Basic theory of lattices.

Def. Let V be a real vector space of dimension n.
~~Then $\Lambda \subseteq V$ is a full lattice if it is an additive subgroup~~
A **full lattice** $\Lambda \subseteq V$ is an additive subgroup

$$\mathbb{Z}e_1 + \mathbb{Z}e_2 + \cdots + \mathbb{Z}e_n$$

where the e_i are linearly independent over $\mathbb{R}$.

Notice we have $\Lambda \otimes_{\mathbb{Z}} \mathbb{R} = V$ (almost by definition).

Properties and questions.

(1) We can speak about them topologically.
Lattices are **discrete** (elts. separated by open sets).
This is not obvious.
Lattices are **cocompact** (i.e. V/Λ is compact)
They have a **volume** induced from that on $\mathbb{R}^n$, which is not 0 or infinity.
Can generalize to nonabelian settings. ($GL_2(\mathbb{Z}) \subseteq GL_2(\mathbb{R})$ is a "lattice".)

(2) We can speak about them analytically.
Given a lattice, which I have described... somehow.

What is the shortest vector?
Can vectors be arbitrarily close to 0?
(Yes, draw picture)
Can 0 be arbitrarily far away?
(no, convex body theorem)
What can we say? (Minkowski's second theorem)

(3) We can speak about them algebraically.

e.g. let $\phi : \Lambda \to \Lambda$ be an isomorphism.

Then $\phi \in GL_n(\mathbb{Z})$.

If $\phi : \Lambda \to \Lambda$ is merely an injection, can still write ϕ as a matrix.

Relate $\det(\phi)$ to $|\Lambda : \mathrm{Im}(\phi)|$.

Smith normal form, etc.

(4) Talk about the space of lattices, etc.

e.g. space of n-dimensional lattices is

$GL_n(\mathbb{Z}) \backslash GL_n(\mathbb{R})$.

This gives it the structure of a smooth manifold, Haar measure, etc.

Plan. Cover intro material.

Proposition. (Cassels, p. 66)

Let $\Lambda \subset \mathbb{R}^n$ be a full lattice. Then there are constants η_1, η_2 depending only on Λ s.t.

(1) If $\vec{u} \in \Lambda$, $\vec{v} \in \Lambda$, $|\vec{u} - \vec{v}| < \eta_1$, then $\vec{u} = \vec{v}$.

(2) The number $N(R)$ of points of Λ in a sphere $|\vec{x}| < R$ is at most $\eta_2(R^n + 1)$.

Cor. of (1). Λ has the discrete topology.

Proof. Immediate. Given $\vec{u} \in \Lambda$, then let

$$B := \{ x \in \mathbb{R}^n \mid |\vec{x} - \vec{u}| < \eta_1 \}.$$

Then $B \cap \Lambda$ is equal to $\{\vec{u}\}$.

So it follows by definition.

Lemma. Suppose $\vec{x}, \vec{y} \in \mathbb{R}^n$, where $\vec{y} = M \cdot \vec{x}$ for some $M \in GL_n(\mathbb{R})$.

Then there exist constants c_1, c_2 depending only on M (not $\vec{x}, \vec{y}$) s.t.

$$0 < c_1 \leq \frac{|\vec{x}|}{|\vec{y}|} \leq c_2 < \infty .$$

Proof. We have $|\vec{y}|^2 = y_1^2 + y_2^2 + \cdots + y_n^2 = \sum_i y_i^2$

$$= \sum_i \left(\sum_j m_{ij} x_j \right)^2 \qquad \text{(with } M = (m_{ij})\text{)}$$

$$\leq n^3 \cdot A^2 \cdot \sum x_i^2 . \qquad \text{(with } A = \max_{i,j} |m_{ij}|\text{)}$$

So $|\vec{y}|^2 \leq n^3 \cdot A^2 |\vec{x}|^2$.

This gives one direction of the conclusion.

For the other, use $\vec{x} = M^{-1} \cdot \vec{y}$, and

$$|\vec{x}|^2 \leq n^3 \cdot (A')^2 |\vec{y}|^2 ,$$

where A' is the max of the entries of M^{-1}.

