AS, 1

Typical questions

- what is the probability that a random integer is even?

  $\mathbb{P}(x \text{ even} \mid x \in \mathbb{Z}) = \frac{1}{2}$?

- $\mathbb{P}(x \text{ squarefree} \mid x \in \mathbb{Z}) = ?$

- $\mathbb{P}(p \equiv 1 \bmod 4 \mid p \text{ prime}) = ?$

- Fix a pol. $f(x) \in \mathbb{Z}[x]$.

  $\mathbb{E}(\#\{x \in \mathbb{F}_p \mid f(x) = 0\} \mid p \text{ prime}) = ?$

- ~~What about~~ Fix an ell. curve $E/\mathbb{Q}$.

  How does $\#E(\mathbb{F}_p)$ behave for random p?

- Fix a number field K.

  $\mathbb{P}(\mathfrak{a} \text{ principal ideal} \mid \mathfrak{a} \subseteq \mathcal{O}_K \text{ ideal}) = ?$

- $\mathbb{P}(\mathrm{cl}(K) = 1 \mid K \text{ (random) number field}) = ?$

- $\#\{K \text{ number field of deg. } n \mid |\mathrm{disc}(K)| \leq T\} \approx ?$ for $T \to \infty$

- $\mathbb{P}(f(x) \text{ irred.} \mid f(x) \in \mathbb{Z}[x] \text{ of deg. } n) = ?$

- $\mathbb{P}(\mathrm{Gal}(f(x)) = S_n \mid$ — " — $) = ?$

- $\mathbb{P}(\mathrm{Gal}(K) = S_n \mid K \text{ number field of deg. } n) = ?$

  (Gal. grp. of Gal. cl. of K over $\mathbb{Q}$)

- $\mathbb{E}(\mathrm{rk}(E) \mid E \text{ ell. curve over } \mathbb{Q}) = ?$

  ⋮

- $\mathbb{P}(\text{you want to learn arith. stat.}) = 1$.

What is the [redacted] expected rank of a random elliptic curve over $\mathbb{Q}$?

$\mathbb{E}(\mathrm{rk}(E) \mid E \text{ ell. curve}) = ?$

$\mathbb{P}(\mathrm{rk}(E) = 0 \mid E \text{ ell. curve}) = ?$

...

AS, 2

→ $\mathbb{P}(\text{you want to think about arith. stat.}) = 1$

$\mathbb{E}(\text{fun}) = \infty$

already know how to answer some of these questions, will answer some in this course, some don't make sense, quite a few are still open!

Will focus on methods rather than specific questions/statements of max. generality

Statistics

Def Let X be a set, $A \subseteq X$ a subset, $f: X \to \mathbb{R}$ a function

If X is finite:
(e.g. $X = \mathbb{Z}/N\mathbb{Z}$)

Prob. that random $x \in X$ lies in A:

$$\mathbb{P}(x \in A \mid x \in X) = \frac{\# A}{\# X}$$

Expected val. of $f(x)$ for random $x \in X$:

$$\mathbb{E}(f(x) \mid x \in X) = \frac{\sum_{x \in X} f(x)}{\# X} = \frac{\sum_{x\in X} f(x)}{\sum_{x \in X} 1}$$

If X is countable:
(e.g. $X = \mathbb{N}, \mathbb{Z}, \{\text{primes}\}, \{\text{number fields}\}, \dots$)

Should have $\mathbb{P}(x=1 \mid x \in \mathbb{N}) = \mathbb{P}(x=2 \mid x \in \mathbb{N}) = \dots = 0$.
$\Rightarrow \mathbb{P}$ can't be given by a σ-additive prob. measure

Instead: Order the elements of X by a fct. $\mathrm{inv}: X \to \mathbb{R}$ such that $\{x \in X \mid \mathrm{inv}(x) \le T\}$ is finite for every T.

$$\mathbb{P}(x \in A \mid x \in X) = \lim_{T \to \infty} \mathbb{P}(x \in A \mid x \in X, \mathrm{inv}(x) \le T)$$

$$\mathbb{P}_{\inf} = \liminf$$

$$\mathbb{P}_{\sup} = \limsup$$

$$\mathbb{E}(f(x) \mid x \in X) = \lim_{T \to \infty} \mathbb{E}(f(x) \mid x \in X, \mathrm{inv}(x) \le T)$$

$$\mathbb{E}_{\inf} = \liminf$$

$$\mathbb{E}_{\sup} = \limsup$$

Rmk If $\# X = \# \mathbb{N}$, then removing fin. many $x \in X$ doesn't change $\mathbb{P}$, $\mathbb{E}$.

Rmk Let $\chi_A : X \to \{0,1\}$, $x \mapsto \begin{cases} 1, & x \in A \\ 0, & x \notin A \end{cases}$ be the characteristic function of A. Then, $\mathbb{P}(x \in A \mid x \in X) = \mathbb{E}(\chi_A(x) \mid x \in X)$.

Rmk $\mathbb{P}$ is finitely additive: If $A_1, \dots, A_n \subseteq X$ are disjoint and $\mathbb{P}(x \in A_i \mid x \in X)$ exists for all i, then $\mathbb{P}(x \in \bigcup_i A_i \mid x \in X) = \sum_i \mathbb{P}(x \in A_i \mid x \in X)$.

$\mathbb{E}$ is (finitely) linear: If $f_1, \dots, f_n$ are fcts and $\mathbb{E}(f_i(x) \mid x \in X)$ exists for all i, then

$$\mathbb{E}\Big(\sum_i f_i(x)\Big) = \sum_i \mathbb{E}(f_i(x)).$$

Random integers

If $X=\mathbb{N}$, we'll use $\mathrm{inv}(x)=x$.
If $X\subseteq\mathbb{Z}$, we'll use $\mathrm{inv}(x)=|x|$ (unless specified otherwise)

Ese $\mathbb{P}(x \text{ even} \mid x\in\mathbb{N}) = \frac{1}{2}$

$\mathbb{P}(x \text{ even} \mid x\in\mathbb{Z}) = \frac{1}{2}$.

Pf $\mathbb{P}(x \text{ even} \mid 1\le x\le T) = \dfrac{\lfloor \frac{T}{2}\rfloor}{\lfloor T\rfloor} \xrightarrow{T\to\infty} \frac{1}{2}$. □

Ese $\mathbb{P}(x \text{ (perfect) square} \mid x\in\mathbb{N}) = 0$.

Pf $\dfrac{\lfloor\sqrt{T}\rfloor}{\lfloor T\rfloor} \xrightarrow{T\to\infty} 0$. □

Ese $\mathbb{P}(x \text{ prime} \mid x\in\mathbb{N}) = 0$.

Pf Prime number theorem. □

Ese $\mathbb{E}((-1)^x \mid x\in\mathbb{N}) = 0$.

Rmk $\mathbb{P}, \mathbb{E}$ (might) depend on the ordering:

Order $\mathbb{N}$ by $\mathrm{inv}(x) = \begin{cases} x, & x \text{ even}, \\ x^2, & x \text{ odd}, \end{cases}$

"delaying" odd numbers. Then, $\mathbb{P}(x \text{ even} \mid x\in\mathbb{N}) = 1$.

Pf $\#\{1\le x\le T \text{ even}\} = \lfloor \frac{T}{2} \rfloor$

$\#\{1\le x\le \sqrt{T} \text{ odd}\} = \lceil \frac{\sqrt{T}}{2} \rceil$

$\dfrac{\lfloor \frac{T}{2}\rfloor}{\lceil \frac{\sqrt{T}}{2}\rceil} \xrightarrow{T\to\infty} \infty$ □

Ex $v_p(x) :=$ p-adic valuation of $x \in \mathbb{Z}$. (AS, 5)

$$\mathbb{E}(v_p(x) \mid x \in \mathbb{N}) = \frac{1}{p-1}.$$

Pf
$$\mathbb{E}(v_p(x) \mid x \in \mathbb{N}) = \lim_{T \to \infty} \mathbb{E}(v_p(x) \mid 1 \le x \le T)$$

$$= \lim_{T\to\infty} \sum_{e=1}^{\infty} \mathbb{P}(\underbrace{v_p(x) \ge e}_{\Updownarrow \atop p^e \mid x} \mid 1 \le x \le T)$$

$$= \lim_{T\to\infty} \sum_{e=1}^{\infty} \frac{\lfloor \frac{T}{p^e} \rfloor}{\lfloor T \rfloor}$$

$$= \lim_{T\to\infty} \sum_{e=1}^{\lfloor \log_p T \rfloor} \frac{\lfloor \frac{T}{p^e} \rfloor}{\lfloor T \rfloor}$$

$$= \text{—}\,''\,\text{—} \left(\frac{1}{p^e} + O\left(\frac{1}{T}\right) \right)$$

$$= \lim_{T\to\infty} \left(\sum_{e=1}^{\lfloor \log_p T \rfloor} \frac{1}{p^e} + O\left(\frac{\log_p T}{T} \right) \right)$$

$$= \sum_{e=1}^{\infty} \frac{1}{p^e}$$

$$= \frac{1}{p-1}. \qquad \square$$

Notation

$f(x, T, \dots) \ll g(x, T, \dots)$, $f(\dots) = O(g(x, \dots))$:
$\exists C > 0 \; \forall x, \dots : |f(x, \dots)| \le C g(x, \dots)$

e.g.: $\lfloor T \rfloor = T + O(1)$, $100\sqrt{T} \ll T$,

$f \asymp g$: $f \ll g$ and $f \gg g$

$\ll_x$: C might depend on x, but not on other var. $T, \dots$

$\ll_{x \to \infty}$: for suff. large x

$f(\dots) = o_{x\to\infty}(g(\dots))$: can find $c(x)$ that goes to 0 as $x \to \infty$

$f \sim_{x\to\infty} g$: $\frac{f(\dots)}{g(\dots)} \xrightarrow{x \to \infty} 1$

Lemma 1 If $f(x)$ for $x \in \mathbb{Z}$ depends only on x mod n, then
$$\mathbb{E}(f(x) \mid x \in \mathbb{Z}) = \mathbb{E}(\bar{f}(x) \mid x \in \mathbb{Z}/n\mathbb{Z}),$$
where $f(x) = \bar{f}(x \bmod n)$, $\bar{f}: \mathbb{Z}/n\mathbb{Z} \to \mathbb{R}$.

More generally:

Lemma Order $x \in \mathbb{Z}^d$ by $|x|_\infty = \max_{i=1,\dots,d} |x_i|$ (or by any other norm on $\mathbb{R}^d$).
If $f(x)$ for $x \in \mathbb{Z}^d$ depends only on x mod n, then
$$\mathbb{E}(f(x) \mid x \in \mathbb{Z}^d) = \mathbb{E}(\bar{f}(x) \mid x \in (\mathbb{Z}/n\mathbb{Z})^d)!$$

Thm $\mathbb{P}(x \text{ squarefree} \mid x \in \mathbb{Z}) = \mathbb{P}(x \not\equiv 0 \bmod p^2\ \forall p \mid x \in \mathbb{Z})$

$$\underset{\substack{\uparrow\\ \cancel{\text{CRT}}\ \text{(only applies to fin. many primes)}}}{=} \prod_p \mathbb{P}(x \not\equiv 0 \bmod p^2 \mid x \in \mathbb{Z}/p^2\mathbb{Z})$$

$$= \prod_p \left(1 - \frac{1}{p^2}\right) = \frac{1}{\zeta(2)} = \frac{6}{\pi^2} \approx 0.61.$$

Pf Let's sieve out (remove) $x \equiv 0 \bmod 4$, then $x \equiv 0 \bmod 9, \ldots$, and hope the result converges:

Let $M \geq 2$.

$$\mathbb{P}(x \not\equiv 0 \bmod p^2\ \forall p \leq M) \underset{\substack{\uparrow\\ \text{CRT, twice lemma 1}}}{=} \prod_{p \leq M} \mathbb{P}(x \not\equiv 0 \bmod p^2) = \prod_{p \leq M}\left(1 - \frac{1}{p^2}\right)$$

Goal: $M \to \infty$

$$\mathbb{P}(x \not\equiv 0 \bmod p^2\ \forall p) = \mathbb{P}(x \text{ squarefree}).$$

$$\xrightarrow{M \to \infty} \frac{1}{\zeta(2)}.$$

Clearly,

$$0 \leq \mathbb{P}(x \not\equiv 0 \bmod p^2\ \forall p \leq M) - \mathbb{P}_{\substack{\inf,\\ \sup}}(x \not\equiv 0 \bmod p^2\ \forall p) \leq \mathbb{P}_{\sup}(x \equiv 0 \bmod p^2 \text{ for some } p > M).$$

Goal: $M \to \infty$, $\to 0$

[Note: there are ∞ many $p > M$, so we can't directly use additivity on the RHS.]

Indeed, $\mathbb{P}_{\sup}(x \equiv 0 \bmod p^2 \text{ for some } p > M) \underset{\substack{\uparrow\\ \text{remove } x \geq 0,\\ \text{signs don't matter}}}{=} \limsup_{T \to \infty} \underbrace{\mathbb{P}(x \equiv 0 \bmod p^2 \text{ for some } p > M \mid 1 \leq x \leq T)}_{\leq \sum_{M < p \leq \sqrt{T}} \mathbb{P}(x \equiv 0 \bmod p^2 \mid 1 \leq x \leq T) \leq \sum_{M < p \leq \sqrt{T}} \frac{1}{p^2} \ll \frac{1}{M}} \ll \frac{1}{M} \xrightarrow{M \to \infty} 0.$

Careful!

$\frac{1}{M} \xrightarrow{M\to\infty} 0$ $\square$

Remark Actually, $\mathbb{P}(x \text{ squarefree} \mid 1 \leq x \leq T) = \frac{1}{\zeta(2)} + O\left(\frac{1}{\sqrt{T}}\right)$. (AS,7)

(E.g., use the Möbius inversion formula.)

~~Cautionary~~ ~~Horror story~~ A sieve theorist's nightmare

For any prime p, let $S_p \subseteq \mathbb{Z}/p^4\mathbb{Z}$ be the set of residue classes of the form $c \bmod p^4$, where $p^2 \leq c \leq p^4 - p^2$.

You'd think that (by CRT)

$$\mathbb{P}(x \bmod p^4 \in S_p \ \forall p \mid x \in \mathbb{Z}) = \prod_p \mathbb{P}(x \in S_p \mid x \in \mathbb{Z}) = \prod_p \frac{p^4 - 2p^2 + 1}{p^4} = \prod_p \left(1 - \frac{1}{p^2}\right)^2 = \frac{1}{\zeta(2)^2} > 0.$$

But there are <u>no</u> $x \in \mathbb{Z}$ such that $x \bmod p^4 \in S_p$ for all p.
(Take any p such that $p^2 > |x|$.) $\Rightarrow$ LHS $= 0$

$\rightsquigarrow$ In general (for sets $S_p \subseteq \mathbb{Z}/p^{e_p}\mathbb{Z}$), we only know $\mathbb{P}_{\sup}(x \in S_p \ \forall p) \leq \prod_p \mathbb{P}(x \in S_p)$.

End of lecture 1

AS, 8, 5

<u>Conjecture</u> Let $f(x) \in \mathbb{Z}[x]$ be a nonconstant polynomial. Then,

$$\mathbb{P}(f(x) \text{ squarefree} \mid x \in \mathbb{Z}) = \prod_p \mathbb{P}(f(x) \not\equiv 0 \bmod p^2 \mid x \in \mathbb{Z}).$$

This is known for: $\deg(f) \leq 2$ ("same" proof as last time) $\leftarrow$ try it!
$\deg(f) = 3$ (Hooley, 1967)
$\deg(f)$ arbitrary, assuming the ABC conjecture (Granville, 1998)

(always know $\mathbb{P}_{\sup} \leq \prod_p \mathbb{P}$.)

$$\cancel{\frac{\frac{1}{4}}{\frac{1}{4} + \frac{2}{4}\cdot\frac{1}{4}} = \frac{1}{3}}$$

AS, 9

We can count quadratic number fields:

Thm Let $N(X)$ be the number of quadr. number fields K with $|\mathrm{disc}(K)| \leq X$. Then, $N(X) \sim \frac{1}{\zeta(2)} \cdot X$ as $X \to \infty$.

$f(x) \sim g(x)$: $\lim_{x \to \infty} \frac{f(x)}{g(x)} = 1$

(In other words, $\mathbb{E}\left(\#\{K : |\mathrm{disc}(K)| = x\} \mid x \in \mathbb{N}\right) = \frac{1}{\zeta(2)}$.)

Pf We have a bijection

$$\{\text{Quadr. number field } K\} \longleftrightarrow \{\text{sqfree } t \in \mathbb{Z} \setminus \{1\}\}$$

$$K = \mathbb{Q}(\sqrt{t}) \longleftrightarrow t$$

$$\mathrm{disc}(K) = \begin{cases} t, & t \equiv 1 \bmod 4, \\ 4t, & t \equiv 2,3 \bmod 4. \end{cases}$$

$\Rightarrow N(X) = \#\{t \equiv 1 (4) \text{ sqfree}, |t| \leq X\} + \#\{t \equiv 2,3 (4) \text{ sqfree}, |t| \leq \frac{X}{4}\}$

You can prove like the prev. thm:

$$\mathbb{P}(t \equiv 1 \bmod 4 \text{ and squarefree} \mid t \in \mathbb{Z}) = \frac{1}{4} \cdot \prod_{p>2} \left(1 - \frac{1}{p^2}\right)$$

$$\mathbb{P}(t \equiv 2,3 \bmod 4 \text{ and squarefree} \mid t \in \mathbb{Z}) = \frac{2}{4} \cdot \prod_{p>2} \left(1 - \frac{1}{p^2}\right)$$

$$\Rightarrow \#\{t \equiv 1 (4) \text{ sqfree}, |t| \leq X\} \sim \frac{1}{4} \cdot \prod_{p>2} \left(1 - \frac{1}{p^2}\right) 2X$$

$$\#\{t \equiv 2,3 (4) \text{ sqfree}, |t| \leq \frac{X}{4}\} \sim \frac{2}{4} \cdot \prod_{p>2} \left(1 - \frac{1}{p^2}\right) \cdot \frac{2X}{4}$$

$$\Rightarrow N(X) \sim \underbrace{\frac{3}{4}}_{1 - \frac{1}{2^2}} \cdot \prod_{p>2} \left(1 - \frac{1}{p^2}\right) \cdot X = \prod_{p} \left(1 - \frac{1}{p^2}\right) \cdot X = \frac{1}{\zeta(2)} X.$$

$\square$

AS, 10

Random primes

Prime number theorem for arithmetic progressions (de la Vallée Poussin)

(Order prime numbers by size.)

Let $n \geq 1$ and $a \in (\mathbb{Z}/n\mathbb{Z})^\times$. Then, $\mathbb{P}(p \equiv a \bmod n \mid p \text{ prime})$

$$= \mathbb{P}(x \equiv a \bmod n \mid x \in (\mathbb{Z}/n\mathbb{Z})^\times)$$

$$= \frac{1}{\#(\mathbb{Z}/n\mathbb{Z})^\times}.$$

This is a special case $(L = \mathbb{Q}(\zeta_n), K = \mathbb{Q}, g(\zeta_n) = \zeta_n^a)$ of the

Chebotarev density theorem

Let $L|K$ be a finite Galois extension of number fields with Galois group G. Order the unramified primes $\mathfrak{q}$ of K by $\mathrm{Nm}(\mathfrak{q})$. For any prime $\mathfrak{P}$ of L above $\mathfrak{q}$, let $\mathrm{Frob}(\mathfrak{P}|\mathfrak{q}) \in G$ be the Frob. aut. Let $\mathrm{Frob}(\mathfrak{q}) = \{\mathrm{Frob}(\mathfrak{P}|\mathfrak{q}) \mid \mathfrak{P} \text{ prime above } \mathfrak{q}\} \subseteq G$ be the Frob. conj. class of $\mathfrak{q}$. Fix a conjugacy class $C \subseteq G$. Then,

$$\mathbb{P}(\mathrm{Frob}(\mathfrak{q}) = C \mid \mathfrak{q} \text{ prime of } K) = \mathbb{P}(g \in C \mid g \in G) = \frac{\#C}{\#G}.$$

Equivalently: Order the unram. primes $\mathfrak{P}$ of L by $\mathrm{Nm}(\mathfrak{q})$ where $\mathfrak{q} = \mathfrak{P} \cap K$. Fix an element $g \in G$. Then,

$$\mathbb{P}(\mathrm{Frob}(\mathfrak{P}|\mathfrak{q}) = g \mid \mathfrak{P} \text{ prime of } K) = \mathbb{P}(x = g \mid x \in G) = \frac{\frac{1}{\mathrm{ord}(g)}}{\sum_{h \in G} \frac{1}{\mathrm{ord}(h)}}$$

Rmk If we instead ordered unram. primes $\mathfrak{P}$ of L by $\mathrm{Nm}(\mathfrak{P})$, then

$$\mathbb{P}(\mathrm{Frob}(\mathfrak{P}|\mathfrak{q}) = g \mid \mathfrak{P} \text{ prime of } K) = \begin{cases} 1, & g = \mathrm{id}, \\ 0, & g \neq \mathrm{id}. \end{cases}$$

[Furthermore, $\#\{\mathfrak{P} \mid \mathrm{Nm}(\mathfrak{P}) \leq X\} \approx \frac{X}{\log X}$ for large X.]

Idea of Pf: $\mathrm{Nm}(\mathfrak{P}) = \mathrm{Nm}(\mathfrak{q})^f$, where $f = \#D(\mathfrak{P}|\mathfrak{q}) = \#\langle \mathrm{Frob}(\mathfrak{P}|\mathfrak{q}) \rangle = \mathrm{ord}(\mathrm{Frob}(\mathfrak{P}|\mathfrak{q}))$ is the inertia degree (deg. of ext. of residue fields).

⇝ We're delaying primes with $\mathrm{Frob}(\mathfrak{P}|\mathfrak{q}) \neq \mathrm{id}$ (not completely split).

...

AS, 11

Def Let $L|K$ be a degree n ext. of number fields. A prime $\mathfrak{q}$ of K has <u>splitting type</u> $(k_1, \dots, k_r)$ (where $k_1 + \dots + k_r = n$, $k_1 \geq \dots \geq k_r$) if $\mathfrak{q} = \mathfrak{P}_1 \cdots \mathfrak{P}_r$ for distinct $\mathfrak{P}_i$ of inertia degree $[\kappa(\mathfrak{P}_i) : \kappa(\mathfrak{q})] = k_i$.

Rmk splitting type $(1, \dots, 1)$: completely split / splits into distinct lin. factors
splitting type (n) : inert / irreducible

Def A monic degree n polynomial $f(x) \in K[x]$ has <u>splitting type</u> $(k_1, \dots, k_r)$ if $f(x) = f_1(x) \cdots f_r(x)$ for distinct irreducible $f_i(x) \in K[x]$ of degree k_i.

Thm Assume $L = K(\alpha)$, $\alpha \in \mathcal{O}_L$ has min. pol. $f(x) \in \mathcal{O}_K[x]$. For any unramified prime $\mathfrak{q}$ of K not dividing $[\mathcal{O}_L : \mathcal{O}_K[\alpha]]$, $\mathfrak{q}$ and $(f(x) \bmod \mathfrak{q}) \in \kappa(\mathfrak{q})[x]$ have the same splitting type.

