W4D2

# Geometry of Numbers

## Applications of Minkowski's Theorem for Algebraic Number Theory

Thm (Minkowski's bound)

Let $k$ be a num. field $\deg(k/\mathbb{Q})=n$ with $r$ real embeddings and $s$ pairs of conjugate complex embeddings (so $n=r+2s$). Let $D$ be the discriminant of $k$. Then $|D|\geq\left[\left(\frac{\pi}{4}\right)^s\frac{n^n}{n!}\right]^2$.

Terminology

$\mathbb{Q}\subseteq k$ number field $\Leftrightarrow \deg(k/\mathbb{Q})=n<\infty$.

Fact 1 $n$=number of embeddings $k\hookrightarrow\mathbb{C}$. If $\sigma:k\hookrightarrow\mathbb{C}$ is an embedding so is $\bar{\sigma}:k\hookrightarrow\mathbb{C}$ - different if $\sigma$ isn't a real embedding - pairs of conj. complex embeddings.

$\sigma_1,\sigma_2,\dots\sigma_r,\sigma_{r+1},\dots\sigma_{n}$ where $\bar{\sigma}_{r+i}=\sigma_{r+s+i}$.

$x\in\mathbb{C}$ algebraic-root of a polynomial with int coeffs.

If $x\in k$ then $1,\dots,x^n$ lin. ind so $\forall x\in k$ is algebraic.

If the pol. is monic $x$ is an algebraic integer.

The algebraic integers form a ring $\mathcal{O}_k$

Pf Assume $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$, so $\mathbb{F}_{p^n}$ is a vector space of dim. $d$ over $\mathbb{F}_{p^m}$ so $(p^m)^d = p^{md} = p^n \to m|n$.

Assume $m|n$. ~~So say $y^d - 1 = (y-1)(1 + \dots y^{d-1})$ so take~~ take $d = \frac{m}{n}$. So ~~$x^{p^m} - 1 = (x^{p^m} - 1)(1 + \dots x^{p^m})$. Therefore~~

$x \in \mathbb{F}_{p^m} \to x^{p^m} = x \to x^{p^{2m}} = x^{p^m} = x \to \dots \to x^{p^{md}} = x^{p^n} = x \to x \in \mathbb{F}_{p^n}$.

Lemma $n = \sum_{d|n} \phi(d)$, where $\phi(d) = \#\{1 \leq x < d \mid \gcd(x,d) = 1\}$.

Pf. Since $\phi$ is mult. (i.e. $\phi(mn) = \phi(m)\phi(n)$ whenever $\gcd(m,n) = 1$) $h(n) = \sum_{d|n} \phi(d)$ is mult. Ex. – $f,g$ mult $\to$ $f * g\,(n) = \sum_{d|n} f(d) g(\frac{n}{d})$ is also mult. $id(n) = n$ is also mult, so it suffices to show equality on prime powers: $h(p^\nu) = \sum_{1 \leq e \leq \nu} \phi(p^e) + 1 = (p-1)\sum_{1 \leq e \leq \nu} p^{e-1} + 1 = p^\nu - 1 + 1 = p^\nu$ so $n = \sum_{d|n} \phi(d)$ for any $n$. $\square$

exp. sums

Geometry of Nums

Additively $\mathcal{O}_k = \mathbb{Z}\alpha_1 + \dots \mathbb{Z}\alpha_n$ (rank $n$ abelian group). For each $\alpha \in k$, multiplication by $\alpha$ is a linear transformation $M_\alpha : k \to k$.

trace & det are invariant under conjugation.

$t(\alpha) = tr(M_\alpha)$ the trace of $\alpha$. Independent of basis choice.

$N(\alpha) = \det(M_\alpha)$ the norm of $\alpha$, also ind. of basis.

Let $\alpha_1, \dots \alpha_n \in \mathcal{O}_k$ be a basis for $\mathcal{O}_k$, then

$D = \det\{t(\alpha_i \alpha_j)\}_{1 \leq i,j \leq n}$ is the discriminant of $k$.

Sorry, I had some confusion

We'll see $D$ is ind. on choice of $\alpha_1, \dots \alpha_n$, and give $D$ some "geometric interpretation."

$N(\alpha) : k \to \mathbb{C}$ multiplicative, $t(\alpha) : k \to \mathbb{C}$ additive.

Fact 3 $N(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha)$, $t(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha)$. Idea – $a_0 + a_1\alpha + \dots + a_n\alpha^n = 0 \to$

$0 = M_{a_0 + a_1\alpha + \dots a_n\alpha^n} = a_0 I + a_1 M_\alpha + \dots + a_n M_\alpha^n$. $\rightsquigarrow$ char. pol of $M_\alpha$ = power of min. pol. of $\alpha$.