Proof of proposition. Let Λ be a full lattice, spanned by $f_1, \ldots, f_n$. Then,

$$\Lambda = M \cdot \mathbb{Z}^n , \quad \text{i.e., writing}$$

$$f_i = (m_{i,1}, m_{i,2}, \ldots, m_{i,n})$$

for each i,

since the f_i are linearly independent, we have $M \in GL_2(\mathbb{R})$.

18.4. For each basis vector f_i of Λ we have $f_i = M e_i$ where $e_i = (0, \cdots, 1, 0, \cdots 0)$

$$|f_i|^2 \leq n^3 \cdot A^2 \cdot 1,$$

with $A = \max |m_{ij}|$

but also $1 \leq n^3 \cdot A'^2 \cdot |f_i|^2$,

$$\text{so } |f_i| \geq \frac{1}{A' \cdot n^{3/2}}.$$

Moreover, for any nonzero vector g of Λ we have $g = M \cdot v$ for some $v \neq 0 \in \mathbb{Z}^n$, and

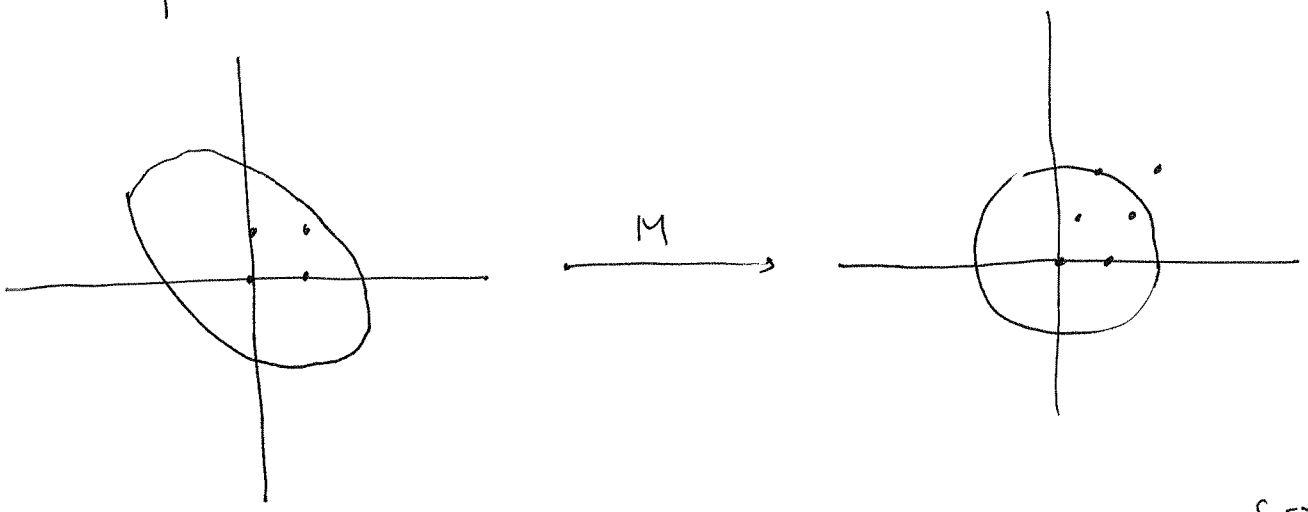
$$1 \leq |v| \leq n^3 \cdot A'^2 \cdot |g|^2$$

$$\text{and } |g| \geq \frac{1}{A' \cdot n^{3/2}}.$$

Remark. This shows g can be small if M is screwy. And indeed it can be.

Proof of part (2). (bounded # of points in a sphere)

One proof.



The number of points of Λ in a sphere $S = \{\vec{x} : |\vec{x}| \leq R\}$ is the number of points of $\mathbb{Z}^n$ in $M^{-1}S$. This has volume $|\det M|^{-1} \cdot \text{Vol}(S)$.

18.5.

(previous part!)

The points of $M^{-1}S$ all have length $\leq CR$, so the projections of $M^{-1}S$ onto the coordinate axes of dimension d all have volume $\leq (2CR)^d$.

~~(Hw: Make this explicit.)~~

And they are all convex.