Def A permutation $\pi \in S_n$ of $\{1, \dots, n\}$ has <u>cycle type</u> $(k_1, \dots, k_r)$
($k_1 + \dots + k_r = n$) if the cycles have lengths $k_1, \dots, k_r$.

Ex $\left(1 \to 2 \to 3 \to 1 \quad 4 \to 5 \to 6 \to 4 \quad 7 \rightleftarrows 8 \quad 9 \circlearrowleft \right)$ has cycle type $(3, 3, 2, 1)$
$= (1\,2\,3)(4\,5\,6)(7\,8)(9)$

Thm $$\mathbb{P}(\pi \text{ has cycle type } (k_1, \dots, k_r) \mid \pi \in S_n) = \prod_{l=1}^{n} \frac{1}{l^{c_l} \cdot c_l!}$$

if the number l occurs c_l times in the list $(k_1, \dots, k_r)$.

(optional) ~~Idea of pf~~ Take any $\rho \in S_n$. Write down $\rho(1), \dots, \rho(n)$.
Add brackets to make it a perm. in cycle notation of cycle type $k_1, \dots, k_r$.

$\rho(1)$ $\rho(2)$ $\rho(3)$ $\rho(4)$ ... $\rho(9)$
$(3\;\;9\;\;2)(4\;\;6\;\;5)(1\;\;8)(7)$.

You get any perm. of cycle type $(k_1, \dots, k_r)$ for exactly $\prod \frac{1}{l^{c_l} \cdot c_l!}$ different ρ. □

better? $\frac{1}{\#\text{fact}}$ ... (~~Different phrasing~~ Or: The permutations with cycle type $(k_1, \dots, k_r)$ form a conjugacy class in S_n. The centralizer has size $\prod_l l^{c_l} \cdot c_l!$. □

AS, 12

Thm Let $M|K$ be a Gal. ext. with Galois group G.
Let L be the subext. corresponding to $H \subseteq G$. Assume that M is the Galois closure of L over K.
G acts on the n-element set G/H (by left mult.)

$= $ the set of embeddings $\sigma_1, \dots, \sigma_n : L \hookrightarrow M$

$= $ the set of roots of the min. pol. of any generator α of $L|K$.

$\rightsquigarrow$ We can interpret any element $g \in G$ as a permutation in S_n.

$(G \subseteq S_n)$. The splitting type of $\mathfrak{q}$ is the cycle type of $\mathrm{Frob}(\mathfrak{P}|\mathfrak{q})$.

an unramified prime

(A5,13)

Cor Let $f(x) \in \mathcal{O}_K[x]$ be a (monic) polynomial with k distinct irreducible factors. Then $\mathbb{E}\left(\#\{x \in \kappa(\mathfrak{p}) \mid f(x) = 0\} \mid \mathfrak{p} \text{ prime}\right) = k$.

(one root per irred. factor)

w.l.o.g. f is separable (= squarefree).

Pf $f(x)$ has no double roots in $\mathbb{F}_p$ unless $p \mid \operatorname{disc}(f) \neq 0$.

$\Rightarrow$ W.l.o.g. $f(x)$ irreducible.

Let $\alpha \in \overline{\mathbb{Q}}$ be a root of $f(x)$, let $L = K(\alpha)$ and let M be its Gal. closure,

$$G = \operatorname{Gal}(M|K)$$
$$\cup\!\!\shortmid \qquad \cup\!\!\shortmid$$
$$H = \operatorname{Gal}(M|L)$$

For suff. large p, the number of roots $x \in \kappa(\mathfrak{p})$ is the number of fixed points of $\operatorname{Frob}(p)$ (left) acting on G/H.

SKIP (not skipped...)

$$\mathbb{E}\left(\#\{x \in \kappa(\mathfrak{p}) \mid f(x)=0\} \mid \mathfrak{p} \text{ prime}\right)$$
$$= \mathbb{E}\left(\#\{\text{fixed pts. of } \operatorname{Frob}(p) \circlearrowright G/H\} \mid p \text{ prime}\right)$$
$$= \mathbb{E}\left(\#\{\text{fixed pts. of } g \circlearrowright G/H\} \mid g \in G\right)$$
$$= \frac{\sum_{g \in G,\, xH \in G/H:\ gxH = xH} 1}{\#G}$$
$$\underset{\uparrow}{=} \frac{\#G/H \cdot \#H}{\#G} = 1 \qquad \square$$

$gxH = xH$
$\Leftrightarrow x^{-1}gx \in H$
$\Leftrightarrow g \in xHx^{-1}$

AS,14

Cor 2 Let $f(x)\in\mathbb{Z}[x]$ be an irreducible monic polynomial of degree n with Galois group S_n. Then,

$$\mathbb{P}\big(f(x) \bmod p \text{ has splitting type } (k_1,\dots,k_r) \;\big|\; p \text{ prime}\big)$$

$$= \mathbb{P}\big(\pi \text{ has cycle type } (k_1,\dots,k_r) \;\big|\; \pi\in S_n\big)$$

$$= \prod_{l=1}^{n} \frac{1}{l^{c_l}\cdot c_l!} \qquad (\text{as above})$$

Ex $\mathbb{P}\big(f(x) \bmod p \text{ splits completely} \,|\, p \text{ prime}\big) = \frac{1}{n!}$

Ex $\mathbb{P}\big(f(x) \bmod p \text{ irreducible} \,|\, p \text{ prime}\big) = \frac{1}{n}$

Random polynomials

AS, 15

Over $\mathbb{F}_q$

compare with Cor 2:

Thm (Chebotarev's little sibling)

$$\lim_{\substack{q \to \infty \\ \text{prime power}}} \mathbb{P}\big(f(x) \text{ has splitting type } (k_1, \dots, k_r) \mid f(x) \in \mathbb{F}_q[X] \text{ (monic) of degree } n\big)$$

$$= \mathbb{P}\big(\pi \text{ has cycle type } (k_1, \dots, k_r) \mid \pi \in S_n\big)$$

$$= \prod_{l=1}^{n} \frac{1}{l^{c_l} \cdot c_l!} \qquad (\text{where } l \text{ occurs } c_l \text{ times in } (k_1, \dots, k_r))$$

Exe $\lim_{q \to \infty} \mathbb{P}(f(x) \text{ splits completely}) = \frac{1}{n!}$.

Pf of exe $\#\{f(x) \text{ mon. of degree } n\} = q^n$

$$\Rightarrow \mathbb{P} = \frac{1}{q^n} \cdot \#\{f(X) = (X - \alpha_1) \cdots (X - \alpha_n) \mid \alpha_1, \dots, \alpha_n \in \mathbb{F}_q \text{ distinct}\}$$

End of lecture 2

$$= \frac{1}{q^n} \cdot \binom{q}{n} = \frac{q}{q} \cdot \frac{q-1}{q} \cdot \ldots \cdot \frac{q-n+1}{q} \cdot \frac{1}{n!} \xrightarrow{q \to \infty} \frac{1}{n!} \qquad \square$$

Exe $\lim_{q \to \infty} \mathbb{P}(f(x) \text{ irreducible}) = \frac{1}{n}$

Pf of exe Let I_n be the set of irreducible monic degree n polynomials.

Any $\alpha \in \mathbb{F}_{q^n}$ generates a subfield $\mathbb{F}_{q^d} \subseteq \mathbb{F}_{q^n}$ with $d \mid n$. Its min. pol. has degree d. $\Rightarrow$ We get a map

$$\mathbb{F}_{q^n} \xrightarrow{\text{min. pol.}} \coprod_{d \mid n} I_d.$$

Any $f(X) \in I_d$ has exactly d roots ($=$ preimages) in $\mathbb{F}_{q^n}$.

$$\Rightarrow q^n = \# \mathbb{F}_{q^n} = \sum_{d \mid n} d \cdot \# I_d$$

$$\Rightarrow 1 = \sum_{d \mid n} d \cdot \frac{\# I_d}{q^n} \xrightarrow[\substack{\uparrow \\ I_d \leq q^d}]{q \to \infty} \underbrace{n \cdot \frac{\# I_n}{q^n}}_{\lim_{q \to \infty}} = \underbrace{n \cdot \mathbb{P}(f(x) \in I_n)}_{\lim_{q \to \infty}}. \qquad \square$$

Rmk In fact, by Möbius inversion ($=$ inclusion-exclusion), (AS, 16)

$$n \cdot \# I_n = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) \cdot q^d \text{, where } \mu \text{ is the Möbius function.}$$

Pf of thm.

$$\mathbb{P}(f(x) \text{ has splitting type } (k_1, \dots, k_r))$$

$$= \underset{\substack{\uparrow \\ \text{total \# of pol.}}}{\frac{1}{q^n}} \cdot \prod_{l=1}^{n} \underset{\substack{\uparrow \\ \text{choose } c_l \text{ distinct irred. pol. of deg. } l}}{\binom{\# I_l}{c_l}}$$

$$\underset{\substack{\uparrow \\ n = k_1 + \dots + k_r = \sum_l l \cdot c_l}}{=} \prod_{l=1}^{n} \frac{1}{q^{l \cdot c_l}} \cdot \binom{\# I_l}{c_l}$$

$$= \prod_{l=1}^{n} \underbrace{\frac{\# I_l}{q^l}}_{\substack{q \to \infty \downarrow \text{Ex} \\ \frac{1}{l}}} \cdot \dots \cdot \underbrace{\frac{\# I_l - c_l + 1}{q^l}}_{\substack{q \to \infty \downarrow \text{Ex} \\ \frac{1}{l}}} \cdot \frac{1}{c_l!}$$

$$= \prod_{l=1}^{n} \frac{1}{l^{c_l} \cdot c_l!}. \qquad \square$$

Cor $\lim_{q \to \infty} \mathbb{P}(f(x)$ squarefree pol.$) = 1.$

Pf $\mathbb{P} = \sum_{\substack{k_1, \dots, k_r \\ k_1 + \dots + k_r}} \mathbb{P}(f(x) \text{ has splitting type } (k_1, \dots, k_r)) = \sum \mathbb{P}(\pi \text{ has cycle type } (k_1, \dots, k_r)) = 1$ $\square$

Rmk Actually, $\mathbb{P}(f(x) \text{ squarefree pol.}) = \begin{cases} 1, & n = 1, \\ 1 - \frac{1}{q}, & n \geq 2. \end{cases}$

Rmk The theorem also holds e.g. for a) the set of all (not nec. monic) degree n polynomials $f(x) \in \mathbb{F}_q[X]$ (rescale) (AS, 16.5)

b) the set of (monic) degree n polynomials $f(x)$ with X^{n-1}-coefficient zero. (replace X by $X-c$) $\boxed{\text{WHAT IF } \gcd(q,n) \neq 1?}$

Homework For any $t \in \mathbb{F}_q$, the pol. $f_t(X) = X^3 - tX^2 + (t-3)X + 1$ has Gal. group $\underset{\text{(splits completely)}}{1}$ or $\underset{\text{(irred.)}}{A_3} \leq S_3$ (if it's squarefree).

$\mathbb{P}(f_t(X) \text{ squarefree} \mid t \in \mathbb{F}_q) = 1$

$\mathbb{P}(f_t(X) \text{ splits completely} \mid t \in \mathbb{F}_q) = \mathbb{P}(g = id \mid g \in A_3) = \frac{1}{3}$

$\mathbb{P}(f_t(X) \text{ irreducible} \mid t \in \mathbb{F}_q) = \mathbb{P}(g \neq id \mid g \in A_3) = \frac{2}{3}.$

(AS, 17)

Over $\mathbb{Z}$

Some natural ways of ordering monic polynomials $f(X) = X^n + a_{n-1}X^{n-1} + \dots + a_0 \in \mathbb{Z}[X]$:

1) by $\|f\|_\infty = \max_{i=0,\dots,n-1} |a_i|$ (or any other norm of the coeff. vector)

2) by $ht(f) = \max_{i=0,\dots,n-1} |a_i|^{1/(n-i)}$.

This scales like the roots of f: If α is a root of $f(X)$, then $\lambda\alpha$ is a root of $\lambda^n f(\frac{X}{\lambda}) = X^n + \lambda a_{n-1}X^{n-1} + \dots + \lambda^n a_0$, and $ht(\lambda^n f(\frac{X}{\lambda})) = |\lambda| \cdot ht(f)$.

Any of those norms work in the following statements.

Thm Let $n \geq 1$. Then, $\mathbb{P}(f(X) \text{ irred.} \mid f(X) \in \mathbb{Z}[X] \text{ monic of degree } n) = 1$.

Pf If $f(X)$ is irreducible mod some prime p, then $f(X)$ is irreducible in $\mathbb{Z}[X]$.

Now, use a sieve. (We only need an upper bound.)

$$\mathbb{P}_{\sup}(f \text{ not irred} \mid f \in \mathbb{Z}[X] \text{ mon. deg. } n) \leq \mathbb{P}_{(\sup)}(f \bmod p \text{ not irred. } \forall p \leq M \mid f \in \mathbb{Z}[X] \text{ mon. deg. } n)$$

$$\left[= \mathbb{P}(f \bmod p \text{ not irred. } \forall p \leq M \mid f \in \mathbb{Z}/_{\prod_{p \leq M} p}\mathbb{Z}[X] \dots) \right]$$

$$\underset{\text{CRT}}{=} \prod_{p \leq M} \mathbb{P}(f \text{ not irred} \mid f \in \mathbb{F}_p[X] \dots)$$

$$= \prod_{p \leq M} (1 - \underbrace{\mathbb{P}(f \text{ irred.} \mid f \in \mathbb{F}_p[X] \dots)}_{\xrightarrow{p \to \infty} \frac{1}{n} > 0 \text{ (Lemma 3 b)}})$$

$$\xrightarrow{M \to \infty} 0.$$

$\square$

More generally:

Thm Let $k_1 + \dots + k_r = n$. Then,

$$\mathbb{P}\big(f(x) \text{ doesn't have splitting type } (k_1,\dots,k_r) \text{ mod } p \text{ for any } p \;\big|\; f(x) \in \mathbb{Z}[x] \text{ mon. deg. } n \big) = 0.$$

Pf $$LHS \le \prod_{p \le M} \Big(1 - \underbrace{\mathbb{P}\big(f(x) \text{ has splitting type } (k_1,\dots,k_r) \;\big|\; f(x) \in \mathbb{F}_p[x] \text{ mon. deg. } n\big)}_{\xrightarrow[p\to\infty]{} \text{ sth } > 0}\Big)$$

$$\xrightarrow[M \to \infty]{} 0. \qquad \square$$

Cor $$\mathbb{P}\big(f(x) \text{ has Galois group } S_n \;\big|\; f(x) \in \mathbb{Z}[x] \text{ mon. deg. } n \big) = 1.$$

Pf With probability 1, the Galois group $G \subseteq S_n$ contains:

- a 2-cycle: Frobenius aut. of a prime of splitting type $(2,1,\dots,1)$
- an $(n-1)$-cycle: — " — $(n-1, 1)$
- an n-cycle: — " — (n) (inert/irred.)

Any 2-cycle, $(n-1)$-cycle, and n-cycle together generate S_n. $\square$

More generally:

Thm Let $K = \mathbb{Q}(T_1, \dots, T_r)$.
Consider a squarefree polynomial $f(T_1,\dots,T_r)(X) \in K[X]$ of degree n whose splitting field has Galois group $G \subseteq S_n$ over K. For random $t_1, \dots, t_r \in \mathbb{Z}$, the pol. $f(t_1,\dots,t_r)(X) \in \mathbb{Q}[X]$ is well-defined with probability 1. (no zeros in denominators)
Its Gal. group is then a subgroup of G.

In fact, $\mathbb{P}(f(t_1,\dots,t_r)(X) \in \mathbb{Q}[X]$ has Galois group $G) = 1$.

Pf $\mathbb{P}(f(t_1,\dots,t_r)(X)$ well-def.$) = 1$: The denom. are nonzero pol. in $t_1,\dots,t_r$. The number of roots $(t_1,\dots,t_r) \in \mathbb{Z}^r$ of such a pol. with $|t_1|, \dots, |t_r| \leq T$ is $O(T^{r-1})$.

Using resolvent polynomials, we can reduce $\mathbb{P}(f$ has Gal. group $G) = 1$ to the statement that $\mathbb{P}(g_1, \dots, g_s(t_1,\dots,t_r) \in \mathbb{Q}(t_1,\dots,t_r)[X]$ irreducible$) = 1$, which follows from a sieve and a lemma stating that

$$\limsup_{q \to \infty} \mathbb{P}(g_1(t_1,\dots,t_r), \dots \in \mathbb{F}_q[X] \text{ irred.} \mid t_1,\dots,t_r \in \mathbb{F}_q) < 1.$$

(See Serre: Lectures on the Mordell-Weil Theorem, Chapters 9, 13.)

"$\square$"

(15, 20)

Lattices

Def A *rank r lattice* in $\mathbb{R}^n$ is a subgroup Λ of $\mathbb{R}^n$ generated by r linearly independent vectors $(r \leq n)$. A *full lattice* is a lattice of rank $r = n$.

A *basis* $(b_1, \dots, b_r)$ of Λ is a set of r generators of Λ: $\Lambda = \mathbb{Z}b_1 + \dots + \mathbb{Z}b_r \cong \mathbb{Z}^r$.

The *covolume* of Λ is the abs determinant of the matrix with columns $b_1, \dots, b_r$ (Indep. of the basis!) It's the volume of the *fundamental cell* $\{x_1 b_1 + \dots + x_r b_r \mid 0 \leq x_i < 1\}$

Can identify a full lattice with an el. of $SL_n(\mathbb{Z}) \backslash GL_n(\mathbb{R})$.

Ese $\Lambda = \mathbb{Z}^n \subseteq \mathbb{R}^n$ (corr. to I_n) has covol 1.

Ese Let K be a number field of degree n with r_1 real embeddings and r_2 pairs of complex embeddings $(n = r_1 + 2r_2)$. Then, $K \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ (as $\mathbb{R}$-algebras). Some lattices associated to K:

a) Identify $\underset{x+iy \leftrightarrow \binom{x}{y}}{\mathbb{C} \cong \mathbb{R}^2}$ as $\mathbb{R}$-vector spaces. $\rightsquigarrow K \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{R}^{r_1 + 2r_2} = \mathbb{R}^n$

The ring of integers $\mathcal{O}_K \subset K \subset K \otimes \mathbb{R} \cong \mathbb{R}^n$ is a full lattice of covolume $2^{-r_2} \cdot \sqrt{|D_K|}$, where D_K is the discr. of K.

Any fractional ideal $\mathfrak{a} \subset K \subset K \otimes \mathbb{R} \cong \mathbb{R}^n$ is a full lattice of covolume $Nm(\mathfrak{a}) \cdot \mathrm{covol}(\mathcal{O}_K) = Nm(\mathfrak{a}) \cdot 2^{-r_2} \cdot \sqrt{|D_K|}$.

b) Combine the homom. $\underset{x \mapsto \log|x|}{\log \|\cdot\| : \mathbb{R}^\times \to \mathbb{R}}$ and $\underset{x \mapsto \log|x|^2 = 2\log|x|}{\log \|\cdot\| : \mathbb{C}^\times \to \mathbb{R}}$

to a homom. $\log \|\cdot\| : \underset{(\mathbb{R}^\times)^{r_1} \times (\mathbb{C}^\times)^{r_2}}{\overset{\|}{(K \otimes_{\mathbb{Q}} \mathbb{R})^\times}} \longrightarrow \mathbb{R}^{r_1 + r_2}$

The norm $Nm_{K|\mathbb{Q}} : K \to \mathbb{Q}$ extends to the map $Nm : K \otimes \mathbb{R} \longrightarrow \mathbb{R}$.

$$\mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \ni x = (a_1, \dots, a_{r_1}, b_1, \dots, b_{r_2}) \mapsto \prod_i a_i \cdot \prod_i b_i \bar{b}_i$$

If $\log \|(x_i)\| = (y_i)_i$, then $\log |Nm(x_i)| = \sum_i y_i$

In particular, $|Nm(x)| = 1$ if and only if y lies on the hyperplane $H = \{\sum_i y_i = 0\} \subset \mathbb{R}^{r_1 + r_2}$.

$\Rightarrow$ We get a map

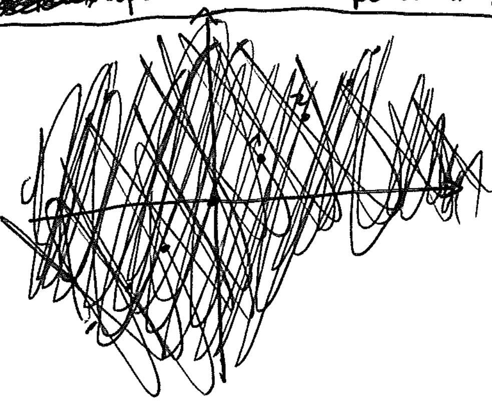
$$\begin{array}{ccc} \mathcal{O}_K^\times & \longrightarrow & H \\ \cap & & \cap \\ K^\times & & \mathbb{R}^{r_1+r_2} \\ \cap & \nearrow & \\ (K\otimes\mathbb{R})^\times & & \end{array}$$

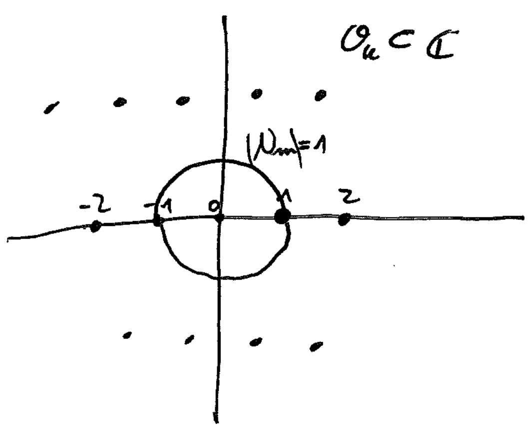
whose kernel is the group μ_K of roots of unity in K. The image of $\mathcal{O}_K^\times$ is a full lattice in $H \cong \mathbb{R}^{r_1+r_2-1}$ ... Identify H with $\mathbb{R}^{r_1+r_2-1}$ by projecting onto any r_1+r_2-1 coordinates in $\mathbb{R}^{r_1+r_2}$.

