T$ of $G_\infty$ w.r.t. $\Lambda_{\infty}$ is

$\Lambda_n := \inf \{ x \in \Lambda_{\infty} : x \not\in S_0 \}$

contains $n$ linearly independent vectors of $\Lambda_{\infty}$.

New Adelic Minkowski's Second theorem

The successive minima satisfy

\[
\sum_{n=1}^{\infty} \Lambda_n \leq 2 \text{dim } K.
\]

Rem

Now let $Q_N$ be the unit cube in $E_N$ of volume $1$ w.r.t. Haar measure $\nu$.

\[
Q_N := \prod_{i=1}^{\text{max } i \leq \frac{1}{2N}} v_{\mathbb{C}}
\]

Now $A$ matrix rank $N$, entries in $K$.
Set $S_v = \{ y \in K^M | A^* y \in \mathbb{Q}^n \}$.

If $v$ archimedean, $S_v \neq \emptyset$, convex, symmetric, bounded open set of $K^M$ want to inject the map $x \mapsto A^* x$, $\varphi_n(S_v)$ is a linear slice of $\mathbb{Q}^n$.

2.9.1

If $v$ non-arch. then:

$\varphi_n(S_v) \preceq 11 \det(A^* A) 11_n^2$

$v$ non-arch. where $A^* = A^T$ is transpose conjugate of $A$. ($\nu$ is Haar measure of $v$).

Prop

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

$\varphi_n(S_v) = \prod_{\ell \in \mathbb{L}} \varphi_n(S_v) \cdot \prod_{m \in M} \varphi_n(S_v)\phantom{.} = 11 \det(A^* A) 11_n^2$

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

The above prop shows $S_v$ is a $K_v$-lattice in $K^M$ for $v$ non-archimedean $v$ and $S_v = \mathbb{R}^M$ for all but finitely many $v$. 
Now ready for main results.

App. let $A$ be defined as before ($\mathbb{M} \times \mathbb{N}, r \times M$ entries in $K$). Then image of $A$ has a basis $\tilde{x}_1, \ldots, \tilde{x}_M$, with

$$M \prod_{m=1}^{M} H(\tilde{x}_m) > \left( \frac{2}{\pi} \right) \frac{M}{2} \log \frac{M}{2} \log |D_K / K| \log |H_{ar}(A)|,$$

where $s$ is the # of complex places of $K$.

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

Thus, let $K$ be a # field, $d = d_K$, discriminant $D_K$. Let $F$ be a finite field extension of $K$ of degree $r = [F:K]$. Let $A$ be $\mathbb{M} \times \mathbb{N}$ matrix entries in $F$; assume $r \times M \times N$. Then there are $K$-linearly independent vectors $\tilde{x}_e \in \mathbb{O}_K^N$ such that

$$A \tilde{x}_e = 0, \quad e = 1, 2, \ldots, N - rM.$$

and

$$M \prod_{m=1}^{M} H(\tilde{x}_e) > \left( \frac{2}{\pi} \right) \frac{M}{2} \log \frac{M}{2} \log |D_K / K| \log |H_{ar}(A)|,$$

where $A_i$ is the $i$th row of $A$.

Roth Theorem