So, by Davenport's Lemma, the number of lattice points in $M^{-1}S$ is

$$|\det M|^{-1} \cdot \underbrace{\mathrm{Vol}(S)}_{\substack{\text{Some constant} \\ \text{times } R^n.}} + \underbrace{O\left(\sum_{d<n} (2CR)^d\right)}_{\substack{\text{This is } O(R^{n-1}). \\ \text{Constant depends only on } M.}}$$

QED.

19.1. Lattices and sublattices.

Goal: Given lattices $\Lambda' \subseteq \Lambda$, show that

$$|\Lambda : \Lambda'| = \frac{\cancel{|\det(\Lambda')|}}{\cancel{|\det(\Lambda}} \quad \frac{\mathrm{Vol}(\Lambda')}{\mathrm{Vol}(\Lambda)}.$$

Here the volume of a lattice is the volume of a fundamental region.

If $x_1, \dots, x_n$ is a basis of Λ, then

$$\mathrm{Vol}(\Lambda) = \left|\det(x_1, x_2, \dots, x_n)\right|.$$

We argued previously that if $y_1, \dots, y_n$ is another basis, the volume doesn't change.

We have $(y_1, \dots, y_n) = M \cdot (x_1, \dots, x_n)$

for $M \in GL_n(\mathbb{R})$ with integer entries,

and $(x_1, \dots, x_n) = M^{-1} \cdot (y_1, \dots, y_n)$

M^{-1} also has integer entries

so $\det(M) = \pm 1$.

In fact, $M \in GL_2(\mathbb{Z}) = \{ M \in GL_2(\mathbb{R}) :$ all entries integers and same is true of $M^{-1} \}$

$= \{ M \in GL_2(\mathbb{R}) :$ all entries integers, $\det = \pm 1 \}$.

Theorem. (Cassels, p. 11)
~~19.20~~ (1) Given $\Lambda' \subseteq \Lambda$ and a basis $x_1, \dots, x_n$ of Λ.
There is a basis of Λ' ~~elements~~ $y_1, \dots, y_n$ s.t.

$$y_1 = v_{11} x_1$$
$$y_2 = v_{21} x_1 + v_{22} x_2$$
$$\vdots$$
$$y_n = v_{n1} x_1 + v_{n2} x_2 + \cdots + v_{nn} x_n$$

for v_{ij} integers, $v_{ii} \neq 0$ for all i.

19.2. (2) Given $\Lambda' \subseteq \Lambda$ and $y_1, \dots, y_n$ there are $x_1, \dots, x_n$ such that the previous holds.

Proof. (0) We can certainly write, for some basis $z_1, \dots, z_n$ of Λ'

$$(z_1, \dots, z_n) = M \cdot (x_1, \dots, x_n)$$

where $M \in GL_n(\mathbb{R})$ has integral entries.
(But maybe $M \notin GL_n(\mathbb{Z})$.)

Now, by the cofactor expansion, $(\det M) \cdot M^{-1}$ has integral entries as well.

We have

$$(\det M) \cdot M^{-1}(z_1, \dots, z_n) = (\det M) M^{-1} M (x_1, \dots, x_n)$$
$$= (\det M)(x_1, \dots, x_n).$$

Therefore, since $(\det M) \cdot M^{-1}$ is an injective map from Λ' to itself, we have

$$(\det M) \cdot \Lambda = (\det M) \cdot M^{-1} \Lambda' \subseteq \Lambda'$$

and hence $\boxed{(\det M) \cdot \Lambda \subseteq \Lambda' \subseteq \Lambda.}$

(1) Given $\Lambda' \subseteq \Lambda$, basis $x_1, \dots x_n$ of Λ.

~~(Choose some basis $z_1, \dots, z_n$ of Λ' satisfying~~

~~$z_i \in a_{i1} x_1 + a_{i2} x_2 + \dots + a_{ii} x_i$ (for each i).~~

~~Among all such choices, choose the z_i such that~~
~~$|a_{ii}|$ is as small as possible but nonzero.~~

There are certainly some points $z_1, \dots, z_n \in \Lambda'$

$$z_1 = v_{11} x_1$$
$$z_2 = v_{21} x_1 + v_{22} x_2$$
$$\vdots$$
$$z_n = v_{n1} x_1 + \dots + v_{nn} x_n$$

with all v_{ij} integers, $v_{ii} \neq 0$.