AS, 21

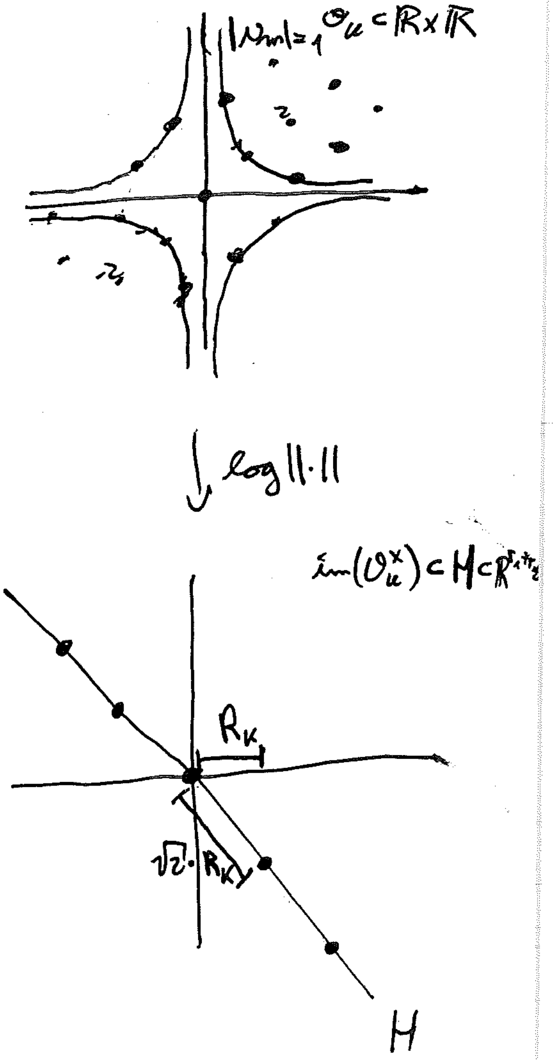
... whose covolume is called the <u>regulator</u> R_K of K.
(If $r_1+r_2-1=0$, then $R_K = 1$. The covol. w.r.t. the standard area measure on $H \subseteq \mathbb{R}^{r_1+r_2}$ would be $\sqrt{r_1+r_2}\cdot R_K$.)

~~Ex~~ In imag. quadr. number field ($r_1=0, r_2=1$)



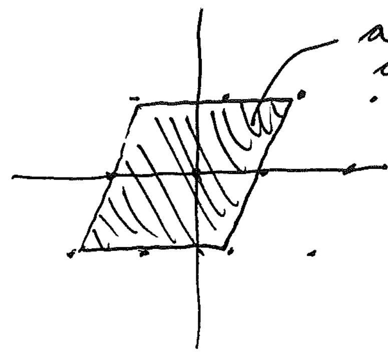


A real quadr. number field ($r_1=2, r_2=0$)



Minkowski's first theorem

Let $\Lambda \subset \mathbb{R}^n$ be a full lattice and let $K \subset \mathbb{R}^n$ be a centrally symmetric $(K=-K)$ convex subset. If $\mathrm{vol}(K) \geq 2^n \cdot \mathrm{covol}(\Lambda)$, then K contains a lattice vector $0 \neq v \in \Lambda$.

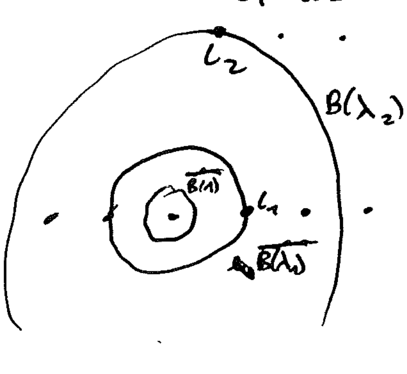


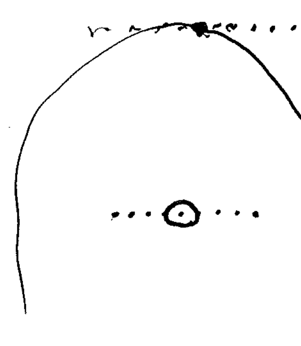
Def Let Λ, K as above and assume that K contains a nbhd of the origin. The *i-th successive minimum* λ_i $(i=1,\dots,n)$ is the smallest pos. real number such that $\lambda_i \cdot K$ contains i linearly independent lattice vectors $v_1,\dots,v_i \in \Lambda$.
(The minima are attained because K is compact and Λ is discrete.)

Rmk Of course $0 < \lambda_1 \leq \lambda_2 \leq \dots \leq \lambda_n$.

Rmk The vector space $\mathbb{R}^n$ has a basis $(l_1,\dots,l_n)$ such that l_i lies on the boundary of $\lambda_i \cdot K$, called a *reduced basis of $\mathbb{R}^n$ in Λ*.

Exe If $K = \overline{B(1)}$ is the disc of radius 1 around the origin, then λ_i is the smallest pos. real numbers s.t. Λ contains i lin. indep. el. of length $\leq \lambda_i$. The vector l_i has length λ_i.





AS, 23

Minkowski's second theorem

We have

$$\frac{1}{n!} \le \lambda_1\cdots\lambda_n \cdot \frac{\mathrm{vol}(K)}{2^n\cdot \mathrm{covol}(\Lambda)} \le 1. \quad \left(\text{In part., } \lambda_1\cdots\lambda_n \overset{\ll_n \text{ and } \gg_n}{\asymp_n} \frac{\mathrm{covol}(\Lambda)}{\mathrm{vol}(K)}.\right)$$

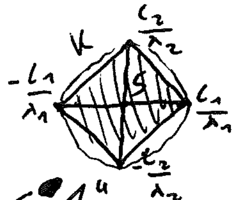
~~For M's first theorem: if $\mathrm{vol}(K)\ge 2^n \mathrm{covol}(\Lambda)$, then $\lambda_1\cdots\lambda_n\le 1$, so $\lambda_1\le 1$.~~
~~$\Rightarrow \lambda_1 K \subseteq K$ contains $0\ne \ell_1\in\Lambda$.~~

Pf "$\frac{1}{n!}\le\ldots$"

K contains the convex set S spanned by $\pm\frac{\ell_1}{\lambda_1},\ldots,\pm\frac{\lambda_n}{\lambda_n}$.
Let $\Lambda'\subseteq\Lambda$ be the lattice generated by $\ell_1,\ldots,\ell_n\in\Lambda$.

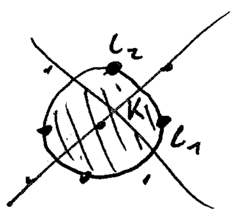
$$\Rightarrow \mathrm{vol}(K)\ge\mathrm{vol}(S) = 2^n\cdot\mathrm{vol}\left(\text{conv. set spanned by } \frac{\ell_1}{\lambda_1},\ldots,\frac{\ell_n}{\lambda_n}\right)$$

$$= 2^n\cdot\frac{1}{n!}\cdot\frac{\mathrm{covol}(\Lambda')}{\lambda_1\cdots\lambda_n} \ge \frac{2^n}{n!}\cdot\frac{\mathrm{covol}(\Lambda)}{\lambda_1\cdots\lambda_n}.$$



"$\ldots\le 1$" This is Minkowski's first theorem.

If $\lambda_1\ge 1$: ~~Let U be the interior of K. $\Rightarrow U$ contains no $0\ne v\in\Lambda$.~~
~~For any $x,y\in U$, $\frac{x-y}{2}=\frac{x+(-y)}{2}\in U$. $\Rightarrow \forall x\ne y\in U$, $\frac{x}{2}-\frac{y}{2}\notin\Lambda$.~~



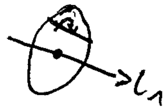
~~$\Rightarrow \mathrm{vol}\left(\frac{K}{2}\right)=\mathrm{vol}\left(\frac{U}{2}\right)\le\mathrm{covol}(\Lambda)$.~~

$\cancel{\text{"}\frac{\mathrm{vol}(K)}{2^n}\text{"}}$

In general: For $i=1,\ldots,n$, let $f_i: K\to\mathbb{R}^n$ be given by
$f_i(x) = \mathrm{centroid}(K\cap(x+\mathbb{R}\ell_1+\cdots+\mathbb{R}\ell_{i-1}))\in K\cap(x+\mathbb{R}\ell_1+\cdots+\mathbb{R}\ell_{i-1})$,
only depends on x mod $\mathbb{R}\ell_1+\cdots+\mathbb{R}\ell_{i-1}$.

$f_1(x)=x$ Let $h: K\to\mathbb{R}^n$, $h(x)=\lambda_1 f_1(x)+(\lambda_2-\lambda_1)f_2(x)+\cdots+(\lambda_n-\lambda_{n-1})f_n(x)$.

$f_2(x)$:



On the interior of K, the fct. h is a diffeomorphism with Jacobian determinant $\lambda_1\cdots\lambda_n$.

$h(K\cap(\mathbb{R}\ell_1+\cdots+\mathbb{R}\ell_i))\subseteq\lambda_i K\cap(\mathbb{R}\ell_1+\cdots+\mathbb{R}\ell_i)$.

$\Rightarrow$ (Interior of $h(K)$ doesn't contain any $0\ne v\in\Lambda$.)
"$\mathrm{vol}(h(K))=\lambda_1\cdots\lambda_n\mathrm{vol}(K)$."

~~$\Rightarrow$ apply the case "$\lambda_1\ge 1$" to $K'=h(K)$.~~

Warning: $h(K)$ might not be convex!

(A 5, 23.5)

Claim: For any $x \neq y \in \mathring{K}$, $\frac{h(x)-h(y)}{2} \notin \Lambda$.

The theorem follows since the claim implies that no two el. of the set $\frac{h(K)}{2}$ differ by an el. of Λ, so we can "move" $\frac{h(K)}{2}$ into a fundamental cell and conclude that

$$\mathrm{vol}\left(\frac{h(K)}{2}\right) \le \mathrm{covol}(\Lambda)$$
$$\mathrm{vol}\left(\frac{h(K)}{2}\right) = \frac{\lambda_1 \cdots \lambda_n}{2^n}$$

Pf. of claim: Let $x-y=\sum_{i=1}^{k} a_i l_i$ with $a_k \neq 0$.

$$\Rightarrow f_{k+1}(x) = f_{k+1}(y)$$
$$\vdots$$
$$f_n(x) = f_n(y)$$

$$\Rightarrow \frac{h(x)-h(y)}{2} = \lambda_1 \underbrace{\left(\frac{f_1(x)-f_1(y)}{2}\right)}_{\in \mathring{K}} + (\lambda_2-\lambda_1)\underbrace{\left(\frac{f_2(x)-f_2(y)}{2}\right)}_{\in \mathring{K}} + \dots + (\lambda_k-\lambda_{k-1})\underbrace{\left(\frac{f_k(x)-f_k(y)}{2}\right)}_{\in \mathring{K}}$$

$$\in \lambda_1 \mathring{K} + (\lambda_2-\lambda_1)\mathring{K} + \dots + (\lambda_k-\lambda_{k-1})\mathring{K}$$

$$\underset{\text{convexity}}{\subseteq} \lambda_k \mathring{K}$$

Assume $\frac{h(x)-h(y)}{2} \in \Lambda$.

$$\underset{\text{Def. of } \lambda_{k-1}}{\Longrightarrow} \frac{h(x)-h(y)}{2} \in \mathbb{R}l_1 + \dots + \mathbb{R}l_{k-1}$$

On the other hand,

$$h(x)-h(y) = \lambda_1 \underbrace{(f_1(x)-f_1(y))}_{\substack{=x-y \\ \in \mathbb{R}l_1+\dots+\mathbb{R}l_{k-1}}} + (\lambda_2-\lambda_1)\underbrace{(f_2(x)-f_2(y))}_{\substack{\in x-y+\mathbb{R}l_1 \\ \subseteq \mathbb{R}l_1+\dots+\mathbb{R}l_{k-1}}} + \dots + (\lambda_{k-1}-\lambda_{k-2})\underbrace{(f_{k-1}(x)-f_{k-1}(y))}_{\substack{\in x-y+\dots+\mathbb{R}l_{k-2} \\ \subseteq \mathbb{R}l_1+\dots+\mathbb{R}l_{k-2}}}$$

$$+ (\lambda_k-\lambda_{k-1})\underbrace{(f_k(x)-f_k(y))}_{\in x-y+\mathbb{R}l_1+\dots+\mathbb{R}l_{k-1}},$$

so $\notin \mathbb{R}l_1 + \dots + \mathbb{R}l_{k-1}$

$\lightning$

$\square$

Warning when $n\geq 3$, $(l_1,\dots,l_n) \subset \Lambda$ might not be a basis of Λ! (See HW.)

(AS, 24)

However:

Thm There is a basis $(b_1,\dots,b_n)$ of Λ and numbers $\mu_1\le\dots\le\mu_n$ with $\mu_i \asymp_n \lambda_i$ such that b_i lies on the boundary of $\mu_i K$.

Pf We construct $b_1,\dots,b_n$ iteratively. Assume we've constructed $b_1,\dots,b_{i-1} \in \mathbb{R}l_1+\dots+\mathbb{R}l_{i-1}$ which can be extended to a basis of Λ (i.e. so that the lattice $\Lambda\cap(\mathbb{R}b_1+\dots+\mathbb{R}b_{i-1})$ is generated by $b_1,\dots,b_{i-1}$).

Let $\Lambda\cap(\mathbb{R}b_1+\dots+\mathbb{R}b_{i-1}+\mathbb{R}l_i)$ be generated by $b_1,\dots,b_{i-1}, x_1b_1+\dots+x_{i-1}b_{i-1}+x_i l_i$.
Since $l_i\in\Lambda$, we must have $|x_i|\le 1$. (w.l.o.g. $0<x_i\le 1$.)
w.l.o.g., $0\le x_1,\dots,x_{i-1}<1$. Let $b_i = \underbrace{x_1b_1}_{\in x_1\mu_1K}+\dots+\underbrace{x_{i-1}b_{i-1}}_{x_{i-1}\mu_{i-1}K}+\underbrace{x_il_i}_{x_i\lambda_iK}$.

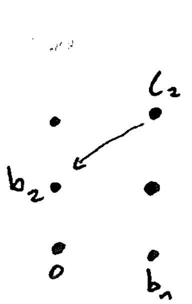
$\Rightarrow b_i\in(x_1\mu_1+\dots+x_{i-1}\mu_{i-1}+x_i\lambda_i)K$

$\Rightarrow \mu_i = \min\{t \mid b_i\in tK\} \le x_1\mu_1+\dots+x_{i-1}\mu_{i-1}+x_i\lambda_i$

$\ll_i \lambda_1+\dots+\lambda_{i-1}+\lambda_i \ll_i \lambda_i$.

By definition, $\mu_i \ge l_i$.

$\square$



AS, 25

Cor

$$\lambda_1^{i-1}\lambda_i^{n-i+1} \le \lambda_1\cdots\lambda_n \asymp_n \frac{\mathrm{covol}(\Lambda)}{\mathrm{vol}(K)}$$

$$\lambda_i^{i}\lambda_n^{n-i} \ge \lambda_1\cdots\lambda_n \asymp_n \frac{\mathrm{covol}(\Lambda)}{\mathrm{vol}(K)}$$

Rmk In the most balanced case $\lambda_1 \asymp \dots \asymp \lambda_n$, we get

$$\lambda_i^n \asymp \frac{\mathrm{covol}(\Lambda)}{\mathrm{vol}(K)}.$$

Rmk $|b_1|\cdots|b_n| \asymp \det\begin{pmatrix} - b_1 - \\ \vdots \\ - b_n - \end{pmatrix}$ if $K = B(1)$ forming a reduced basis of Λ

Rmk Let $K = B(1)$. Then, the vectors $b_1, \dots, b_n$ are "nearly orthogonal":

$$\cancel{\lambda_1 \cdots \lambda_n \asymp_n \mathrm{covol}(\Lambda)}$$

$$\cancel{|b_1|\cdots|b_n| \asymp_n \det\begin{pmatrix} - b_1 - \\ \vdots \\ - b_n - \end{pmatrix}}$$

$$2|b_i \cdot b_j| \le |b_i|^2 \quad \forall i \ne j$$

Pf ~~By definition of reduced~~ Replacing b_j by $b_j \pm b_i$, we get another basis of Λ. ~~By def of~~ Since $(b_1, \dots, b_n)$ is reduced, we must have

IGNORE

Q $\#\{(a,b) \in \mathbb{Z}^2 \mid \gcd = 1, \quad \mathrm{sqf}(a)\,\mathrm{sqf}(b)\,\mathrm{sqf}(a+b)\,\max(|a|,|b|)^{\bullet} < B\}$

$$\sim B^{\frac{1}{2}+\varepsilon} \quad ?$$

$$|b_j \pm b_i| \ge |b_j|$$

$$\Rightarrow |b_j \pm b_i|^2 \ge |b_j|^2$$

$$|b_j \pm b_i|^2 = |b_j|^2 + |b_i|^2 \pm 2\, b_i \cdot b_j$$

$\square$

Back to the lattice $\mathcal{O}_K \subset K \otimes_{\mathbb{Q}} \mathbb{R} = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \cong \mathbb{R}^n$ of int. in a number field K (AS, 26)

Let the compact set K (not to be confused with the number field K) be a closed ball of radius 1 in $\mathbb{R}^n$ w.r.t. the norm $|\cdot|_\infty : \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \to \mathbb{R}$, $((x_i)_i, (y_i)_i) \mapsto \max \{|x_i|\}_i \cup \{|y_i|\}_i$

<u>Lemma</u> $\lambda_1 = 1$

<u>Pf</u> $1 \in \mathcal{O}_K$ has distance $|1| = 1$ from the origin.

Any $\alpha \in \mathcal{O}_K$ with $|\alpha| < 1$ has $|\mathrm{Nm}_{K|\mathbb{Q}}(\alpha)| < 1$, which implies $\alpha = 0$. □

<u>Cor</u> $\lambda_2 \cdots \lambda_n \asymp_n \mathrm{covol}(\mathcal{O}_K) \asymp D_K^{1/2}$

<u>Cor</u> $\lambda_i^{n-i+1} \ll_n \mathrm{covol}(\mathcal{O}_K) \asymp_n D_K^{1/2}$

<u>Rmk</u> In the most balanced case ($\lambda_1 = 1$, $\lambda_2 \asymp \lambda_3 \asymp \cdots \asymp \lambda_n$), we have $\lambda_i^{n-1} \asymp \mathrm{covol}(\mathcal{O}_K) \asymp D_K^{1/2}$

~~Rmk If $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for some $\alpha \in \mathcal{O}_K$, then "usually"~~

$\cancel{\lambda_i \asymp_n D_K^{\frac{i}{n(n-1)}}}$. ~~(??)~~

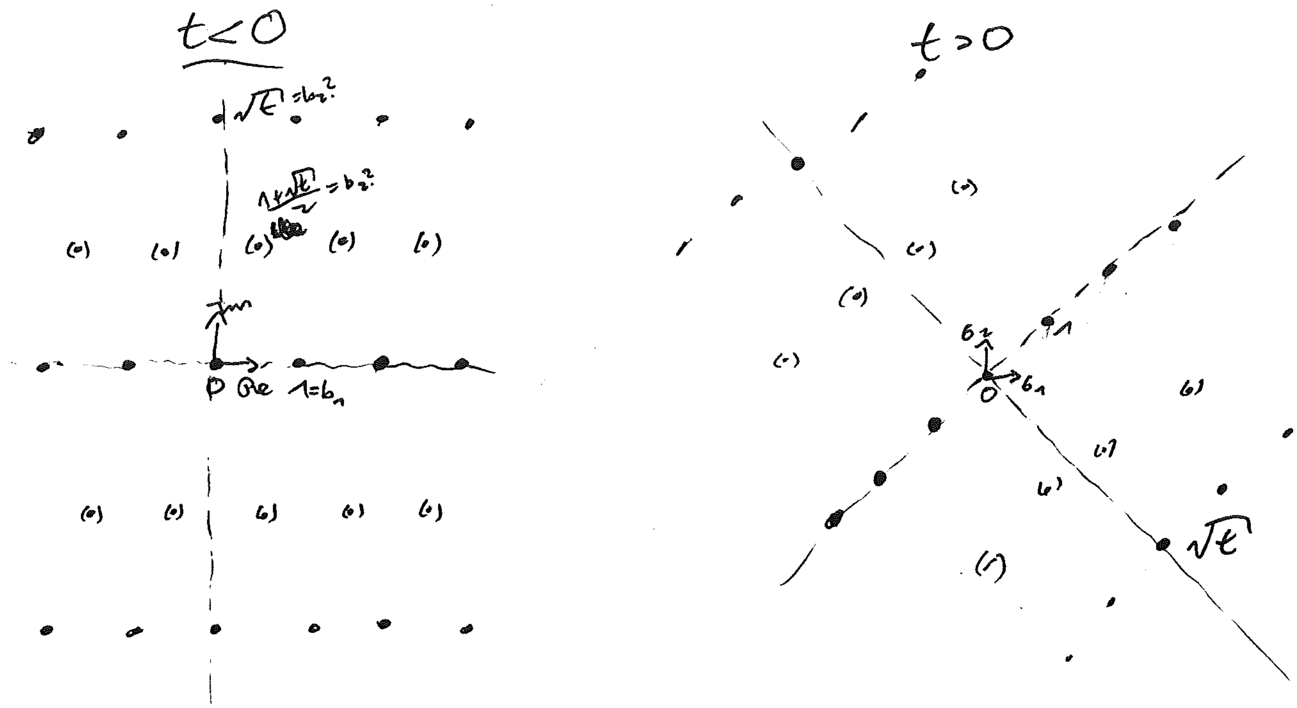
We've seen that the lattice $\mathcal{O}_K$ has a basis $(\underset{\overset{\|}{1}}{b_1}, b_2, \ldots, b_n)$ with $|b_i| \asymp_n \lambda_i$. Even better:

<u>Lemma</u> $\mathcal{O}_K$ has a basis $(\underset{\overset{\|}{1}}{b_1}, b_2, \ldots, b_n)$ with $|b_i| \asymp_n \lambda_i$ and $\mathrm{Tr}_{K|\mathbb{Q}}(b_i) = 0$ for $i = 2, \ldots, n$.

<u>Pf</u> Replace b_i (for $i = 2, \ldots, n$) by $n\left(b_i - \frac{\mathrm{Tr}(b_i)}{n}\right) = n \cdot b_i - \mathrm{Tr}(b_i) \cdot 1$ and note that $\mathrm{Tr}(n b_i - \mathrm{Tr}(b_i)) = 0$ and $|n b_i - \mathrm{Tr}(b_i)| \ll_n |b_i|$ (and maybe reorder?) □

Ex $K = \mathbb{Q}(\sqrt{t})$, t squarefree integer

(1S, 27)



$\lambda_1 = 1$, $\lambda_2 \asymp \sqrt{t} \asymp D_K^{1/2}$

AS,28

Ese $K=\mathbb{Q}(\sqrt{101}, \sqrt{1{,}000{,}003})$

$\lambda_1=1,\ \lambda_2\approx\sqrt{101},\ \lambda_3\approx\sqrt{1{,}000{,}003},\ \lambda_4\approx\sqrt{101\cdot 1{,}000{,}003}$

(very unbalanced)

$D_K\approx(101\cdot 1{,}000{,}003)^2$

Ese Yesterday, I picked a random monic pol. $f(x)$ of degree 3, ordered by $ht(f)$

$\lambda_1=1,\ \lambda_2\approx 60,\ \lambda_3\approx 3000$ (very unbalanced)

$D_K\approx -4\cdot 10^{11}$

Ese Yesterday, I picked a random ext. $K|\mathbb{Q}$ of degree 3, ordered by $|disc(K)|$

$\lambda_1=1,\ \lambda_2\approx 570,\ \lambda_3\approx 580$ (very balanced)

$D_K\approx -1.7\cdot 10^{12}$

End of lecture 4

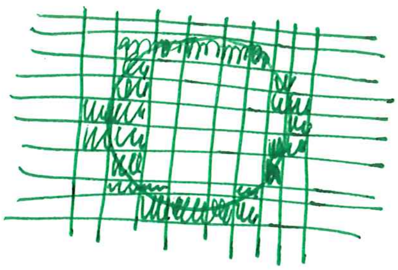
Point counting

Theorem. Let $A \subseteq \mathbb{R}^2$ be a disc of radius $T \geq 0$.