Cor. $\alpha \in \mathcal{O}_k \to N(\alpha), t(\alpha) \in \mathcal{O}_k$.

Fact 4 $\mathbb{Q} \cap \mathcal{O}_k = \mathbb{Z}$.

Cor $N(\alpha), t(\alpha) \in \mathbb{Z}$ for $\alpha \in \mathcal{O}_k$. So, $D \in \mathbb{Z}$.

Let $\alpha_1, \dots \alpha_n$ be a basis of $\mathcal{O}_k$ and $\alpha_i^{(j)} = \sigma_j(\alpha_i)$.

Since $\omega \in \mathcal{O}_k$ is $\sum_{i=1}^{n} a_i \alpha_i$, $\sigma_j(\omega) = \sum_{i=1}^{n} a_i \alpha_i^{(j)}$. Extend this formula for $a_i \in \mathbb{R}$ – $\xi_j : \mathbb{R}^n \to \mathbb{C}^n$. $\xi_j(x_1, \dots x_n) = \sum^{n} x_i \alpha_i^{(j)}$.

The image of $\bar{\xi}$ is a real vector space $V$ in $\mathbb{C}^n$.
$\bar{\xi}(Q_n)$ is dense in it.

<u>Claim</u> $V$ is $n$-dimentional over $\mathbb{R}$ (equiv. $\det\{(\alpha_i^{(j)})\}_{1\le i,j\le n} \neq 0$

<u>Fact 5</u> $\mathcal{O}_k$ contains $n$ lin. ind. (over $\mathbb{Q}$) elements, That is, $\mathcal{O}_k$ contains a basis of $k$ (as a rational vector space). Idea $\forall \alpha\in k \exists p\in\mathbb{Z}, p\alpha\in\mathcal{O}_k$.

So to prove <u>claim</u>, we can replace $\alpha_1,\dots,\alpha_n$ with any basis $\beta_1,\dots,\beta_n$ of $k$ (as a $\mathbb{Q}$ vector space).

<u>Fact 6</u> (hopefully the last one) $\exists \beta\in k, 1,\beta,\dots,\beta^{n-1}$ is a basis of $k$.

<u>proof:</u> Enough to show $\det\{\sigma_j(\beta^i)\}_{1\le i,j\le n} = \det\{(\sigma_j\beta)^i\}_{1\le i,j\le n}$ which is a determinant of a vandemonde matrix, and therefore non-zero.

<u>Geometric Interpretation of $D$:</u>

<u>Claim</u> $D = \left(\det\{(\alpha_i^{(j)})_{1\le i,j\le n}\}\right)^2 \left[= \det(\bar{\xi})^2\right]$

<u>proof</u> $\det(\{\alpha_i^{(j)}\}_{1\le i,j\le n})^2 = \det(\{\alpha_i^{(j)}\}_{1\le i,j\le n})\cdot\det(\{\alpha_j^{(i)}\}_{1\le i,j\le n}) =$

$$= \det\left(\left\{\sum_{j=1}^n \alpha_k^{(j)}\alpha_\ell^{(j)}\right\}_{1\le k,\ell\le n}\right) = \det\left(\left\{\sum_{j=1}^n \sigma_j(\alpha_k\alpha_\ell)\right\}_{1\le k,\ell\le n}\right) =$$

$$= \det\left(\{t(\alpha_k\alpha_\ell)\}_{1\le k,\ell\le n}\right) = D.$$

This computation also shows $D$ is ind. of choice of $\alpha_1,\dots,\alpha_n$.

<u>Minkowski's bound - proof:</u> Let $S = \{x=(x_1,\dots,x_n)\in\mathbb{R}^n \mid |\xi_1(x)|+\dots+|\xi_n(x)|<\lambda\}$.

We can compute $\operatorname{Vol} S = \frac{2^r\pi^s\lambda^n}{n!\sqrt{|D|}}$. (Choose $\lambda = \left(\left(\frac{4}{\pi}\right)^s n!\sqrt{|D|}\right)^{1/n}$,

So $\operatorname{Vol}(S) = 2^n$. By Minkowski $\exists x\in\mathbb{Z}^n\cap S\setminus\{0\}$.