This is because $(\det M) \cdot \Lambda \subseteq \Lambda'$.

19.3. Among all such choices, choose them so the positive integer $|v_{ii}|$ is as small as possible, but not zero.

We claim that $z_1, \dots, z_n$ are in fact a basis for Λ'.

To prove this, suppose to the contrary there is some $c \in \Lambda'$ not of the form

$$c = a_1 z_1 + \cdots + a_n z_n .$$

Since $\Lambda' \subseteq \Lambda^*$, write

$$c = b_1 x_1 + \cdots + b_k x_k \quad \text{for some } b_1, \dots, b_k \in \mathbb{Z},\ b_k \neq 0,\ k \leq n.$$

If there are multiple such reps, choose one minimizing k.

Since $v_{kk} \neq 0$, we can choose an integer s with

$$|b_k - s \cdot v_{kk}| < v_{kk} .$$

Look at

$$c - s \cdot z_k = (b_1 - s \cdot v_{1k}) x_1 + \cdots + (b_k - s \cdot v_{kk}) x_k$$

This is in Λ' because c and z_k are.

Have $b_k - s \cdot v_{kk} \neq 0$ because k was chosen minimal.

But, this violates minimality of our choice of the v's.

So, we have a contradiction.

(2) Given $\Lambda' \subseteq \Lambda \subseteq (\det M)\Lambda'$ and $y_1, \dots, y_n$, basis of Λ'.

By (1) there is a basis $Dx_1, \dots, Dx_n$ of $D\Lambda$ with

$$\begin{aligned} Dx_1 &= w_{11} y_1 \\ Dx_2 &= w_{21} y_1 + w_{22} y_2 \\ &\vdots \\ Dx_n &= w_{n1} y_1 + \cdots + w_{nn} y_n . \end{aligned}$$

$(w_{ij} \in \mathbb{Z})$
$(w_{ii} \neq 0)$.

Solve for the y_i in terms of the x_i.

17.4.

Obtain $y_1 = v_{11} x_1$

$y_2 = v_{21} x_1 + v_{22} x_2$

$\vdots$

$y_n = v_{n1} x_1 + \cdots + v_{nn} x_n$ with v_{ij} rational

But the x's are a basis for Λ so the v's are all integers.

The proof reinterpreted. (of (11))

Given Λ with basis $x_1, \cdots, x_n$,

~~there is a basis $y_1, \cdots, y_n$ of Λ etc with~~

Represent Λ' as a matrix M as before.

"There is a basis of Λ'" = "There is $U \in GL_2(\mathbb{Z}) \cdots$"

Theorem says, given $M \in GL_n(\mathbb{R})$ with entries in $\mathbb{Z}$.

Then there is $U \in GL_n(\mathbb{Z})$ with

$$UM = \begin{pmatrix} v_{11} & v_{21} & v_{31} & & v_{n1} \\ 0 & v_{22} & v_{32} & \cdots & v_{n2} \\ \vdots & 0 & v_{33} & & \vdots \\ \vdots & \vdots & 0 & & \vdots \\ 0 & 0 & 0 & & v_{nn} \end{pmatrix},$$

and all the v_{ii} are positive.

Says the same as: There is a basis $(y_1, \cdots, y_n)$ with

$$(y_1, \cdots, y_n) = \begin{pmatrix} v_{11} & v_{21} & & v_{n1} \\ 0 & v_{22} & \cdots & \vdots \\ \vdots & 0 & & \vdots \\ 0 & 0 & & v_{nn} \end{pmatrix} \begin{pmatrix} x_1, \cdots, x_n \end{pmatrix}.$$

19.5. Definition. A nonsingular integral square matrix M is in Hermite normal form if

(1) it is upper triangular ($m_{ij} = 0$ if $i > j$)

(2) $m_{ii} > 0$ for each i,

(3) All entries are nonnegative and in each row the diagonal entry is largest.

$(m_{ij}) = \begin{pmatrix} m_{11} & \cdots & m_{1n} \\ & & \\ m_{n1} & \cdots & m_{nn} \end{pmatrix}$

Caution! Different indexing convention!