Then, $$\#(A \cap \mathbb{Z}^2) = \underbrace{\mathrm{vol}(A)}_{\pi T^2} + O(\underset{\text{for large } T}{T} + \underset{\text{for small } T}{1}).$$

Pf. Split the plane into grid cells. Then,

$$|\#(A \cap \mathbb{Z}^2) - \mathrm{vol}(A)| \leq \#(\text{cells intersecting the boundary } \partial A).$$



$$\ll T + 1.$$

$\square$

Conjecture ("Gauß circle problem") Let $A \subseteq \mathbb{R}^2$ be a disc centered at the origin of radius $T \geq 1$. Then,

$$|\#(A \cap \mathbb{Z}^2) - \mathrm{vol}(A)| \ll_\varepsilon T^{\frac{1}{2}+\varepsilon} \quad \forall \varepsilon > 0.$$

Known: $\ll_\varepsilon T^{\frac{131}{208}+\varepsilon}$ $\forall \varepsilon > 0$. (Huxley)

We will instead generalize to many other sets (and lattices)! The error bound will depend on how "large" the boundary ∂A is, and on how unbalanced the lattice is.

Def Let $M \in \mathbb{N}$ and $L \geq 0$. A set $B \subseteq \mathbb{R}^n$ is <u>(M,L)-Lipschitz</u> if it can be covered by the images of M maps $\varphi_i : [0,1]^{n-1} \longrightarrow \mathbb{R}^n$ satisfying $|\varphi_i(x)-\varphi_i(y)| \leq L \cdot |x-y|$ for all $x,y \in [0,1]^{n-1}$, where $|\cdot|$ denotes Euclidean length. A set $B \subseteq \mathbb{R}^n$ is <u>Lipschitz</u> if it is (M,L)-Lipschitz for any M and L.

Exe A circle of radius T is e.g. $(1, 2\pi T)$-Lipschitz (stretch $[0,1)$ by $2\pi T$, then wrap around).
Use $M \geq 2$ for exe. if there are holes in A.

Thm (Widmer) Let $\Lambda \subseteq \mathbb{R}^n$ be a full lattice with successive minima $\lambda_1 \leq \dots \leq \lambda_n$ w.r.t. $|\cdot|$. Let $A \subseteq \mathbb{R}^n$ be a measurable set whose boundary $\partial A \subseteq \mathbb{R}^n$ is (M,L)-Lipschitz. Then,

$$\#(A \cap \Lambda) = \frac{\mathrm{vol}(A)}{\mathrm{covol}(\Lambda)} + \sum_{k=0}^{n-1} O_n\left(M \cdot \frac{L^k}{\lambda_1 \cdots \lambda_k}\right).$$

const. depends only on n, not on A or Λ

Exe($n=2$): error $\ll_n M + M \cdot \frac{L}{\lambda_1}$

Rmk For constant $M, L, \mathrm{covol}(L)$, the error gets smaller, the more balanced Λ is (meaning $\lambda_1, \dots, \lambda_n$ aren't too small).

Cor For any $T \geq 0$,

$$\#((T \cdot A) \cap \Lambda) = \frac{\mathrm{vol}(A)}{\mathrm{covol}(\Lambda)} \cdot T^n + \sum_{k=0}^{n-1} O_n\left(M \cdot \frac{L^k}{\lambda_1 \cdots \lambda_k} \cdot T^k\right),$$

so $\quad$ — " — $$= \frac{\mathrm{vol}(A)}{\mathrm{covol}(\Lambda)} \cdot T^n + \sum_{k=0}^{n-1} O_{n,A}\left(\frac{T^k}{\lambda_1 \cdots \lambda_k}\right).$$

In particular,

$$\#((T \cdot A) \cap \Lambda) \sim_{n,A} \frac{\mathrm{vol}(A)}{\mathrm{covol}(\Lambda)} \cdot T^n \quad \text{for } T \to \infty.$$

Pf $\partial(T \cdot A)$ is (M, TL)-Lipschitz and $\mathrm{vol}(T \cdot A) = T^n \cdot \mathrm{vol}(A)$. $\square$

Rmk If $A \subset \mathbb{R}^n$ is an n-dimensional polytope whose vertices lie in Λ, there is a degree n polynomial $f(x) \in \mathbb{Q}[x]$ (called the <u>Ehrhart pol.</u>) such that $\#((T \cdot A) \cap \Lambda) = f(T)$ for all <u>integers</u> $T \geq 1$. [Also mention Pick's Thm for $n=2$.]

Scaling in different directions:

<u>Cor</u> Let $A \subseteq \mathbb{R}^n$ be measurable with Lipschitz boundary. Let $0 < T_1 \leq \ldots \leq T_n$ and consider the diagonal matrix $D = \begin{pmatrix} T_1 & & \\ & \ddots & \\ & & T_n \end{pmatrix}$.

Then, $\#((DA) \cap \mathbb{Z}^n) = \mathrm{vol}(A) \cdot T_1 \cdots T_n + \sum_{k=1}^{n} O_{n,A}(T_{k+1} \cdots T_n)$.

In particular, $\#((DA) \cap \mathbb{Z}^n) \underset{n,A}{\sim} \mathrm{vol}(A) \cdot T_1 \cdots T_n$ for $\underset{\substack{\wedge \\ T_2 \leq \ldots}}{T_1} \to \infty$.

<u>Pf</u> <u>1st attempt</u>: If ∂A is (M,L)-Lipschitz, then DA is $(M, T_n L)$-Lipschitz.

$\Rightarrow \#((DA) \cap \mathbb{Z}^n) = \mathrm{vol}(A) \cdot T_1 \cdots T_n + \sum_{k=0}^{n-1} O_{n,A}(T_n^k)$,

which isn't good enough when T_n is far larger than T_2.

<u>2nd attempt</u>: Instead of rescaling A, rescale the lattice:

$\#((DA) \cap \mathbb{Z}^n) = \#(A \cap (D^{-1} \mathbb{Z}^n))$.

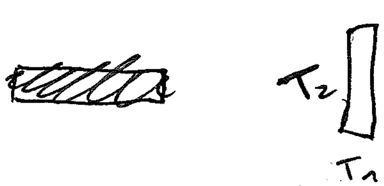
The successive minima of $D^{-1}\mathbb{Z}^n$ are $T_n^{-1} \leq \ldots \leq T_1^{-1}$ and the covolume is $T_1^{-1} \cdots T_n^{-1}$.

$\Rightarrow \mathrm{LHS} = \dfrac{\mathrm{vol}(A)}{T_1^{-1} \cdots T_n^{-1}} + \sum_{k=0}^{n-1} O_n\left(M \cdot \dfrac{L^k}{T_n^{-1} \cdots T_{n-k+1}^{-1}}\right)$.

□

<u>Exe</u> $\#([0,T_1] \times \ldots \times [0,T_n] \cap \mathbb{Z}^n) = T_1 \cdots T_n + \sum_{k=1}^{n} O(T_{k+1} \cdots T_n)$ for $T_1 \leq \ldots \leq T_n$.

$\prod_{i=1}^{n} (T_i + O(1))$



Cor For any $a \in \mathbb{Z}^n$, $B \geq 1$, $T_1 \leq \dots \leq T_n$,

$$\mathbb{P}\left(x \equiv a \bmod B \;\middle|\; {}^{x \in \mathbb{Z}^n}_{|x_i| \leq T_i \ \forall i} \right) \xrightarrow{T_1 \to \infty} \frac{1}{B^n}.$$

(AS, 32)

Pf Apply "the obvious" affine lin. transf. to turn the set $\{x \equiv a \bmod B \mid x \in \mathbb{Z}^n\}$ into the lattice $\mathbb{Z}^n$. $\square$

Pf of Weidner's thm

Let $(b_1,\dots,b_n)$ be a reduced basis of Λ, i.e. a basis such that $(|b_1|,\dots,|b_n|)$ is lexicographically minimal. We've seen that $|b_i| \asymp \lambda_i$ and $\lambda_1\cdots\lambda_n \asymp_n \mathrm{covol}(\Lambda)$ ("almost orthogonal").

Step 1: For any $x_1,\dots,x_n\in\mathbb{R}$, we have $|x_i| \ll_n \dfrac{\left|\sum_i x_i b_i\right|}{\lambda_i}$.

Let $v=\sum x_i b_i$. By Cramer's rule,

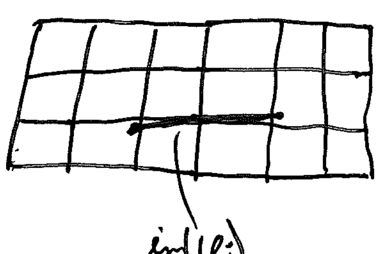
$$|x_i| = \frac{|\det(b_1 \cdots b_{i-1}\; v\; b_{i+1}\cdots b_n)|}{|\det(b_1 \; \cdots \; b_n)|} \le \frac{|b_1|\cdots|b_{i-1}||v||b_{i+1}|\cdots|b_n|}{\mathrm{covol}(\Lambda)}$$

$$\asymp_n \frac{|v|}{\lambda_i}.$$

Step 2: The claim is correct if $L\le\lambda_n$.

The image of $\varphi_i:[0,1]^{n-1}\to\mathbb{R}^n$ has diameter $\ll_n L$.

$\Rightarrow$ By step 1, it can only intersect $\ll_n \prod_{i=1}^n\left(\frac{L}{\lambda_i}+1\right)$ of the Λ-translates of a fundamental cell of Λ.



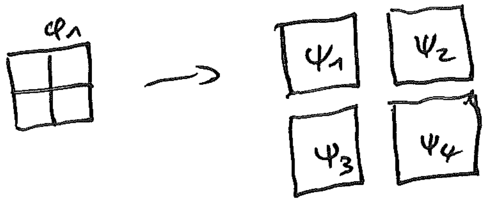
But $\displaystyle\prod_{i=1}^n\left(\frac{L}{\lambda_i}+1\right) \underset{L\le\lambda_n}{\ll} \prod_{i=1}^{n-1}\left(\frac{L}{\lambda_i}+1\right) \underset{\lambda_1\le\dots\le\lambda_n}{\ll_n} \sum_{k=0}^{n-1}\frac{L^k}{\lambda_1\cdots\lambda_k}.$

There are M functions, so error bound is M times this number.

(AS, 34)

Step 3: The claim is correct if $L > \lambda_n$. We need to make use of the fact that in φ_i is only $(n-1)$-dimensional (not reflected in the diameter).

Let $Q \geq 1$. Split $[0,1]^{n-1}$ into Q^{n-1} cubes of side length $\frac{1}{Q}$ and rescale each cube. $\rightsquigarrow$ Obtain $Q^{n-1} \cdot M$ functions $\psi_i : [0,1]^{n-1} \to \mathbb{R}^n$ with Lipschitz constant $\leq \frac{L}{Q}$.



$\Rightarrow \partial A$ is $\left(Q^{n-1}M, \frac{L}{Q}\right)$-Lipschitz.

Apply step 2 with $Q = \left\lceil \frac{L}{\lambda_n} \right\rceil$.

$\rightsquigarrow$ error bound

largest summand in the claimed error bound

$$\ll_n \sum_{k=0}^{n-1} Q^{n-1} M \cdot \frac{(L/Q)^k}{\lambda_1 \cdots \lambda_k} \ll_n M \cdot \frac{L^{n-1}}{\lambda_1 \cdots \lambda_{n-1}}$$

$$Q^{n-k-1} \cdot \lambda_{k+1} \cdots \lambda_{n-1} \ll L^{n-k-1} \cdot \frac{\lambda_{k+1}}{\lambda_n} \cdots \frac{\lambda_{n-1}}{\lambda_n} \leq L^{n-k-1}$$

$\square$

Counting short integers in a number field

Let $\rho : \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \longrightarrow \mathbb{C}^{r_1+2r_2}$

$$((x_i)_i, (y_i)_i) \longmapsto (x_1, \dots, x_{r_1}, y_1, \overline{y}_1, \dots, y_{r_2}, \overline{y}_{r_2})$$

and let $|z| = \max\limits_{i=1,\dots,r_1+2r_2} |(\rho(z))_i|$ for $z \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ as before.
$= \max(\{x_i\} \cup \{y_i\})$

Thm For any number field K of degree n and signature (r_1, r_2), we have

$$\#\{\alpha \in \mathcal{O}_K \mid |\alpha| \leq T\} \sim_K \frac{2^{r_1} \pi^{r_2}}{|D_K|^{1/2}} \cdot T^n \quad \text{as } T \to \infty.$$

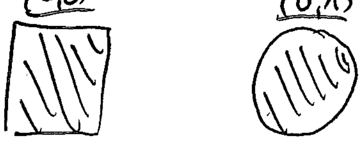
More precisely, if $\lambda_1 \leq \dots \leq \lambda_n$ are the successive minima of $\mathcal{O}_K$ (w.r.t. $|\cdot|$, say), then

$$\#\{\alpha \in \mathcal{O}_K \mid |\alpha| \leq T\} = \frac{2^{r_1}\pi^{r_2}}{|D_K|^{1/2}} \cdot T^n + \sum_{k=0}^{n-1} \mathcal{O}_n\left(\frac{T^k}{\lambda_2 \cdots \lambda_k}\right)$$

for any $T \geq 0$.

Pf By equivalence of norms, it "doesn't matter" whether we compute $\lambda \leq \dots \leq \lambda_n$ w.r.t. $|\cdot|$ on $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ or w.r.t. Euclidean length. Furthermore, $\lambda_1 = 1$. The volume of the closed unit ball $\{x \mid |x| \leq 1\}$ is $2^{r_1}\pi^{r_2}$ and its boundary is Lipschitz, with constants only depending on r_1 and r_2. $\square$

(2,0) (0,1)



Ex For $K = \mathbb{Q}(i)$, we have $|x+iy| \leq T \iff x^2+y^2 \leq T^2$, so we're back at the Gauß circle problem.

Counting short alg. integers of fixed degree

Let $\overline{\mathbb{Z}} \subseteq \overline{\mathbb{Q}}$ be the set of alg. integers. (The degree of $\alpha \in \overline{\mathbb{Q}}$ is the degree of its min. pol.) Let $|\alpha| = \max_{\sigma : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}} |\sigma(\alpha)|$ for $\alpha \in \overline{\mathbb{Q}}$.

Thm Fix some $n \geq 1$. There is a constant $C_n > 0$ such that
$$\#\{\alpha \in \overline{\mathbb{Z}} \text{ of degree } n \text{ and length } |\alpha| \leq T\} \sim_n C_n \cdot T^{n(n+1)/2}$$
for $T \to \infty$.

Ex $\#\{\alpha \in \mathbb{Z} : |\alpha| \leq T\} \sim 2T$ ⇝ $C_1 = 2$

In fact:

Thm Fix (r_1, r_2) with $n = r_1 + 2r_2$. There is a constant $C_{r_1, r_2} > 0$ such that
$$\#\{\alpha \in \overline{\mathbb{Z}} \text{ of signature } (r_1, r_2) \text{ and length } |\alpha| \leq T\} \sim_n C_{r_1, r_2} \cdot T^{n(n+1)/2}$$

End of lecture 5

Pf Let $A \subseteq \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ be the closed ball $A = \{x \mid |x| \leq 1\}$.

SHOW PICTURES ON PAGE 38 IN PARALLEL

Consider the map
$$\psi : \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \longrightarrow \{\text{monic } f(X) \in \mathbb{R}[X] \text{ of degree } n\}$$
$$x \longmapsto \prod_{i=1}^{n} (X - (\rho(x))_i)$$

("sending α to its min. pol.")

Identify $f(X) = X^n + a_{n-1}X^{n-1} + \dots + a_0 \in \mathbb{R}[X]$ with the vector $(a_{n-1}, \dots, a_0) \in \mathbb{R}^n$.

If $\psi(x) = (a_{n-1}, \dots, a_0)$, then $\psi(\lambda x) = (\lambda a_{n-1}, \lambda^2 a_{n-2}, \dots, \lambda^n a_0) = D_\lambda \psi(x)$ for any $\lambda \in \mathbb{R}$,

where $D_\lambda = \begin{pmatrix} T & & \\ & \ddots & \\ & & T^n \end{pmatrix}$.

$$\Rightarrow \#\{\alpha \in \overline{\mathbb{Z}} \text{ of sig. } (r_1, r_2) \text{ and } |\alpha| \leq T\} = n \cdot \#\{\text{irreducible } f(X) \in ((D_T\psi(A)) \cap \mathbb{Z}[X])\}$$
$$= n \cdot \#((D_T\psi(A)) \cap \mathbb{Z}^n) + O_n(\#\{\text{reducible } f(X) \in ((D_T\psi(A)) \cap \mathbb{Z}[X])\})$$

(AS, 37)

By def., all $f(x) \in D_T \cdot \psi(A)$ have $ht(f) \ll_n T$.
We previously showed that, ordered by ht,

$$\mathbb{P}(f(x) \text{ reducible} \mid \text{monic } f(x) \in \mathbb{Z}[x] \text{ of degree } n) = 0.$$

$$\Rightarrow \#\{\text{reducible monic } f(x) \in \mathbb{Z}[x] \text{ with } ht(f) \ll T\}$$

$$= o(\#\{\text{monic } f(x) \in \mathbb{Z}[x] \text{ with } ht(f) \ll T\})$$

$$= o(T^{1+\dots+n}) = o(T^{n(n+1)/2}).$$

choose a_{n-1} choose a_0

It remains to show that

$$n \cdot \#((D_T \psi(A)) \cap \mathbb{Z}^n) \sim_n C_{r_1, r_2} \cdot T^{n(n+1)/2} \quad \text{for } T \to \infty.$$

By (a cor. to) Widmer's thm., this is true (with $C_{r_1 r_2} = n \cdot \mathrm{vol}(\psi(A))$, which can be computed)
if the boundary of $\psi(A) \subseteq \mathbb{R}^n$ is Lipschitz.
The Jacobian det of ψ is a (nonzero) constant times $\prod_{i \neq j}(x_i - x_j)$.
Since $\psi(A)$ is compact, every boundary point has a preimage x,
which must either

a) lie on the boundary of A, or

b) ψ must have noninvertible Jacobian at x.

Clearly, ∂A is Lipschitz, and so is $\psi(\partial A)$ because ψ is continuously differentiable.
Furthermore, $I := \{x \mid \text{Jacobian of } \psi \text{ at } x \text{ noninvertible}\}$

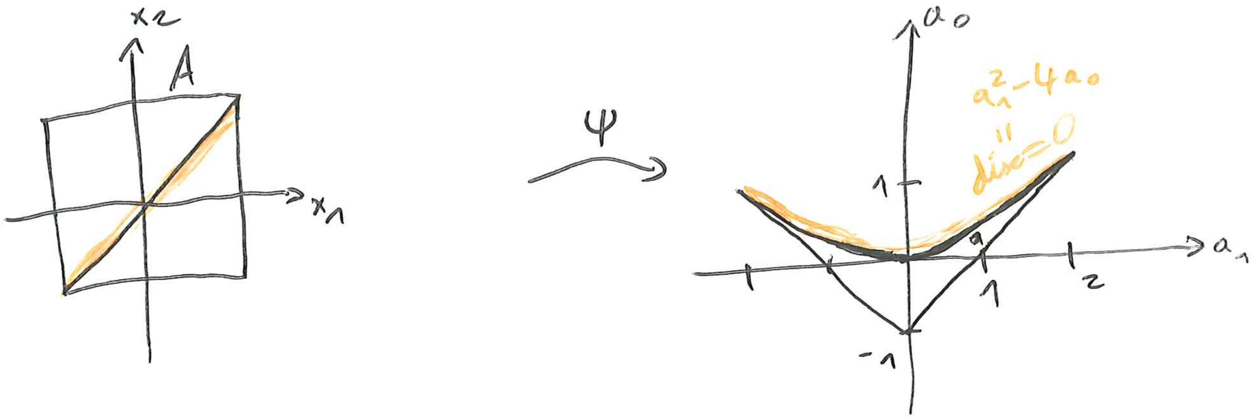
$$= \{x \mid (\rho_\psi(x))_i = (\rho(x))_j \text{ for some } i \neq j\},$$

(so $\psi(I) = \{f(x) \mid \mathrm{disc}(f) = 0\}$).

Now, $A \cap I$ is Lipschitz and therefore $\psi(A \cap I)$ is. $\square$

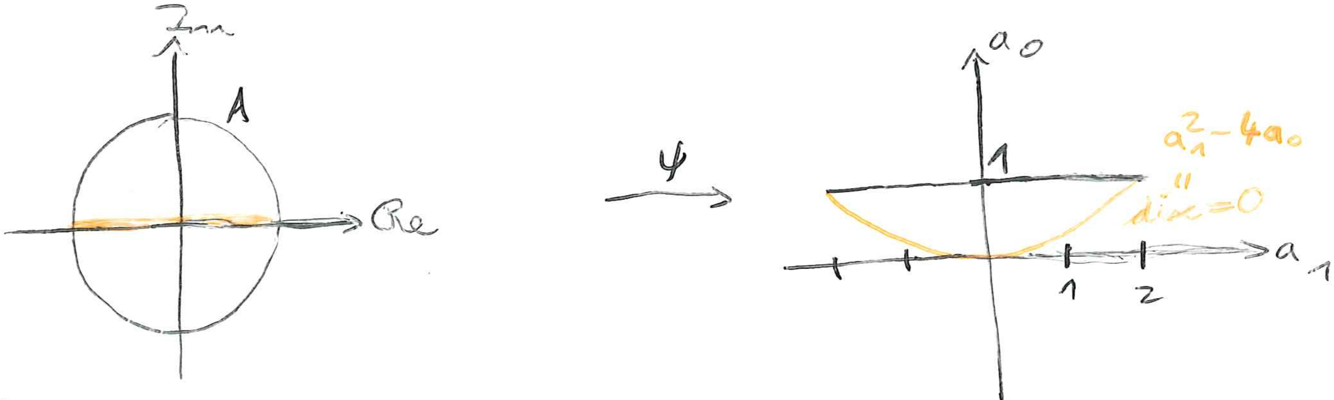
<u>Ex</u> Signature (2,0):

The Jacobian of $\psi : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$, $(x_1, x_2) \longmapsto (-(x_1+x_2), x_1 x_2)$ has absolute determinant $|x_1 - x_2|$. We have $\mathrm{vol}(\psi(A)) = \frac{4}{3}$, so $C_{2,0} = \frac{8}{3}$.



<u>Ex</u> Signature (0,1):

The Jacobian of $\psi : \mathbb{C} \longrightarrow \mathbb{R}^2$, $a+bi \longmapsto (-2a, a^2+b^2)$ has abs. determinant $4|b|$. We have $\mathrm{vol}(\psi(A)) = \frac{8}{3}$, so $C_{0,1} = \frac{16}{3}$.