$\sum_{j=1}^n |\sigma_j(x)|<\lambda$. Then, for $\alpha=\sum_{i=1}^n x_i\alpha_i$ $1\le N(\alpha)\le\left(\frac{1}{n}\sum_{j=1}^n|\sigma_j(\alpha)|\right)^n \le \frac{\lambda^n}{n^n} =$

$$\frac{\left(\frac{4}{\pi}\right)^s n!\sqrt{|D|}}{n^n} = \frac{4^s\, n!\sqrt{|D|}}{\pi^s\, n^n}.$$

Therefore $\left[\frac{\pi^s n^n}{4^s n!}\right]^2 \le |D|$.

<u>Some conclusions of this bound:</u>

- Dirichlet's theorem on Units

* Finiteness of class numbers.

* No unramified extensions over $\mathbb{Q}$.

Warning $D = (\det(\cdot))^2 = d$. In the literature $\Delta$ may denote $D$ or $d$ arbitrarily.

Dirichlet's Thm. on Units:

A unit in $\mathcal{O}_k$ is an alg. int. whose inverse in an alg. int. – alt. $\alpha \in \mathcal{O}_k$ with $N(\alpha) = 1$ – alt. $\alpha$ is root of monic pol with last coeff. $\pm 1$. The units $\mathcal{O}_k^*$ form a multiplicative group.

Dirichlet's Theorem $\mathcal{O}_k^*$ contains a finite index subgroup isomorphic to $\mathbb{Z}^{r+s-1}$. In particular of rank $n-1$ if $k$ is totally real. Will be in one of the excersices.

Quadratic Forms

$Q: \mathbb{R}^n \to \mathbb{R}$ homogenous polynomial of deg. 2. That is, $Q(x_1, \dots x_n) = \sum_{i,j=1}^{n} a_{ij} x_i x_j$. This way there's some ambiguity so sometimes we'll insist $a_{ij} = a_{ji}$ (no loss of generality – can replace both with the average). However, when we disuss quad. forms with int. coefts we can't require symmetry WLG.

It's convenient to think of $Q(x)$ as $L(x,x)$ where $L: \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^n$, $L(x,y) = \sum_{i=1}^{n} a_{ij} x_i y_j$ a bilinear form.

Equiv., $(x_1, \dots x_n)(a_{ij})\begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$ or $\langle x, (a_{ij}) y \rangle$. When extendind quad. forms we insint on symmetry and a symmetric quad. form $L(x,y) = L(y,x)$.

Classical question – find $x \in \mathbb{Z}^n \setminus \{0\}$ to minimize $|Q(x)|$. (Find the inf?)

Note: base change $\underset{\text{original base}}{\overset{\text{transition matrix}}{B}x} = \underset{\text{new base}}{\xi}$, $By = \eta$, $L(\xi, \eta) = x^{tr} \underbrace{B^{tr}(a_{ij})B}\, y$.

Symm. Bilinear forms up to some such transformation (over $\mathbb{R}$) are just $\begin{pmatrix} I_p & & \\ & -I_q & \\ & & 0 \end{pmatrix}$ for $p, q \in \{0, \dots, n\}$, $p+q \leq n$. $(p,q)$ are called the signature of $L$. If $p+q = n$ then $L$ (sometimes $Q$) is nondegenerate $\iff \forall x \in \mathbb{R}^n\ \exists y \in \mathbb{R}^n\ L(x,y) \iff \det(a_{ij}) \neq 0$.

If $p=n$ $L$ is positive definite $\iff \forall x\in\mathbb{R}^n\setminus\{0\}, Q(x)>0$.

If $Q$ has signature $(p,q)$, then after change of variables $Q(x)=x_1^2+\dots+x_p^2-(x_{p+1}^2+\dots+x_{p+q}^2)$.

Lemma let $Q$ be a quad. form, $K_{>0}\in\mathbb{R}$.

TFAE:

(i) In every lattice $\Lambda$ there is $\lambda\in\Lambda\setminus\{0\}$ s.t. $|Q(\lambda)|\leq K\, d(\Lambda)^{2/n}$.

(ii) for every $\Lambda\in\mathcal{L}_n$, $\exists\lambda\in\Lambda\setminus\{0\}$ s.t. $|Q(\lambda)|\leq K$.

lattices of covolume 1.

(iii) for every $\Lambda$ with $d(\Lambda)\leq K^{-n/2}$ $\exists x\in\Lambda\setminus\{0\}$ with $|Q(\lambda)|\leq 1$.

Some mistake here (iv) for every quad. form $\tilde{Q}(x)=\sum_{i,j=1}^{n}a_{ij}x_ix_j$ with same signature $\exists u\in\mathbb{Z}^n\setminus\{0\}$, $|\tilde{Q}(x)|\leq K(\det(a_{ij}))^{1/n}$. $a_{ij}=a_{ji}$

Obviously (i-iii) all equiv. up to rescaling. The interasting part is the equivalence to (iv).

proof (i)$\iff$(ii)$\iff$(iii) trivially, as explained above.