Theorem. (Hermite) Let $M \in M_n(\mathbb{Z})$ with $\det M \neq 0$. Then there is a unique matrix H in Hermite normal form with $H = UM$ for some $U \in GL_n(\mathbb{Z})$.

Basically says the same with more conditions.

Corollary. Given $\Lambda' \subseteq \Lambda$ as before. The index of Λ' in Λ (as abelian groups) is $\dfrac{|\det(\Lambda')|}{|\det(\Lambda)|}$.

Proof. ~~Choose bases as before~~

We have bases $(y_1, \cdots, y_n)$, $(x_1, \cdots, x_n)$ of Λ', Λ with

$$(y_1, \cdots, y_n) = \begin{bmatrix} v_{11} & v_{21} & \cdots & v_{n1} \\ 0 & v_{22} & & \vdots \\ 0 & 0 & & \vdots \\ \vdots & \cdots & 0 & v_{nn} \end{bmatrix} (x_1, \cdots, x_n).$$

So, the index of Λ' in Λ is precisely $\prod_i v_{ii}$, which is the ratio of determinants.

Note. Can in fact write $H = UMV$ $U, V \in GL_n(\mathbb{Z})$, H in Smith normal form $\begin{bmatrix} a_{11} & & 0 \\ & a_{22} & \\ & & \ddots \\ 0 & & a_{nn} \end{bmatrix}$ $a_{ii} \mid a_{(i+1)(i+1)}$. Then this is really obvious.

A classical theorem. (Following: Siegel, Lectures on GON, p.27)

Thm. Let $P(z) = z^n + a_1 z^{n-1} + \cdots + a_n$ be an irreducible polynomial with integral coeffs $a_1, \ldots, a_n$ and all roots real. We have

$$\mathrm{Disc}(P) \geq \left(\frac{n^n}{n!}\right)^2.$$

Proof will use Minkowski's convex body theorem.

Prop. (involving alg. NT) Let K be a totally real number field, of degree n. Then,

$$\mathrm{Disc}(K) \geq \left(\frac{n^n}{n!}\right)^2 \qquad \mathcal{O}_K = \mathbb{Z}[\theta]$$

Proof uses the same ideas. If ~~$K = \mathbb{Q}(\theta)$~~, where θ is a root of a monic polynomial $P(x)$, then $\mathrm{Disc}\, K = \mathrm{Disc}\, P$. But this is not always true.

Def. If $P(z) = \prod_{i=1}^{n} (z - \theta_i)$ then

$$\mathrm{Disc}(P) = \prod_{1 \leq j < k \leq n} (\theta_j - \theta_k)^2.$$

Properties.

(1) Disc is a polynomial in $a_1, \ldots, a_n$ of degree $2n-2$.

(2) Disc can be expressed as the square of a Vandermonde determinant,

$$\Delta = \det \begin{bmatrix} \theta_1^{n-1} & \theta_1^{n-2} & \cdots & \theta_1 & 1 \\ \theta_2^{n-1} & \theta_2^{n-2} & \cdots & \theta_2 & 1 \\ \vdots & & & & \\ \theta_n^{n-1} & \theta_n^{n-2} & \cdots & \theta_n & 1 \end{bmatrix}^2.$$

20.2. Some proofs.

For (2), we argue that

$$\prod_{1 \le j < k \le n} (\theta_k - \theta_j) = \det \begin{bmatrix} 1 & \theta_1 & \cdots & \theta_1^{n-1} \\ \vdots & & & \\ 1 & \theta_n & \cdots & \theta_n^{n-1} \end{bmatrix}.$$

The RHS is $\sum_{\sigma \in \mathrm{Sym}(n)} \mathrm{sgn}(\sigma) \prod_{i=1}^{n} \theta_i^{\sigma(i)-1}$.

This is a polynomial of degree $\frac{(n-1)n}{2}$.

If you set $\theta_k = \theta_j$, you get zero, so $\theta_k - \theta_j \mid \mathrm{RHS}$ for each k, j.

Finally, look at the term on LHS always taking +.
You get $\theta_n^{n-1} \theta_{n-1}^{n-2} \cdots \theta_2^1$, and this doesn't cancel with anything, so you must have the same coeff on the right: you get $\mathrm{sgn}(\mathrm{id}) = 1$.