$\rightarrow$ <u>Ex</u> $C_2 = 8$

AS, 39

Counting only polynomials with $a_{n-1}=0$:

<u>Thm</u> Fix some $n \geq 2$. There is a constant $C_n' > 0$ such that

$$\#\{\alpha \in \overline{\mathbb{Z}} \text{ of degree } n \text{ and length } |\alpha| \leq T \text{ and trace } 0\} \sim_n C_n' \cdot T^{(n-1)(n+2)/2}.$$

<u>"Pf"</u> $2 + \dots + n = \frac{(n-1)(n+2)}{2}$. □

counting number fields with a short generator

(AS, 40)

Let $n \geq 2$ and let C_n, C_n' as in the prev. section (counting short alg. integers).

<u>Thm A</u> For large T,

$$\#\{\text{number fields } K \subseteq \overline{\mathbb{Q}} \text{ of degree } n \text{ generated by some } \alpha \in \mathcal{O}_K \text{ of trace } 0 \text{ and length } |\alpha| \leq S\}$$

$$\asymp_n \; S^{(n-1)(n+2)/2} \, .$$

(seems to be unknown whether the quotient converges for $S \to \infty$, or to what number.)

<u>Thm B</u> For $T \to \infty$,

$$\#\{\text{rings (with unit) ("orders") } \mathcal{O} \subseteq \overline{\mathbb{Z}} \text{ of rank } n \text{ such that } \mathcal{O} = \mathbb{Z}[\alpha] \text{ for some } \alpha \text{ as above}\}$$

$$\sim_n \tfrac{1}{2} \#\{\alpha \in \overline{\mathbb{Z}} \text{ as above}\} \sim_n \tfrac{1}{2} C_n' \cdot S^{(n-1)(n+2)/2} \, .$$

Clearly, Thm B implies $\ll$ in Thm A:

The map $\{\mathcal{O}\} \longrightarrow \{K\}$ is surjective.

$\mathcal{O} \longmapsto$ field gen. by el. of $\mathcal{O}$

Bhargava, Shankar, Wang: Sqfree values of pol. disc. (2016)

Using a (difficult!) sieve, one can show that $\mathbb{Z}[\alpha]$ is the ring of integers $\mathcal{O}_K$ of $K = \mathbb{Q}(\alpha)$ for a positive proportion of α (ordered by $|\alpha|$). In fact, $\mathbb{Z}[\alpha]$ has squarefree discriminant for a (smaller) positive probability.

Hence, Thm B also implies $\gg$ in Thm B.

(AS, 41)

Pf of Thm B

(so $\#\{\alpha\} > \#\{\mathcal{O}\}$)

Consider the map $\{\underset{\text{as above}}{\alpha}\} \longrightarrow \{\underset{\text{as above}}{\mathcal{O}}\}$, $\alpha \longmapsto \mathbb{Z}[\alpha]$ ~~is surjective, but not injective.~~

~~The preimages have unbounded size as $T\to\infty$.~~ ~~(?)~~

It's surjective, and in fact each $\mathcal{O} = \mathbb{Z}[\alpha]$ has at least two preimages: α and $-\alpha$.

$\Rightarrow \#\{\alpha\} \geq 2\cdot\#\{\mathcal{O}\}$.

Unfortunately, the sets of preimages sometimes have size > 2,

so "$\leq$" is harder.

Call $\alpha \in \overline{\mathbb{Z}}$ as above good if α and $-\alpha$ are the only two Euclidean-shortest elements of the lattice $\{r - \frac{\mathrm{Tr}(r)}{n} \mid r \in \mathcal{O}_\alpha\}$. ~~that have~~

Clearly, each $\mathcal{O}$ has at most two good preimages α.

$\Rightarrow \#\{\alpha \text{ as above, good}\} \leq 2\cdot\#\{\mathcal{O}\}$.

$\Rightarrow$ It suffices to show that

$$\mathbb{P}(\alpha \text{ good} \mid \alpha \in \overline{\mathbb{Z}} \text{ of degree } n \text{ and trace } 0) = 1.$$

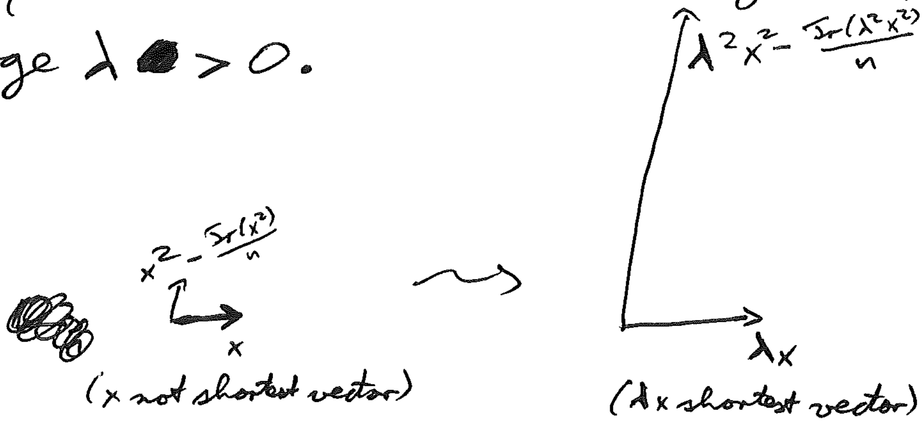
We can do this separately for each signature (r_1, r_2).
Let $(\mathbb{R}^{r_1}\times\mathbb{C}^{r_2})_0$ be the set of el. of $\mathbb{R}^{r_1}\times\mathbb{C}^{r_2}$ of trace 0.
Recall the map $\psi: \mathbb{R}^{r_1}\times\mathbb{C}^{r_2} \longrightarrow \{\text{monic } f(X) \in \mathbb{R}[X] \text{ of deg. } n\}$, $x = (x_i)_i \longmapsto \prod_i (X - x_i)$ and the set $I = \{(x_i)_i \mid x_i = x_j \text{ for some } i \neq j\}$

and let $A_0^0 = \{x \in (\mathbb{R}^{r_1}\times\mathbb{C}^{r_2})_0 \mid |x|_\infty \leq 1\}$.

Call $x \in (\mathbb{R}^{r_1}\times\mathbb{C}^{r_2})_0 \setminus I$ good if x and $-x$ are the only two Euclidean-shortest elements of the full lattice $\Lambda_x \subseteq (\mathbb{R}^{r_1}\times\mathbb{C}^{r_2})^0$ spanned

by $y_1 := x$, $y_2 := x^2 - \frac{\mathrm{Tr}(x^2)}{n}$, $\ldots$, $y_{n-1} := x^{n-1} - \frac{\mathrm{Tr}(x^{n-1})}{n}$.

Now, the idea is that λx becomes good for sufficiently large $\lambda > 0$.

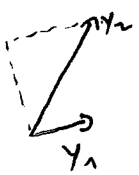


For $i = 1, \dots, n-1$, let $g_i(x) \geq 0$ be the distance of $y_i \in \mathbb{R}^n$ from the subspace spanned by $y_1, \dots, y_{i-1}$.

By Vandermonde, $1, x, \dots, x^{n-1}$ are linearly independent if and only if $x \notin I$. This is equivalent to $y_1, \dots, y_{n-1}$ being lin. indep.

For $x \notin I$, let $h(x) = \min\limits_{i=2,\dots,n-1} \frac{g_i(x)}{g_1(x)}$.

Any $x \notin I$ such that $h(x) > 1$ is good:



The length of $v = \sum_{i=1}^{k} a_i y_i$ with $a_i \in \mathbb{Z}$ and $a_k \neq 0$ is at least $|a_k| \cdot g_k(x)$. Since $g_i(x) > g_1(x)$ for $i \neq 1$, we have $|v| \leq |y_1|^{(=|x|)}$ only for $v = \pm x$. $\Rightarrow$ x is good.

Note that $g_i(\lambda x) = \lambda^i g_i(x)$ for $\lambda \geq 0$, so $h(\lambda x) \geq \lambda h(x)$ for $\lambda \geq 1$.

For any $B > 0$, let $A^0_B = \{x \in A^0 \mid h(x) > \frac{1}{B}\}$.

$\Rightarrow$ For $S > B$, every $x \in S \cdot A^\circ_B$ is good.

The boundary of A°_B is Lipschitz.

$\Rightarrow$ Applying Widmer's theorem to $\psi(A^\circ_B)$ and $\psi(A^\circ)$, we get:

$$\mathbb{P}_{\inf}(\alpha \text{ good} \mid \alpha \in \bar{\mathbb{Z}} \text{ of degree } n \text{ and trace } 0) \geq \frac{\operatorname{vol}(\psi(A^\circ_B))}{\operatorname{vol}(\psi(A^\circ))},$$

which converges to 1 for $B \to \infty$ by the monotone convergence theorem, since

$$A^\circ = \bigcup_{B>0} A^\circ_B \quad \text{and} \quad A^\circ_{B_1} \subseteq A^\circ_{B_2} \text{ whenever } B_1 \leq B_2. \qquad \square$$

End of lecture 6

To prove that ∂A°_B is Lipschitz, use that $g_i^2(x)$ is a (nonconst.) rational function in $x_1, \dots, x_n$ and the following theorem:

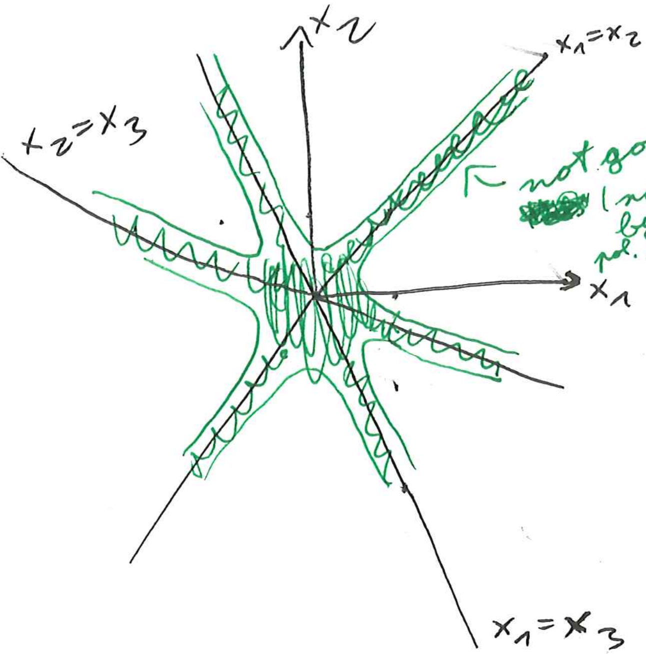
Theorem (?) Let $P(x_1, \dots, x_n) \in \mathbb{R}[x_1, \dots, x_n]$ be a nonzero polynomial and let $\mathcal{C} \subseteq \mathbb{R}^n$ be a bounded set of points $x = (x_1, \dots, x_n) \in \mathbb{R}^n$ with $P(x) = 0$. Then, $\mathcal{C}$ is Lipschitz.

signature (3,0):

$x_1+x_2+x_3=0$

A S, 44

$$\left(\frac{2x_1^2-x_2^2-x_3^2}{3}, \frac{-x_1^2+2x_2^2-x_3^2}{3}, \frac{-x_1^2-x_2^2+2x_3^2}{3}\right)$$



not good (REALLY!)
(not described by fin. many pol. inequalities...)

bad:

$$x_1^2+x_2^2+x_3^2 \geq \left(\frac{2x_1^2-x_2^2-x_3^2}{3}\right)+\dots$$

or
$$\left|x_1\cdot\frac{2x_1^2-x_2^2-x_3^2}{3}+\dots\right|$$

$$\geq \frac{1}{2}\cdot(x_1^2+x_2^2+x_3^2)$$

To prove Lipschitzness:

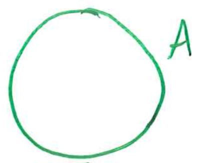
(AS, 44.1)

Thm (?) Let $P(X_1,\dots,X_n)\in\mathbb{R}[X_1,\dots,X_n]$ be a nonzero polynomial and let $A\subseteq\mathbb{R}^n$ be a bounded set of points $x\in\mathbb{R}^n$ with $P(x)=0$.

Then, A is Lipschitz.

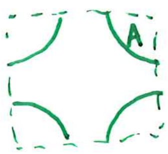
Rmk We could bound the Lipschitz constants in terms of n, $\deg(P)$, diameter of A. (?)

Ex



Ex

Ex



SKIP

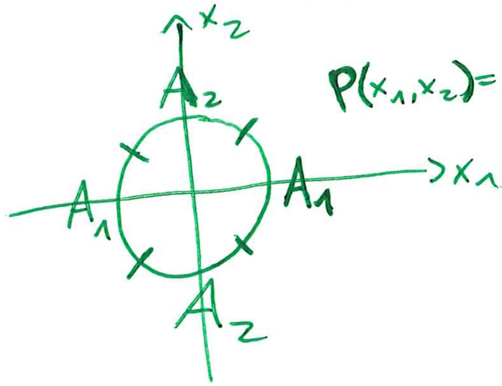
Idea of pf Use induction over n and the total degree of P. (Clear for $\deg(P)\leq 1$. Also clear for $n=1$.)

W.l.o.g. $A=\{x\in[0,1]^n \mid P(x)=0\}$.

For $i=1,\dots,n$, let after a lin. transf., $P_1(X),\dots,P_n(X)$ are distinct nonzero pol.

$P_i(X)=\frac{\partial P(X)}{\partial X_i}$ and let $A_i(X)=\{x\in A \mid P_i(x)\neq 0$ and $|P_i(x)|>|P_j(x)|\ \forall j\neq i\}$.

$P(x_1,x_2)=x_1^2+x_2^2-1$



The set $A\setminus\bigcup_{i=1}^{n}A_i\subseteq\{x\in A \mid P_i(x)=0\ \forall i=1,\dots,n$ or $|P_i(x)|=|P_j(x)|$ for some $i\neq j\}$ is Lipschitz by the induction hypothesis. ~~some pol. P_i is nonzero, $\deg(P_i)\leq\deg(P)$~~

$\Rightarrow$ It suffices to show that each set A_i is Lipschitz.

W.l.o.g. $i=n$.

SKIP

(AS, 44.2)

A result in real algebraic geometry ("semialgebraic sets have fin. many conn. cp.")

implies that A_n has finitely many connected components.

For any conn. component C:

~~By induction~~ Let $f: \mathbb{R}^n \to \mathbb{R}^{n-1}$ be the proj. onto the first $n-1$ coordinates.

~~By induction over n, $f^{-1}(\partial f(C))$ is Lipschitz.~~

~~(Actually, $f(C)$ is open by the impl. fct. thm.)~~

The restriction of f to C has an inverse $g: f(C) \to C$ whose derivatives $x_n \ldots x_{n-1}$ of the n-th coordinate are $-\frac{P_1(g(x))}{P_n(g(x))}, \ldots, -\frac{P_{n-1}(g(x))}{P_n(g(x))}$, which are bounded because $|P_n(g(x))| \geq |P_{n-1}(g(x))|$.

See Bochnak, Coste, Roy: Real alg. geometry, chapter 2.3

Counting [redacted] number fields of small discriminant

Conjecture Let $n \geq 2$. [redacted] There [redacted] are constants [redacted] $C_n, C_n' > 0$ such that

$$\#\{\text{number field } K \subseteq \overline{\mathbb{Q}} \text{ of degree } n \text{ and } |D_K| \leq T\} \underset{n}{\sim} C_n \cdot T \text{ for } T \to \infty.$$

$$\#\{\quad \text{— " —} \quad \text{and Galois group of the Gal. cl.} \cong S_n\} \underset{n}{\sim} C_n' \cdot T \quad \text{— " —}.$$

We have $C_n = C_n'$ if and only if n is prime. (Malle)

[redacted] Bhargava predicts the constant C_n'.

Rmk The same should hold for base number fields other than $\mathbb{Q}$ (with different constants $C_{n,F}, C_{n,F}'$)

Known: $n=2$: we've shown this

$n=3$: Davenport–Heilbronn, we'll show this later

$n=4,5$: Bhargava, we'll (at least) sketch this

[redacted]

Upper bounds (for $n \geq 6$):

Schmidt: $\#\{\text{number field } K \subseteq \overline{\mathbb{Q}} \text{ of degree } n \text{ and } |D_K| \leq T\} \underset{n}{\ll} T^{(n+2)/4}$ for large T.

Ellenberg–Venkatesh: $\quad \ldots \underset{n}{\ll} T^{\exp(O(\sqrt{\log n}))}$

(Note: $(\log n)^k \underset{k}{\ll} \exp(O(\sqrt{\log n})) \underset{\varepsilon}{\ll} n^{\varepsilon}$ for all $k, \varepsilon > 0$.)

Couveignes: $\quad \ldots \underset{n}{\ll} T^{O((\log n)^3)}$

Lower bound (for $n \geq 6$):

$\ldots \underset{n}{\gg} T \qquad$ for example if $p \mid n$ for some $p \leq 5$

$\{\ldots \text{ Gal} \cong S_n\} \gg T^{\frac{1}{2} + \frac{1}{n}}$ (Bhargava, Shankar, Wang)

Rmk The same conjectures are expected to hold for

$\#\{\text{extensions } L \subseteq \overline{\mathbb{Q}} \text{ of } K \text{ of deg. } n \text{ and } |D_L| \leq T\}$, where K is a fixed number field. (But the constants C_n, C_n' will depend on K!)

Upper bound

AS, 46

Thm (Schmidt)

$$\#\{K\subseteq\overline{\mathbb{Q}} \text{ of degree } n,\ |D_K|\le T\} \ll_n T^{(n+2)/4} \quad \text{for large } T.$$

(Rmk This is the conjectured asymptotic only for $n=2$.)

Lemma $\#\{K \text{ as above s.t. } \nexists \text{ subext. } \mathbb{Q}\subsetneq F\subsetneq K\} \ll_n T^{(n+2)/4}$

Pf Let $\underset{\substack{\| \\ 1}}{\lambda_1} \le \lambda_2 \le \dots \le \lambda_n$ be the succ. min. of $\mathcal{O}_K$ for K as above.

We've seen that $\lambda_2 \ll_n |D_K|^{\frac{1}{2(n-1)}} \le T^{\frac{1}{2(n-1)}}$ and that there is a nonzero $\alpha\in\mathcal{O}_K$ (of trace 0) with $|\alpha| \asymp_n \lambda_2$.

But $\mathbb{Q}\subsetneq\mathbb{Q}(\alpha)$, so $\mathbb{Q}(\alpha)=K$.

$\Rightarrow LHS \le \#\{K$ of degree n, gen. by some $\alpha\in\mathcal{O}_K$ of trace 0 and length $|\alpha| \ll T^{\frac{1}{2(n-1)}}\}$

WEAK! (Many K gen by α s.t. .. have disc. far larger than T)

$$\ll_n \left(T^{\frac{1}{2(n-1)}}\right)^{\frac{(n-1)(n+2)}{2}} = T^{(n+2)/4}.$$

$\square$

Rmk This shows Schmidt's thm when n is prime.

PROCEED with (*)!

(**) A similar argument shows:

Rmk Let $d<n$. Then,

$$\#\{K \text{ as above s.t. } \nexists \text{ subext. } \mathbb{Q}\subseteq F\subsetneq K \text{ with } [F:\mathbb{Q}]>d\} \ll T^{\frac{(n-1)(n+2)}{4(n-d)}}.$$

(Rmk Can always take d = largest div. of n, so $\#\{K$ as above$\} \ll \dots$

Pf of Rmk Consider $\alpha_2,\dots,\alpha_n\in\mathcal{O}_K$ of trace 0 with $|\alpha_i|\asymp\lambda_i$ (lin. indep.). By Galois theory, field K as above has $\le B_n$ proper subfields F (where B_n (is indep. of K) only depends on n). We always have ~~$\mathbb{Q}\alpha_2+\dots+\mathbb{Q}\alpha_d \not\subseteq F$ and therefore~~

$$\{\mathbb{Q}\alpha_2+\dots+\mathbb{Q}\alpha_{d+1}\}\not\subseteq F, \text{ since } [F:\mathbb{Q}]\le d, \text{ so}$$

$$\dim\left(F\cap\{x\in K \mid \mathrm{Tr}_{K|\mathbb{Q}}(x)=0\}\right)\le d-1.$$

~~Choosing B_n large shows~~

$\Rightarrow$ For some $0\le x_2,\dots,x_{d+1}\le B_n$, the integer $\beta = x_2\alpha_2+\dots+x_{d+1}\alpha_{d+1}$ doesn't lie on any of the $\le B_n$ proper subspaces $(\mathbb{Q}\alpha_2+\dots+\mathbb{Q}\alpha_{d+1})\cap F$ of $\mathbb{Q}\alpha_2+\dots+\mathbb{Q}\alpha_{d+1}$ $\Rightarrow \beta$ generates the field K.

$$|\beta| \ll_n \lambda_{d+1} \ll |D_K|^{\frac{1}{2(n-d)}}.$$

$$\Rightarrow LHS \ll \left(T^{\frac{1}{2(n-d)}}\right)^{\frac{(n-1)(n+2)}{2}} = T^{\frac{(n-1)(n+2)}{4(n-d)}}. \qquad \square$$

We used:

Lemma The points $(x_1, \dots, x_n) \in \mathbb{Z}^n$ with $0 \le x_1, \dots, x_n \le B$ cannot be covered by B (affine) linear subspaces.

Eg
$$\begin{matrix} \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \end{matrix}$$
can't be covered by 2 lines.

(*) When n is not prime, Schmidt ~~essential~~ essentially proves his result by induction over (AS, 48)
n (over proper subfields), using the following more general hypothesis:

<u>Thm</u> Let F be a number field of degree $f \geq 1$. For any $n \geq 2$,

$$\#\{F \subseteq K \subseteq \overline{\mathbb{Q}} \text{ with } [K:F]=n,\ |D_L| \leq T\} \ll_{n,f} |D_F|^{-\frac{1}{2f}} \cdot \left(\frac{T}{|D_F|}\right)^{\frac{n+2}{4}}.$$

RETURN TO (**)

Lower bound

<u>Thm</u> (Bhargava, Shankar, Wang) with Galois group S_n

$$\#\{K \subseteq \overline{\mathbb{Q}} \text{ of degree } n,\ |D_K| \leq T\} \gg_n T^{\frac{1}{2}+\frac{1}{n}}.$$

<u>Pf</u> ~~For~~ any $\alpha \in \overline{\mathbb{Z}}$ (of deg. n and signature (r_1, r_2)), we have $|D_{\mathbb{Q}(\alpha)}| \leq |\operatorname{disc}(\mathbb{Z}[\alpha])| = |\operatorname{disc}(\langle \alpha, \alpha^2, \ldots, \alpha^{n-1}\rangle)|$

$$= |\alpha|^{2(1+2+\ldots+n-1)} \cdot |\operatorname{disc}(\langle x, x^2, \ldots, x^{n-1}\rangle)|, \text{ where } x = \frac{\alpha}{|\alpha|} \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$$

with $|x| \leq 1$.

$$\ll_n |\alpha|^{n(n-1)}$$

$\{x \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \mid |x| \leq 1\}$ compact

(Many K with $|D_K| \leq T$ aren't gen. by α with $|\alpha| \ll_n T^{\frac{1}{n(n-1)}}$.)

$$\Rightarrow \#\{K \mid |D_K| \leq T\} \overset{\text{WEAK!}}{\geq} \#\{K \text{ with } \mathrm{Gal} = S_n \text{ gen. by some } \alpha \in \overline{\mathbb{Z}} \text{ of trace } 0 \text{ with } |\alpha| \ll_n T^{\frac{1}{n(n-1)}}\}$$

$$\underset{\text{BSW}}{\gg_n} \left(T^{\frac{1}{n(n-1)}}\right)^{(n-1)(n+2)/2} = T^{\frac{n+2}{2n}} = T^{\frac{1}{2}+\frac{1}{n}}. \qquad \square$$

(15,49)

Thm $\#\{K \subseteq \overline{\mathbb{Q}} \text{ of deg. } n,\ |D_K| \leq T\} \gg_n T$ if $p \mid n$ for some $p \leq 5$.