(iv)$\Rightarrow$(iii) Let $\Lambda$ be a lattice. Choose $B$ invertible s.t. $\Lambda=B\mathbb{Z}^n$. $d(\Lambda)=|\det B|\leq K^{-n/2}$.

Define $\tilde{Q}(x)=Q(Bx)$ - it's signature is equal to $Q$'s signature, $\tilde{Q}(x)=x^tB^t(a_{ij})Bx$ and by (iv) $\exists\mu\in\mathbb{Z}^n\setminus\{0\}$, $\underbrace{|\tilde{Q}(\mu)|}_{=Q(Bu)}\leq K\det(B^t(a_{ij})B)^{1/n}=$

$K\underbrace{\det B^{2/n}}_{d(\Lambda)^{1/n}}$ and (iii) follows.

The oter direction is similar.

Cor. Let $Q$ be positive definite $\sum_{i,j=1}^{n}a_{ij}x_ix_j$. Then $\exists u\in\mathbb{Z}^n\setminus\{0\}$ s.t. $|Q(u)|\leq 4\left[\frac{|\det(a_{ij})|}{V_n^2}\right]^{\frac{1}{n}}$ ($V_n$ - volume of the unit ball in $n$ dimensions).

pf: this is part (iv) of the lemma with $K=\frac{4}{V_n^{2/n}}$. By (iii) it suffices to show $d(\Lambda)\leq K^{-\frac{n}{2}}=\frac{V_n}{2^n}$ then $\Lambda\setminus\{0\}$

intersects the unit ball, which is true by Minkovski.
$Q(x) \leq 1$ for $Q(x) = \sum_{i=1} x_i^2$
with equal signature.

$f$ is ~~pos. def.~~ pos. def. or neg. def.

$A, 2B, C \in \mathbb{Z}$

Cor 2 If $f(x,y) = Ax^2 + 2Bxy + Cy^2$ with $\boxed{AC - B^2 > 0,}$ we can solve $|f(x,y)| \leq \frac{2}{\sqrt{3}}\sqrt{AC-B^2}$ in integers. Not true for any smaller const. instead of $\frac{2}{\sqrt{3}}$.

pf Lemma (iv) with $\underset{f(u)}{f(x,y)} = \tilde{Q}(x)$ says we can solve $|f(u)| \leq \lambda\sqrt{AC-B^2}$ iff we can solve $\sum_{i=1}^{n} \lambda_i^2 \leq 1$ for some $\lambda \in \Lambda$ in every $\Lambda$ of $d(\Lambda) \leq \frac{1}{\lambda}$, $\Leftrightarrow \Delta_2 \geq \frac{1}{\lambda}$ ($\Delta_2$ = lattice const. for euclidean unit ball, which we've calculated to be $\frac{2}{\sqrt{3}}$). So $\lambda$ must be at least $\frac{2}{\sqrt{3}}$ for the above to hold.

Algebraic proof of Cor 2

Tak $u$ that minimizes $|f(u)|$. So $u \neq cw$ for $w \in \mathbb{Z}^2$ and $c \neq \pm 1$, $u$ is primitive. By prev. lacture, we can complete $u$ to a basis $u, v$. Choose $v$ for which $|f(v)|$ is minimal. Let $A \in GL_2(\mathbb{Z})$ s.t. $Ae_1 = u$, $Ae_2 = v$, $g = f \circ A^{-1}$, then $g(x,y) = A'x^2 + 2B'xy + C'y^2$ with $A'C' - B'^2 = AC - B^2 > 0$.

$g(e_1) = A'$, so $g(x,y) = A'(x + \frac{B'}{A'}y)^2 + (C' - \frac{B'^2}{A'^2})y^2$.

Let $y = 1$, choose $x$ with $|x + \frac{B'}{A'}| \leq \frac{1}{2}$, so

$$A' = g(e_1) \leq g(x,1) \leq \frac{A'}{4} + \left(C' - \left(\frac{B'}{A'}\right)^2\right) = \frac{A'}{4} + \frac{AC - B^2}{A'}.$$ So

[Denote $D = AC - B^2$] $\frac{D}{A'} \geq \frac{3}{4}A' \Leftrightarrow D \geq \frac{3}{4}A'^2$. So,

$$A' = g(e_1) = \min_{u \in \mathbb{Z}^2 \setminus \{0\}} f(u) \leq \frac{2D}{\sqrt{3}} = \frac{2\sqrt{AC - B^2}}{\sqrt{3}}$$