We'll return to (1) later.

Proof of theorem.

Consider the linear forms $Y_j = \sum_{k=0}^{n} \theta_j^{n-k} X_k$,

in other words

$$\begin{bmatrix} Y_1 \\ \vdots \\ Y_n \end{bmatrix} = \begin{bmatrix} \theta_1^{n-1} & \cdots & 1 \\ \vdots & & \vdots \\ \theta_n^{n-1} & \cdots & 1 \end{bmatrix} \begin{bmatrix} X_1 \\ \vdots \\ X_n \end{bmatrix}.$$

Let $X_1, \cdots, X_n$ range over integers.

20.3. The forms y_j are never zero, unless $x_1 = \cdots = x_n = 0$.

Because then θ_j would be a root of an integral polynomial of degree $\leq n-1$. But P was irreducible.

So, excluding $x_1 = \cdots = x_n = 0$, we have

$$|y_1 \cdots y_n| \geq 1.$$

Introduce the function

$$f(y) = \frac{1}{n} \sum_{i=1}^{n} |y_j| \qquad y = (y_1, \ldots, y_n).$$

Let T be the region $\{ y \in \mathbb{R}^n : f(y) < 1 \}$.

Then, invoking Minkowski (the compact form),

if $\mathrm{Vol}(T) \geq 2^n \mathrm{Vol}(\Lambda)$

for a lattice Λ, T contains a nonzero point of Λ.

We let Λ be the lattice of values $y = (y_1, \ldots, y_n)$ assumed for $x = (x_1, \ldots, x_n) \in \mathbb{Z}^n$.

By construction, we have $\mathrm{Vol}(\Lambda) = \sqrt{\mathrm{Disc}(P)}$.

We will show that T cannot contain a point of Λ.

It will then follow that $\mathrm{Disc}(P) \geq 2^{-2n} \cdot \mathrm{Vol}(T)^2$.

19.4.

Claim. T cannot contain a point of Λ.

Proof. The AM-GM inequality says that

$$f(y) = \frac{1}{n}\sum_{i=1}^{n} |y_i| \geq |y_1 \cdots y_n|^{1/n}.$$

If y is a point of Λ inside T, nonzero, then

* $|y_1 \cdots y_n|^{1/n} \leq f(y) < 1$ by def. of T,
* $|y_1 \cdots y_n| \geq 1$.

contradiction.

Claim. $\mathrm{Vol}(T) = \dfrac{(2n)^n}{n!}$.

Proof. ~~Exercise~~ will show that

$$\mathrm{Vol}\left(\{y \in \mathbb{R}^n : f(y) < \lambda\}\right) = \frac{(2\lambda n)^n}{n!}$$

This volume is

$$\int_{y_n=-\lambda n}^{\lambda n} \mathrm{Vol}\left(\{(y_1,\cdots,y_{n-1}) \in \mathbb{R}^{n-1} : \frac{1}{n}\sum_{i=1}^{n-1}|y_i| < \lambda - \frac{|y_n|}{n}\}\right) dy$$

$$= 2\int_{y_n=0}^{\lambda n} \mathrm{Vol}\left(\{(y_1,\cdots y_{n-1}) \in \mathbb{R}^{n-1} : \frac{1}{n}\sum_{i=1}^{n-1}|y_i| < \lambda - \frac{y_n}{n}\}\right) dy_n$$

$$= 2\int_{y_n=0}^{\lambda n} \mathrm{Vol}\left(\{(y_1,\cdots y_{n-1}) : \frac{1}{n-1}\sum_{i=1}^{n-1}|y_i| < \frac{n}{n-1}\lambda - \frac{y_n}{n-1}\}\right) dy_n$$

(induction)

$$= 2\int_{y_n=0}^{\lambda n} \frac{2^{n-1}(n-1)^{n-1}}{(n-1)!} \cdot \left[\frac{n}{n-1}\lambda - \frac{y_n}{n-1}\right]^{n-1} dy_n$$

$(t = n\lambda - y_n)$

$$= \frac{2^n}{(n-1)!}\int_{t=0}^{\lambda n} t^{n-1} = \frac{2^n}{(n-1)!}\,\frac{(\lambda n)^n}{n}, \quad \text{QED.}$$

Therefore, in conclusion, we get

$$\text{Disc}(P) \geq 2^{-2n} \cdot \left(\frac{(2n)^n}{n!} \right)^2 = \left(\frac{n^n}{n!} \right)^2, \text{ q.e.d.}$$

Example. If $n = 3$, $\text{Disc}(P) \geq \left(\frac{27}{6} \right)^2 = 20.25$.