Pf Fix any number field F of degree $\frac{n}{p}$. Datskovski-Wright ($p=2$) / Davenport-Heilbronn ($p=3$) / Bhargava ($p=5$) showed that

$$\#\{K \text{ deg. } p \text{ ext. of } F \text{ (with Gal. gp. } S_p) \mid |D_K| \leq T\} \sim_{n,F} C'_{n,F} \cdot T$$

for some constant $C'_{n,F} > 0$. $\square$

__Strategic considerations__

We've described number fields K by the min. pol. $f(x)$ of a generator α. It's

~~To prove the conjecture for $n = 2, 3, 4, 5$, we'll use a de~~

difficult to determine D_K from $f(x)$. (We only used very weak relationships: $|D_K| \leq |\mathrm{disc}(f)|$, "$|\alpha| \ll T^{\frac{1}{2(n-1)}}$".)

To prove the conjecture for $n = 3, 4, 5$, we'll (later) use another description of number fields K where you can easily read off the discriminant K. (The descr. involves an __entire__ basis of $\mathcal{O}_K$ rather than just one short element!)

End of lecture 7

Weighted sets

Insult in BE...

Def A *weighted set* (=wet) A (on X) corresponds to a function

$\chi_A : X \to \mathbb{R}^{\geq 0}$ called its *characteristic function*.

The value $\chi_A(x)$ is the weight of x in A.

Ex Any set $A \subseteq X$ is a wet (on X) with $\chi_A(x) = \begin{cases} 0, & x \notin A \\ 1, & x \in A \end{cases}$ (A multiset has $\chi_A(x) \in \{0,1,2,\dots\}$.)

generalize

Def The *size* / *total weight* of A is $\# A = \sum_{x \in X} \chi_A(x)$.

For any function f on X,
$$\sum_{x \in A} f(x) = \sum_{x \in X} \chi_A(x) f(x)$$
$$\int_A f(x)\,dx = \int_X \chi_A(x) f(x)\,dx.$$
(if well def.)

The *support* of A is the set $\mathrm{supp}(A) = \{x \in X \mid \chi_A(x) > 0\}$.

For a collection $(A_i)_{i \in I}$ of wets on X, define $\bigcup_{i \in I} A_i$, $\bigsqcup_{i \in I} A_i$ by

$$\chi_{\cup A_i}(x) = \sup_{i \in I} \chi_{A_i}(x)$$
$$\chi_{\sqcup A_i}(x) = \sum_{i \in I} \chi_{A_i}(x)$$
(if exist, $< \infty$)

For a fin. collection, $(A_i)_{i \in I}$, define $\bigcap_{i \in I} A_i$ by

$$\chi_{\cap A_i}(x) = \prod_{i \in I} \chi_{A_i}(x).$$

For a wet A and any $r \geq 0$ define $A^{\sqcup r}$ by

$$\chi_{A^{\sqcup r}}(x) = r \cdot \chi_A(x).$$

For wets A on X and B on Y, define $A \times B$ on $X \times Y$ by

$$\chi_{A \times B}(x,y) = \chi_A(x)\chi_B(y).$$

The preimage of a wet B on Y under a map $f : X \to Y$ is $f^{-1}(B)$ given by

$$\chi_{f^{-1}(B)}(x) = \chi_B(f(x)).$$

The image of a set A in X under a bijection $f: X \to Y$ is $f(A)$ $= (f^{-1})^{-1}(A)$ given by

AS, 51

$$\chi_{f(A)}(y) = \chi_A(f^{-1}(y)).$$

(It's unclear whether we should use Σ or sup when defining $f(A)$ for maps that are not injective.)

~~These definitions agree with the usual ones~~

We get "the usual" relations, like

$$A \cap \bigcup_i B_i = \bigcup_i (A \cap B_i),$$

$$A \cap \bigsqcup_i B_i = \bigsqcup_i (A \cap B_i),$$

$$f^{-1}\Big(\bigcup_i A_i\Big) = \bigcup_i f^{-1}(A_i)$$

$$f^{-1}\Big(\bigsqcup_i A_i\Big) = \bigsqcup_i f^{-1}(A_i)$$

$$\vdots$$

Fundamental domains

Def Let G be a group acting on a set X.
A fundamental domain for $G \backslash X$ is a set $\mathcal{F}$ on X such that $X = \bigsqcup_{g \in G} g\mathcal{F}$,

i.e. $1 = \sum_{g \in G} \chi_{\mathcal{F}}(gx) \quad \forall x \in X$.

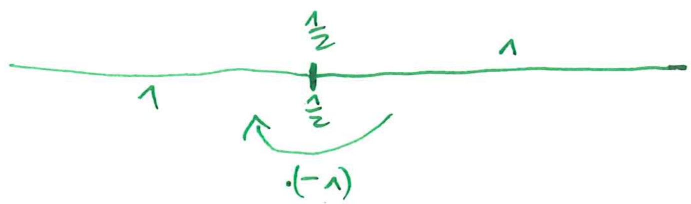
Rmk It suffices to check this for one element x of each G-orbit in X.

Rmk Let $\mathcal{F}$ be a fund. dom., then $g\mathcal{F}$ is a fund. dom. for any $g \in G$. If $\mathcal{F} = A \sqcup B$, then $A \sqcup gB$ is also a fund. dom.

Ex If G is finite, we can take $\chi_{\mathcal{F}}(x) = \frac{1}{\# G}$ for all $x \in X$.
$\rightsquigarrow$ Trivial fundamental domain $\mathcal{F}$.

AS, 53

Exe Fund. dom. for $\{\pm 1\} \curvearrowright \mathbb{R}$ (by mult.) : $\mathcal{F} = \mathbb{R}^{>0} \cup \{0\}^{\sqcup \frac{1}{2}}$

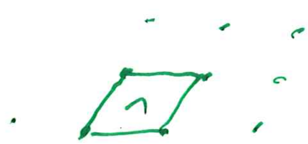


Exe Fund. dom. for $\mathbb{Z} \curvearrowright \mathbb{R}$ (by translation): $\mathcal{F} = [0,1)$

or $\mathcal{F} = (0,1) \sqcup \{0,1\}^{\sqcup \frac{1}{2}}$

Exe Fund. dom. for full lattice Λ spanned by $b_1, \ldots, b_n$ acting on $\mathbb{R}^n$ by transl.:

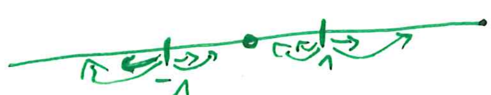
fundamental cell $\mathcal{F} = [0,1)\cdot b_1 + \ldots + [0,1)\cdot b_n$.



Exe Fund. dom. for $\mathbb{R}^{>0} \curvearrowright \mathbb{R}^\times$ (by mult.): $\mathcal{F} = \{\pm 1\}$

or $\mathcal{F} = \{-5, \pi\}$

...



Exe There is no fund. dom. for $\mathbb{R}^{>0} \curvearrowright \mathbb{R}$ (by mult.): what would $\chi_{\mathcal{F}}(0)$ be?

Exe Fund. dom. for $\mathbb{Q}^{\times 2} \curvearrowright \mathbb{Q}^\times$ (by mult.): $\mathcal{F} = \{t \in \mathbb{Z} \text{ squarefree}\}$

$\mathbb{Q}^\times \curvearrowright \mathbb{Q}^\times$ (by mult. by square): $\mathcal{F} = \{t \in \mathbb{Z} \text{ squarefree}\}^{\sqcup \frac{1}{2}}$

ker $= \{\pm 1\}$

Exe Let K be a number field.
Fund. dom. for $K^{\times 2} \curvearrowright K^\times$: $\mathcal{F} = ?$

Rmk 100 There is a fund. dom $\mathcal{F}$ for $G \backslash X$ if and only if $\mathrm{Stab}_G(x) = \{ g \in G \mid gx = x \}$ is finite for each $x \in X$.

Pf "$\Rightarrow$" $\sum_{g \in G} \chi_{\mathcal{F}}(gx) = \# \mathrm{Stab}(x) \cdot \sum_{[g] \in G/\mathrm{Stab}(x)} \chi_{\mathcal{F}}(gx) = 1$

$\Rightarrow \# \mathrm{Stab}(x) < \infty$.

"$\Leftarrow$" e.g. pick a representative $r(Gx) \in X$ in each orbit Gx.

Let $\chi_{\mathcal{F}}(x) = \begin{cases} \frac{1}{\# \mathrm{Stab}(x)}, & x = r(Gx) \\ 0, & \text{otherwise.} \end{cases}$ $\square$

There are many fund. domains, but:

Thm Any two fund. dom $\mathcal{F}, \mathcal{F}'$ for $G \backslash X$ have the same size.

Pf For any $g \in G$, let $A_g = \mathcal{F} \cap g\mathcal{F}'$ and $A'_g = g\mathcal{F} \cap \mathcal{F}'$.

$\Rightarrow \mathcal{F} = \mathcal{F} \cap X = \mathcal{F} \cap \bigsqcup_g g\mathcal{F}' = \bigsqcup_g (\mathcal{F} \cap g\mathcal{F}') = \bigsqcup_g A_g$

and $\mathcal{F}' = \quad \dots = \bigsqcup_g A'_g$.

Also, $g A_{g^{-1}} = A'_g$, so $\# A_{g^{-1}} = \# A'_g$ for all $g \in G$.

$\Rightarrow \# \mathcal{F} = \sum_g \# A_g = \sum_g \# A'_g = \# \mathcal{F}'$. $\square$

Cor $\# \mathcal{F} = \sum_{\text{orbit } Gx} \frac{1}{\# \mathrm{Stab}(x)}$.

Pf The fund. dom. constructed in the pf of Rmk 100 has this size. $\square$

(A5,55)

Cor (Orbit-stabilizer theorem)

If G is finite, then

$$\# \mathcal{F} = \frac{\# X}{\# G} = \sum_{Gx} \frac{1}{\# \mathrm{Stab}(x)}.$$

Pf The triv. fund. dom. has size $\frac{\# X}{\# G}$. $\square$

Thm Let X be a measure space and assume that the action of G the countable group is measure-preserving: $\mathrm{vol}(gA) = \mathrm{vol}(A)$ [$\forall g \in G$, measurable $A \subseteq X$]

Let the measure of a set A on X be $\mathrm{vol}(A) = \int_X \chi_A(x)\,dx$.

Then, any two measurable fund. dom. $\mathcal{F}, \mathcal{F}'$ for $G \backslash X$ have the same measure.

Pf "Same as for sizes." $\square$

[Point out that different fund. cells of $\Lambda \subset \mathbb{R}^n$ all have the same measure.]

Cor If G is fin., then $\mathrm{vol}(\mathcal{F}) = \frac{\mathrm{vol}(X)}{\# G}$.

Some helpful constructions:

Rmk If $\mathcal{F}$ is a fund. dom. for $G \backslash X$ and $Y \subseteq X$ is a subset with $GY = Y$, then $\mathcal{F} \cap Y$ is a fund. dom. for $G \backslash Y$.

the restriction

Ex $\{1,2,\dots\} \sqcup \{0\}^{\sqcup \frac{1}{2}} = (\mathbb{R}^{>0} \sqcup \{0\}^{\sqcup \frac{1}{2}}) \cap \mathbb{Z}$ is a fund. dom. for $\{\pm 1\} \backslash \mathbb{Z} \subseteq \mathbb{R}$.

Rmk If $f : X \to Y$ is a G-equivariant map ($f(gx) = gf(x)$) and $\mathcal{F}$ is a fund. dom. for $G \backslash Y$, then the preimage $f^{-1}(\mathcal{F})$ is a fund. dom. for $G \backslash X$.

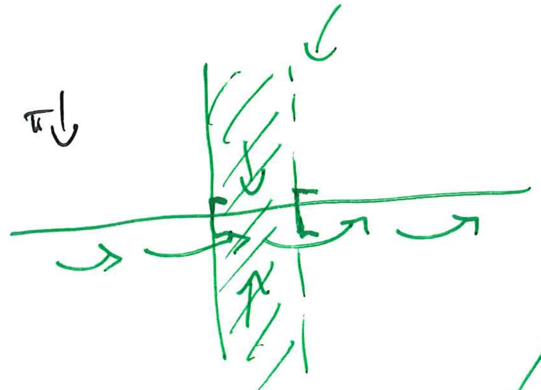
Ex If $\mathcal{F}$ is a fund. dom. for $G \backslash X$ and $f : X \to X$ is a G-equivariant autom., then $f(\mathcal{F})$ is another fund. dom.

Ex

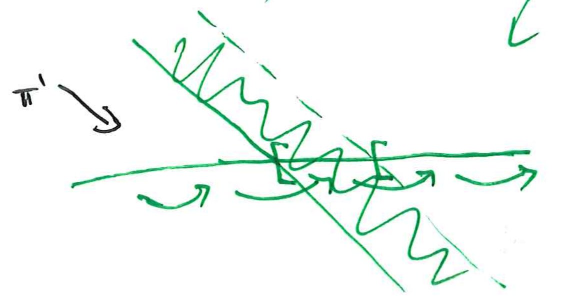
Let $g \in \mathbb{Z}$ act on $(x,y) \in \mathbb{R}^2$ by translation in the x-dir: $g(x,y) = (g+x, y)$ and on $\mathbb{R}$ by translation.

The projection $\pi : \mathbb{R}^2 \to \mathbb{R}$, $(x,y) \mapsto x$ is $\mathbb{Z}$-invariant.

The preimage $\pi^{-1}([0,1)) = [0,1) \times \mathbb{R}$ is a fund. dom. for $\mathbb{Z} \backslash \mathbb{R}^2$.



Other projections, ~~like~~ $\pi' : \mathbb{R}^2 \to \mathbb{R}$ ~~$(x,y) \mapsto x+y$,~~ lead to other preimages. ~~$\pi'^{-1}([0,1)) = \{(x,y) \mid 0 \le x+y < 1\}$.~~



(A5,57)

It can be difficult to choose exactly one element of each orbit. Slightly easier:

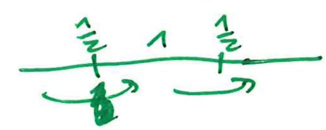
Def An almost fund. dom. $\widetilde{\mathcal{F}}$ of $G \backslash X$ is a subset of X containing ≥ 1 and $< \infty$ elements of each orbit: $1 \leq \#(\widetilde{\mathcal{F}} \cap Gx) < \infty$ for each $x \in X$.

Rmk Assume that $\#\,\mathrm{Stab}(x) < \infty$ for all $x \in X$. Then, each almost fund. dom. $\widetilde{\mathcal{F}}$ is the support of an associated fund. dom. $\mathcal{F}$ defined by

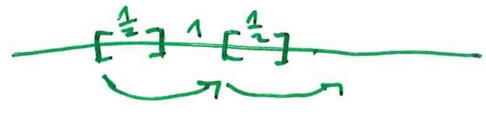
$$\chi_{\mathcal{F}}(x) = \begin{cases} \dfrac{1}{\#(\widetilde{\mathcal{F}} \cap Gx) \cdot \#\mathrm{Stab}(x)} = \dfrac{1}{\#\{g \in G \mid gx \in \widetilde{\mathcal{F}}\}}, & x \in \widetilde{\mathcal{F}} \\ 0 & x \notin \widetilde{\mathcal{F}}. \end{cases}$$

Ex If $\#G < \infty$, $\widetilde{\mathcal{F}} = X$, we get the triv. fund. dom. $\mathcal{F}$.

Ex $\mathbb{Z} \backslash \mathbb{R}$: $\widetilde{\mathcal{F}} = [0,1] \rightsquigarrow \mathcal{F} = (0,1) \sqcup \{0,1\}^{\sqcup \frac{1}{2}}$



$\widetilde{\mathcal{F}} = [0,1.5] \rightsquigarrow \mathcal{F} = [0,0.5]^{\sqcup \frac{1}{2}} \sqcup (0.5,1) \sqcup [1,1.5]^{\sqcup \frac{1}{2}}$



End of lecture 8

~~**Thm** If G is countable and the action of G on X is measurable (A measurable $\Rightarrow gA$ measurable) and $\widetilde{\mathcal{F}}$ is a measurable almost fund. dom., then the associated fund. dom. $\mathcal{F}$ is measurable.~~

~~**Pf** For any k-element subset $S = \{g_1, \dots, g_k\}$ of $G \setminus \{id\}$, let $A_S \subseteq X$ be set of $x \in \widetilde{\mathcal{F}}$ such that $x, g_1 x, \dots, g_k x \in \widetilde{\mathcal{F}}$. It is measurable: With $g_0 = id$, we have~~

~~$A_S = \bigcap_{i=0}^{k} \{g_i^{-1} \widetilde{\mathcal{F}}\}$~~

AS, 58

Thm If G is countable ~~and the action of G on X is measurable ($A \subseteq X$ measurable $\Rightarrow gA$ measurable)~~ and $\tilde{\mathcal{F}} \subseteq X$ is an almost fund. dom. for ~~$G \backslash X$~~ a measurable action $G \curvearrowright X$ ($A \subseteq X$ measurable $\Rightarrow gA \subseteq X$ measurable), then the associated fund. dom. $\mathcal{F}$ is measurable.

Pf For any finite subset $S \subseteq G \backslash \{id\}$, the set

$$A_S = \tilde{\mathcal{F}} \cap \bigcap_{g \in S} g^{-1} \tilde{\mathcal{F}} = \{x \in \tilde{\mathcal{F}} \mid gx \in \tilde{\mathcal{F}} \text{ for all } g \in S\}$$

is measurable.

$\Rightarrow$ For any $k \geq 1$, the set

$$B_k = \bigcup_{\substack{S \subseteq G \backslash \{id\} \\ \#S = k-1}} A_S = \{x \in \tilde{\mathcal{F}} \mid \#\{g \in G \mid gx \in \tilde{\mathcal{F}}\} \geq k\}$$

is measurable.

$\Rightarrow$ $C_k = B_k \backslash B_{k+1} = \{x \in \tilde{\mathcal{F}} \mid \#\{g \in G \mid gx \in \tilde{\mathcal{F}}\} = k\}$

is measurable.

$\Rightarrow$ $\mathcal{F} = \bigsqcup_{k \geq 1} C_k^{\sqcup \frac{1}{k}}$ is measurable. $\square$

Burnside's lemma If $\mathcal{F}$ is a fund. dom. for $G \backslash X$, then the number of orbits is $\#(G \backslash X) = \sum_{x \in \mathcal{F}} \mathrm{Stab}_G(x)$.

~~Units~~

Unit groups of number fields

Let K be a number field of deg. n and signature (r_1, r_2).

$\mathcal{O}_K$ is a full lattice in $\underset{\substack{\uparrow \\ \mathbb{R}\text{-alg}}}{K \otimes \mathbb{R} \cong} \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \underset{\substack{\uparrow \\ \mathbb{R}\text{-vector space}}}{\cong} \mathbb{R}^n$ of covolume $2^{-r_2} \cdot \sqrt{|D_K|}$.

Combine $\log_{\mathbb{R}}: \mathbb{R}^\times \to \mathbb{R}$, $x \mapsto \log|x|$ and $\log_{\sigma}: \mathbb{C}^\times \to \mathbb{R}$, $x \mapsto 2\log x = \log(x\bar{x})$

to a group hom. $\log: (K \otimes \mathbb{R})^\times \longrightarrow \mathbb{R}^{r_1+r_2}$.

The kernel of $\log: \mathcal{O}_K^\times \longrightarrow \mathbb{R}^{r_1+r_2}$ is the group μ_K of roots of unity in K. Let $w_K = \# \mu_K$.

If $\underset{K\otimes\mathbb{R}}{\log(x)} = \underset{\mathbb{R}^{r_1+r_2}}{(y_i)_i}$, then $\log|\mathrm{Nm}_{K\otimes\mathbb{R}|\mathbb{R}}(x)| = \sum_i y_i$.

In particular, $x \in S := \{x : |\mathrm{Nm}(x)| = 1\}$

if and only if $\log(x) \in H := \{(y_i)_i : \sum_i y_i\}$.

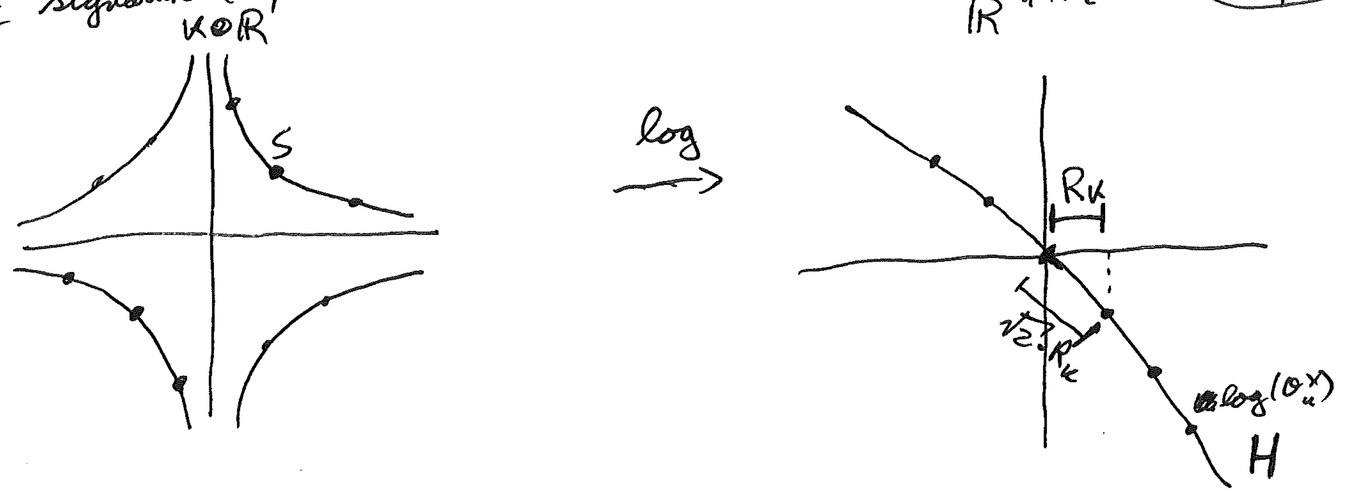
~~$\log(\mathcal{O}_K^\times) \subseteq H$~~

$\mathcal{O}_K^\times \subseteq S$, so $\log(\mathcal{O}_K^\times) \subseteq H$.

Identify H with $\mathbb{R}^{r_1+r_2-1}$ by forgetting one of the coordinates y_i.

Then, $\log(\mathcal{O}_K^\times)$ is a full lattice in $H \cong \mathbb{R}^{r_1+r_2-1}$ whose covolume is called the <u>regulator</u> R_K of K.

Ex signature (2,0)



Rmk W.r.t. the standard "area" measure on $H \subseteq \mathbb{R}^{r_1+r_2}$, the covol. would be $\sqrt{r_1+r_2}\cdot R_K$.

Ex If $r_1+r_2=1$, then $H \cong \mathbb{R}^0$ and $R_K = 1$.

Cor $\mathcal{O}_K^\times \cong \mu_K \times \mathbb{Z}^{r_1+r_2-1}$

Counting ideals (the class number formula)

[If $r_1+r_2 \geq 2$, there are infinitely many $x \in \mathcal{O}_K$ of norm 1 (the el. of $\mathcal{O}_K^\times$). But there are only fin. many ideals $\mathfrak{a} \subseteq \mathcal{O}_K$ of norm $Nm(\mathfrak{a}) \leq T$. How many?]

Thm Let $c \in Cl_K$ be an ideal class of K. Then,

$$\#\{\mathfrak{a} \subseteq \mathcal{O}_K \mid \mathfrak{a} \in c,\ Nm(\mathfrak{a}) \leq T\} \underset{K}{\sim} \frac{2^{r_1}(2\pi)^{r_2} R_K}{w_K \sqrt{|D_K|}} \cdot T$$

for $T \to \infty$.

Cor (Class number formula)

Let $h_K = \# Cl_K$. Then,

$$\#\{\mathfrak{a} \subseteq \mathcal{O}_K \mid Nm(\mathfrak{a}) \leq T\} \underset{K}{\sim} \frac{2^{r_1}(2\pi)^{r_2} R_K h_K}{w_K \sqrt{|D_K|}} \cdot T \text{ for } T \to \infty.$$

Cor Let $c \in Cl_K$. Ordering $\mathfrak{a} \subseteq \mathcal{O}_K$ by $Nm(\mathfrak{a})$,

$$\mathbb{P}(\mathfrak{a} \in c \mid \mathfrak{a} \subseteq \mathcal{O}_K) = \frac{1}{h_K}.$$

[All ideal classes occur equally often.]

Ex ($K=\mathbb{Q}$) $r_1 = 1, r_2 = 0$, $R_K = 1$, $h_K = 1$, $w_K = 2$, $D_K = 1$

$$\#\{\mathfrak{a} \subseteq \mathbb{Z} \mid Nm(\mathfrak{a}) \leq T\} \underset{\substack{\mathfrak{a}=(a)\\ a \geq 1}}{=} \#\{1 \leq a \leq T\} \sim T \text{ for } T \to \infty.$$

Pf of Thm (AS, 62)

We have a bijection

$$\{\text{principal ideal } \mathfrak{a} \subseteq \mathcal{O}_K\} \longleftrightarrow \mathcal{O}_K^\times \backslash \mathcal{O}_K$$

$$\mathfrak{a} = (x) \longleftrightarrow x$$

with $Nm(\mathfrak{a}) = |Nm_{K|\mathbb{Q}}(x)|$.

More generally, if $\mathfrak{b} \in \mathfrak{c} \in Cl_K$ is any (fractional) ideal, then

$$\{\mathfrak{a} \subseteq \mathcal{O}_K \mid \mathfrak{a} \in \mathfrak{c}\} \longleftrightarrow \mathcal{O}_K^\times \backslash \mathfrak{b}^{-1}$$

$$\mathfrak{a} = \mathfrak{b} \cdot (x) \longleftrightarrow x$$

with $Nm(\mathfrak{a}) = Nm(\mathfrak{b}) \cdot |Nm(x)|$.

It remains to show: $\square$

Lemma $\#\left(\mathcal{O}_K^\times \backslash \{x \in \mathfrak{b}^{-1} \mid |Nm(x)| \leq T\}\right) \sim \frac{2^{r_1}(2\pi)^{r_2} R_K}{w_K \sqrt{|D_K|}} \cdot (T \cdot Nm(\mathfrak{b}))$.

$$\Big\| \leftarrow \text{covol}(\mathfrak{b}^{-1}) = Nm(\mathfrak{b}^{-1}) \cdot \text{covol}(\mathcal{O}_K)$$

$$\frac{2^{r_1} \pi^{r_2} R_K}{w_K \,\text{covol}(\mathfrak{b}^{-1})} \cdot T.$$

Pf of Lemma Let $A_T = \{x \in K \otimes \mathbb{R} \mid |Nm(x)| \leq T\}$.

[If the sig. is $(0,1)$, then $A_T \subseteq \mathbb{C}$ is the cl. disc of radius $T^{1/2}$.

$\Rightarrow \#\{x \in \mathfrak{b}^{-1} \mid |Nm(x)| \leq T\} = \#(A_T \cap \mathfrak{b}^{-1}) \sim \frac{\pi (T^{1/2})^2}{\text{covol}(\mathfrak{b}^{-1})} = \frac{\pi}{\text{covol}(\mathfrak{b}^{-1})} \cdot T$.

Every $\underset{\mu_K}{\mathcal{O}_K^\times}$-orbit contains exactly w_K el.]

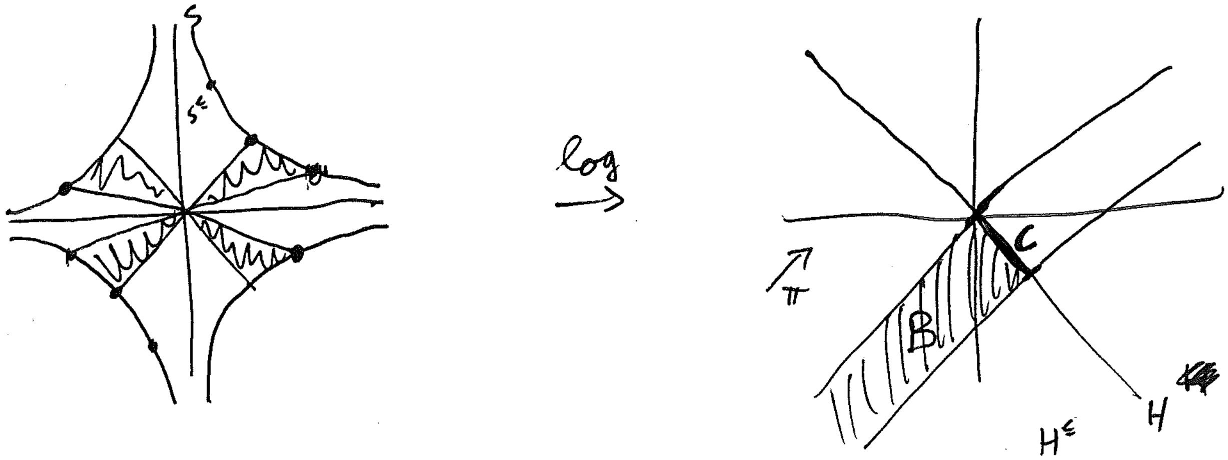
A5,63

[let's construct a fund. dom. for $\mathcal{O}_u^\times \backslash (K\otimes\mathbb{R})^\times$.]

Let $C \subseteq H \subset \mathbb{R}^{r_1+r_2-1}$ be a fund. cell of $\log(\mathcal{O}_u^\times) \subset H$.

$\Rightarrow C^{\sqcup \frac{1}{w_u}}$ is a fund. dom. for $\mathcal{O}_u^\times \backslash H$.

Choose a projection $\pi : \mathbb{R}^{r_1+r_2} \twoheadrightarrow H$.



$\Rightarrow \pi^{-1}(C)^{\sqcup \frac{1}{w}}$ is a fund. dom. for $\mathcal{O}_u^\times \backslash \mathbb{R}^{r_1+r_2}$.

Let $H^{\le 0} = \{ y \in \mathbb{R}^{r_1+r_2} \mid \sum y_i \le 0 \}$ and $S^{\le T} = \{ x \in (K\otimes\mathbb{R})^\times \mid |N_m(x)| \le T \}$.

$\Rightarrow \Big(\underbrace{\pi^{-1}(C) \cap H^{\le 0}}_{=:B}\Big)^{\sqcup \frac{1}{w}}$ is a fund. dom. for $\mathcal{O}_u^\times \backslash H^{\le 0}$.

$\Rightarrow \mathcal{F}^{\le 1} := \log^{-1}(B)^{\sqcup \frac{1}{w}}$ is a fund. dom. for $\mathcal{O}_u^\times \backslash S^{\le 1}$.

$\Rightarrow T^{\frac{1}{n}} \cdot \mathcal{F}^{\le 1}$ is a fund. dom. for $\mathcal{O}_u^\times \backslash S^{\le T}$.

$\Rightarrow T^{\frac{1}{n}} \cdot \mathcal{F}^{\le 1} \cap \mathfrak{b}^{-1}$ is a fund. dom. for $\mathcal{O}_u^\times \backslash (S^{\le T} \cap \mathfrak{b}^{-1})$.

$\Rightarrow \#(\mathcal{O}_u^\times \backslash (S^{\le T} \cap \mathfrak{b}^{-1})) \underset{\text{all stabilisers are trivial}}{=} \#(T^{\frac{1}{n}} \cdot \mathcal{F}^{\le 1} \cap \mathfrak{b}^{-1})$

$= \#(T^{\frac{1}{n}} \cdot \log^{-1}(B)^{\sqcup \frac{1}{w}} \cap \mathfrak{b}^{-1}) = \frac{1}{w} \cdot \#(T^{\frac{1}{n}} \cdot \log^{-1}(B) \cap \mathfrak{b}^{-1})$.

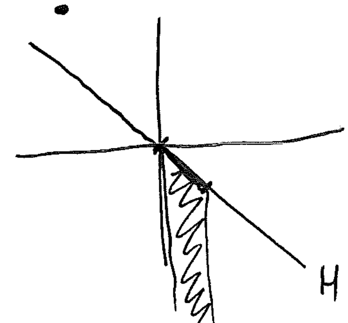
AS, 64

If the projection π is (for example) along $(1,\dots 1)\in\mathbb{R}^{r_1+r_2}$, then the boundary of $\log^{-1}(B)$ is Lipschitz, so

$$\mathrm{LHS}\sim\frac{1}{w}\cdot\frac{\mathrm{vol}(\log^{-1}(B))}{\mathrm{covol}(\mathfrak{b}^{-1})}\cdot\left(T^{1/n}\right)^n.$$

The action $\mathcal{O}_u^\times \circlearrowright K\otimes\mathbb{R}$ is measure-preserving (because $|N_m(x)|=1$ (det Jacobian) for all $x\in\mathcal{O}_u^\times$), so ~~to compute vol(log⁻¹ B~~
any two fund. dom. (measurable) have the same volume, so

to compute $\mathrm{vol}(\log^{-1}(B))$, we can instead let π be the proj. along $(0,\dots,0,1)\in\mathbb{R}^{r_1+r_2}$.



$$\mathrm{vol}(\log^{-1}(B))=\int_{(K\otimes\mathbb{R})^\times\cong(\mathbb{R}^\times)^{r_1}\times(\mathbb{C}^\times)^{r_2}}\chi_B(\log(x))\,dx$$

$$=\int_{(\mathbb{R}^\times)^{r_1}}\int_{(\mathbb{R}^{>0})^{r_2}}\int_{[0,2\pi]^{r_2}}\chi_B(\log|x_1|,\dots,\log|x_{r_1}|,2\log\rho_1,\dots,2\log\rho_{r_2})\,\rho_1\cdots\rho_{r_2}\,d\varphi\,d\rho\,dx$$

write $z\in\mathbb{C}^\times$ in polar coord.: $z=\rho e^{i\varphi}$. $\rightsquigarrow dz=\rho\,d\rho\,d\varphi$ ("area")

$$=2^{r_1}(2\pi)^{r_2}\int_{(\mathbb{R}^{>0})^{r_1}}\int_{(\mathbb{R}^{>0})^{r_2}}\chi_B(\log x_1,\dots,\log x_{r_1},2\log\rho_1,\dots,2\log\rho_{r_2})\,\rho_1\cdots\rho_{r_2}\,d\rho\,dx$$

$$\underset{\substack{\log x_i=a_i\\ 2\log\rho_i=b_i}}{=}2^{r_1}(2\pi)^{r_2}\int_{\mathbb{R}^{r_1}}\int_{\mathbb{R}^{r_2}}\chi_B(a_1,\dots,b_1,\dots)\cdot\frac{e^{a_1+\dots+b_1+\dots}}{2^{r_2}}\,db\,da$$

AS, 65

$$= 2^{r_1}\pi^{r_2}\int_{\mathbb{R}^{r_1+r_2}} \chi_B(a)\cdot e^{\sum_i a_i}\,da$$

$$= 2^{r_1}\pi^{r_2}\,\mathrm{vol}(C)\int_{\mathbb{R}^{<0}} e^{t}\,dt$$

$\uparrow$

$t=\sum_i a_i\ (\leq 0)$

$$= 2^{r_1}\pi^{r_2}\,R_K\,. \qquad \square$$

end of lecture 9

Ideal class groups

Brauer–Siegel Theorem (worst case)

Let K be a number field of degree n and let $\varepsilon > 0$. Then,

$$|D_K|^{\frac{1}{2}-\varepsilon} \ll_{n,\varepsilon} h_K R_K \ll_{n,\varepsilon} |D_K|^{\frac{1}{2}+\varepsilon}.$$

Rmk: If K is imag. quadr. (signature $(0,1)$), then $R_K = 1$.

Conjecture (average case)

Let $n \geq 2$. There is a constant $C_n > 0$ such that

$$\sum_{\substack{K \text{ of deg. } n \\ |D_K| \leq T}} h_K R_K \sim C_n \cdot T^{3/2}.$$

We'll prove this for imaginary quadratic number fields.

AS, 67

Binary quadratic forms

For any int. domain R, let $V(R)$ be the set of binary quadr. forms with coeff. in R:

$$\text{polynomials } f(X,Y) = aX^2 + bXY + cY^2 \in R[X].$$

The discriminant of f is $b^2 - 4ac$.

$M = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in GL_2(R)$ acts on $f \in V(R)$ by

$$(Mf)(X,Y) = f(pX + rY, qX + sY)/\det(M)$$

$\left(\text{i.e. } (Mf)(v) = f(M^T v)/\det(M).\right)$

We have $\operatorname{disc}(Mf) = \cdot \operatorname{disc}(f)$.

~~In part., $\operatorname{disc}(Mf) = \operatorname{disc}(f)$ if $M \in SL_2(R)$.~~

Also, $\begin{pmatrix} u & 0 \\ 0 & u \end{pmatrix} f = f$, so we obtain an action $PGL_2(R) \circlearrowleft V(R)$. ~~preserving discriminants~~.

$$PGL_2(R) = GL_2(R)/R^\times$$

Quadratic number fields

Def An integer $D \in \mathbb{Z}$ is a fund. disc. if there is a quadr. number field with discriminant D.

Rmk D is a fund. disc. if and only if $D \neq 1$ and either

a) $D \equiv 1 \mod 4$ is squarefree, or

b) $\mathbb{Z} \ni \frac{D}{4} \equiv 2,3 \mod 4$ is squarefree.

Rmk Let K be a quadr. number field of disc. D. Then [$\sqrt{D} \in K$ and]

$$\mathcal{O}_K = \mathbb{Z} + \frac{D+\sqrt{D}}{2}\mathbb{Z}.$$

~~Rmk Let $\mathfrak{a} \subseteq \mathcal{O}_K$, where $\mathfrak{a} = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$. Then~~
~~$\frac{\omega_2}{\omega_1} = \frac{-b+\sqrt{D}}{2}$~~

Lemma Let $\omega_1, \omega_2 \in K$ be lin. indep. over $\mathbb{Q}$. Write

$$\frac{\omega_2}{\omega_1} = \frac{b+\sqrt{D}}{2a} \quad \text{with } a, b \in \mathbb{Q} \ (a \neq 0) \text{ and let } c = \frac{b^2-D}{4a}$$

(so $D = b^2 - 4ac$). Then, $I := \omega_1\mathbb{Z} + \omega_2\mathbb{Z} \subset K$ is a fractional ideal if and only if $a, b, c \in \mathbb{Z}$.

Ex $\omega_1 = 1, \omega_2 = \frac{D+\sqrt{D}}{2}$
$\Rightarrow I = \mathcal{O}_K$,
$a = 1, b = D, c = \frac{D^2-D}{4}$.

Pf I is a frac. id. if and only if $\frac{D+\sqrt{D}}{2}\omega_1, \frac{D+\sqrt{D}}{2}\omega_2 \in I$.

$$\frac{D+\sqrt{D}}{2}\omega_1 \in I \iff a, \frac{D+b}{2} \in \mathbb{Z}$$
$$\frac{D+\sqrt{D}}{2}\omega_1 = a\omega_2 + \frac{D-b}{2}\omega_1$$

$$\frac{D+\sqrt{D}}{2}\omega_2 \in I \iff \frac{D+b}{2}, c \in \mathbb{Z}$$

$$\frac{D+\sqrt{D}}{2}\omega_2 = \frac{D+\sqrt{D}}{2} \cdot \frac{b+\sqrt{D}}{2a}\omega_1 = \frac{bD + D + b\sqrt{D} + D\sqrt{D}}{4a}\omega_1 = \frac{D+b}{2}\omega_2 + \frac{D-b^2}{4a}\omega_1$$
$$= \frac{D+b}{2}\omega_2 + c\omega_1$$

$\square$

AS, 69

Remark Let a, b, c, I as above. Let $S \in \mathrm{End}_{\mathbb{Q}\text{-vector space}}(K)$ send 1 to ω_1 and $\frac{D+\sqrt{D}}{2}$ to ω_2.

Then,
$$\frac{\mathrm{Nm}_{K|\mathbb{Q}}(\omega_1 X + \omega_2 Y)}{\det(S)} = aX^2 + bXY + cY^2.$$

Note: $\det(S) = \pm \mathrm{Nm}(I)$.

Pf

Replacing ω_1, ω_2 by $r\omega_1, r\omega_2$ for some $r \in K^\times$ doesn't change the LHS or RHS.

$\Rightarrow$ We may assume that $\omega_1 = 1$, so $\omega_2 = \frac{-b+\sqrt{D}}{2a}$.

$$\Rightarrow \det(S) = \det \begin{bmatrix} 1 & * \\ 0 & \frac{1}{a} \end{bmatrix} = \frac{1}{a}$$

$$\Rightarrow \mathrm{LHS} = a \cdot \mathrm{Nm}_{K|\mathbb{Q}}(\omega_1 X + \omega_2 Y) = a \cdot \mathrm{Nm}\left(X + \frac{bY + \sqrt{D}Y}{2a}\right)$$

$$= a \cdot \left(\left(X + \frac{b}{2a}Y\right)^2 - D \cdot \left(\frac{Y}{2a}\right)^2\right)$$

$$= aX^2 + bXY + \frac{b^2 - D}{4a} \cdot Y^2 = aX^2 + bXY + cY^2$$

$\square$

$\Rightarrow$ We obtain a bijection

$$K^\times \backslash \{(\omega_1, \omega_2) \text{ basis of frac. ideal } I \text{ of } K\} \longleftrightarrow \underbrace{\{f \in V(\mathbb{Z}) \mid \mathrm{disc}(f) = D\}}_{V_{\mathrm{disc}=D}(\mathbb{Z})}$$

(If $b^2 - 4ac = D$, then $a \neq 0$ because D is not a square.)

(AS, 70)

The group $GL_2(\mathbb{Z})$ acts transitively on the set of bases (ω_1,ω_2) of a given frac. ideal I. Let $M=\begin{pmatrix} p & q \\ r & s\end{pmatrix}$.

$$\begin{array}{ccc} (\omega_1,\omega_2) & \rightsquigarrow & f(X,Y)=aX^2+bXY+cY^2 \in V(\mathbb{Z}) \\ \Big\downarrow & & \Big\downarrow \\ M(\omega_1,\omega_2) = (p\omega_1+q\omega_2,\ r\omega_1+s\omega_2) & \rightsquigarrow & \dfrac{Nm\big((p\omega_1+q\omega_2)X+(r\omega_1+s\omega_2)Y\big)}{\det(M)\det(S)} = \dfrac{f(pX+rY,\ qX+sY)}{\det(M)} = Mf \end{array}$$

$\Rightarrow$ We obtain a bijection

$$Cl_K \longleftrightarrow GL_2(\mathbb{Z})\backslash V_{disc=D}(\mathbb{Z})$$

Lemma

Any $f \in V(\mathbb{Z})$ with $\mathrm{disc}(f)=D$ has $GL_2(\mathbb{Z})$-stabilizer

$$\mathrm{Stab}(f) \cong \mathcal{O}^\times$$

Pf: Fix some basis (ω_1,ω_2) of a frac. id. I. If another basis $(\omega_1',\omega_2') = M(\omega_1,\omega_2)$ of the same frac. ideal I corresponds to the same $f(X,Y)=aX^2+bXY+cY^2$, then

$$\frac{\omega_2}{\omega_1} = \frac{-b+\sqrt{D}}{2a} = \frac{\omega_2'}{\omega_1'}. \quad \text{Let } \varphi(M) = \frac{\omega_1'}{\omega_1} = \frac{\omega_2'}{\omega_2} \in K^\times.$$

We have

$I = \omega_1'\mathbb{Z}+\omega_2'\mathbb{Z} = \varphi(M)\cdot(\omega_1\mathbb{Z}+\omega_2\mathbb{Z}) = \varphi(M)\cdot I$, so in fact $\varphi(M)\in\mathcal{O}_K^\times$. $\Rightarrow$ We get a hom. $\varphi: \mathrm{Stab} \longrightarrow \mathcal{O}_K^\times$, which is

- clearly injective: if $\varphi(M)=1$, then $\omega_1'=\omega_1$, $\omega_2'=\omega_2$, so $M=\mathrm{id}$. (AS, 71)
- surjective: if $r \in \mathcal{O}_K^\times$, then $(r\omega_1, r\omega_2)$ is another basis of I.

$\square$

__Cor__ let D be a fund. disc. There exists a fund. dom. for $GL_2(\mathbb{Z})\backslash V_{disc=D}(\mathbb{Z})$ if and only if $D<0$. (imaginary quadratic number field K)

__Pf__ $\exists$ fund. dom. $\iff$ all stabilizers finite $\iff \#\mathcal{O}_K^\times < \infty \iff$ sig. $(0,1) \iff D<0$. $\square$

[$V_{disc=D}(\mathbb{Z}) \neq \emptyset$ because $\mathcal{C}\ell_K \neq \emptyset$]

We can explicitly construct a fund. dom.:

__Thm__ Let $V_{disc<0} = \{f : disc(f)<0\}$. Then,

$$\tilde{\mathcal{F}} := \{ f=ax^2+bxy+cy^2 \in V(\mathbb{R}) \mid b^2-4ac<0,\ |b| \le a \le c \} \subseteq V_{disc<0}(\mathbb{R})$$

is an almost fund. dom. for $GL_2(\mathbb{Z})\backslash V_{disc<0}(\mathbb{R})$. Let $\mathcal{F}$ be the corr. fund. dom. For each f in the interior of $\tilde{\mathcal{F}} \subset V_{disc<0}(\mathbb{R}) \subset \mathbb{R}^3$, we have $\chi_{\mathcal{F}}(x) = \frac{1}{2}$.