In fact, the smallest discriminant is 49, of

$$x^3 - x^2 - 2x + 1.$$

$n = 4$: Lower bound $\left(\frac{4^4}{24} \right)^2 = 113.77\ldots$

Smallest $x^4 - x^3 - 3x^2 + x + 1$ disc 725.

$n = 5$: Bound $\left(\frac{5^5}{120} \right)^2 = 678.16\ldots$

Smallest $x^5 - x^4 - 4x^3 + 3x^2 + 3x - 1$.

Disc $14641 = 11^4$.

Generates a C_5 extension.

$n = 6$: A bunch of C_6 extensions.

Exercise. For $n = 3$, prove directly there is no smaller discriminant.

Yet another application of Minkowski's theorem.

(Hermite/Minkowski. Neukirch, p. 203)

Theorem. Given positive integers n and X, there are only finitely many number fields K of degree n with $|\mathrm{Disc}(K)| < X$.

Now, recall also that for any such K,

$$|\mathrm{Disc}(K)| \geq \left(\frac{n^n}{n!}\right)^2 \cdot \left(\frac{\pi}{4}\right)^n$$

by an extension of what we did last time.

Cor. Given X, there are only finitely many number fields K with $|\mathrm{Disc}(K)| < X$.

Cor. Given a positive integer n, and a set of primes S, there are only finitely many NFs of degree n unramified outside S.

[Note: $v_p(\mathrm{Disc}\, K)$ is bounded in terms of n.]

Analogy:

Theorem. (Faltings) Given a number field K & a set of primes There are only finitely many smooth complete curves of genus g over K with good reduction outside S.

(Mordell conjecture)

Cor. Every algebraic equation $f(x,y) = 0$ of genus $g > 1$ with coefficients in K has only finitely many solutions in K.

[Note: Genus $g=1$: elliptic curves finitely generated.

$g=0$: conics, e.g. $x^2 + y^2 = 1$. Birational to $\mathbb{P}^1$.]

Proof. (uses alg. NT)

(1) WLOG, $\sqrt{-1} \in K$.

Why is that? If $\sqrt{-1} \notin K$, let $L = K(\sqrt{-1})$.

Degree $2n$, totally complex (no maps $L \hookrightarrow \mathbb{R}$)

We have $\mathrm{Disc}(L) = \mathrm{Disc}(K)^2 \cdot \underbrace{N_{K/\mathbb{Q}}\,\partial(L/K)}_{\text{a positive integer}}$

$\geq \mathrm{Disc}(K)$.

So, if we bound all NFs of disc $\leq X$ and deg n containing $\sqrt{-1}$ and all NFs of disc $\leq X$ and deg $2n$ containing $\sqrt{-1}$ then we get a bound on all NFs of disc $\leq X$ and deg n.

(2). Given such a K, we have n embeddings $K \hookrightarrow \mathbb{C}$.

Write $n = 2m$, call embeddings $\tau_1, \bar{\tau}_1, \tau_2, \bar{\tau}_2, \cdots, \tau_m, \bar{\tau}_m$.

Consider the map $K \xrightarrow{\iota} \mathbb{C}^m = \mathbb{R}^n$

$x \longrightarrow (\tau_1(x), \tau_2(x), \cdots, \tau_m(x))$.

Define a ball in $\mathbb{C}^m$ consisting of

$$B(c) := \{x : |\tau_2(x)|, \cdots, |\tau_m(x)| < 1,\ \mathrm{Re}(\tau_1(x)) < 1,\ \mathrm{Im}(\tau_1(x)) < c \cdot \sqrt{X}\}.$$

We have $\mathrm{Vol}(\iota(\mathcal{O}_K)) = 2^{-m} \cdot |\mathrm{Disc}(K)|^{1/2}$.

(To be proved)

So if $c > 2^{-m}$ (i.e. $c = 1$), $B(c)$ will contain a point of $\iota(\mathcal{O}_K)$.

Why is this? If $x_1, \ldots, x_n$ is an integral basis for $\mathcal{O}_K$, then

$$|\mathrm{Disc}(K)| = \det \begin{bmatrix} \tau_1(x_1) & \overline{\tau_1(x_1)} & \cdots & \overline{\tau_n(x_n)} \\ \tau_1(x_2) & & & \\ \vdots & & & \\ \tau_1(x_n) & \overline{\tau_1(x_n)} & & \overline{\tau_n(x_n)} \end{bmatrix}^2$$

$$\mathrm{Vol}(\iota(\mathcal{O}_K)) = \det \begin{bmatrix} \mathrm{Re}\,\tau_1(x_1) & \mathrm{Im}\,\tau_1(x_1) & \cdots & \mathrm{Im}\,\tau_n(x_1) \\ & & & \\ & & & \\ \mathrm{Re}\,\tau_1(x_n) & & \cdots & \mathrm{Im}\,\tau_n(x_n) \end{bmatrix}$$

How to compare the determinants?

Column operations, starting at the bottom.

$\mathrm{Re}(a)$ $\quad$ $\mathrm{Im}(a)$

a $\quad$ $\mathrm{Im}(a)$ $\quad$ $(a = \mathrm{Re}(a) + i\,\mathrm{Im}(a))$

a $\quad$ $-2i\,\mathrm{Im}(a)$ $\quad$ (det $x \cdot -2i$)

a $\quad \cdots \quad a - \bar{a}$ $\quad 2i\,\mathrm{Im}(a) = \bar{a}$.

So if the matrices are A and B, $|\det A| = (-2i)^m \det B$,

and so $|\mathrm{Disc}\ K| = 2^n \cdot \mathrm{Vol}(\iota(\mathcal{O}_K))^2$.

24.4.

So, we conclude that there is $x \in \mathcal{O}_K$ with

$$|\tau_2(x)| < 1, \dots, |\tau_m(x)| < 1,$$

$$\mathrm{Re}(\tau_1(x)) < 1$$

$$\mathrm{Im}(\tau_1(x)) < \sqrt{X}.$$

Claim. x is a primitive element of K, i.e. $K = \mathbb{Q}(x)$.

Proof. We have $|N_{K/\mathbb{Q}}(a)| = \prod_{i=1}^{m} |\tau_i(a)\,\overline{\tau_i(a)}| \geq 1$

(it is an integer!)

and so $\mathrm{Im}(\tau_1(x)) \neq 0$, so $\tau_1(x) \neq \overline{\tau_1(x)}$.

Moreover, $\tau_i(x) \neq \tau_1(x)$ for $i = 2, \dots, m$ because

$$|\tau_i(x)| < 1, \quad |\tau_1(x)| > 1.$$

If x generated a proper subfield of K then at least two of these embeddings would be equal to τ_1. But they're not

Now, the coefficients of the minimal polynomial are integers. For fixed n, they are symmetric polynomials in $\tau_1(x), \overline{\tau_1(x)}, \dots, \tau_m(x), \overline{\tau_m(x)}$.

We have bounds on all of these.

In fact, min poly is $(X - \tau_1(x))(X - \overline{\tau_1(x)}) \cdots (X - \overline{\tau_m(x)})$

Each coefficient is $\ll \sqrt{X}$, because there is at most one coeff allowed to be bigger than 1.

So, there are $\ll X^{n/2}$ possibilities.

[Careful: To get this, one must be more careful about the wlog $\sqrt{-1} \in K$.]

Remarks.

It is believed that there are $\sim C_n \cdot X$ NFs of ~~disc~~ degree n and $|\mathrm{Disc}(K)| < X$.

This argument is very coarse! Does not show:

(*) Every poly of degree n with coeffs bounded by $C \cdot X^{1/2}$ is the min. poly of an element x satisfying the bounds described earlier.

Best known bound (Ellenberg - Venkatesh):

$$\ll X^{\exp(c\sqrt{\log n})} \quad \text{for some } n.$$

$n = 3, 4, 5$ we do have asymptotics!

Get a different GON problem. We will discuss.