Thm $$\sum_{\substack{K \text{ quadr. n.f.} \\ 0 < -D_K \leq T}} \overset{\#\mathrm{Cl}_K}{\overset{\sim}{h_K}} \sim C \cdot T^{3/2} \quad \text{for } T \to \infty,$$

where $$C \overset{?}{=} \frac{\pi}{36} \cdot \prod_p \left(1 - p^{-2} - p^{-3} + p^{-4}\right).$$

Rmk We've previously shown that

$$\sum_{\substack{K \text{ quadr. n.f.} \\ 0 < -D_K \leq T}} 1 \sim C' \cdot T,$$

where $C' = \frac{1}{2} \cdot \prod_p (1 - p^{-2})$.

This means that we expect h_K to "on average" be roughly

$$\frac{\frac{3}{2} C |D_K|^{1/2}}{C'}.$$

Pf of Thm

AS, 73

$\mathcal{O}_K^\times = \{\pm 1\}$ for all but fin. many K

$$\sum_{\substack{K \text{ quadr.} \\ 0 < -D_K \le T}} h_K \sim \sum_{K \atop \dots} \frac{2}{\mathcal{O}_K^\times} \cdot h_K$$

orbit-stabiliser Thm, $\# \mathrm{Stab} = \# \mathcal{O}_K^\times$

$$= 2 \cdot \sum_K \# (\mathcal{F} \cap V_{disc = D} (\mathbb{Z}))$$

$$= 2 \cdot \# (\mathcal{F} \cap V^{fund}_{0 < -disc \le T} (\mathbb{Z}))$$

$V^{fund}(\mathbb{Z}) := \{ f \in V(\mathbb{Z}) \mid disc(f) \text{ is fund. disc.}\}$

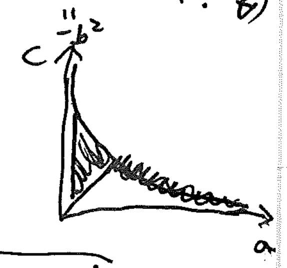
Remember that $-disc(f) = 4ac - b^2$.

Problem: $\mathrm{supp}(\mathcal{F} \cap V_{0 < -disc \le T}(\mathbb{R}))$ is unbounded!

(We could have $b = 0$, $a = \varepsilon$, $c = \frac{T}{4\varepsilon}$ for any $\varepsilon > 0$.) "cusp"

Solution: For $f = aX^2 + bXY + cY^2 \in \mathcal{F} \cap V^{fund}_{0 < -disc \le T}(\mathbb{Z})$,
we can't have $a = 0$. (It would imply $0 < 4ac - b^2 \le T$. ↯)

$\Rightarrow a \ge 1$



Also, $T \ge 4ac - b^2 \underset{|b| \le a \le c}{\ge} 3b^2$, so $\boxed{b \ll T^{1/2}}$.

$\Rightarrow$ $4ac \le T + b^2 \ll T$, so $\boxed{ac \ll T}$.

Since $a \le c$, $\boxed{a \ll T^{1/2}}$.
Since $a \ge 1$, $\boxed{c \ll T}$.

Let $\mathcal{F}' = \mathcal{F} \cap \{ f = aX^2 + bXY + cY^2 \in V(\mathbb{R}) \mid a \ge 1 \}$.
("cut off the cusp").

(AS, 74)

$\Rightarrow LHS \sim 2 \cdot \#(\mathcal{F}' \cap V^{fund}_{0<-disc\leq T}(\mathbb{Z}))$.

End of lecture 10

We have $\chi_{\mathcal{F}'}(f) = \frac{1}{2}$ in the interior of $supp(\mathcal{F}' \cap V_{0<-disc\leq T}(\mathbb{R})) = \{f \mid |b| \leq a \leq c$ and $a \geq 1\}$ and $0 < 4ac - b^2 \leq T\}$

The boundary of $supp(\ldots)$ is $(\mathcal{O}(1), \mathcal{O}(T))$-Lipschitz.

$\Rightarrow$ By Widmer's thm,

$$2 \cdot \#(\mathcal{F}' \cap V_{0<-disc\leq T}(\mathbb{Z}))$$

$$\sim vol(supp(\mathcal{F}' \cap V_{\ldots}(\mathbb{R})))$$

$$\sim vol(supp(\mathcal{F} \cap \underbrace{V_{0<-disc\leq T}(\mathbb{R})}))$$

"the fraction of vol. in the cusp goes to 0 as $T \to \infty$"

$T^{1/2} \cdot (\mathcal{F} \cap V_{0<-disc\leq 1}(\mathbb{R}))$

($disc(f) = b^2 - 4ac$ is hom. of degree 2)

$$= vol(supp(\mathcal{F} \cap V_{0<-disc\leq 1}(\mathbb{R}))) \cdot T^{3/2}$$

$V(\mathbb{R})$ is 3-dimensional

$$= \frac{\pi}{36} \cdot T^{3/2}.$$

$\Rightarrow$ For fundamental discriminants, we need a <u>sieve</u>.

Remember that $D<0$ fund. $\Leftrightarrow$ $D \equiv 1 \bmod 4$ squarefree or $\mathbb{Z} \ni \frac{D}{4} \equiv 2,3 \bmod 4$ squarefree.

15,7.05

Another point-counting theorem:

~~Instead of Widmer's Thm, we could have used:~~

Davenport's Lemma

Let $A \subset \mathbb{R}^n$ be compact and semialgebraic:

Assume there are pol. $P_1, \dots, P_s \in \mathbb{R}[X_1, \dots, X_n]$ of degree $\leq d$ such that

$(x_1, \dots, x_n) \in A$ if and only if $P_i(x_1, \dots, x_n) \geq 0$ for all $i = 1, \dots, s$.

Then,
$$\#(A \cap \mathbb{Z}^n) = \mathrm{vol}(A) + \sum_{k=0}^{n-1} O_{n,s,d}(V_k),$$
where

V_k is the sum of the volumes of the projections of A to k-dimensional coordinate subspaces of $\mathbb{R}^n$.

(And $V_0 = 1$.)

Ex $A \subset \mathbb{R}^n$ disc of radius $R \Rightarrow V_0 = 1, V_1 = 2R + 2R = 4R \Rightarrow \#(A \cap \mathbb{Z}^2) = \pi R^2 + O(R+1)$

Ex $\tilde{\mathcal{F}}' \cap V_{0<-\mathrm{disc} \leq T}(\mathbb{R}) = \{(a, b, c) \mid |b| \leq a \leq c, 0 < 4ac - b^2 \leq T, a \geq 1\}$ $\subseteq \{(a,b,c) \mid a, b \ll T^{1/2}, c \ll T, ac \ll T, bc \ll T\}$ is described by a bounded number of pol. ineq. of bounded degree. The projections have the following sizes:

$V_0 = 1$

$$V_1 \ll \underset{\uparrow\, a}{T^{1/2}} + \underset{\uparrow\, b}{T^{1/2}} + \underset{\uparrow\, c}{T}$$

$$V_2 \ll \underset{\uparrow\, ab}{T^{1/2} \cdot T^{1/2}} + \underset{\uparrow\, ac}{T \log T} + \underset{\uparrow\, bc}{T \log T}$$

$\Rightarrow$ error term $\ll T \log T$.

Reminder $V^{(R)} = \{f = ax^2+bxy+cy^2 \mid a,b,c\in R\} \cong R^3$

$\mathrm{disc}(f) = b^2-4ac$

K quadr. number field of disc. D

$$Cl_K \longleftrightarrow GL_2(\mathbb{Z})\backslash V_{\mathrm{disc}=D}(\mathbb{Z})$$

$$\mathcal{O}_K^\times \cong \mathrm{Stab}(f)$$

Goal: $\sum_{K:\, 0<-D_K\le T} h_K \sim C\cdot T^{3/2}$ where $C=\frac{\pi}{36}\cdot\prod_p (1-p^{-2}-p^{-3}+p^{-4})$

Pf $\tilde{\mathcal F} := \{f\in V(\mathbb R) \mid 0<4ac-b^2,\ |b|\le a\le c\} \subseteq V_{\mathrm{disc}<0}(\mathbb R)$

$\rightsquigarrow$ $\mathcal F$ fund. dom. for $GL_2(\mathbb Z)\backslash V_{\mathrm{disc}<0}(\mathbb R)$ with weight $\frac{1}{2}$ in the interior of $\mathrm{supp}(\mathcal F)=\tilde{\mathcal F}$.

(cut off cusp) Every $f\in V_{\mathrm{disc}<0}(\mathbb Z)$ lies in

$\tilde{\mathcal F}' = \tilde{\mathcal F}\cap\{\dots \mid a\ge 1\} \subseteq \{\ \mid a, |b| \ll T^{1/2},\ c\ll T,\ ac\ll T,\ |b|c\ll T,\ a,c\ge 1\}$

$\mathcal F' := \mathcal F\cap\{\dots\mid a\ge 1\}$.

~~fund. dom.~~

$\Rightarrow \sum h_K \sim 2\cdot\#(\mathcal F'\cap V^{\text{fund}}_{0<-\mathrm{disc}\le T}(\mathbb Z))$.

The set $\tilde{\mathcal F}'\cap V_{0<\mathrm{disc}\le T}(\mathbb R)$ is described by a bdd. number of pol. ineq. of bdd. degrees. The projections have volumes:

$V_0=1$

$V_1\ll \underset{a}{T^{1/2}} + \underset{b}{T^{1/2}} + \underset{c}{T}$

$V_2\ll \underset{a,b}{T^{1/2}\cdot T^{1/2}} + \underset{a,c}{T\log T} + \underset{b,c}{T\log T}$

$\Rightarrow$ By Davenport's lemma, (AS, 77)

$$2 \cdot \#\left(\mathcal{F}' \cap V_{0<-\mathrm{disc}\leq T}(\mathbb{Z})\right)$$

$$\underset{\text{weights}=\frac{1}{2}}{=} \mathrm{vol}\Big(\widehat{\mathcal{F}}' \cap \underbrace{V_{0<-\mathrm{disc}\leq T}(\mathbb{R})}_{T^{1/2}\cdot V_{0<-\mathrm{disc}\leq 1}(\mathbb{R})}\Big) + O(T \log T)$$

$$= T^{3/2} \cdot \mathrm{vol}\Big(\underbrace{\left(T^{-1/2}\widehat{\mathcal{F}}'\right)}_{\substack{\{a \geq T^{-1/2}\} \downarrow \{a > 0\} \\ \text{converges monotonically to } \widehat{\mathcal{F}}}} \cap V_{0<-\mathrm{disc}\leq 1}(\mathbb{R})\Big) + O(T \log T)$$

$$\sim T^{3/2} \cdot \mathrm{vol}\left(\widehat{\mathcal{F}} \cap V_{0<-\mathrm{disc}\leq 1}(\mathbb{R})\right) = \frac{\pi}{36} \cdot T^{3/2}.$$

To count just quadr. forms with fund. disc., use a sieve: (AS, 7B)

Def $D \neq 1$ fund. at p $\Leftrightarrow$ $\begin{cases} p^2 \nmid D, & p \text{ odd} \\ D \equiv 1,5,9,13,8,12 \bmod 16, & p = 2. \end{cases}$

so that D fund. disc. $\Leftrightarrow$ D fund. disc. at every p.

HW: $\mathbb{P}(\operatorname{disc}(f) \text{ fund. at } p \mid f \in V(\mathbb{Z}/p^4\mathbb{Z})) = 1 - p^{-2} - p^{-3} + p^{-4}$.

Let $M \geq 2$. Using the CRT and applying Davenport's lemma separately in each residue class, it follows that

$$\sum h_K \sim \frac{\pi}{36} \cdot \prod_{p \leq M} (1 - p^{-2} - p^{-3} + p^{-4}) \cdot T^{3/2}$$

$$+\, O\Big(\#\{f \in \tilde{\mathcal{F}}' \cap V_{0<-\operatorname{disc}\leq T}(\mathbb{Z}) \mid \underbrace{\operatorname{disc}(f) \text{ not fund. at some } p > M}_{\Leftrightarrow\ p^2 \mid \operatorname{disc}(f) = b^2 - 4ac}\}\Big)$$

Assume $f \in \tilde{\mathcal{F}}' \cap V_{0<-\operatorname{disc}\leq T}(\mathbb{Z})$ with $p^2 \mid b^2 - 4ac$.

$\Rightarrow$ $p^2 \leq 4ac - b^2 \leq T \Rightarrow p \leq T^{1/2}$

If $p \nmid a$, there is ex. one $c \bmod p^2$ s.t. $p^2 \mid b^2 - 4ac$. $\rightsquigarrow \# \ll \underbrace{T^{1/2}}_{\#\{b\}} \cdot \sum_{a \ll T^{1/2}} \underbrace{\left(\frac{T}{p^2 a} + 1\right)}_{\#\{c\}}$

If $p \mid a$, $p^2 \nmid a$ and $p \mid b$, then $p^2 \mid 4ac - b^2 \Leftrightarrow p \mid c$. $\rightsquigarrow \# \ll \frac{T^{3/2}}{p^3} + T$

If $p^2 \mid a$ and $p \mid b$, then $p^2 \mid 4ac - b^2$ for all $c \in \mathbb{Z}$. $\rightsquigarrow \ll \underbrace{\left(\frac{T}{p} + 1\right)}_{\#\{b\}} \cdot \sum_{\substack{a \ll T^{1/2} \\ p^2 \mid a}} \frac{T}{a}$

Otherwise, there is no such c.

$$\underset{\text{for this } p}{\#\text{bad} f} \ll T + \frac{T^{3/2}}{p^2}.$$

$$\Rightarrow \#\text{bad} f \ll \sum_{M < p \leq T^{1/2}} \left(T + \frac{T^{3/2}}{p^2}\right) \ll \underbrace{T \cdot \#\{M < p \leq T^{1/2}\}}_{o(T^{3/2}) \text{ by PNT}} + \frac{T^{3/2}}{M}$$

(AS, 78.5)

$$\Rightarrow \sum_{\cdots} h_k \sim \frac{\pi}{36} \cdot \prod_{p \le M} (1-p^{-2}-p^{-3}+p^{-4}) \cdot T^{3/2} + O\left(\frac{T^{3/2}}{M}\right)$$

for all $M \ge 2$.

$$\underset{M\to\infty}{\Rightarrow} \sum_{\cdots} h_k \sim \frac{\pi}{36} \cdot \prod_{p \le M} (1-p^{-2}-p^{-3}+p^{-4}) \cdot T.$$

$\square$

Fundamental domains for $GL_n(\mathbb{Z})\backslash GL_n(\mathbb{R})$

(AS, 79)

Recall the bijection

$$GL_n(\mathbb{R}) \longleftrightarrow \{\text{basis of } \mathbb{R}^n\}$$

$$\begin{pmatrix} - b_1 - \\ \vdots \\ - b_n - \end{pmatrix} \longleftrightarrow (b_1, \dots, b_n)$$

giving rise to

$$GL_n(\mathbb{Z})\backslash GL_n(\mathbb{R}) \longleftrightarrow \{\text{full lattice } \Lambda \text{ in } \mathbb{R}^n\}$$

$$\begin{pmatrix} - b_1 - \\ \vdots \\ - b_n - \end{pmatrix} \longleftrightarrow \Lambda = \mathbb{Z}b_1 + \dots + \mathbb{Z}b_n$$

[So choosing (almost) fund. dom. for $GL_n(\mathbb{Z})\backslash GL_n(\mathbb{R})$ boils down to selecting representative (fin. many) bases of each lattice.]

Minkowski ~~[illegible]~~ sets

(AS, 80)

Let $|\cdot|$ be the Euclidean norm on $\mathbb{R}^n$.

~~Def The set $\tilde{\mathcal{F}}_{\text{Mink}} \subseteq GL_n(\mathbb{R})$ of~~

Def A ~~[illegible]~~ $\mathbb{Z}$-basis $(b_1, \dots, b_n)$ of a full lattice Λ in $\mathbb{R}^n$ is <u>Minkowski-reduced</u> if it lexicographically minimises $(|b_1|, \dots, |b_n|)$ among all bases of Λ.

Thm Any ~~[illegible]~~ Λ has at least ~~one~~ 2^n, but only fin. many Mink. reduced bases. ~~Hence, the set~~ **Def** Let $\tilde{\mathcal{F}}_{\text{Mink}} \subseteq GL_n(\mathbb{R})$ be the set of ~~Mink. red. bases~~ $\begin{pmatrix} -b_1- \\ \vdots \\ -b_n- \end{pmatrix}$ s.t. $(b_1, \dots, b_n)$ is a Mink. red. basis of Λ.

Cor $\tilde{\mathcal{F}}_{\text{Mink}}$ is a (measurable) almost fund. dom. for $GL_n(\mathbb{Z}) \backslash GL_n(\mathbb{R})$.

~~**Rmk** $\tilde{\mathcal{F}}_{\text{Mink}}$ (and hence the fund. dom. $\mathcal{F}_{\text{Mink}}$) is measurable.~~

(A5, B1)

Rmk $\widetilde{\mathcal{F}}_{Mink}$ and the associated fund. dom. $\mathcal{F}_{Mink} \subseteq GL_n(\mathbb{R})$ are invariant under scaling (right mult. by scalars $\in \mathbb{R}^\times$) and orthogonal transformations (el. of $O_n(\mathbb{R}) \subseteq GL_n(\mathbb{R})$).

$\Rightarrow$ They are the preimages of an (almost) fund. dom. of $GL_n(\mathbb{Z})$ acting on $GL_n(\mathbb{R}) / O_n(\mathbb{R}) \cdot \mathbb{R}^\times$.

The image of a lattice $\Lambda \in GL_n(\mathbb{Z}) \backslash GL_n(\mathbb{R})$ in $GL_n(\mathbb{Z}) \backslash GL_n(\mathbb{R}) / O_n(\mathbb{R}) \cdot \mathbb{R}^\times$ is called the <u>shape</u> of Λ.

Exe (n=1) $GL_1(\mathbb{R}) = \mathbb{R}^\times$

$GL_1(\mathbb{Z}) = \{\pm 1\}$

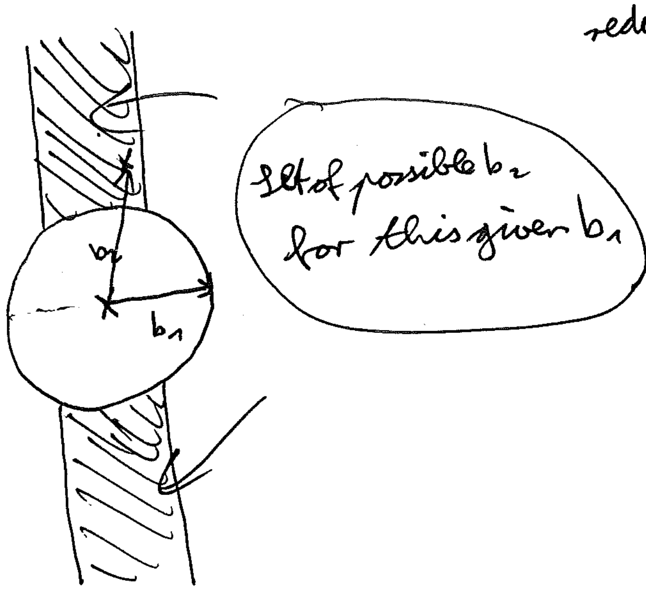
$\tilde{\mathcal{F}}_{\text{Mink}} = \mathbb{R}^\times$

$\mathcal{F}_{\text{Mink}} = (\mathbb{R}^\times) \sqcup \frac{1}{2}$

Exe (n=2) $\tilde{\mathcal{F}}_{\text{Mink}} = \left\{ \begin{pmatrix} -b_1- \\ -b_2- \end{pmatrix} \;\middle|\; |b_1| \le |b_2| \text{ and } |b_1 \cdot b_2| \le \frac{1}{2} |b_1|^2 \right\}$

[or could exchange b_1, b_2 and reduce $(|b_1|, |b_2|)$]

[or could replace b_2 by $b_2 + k b_1$ and reduce $(|b_1|, |b_2|)$.]



For any $g = \begin{pmatrix} -b_1- \\ -b_2- \end{pmatrix}$ with $|b_1| < |b_2|$ and $|b_1 \cdot b_2| < \frac{1}{2}|b_1|^2$, the weight is $\chi_{\mathcal{F}_{\text{Mink}}}(g) = \frac{1}{4}$.

Rmk For large n, it is difficult to [find a Mink. red. basis or even] check whether a given basis is Mink.-reduced! [Need 5 ineq. for $n=3$?]

(AS, 83)

Rmk ~~[illegible]~~

Using the map

$$GL_n(\mathbb{R})/O_n(\mathbb{R}) \longrightarrow \left\{ \begin{array}{l} \text{positive definite quadratic forms in } n \text{ variables} \\ f(x_1,\dots,x_n) \in \mathbb{R}[x_1,\dots,x_n] \end{array} \right\}$$

one can obtain a fund. dom. for $GL_n(\mathbb{Z}) \backslash \{\text{pos. def.} \dots\}$.

(This gave rise to the fund. dom. for $GL_2(\mathbb{Z}) \backslash \mathcal{U}_{\text{disco}}(\mathbb{R})$ when we counted ideal classes.)

Iwasawa decomposition of $GL_n(\mathbb{R})$ / Gram-Schmidt process (AS, 84)

Define subgroups $N, A, K \subseteq GL_n(\mathbb{R})$:

$$N = \left\{ \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ * & & 1 \end{pmatrix} \right\} \text{ (lower triangular unipotent matrices)}$$

$$A = \left\{ \begin{pmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_n \end{pmatrix} \middle| \, a_1, \dots, a_n > 0 \right\} \text{ (diag. matr. w. pos. entries)}$$

$$K = \underset{O_n(\mathbb{R})}{} = \{ g \mid gg^T = id \} \text{ (orth. matrices)}$$

__Thm (Iwasawa decomp.)__
The map $N \times A \times K \longrightarrow GL_n(\mathbb{R})$ is a diffeomorphism.
$$(n, a, k) \mapsto nak$$

[__Not__ a group homomorphism!]

In part. every $g \in GL_n(\mathbb{R})$ can be written uniquely as $g = nak$.

__Idea of Pf (Gram-Schmidt process)__

Let $g = \begin{pmatrix} - b_1 - \\ \vdots \\ - b_n - \end{pmatrix}$. Define $c_1, \dots, c_n \in \mathbb{R}^n$ iteratively by

$$c_i = b_i - \sum_{j=1}^{i-1} n_{ij} c_j, \text{ where } n_{ij} = \frac{b_i \cdot c_j}{|c_j|^2}.$$

Then, $c_1, \dots, c_n$ are pairwise orthogonal and

$$g = \underbrace{\begin{pmatrix} 1 & & \\ n_{21} & 1 & \\ n_{31} & n_{32} & 1 \end{pmatrix}}_{=n \in N} \begin{pmatrix} - c_1 - \\ \vdots \\ - c_n - \end{pmatrix}.$$

Let $a_i = |c_i|$ and $d_i = \frac{c_i}{a_i}$. Then, $d_1, \dots, d_n \in \mathbb{R}^n$ are orthonormal.

$$\Rightarrow g = n \begin{pmatrix} a_1 & & \\ & \ddots & \\ & & a_n \end{pmatrix} \begin{pmatrix} - d_1 - \\ \vdots \\ - d_n - \end{pmatrix} \ni K.$$

"$\square$"

Cor (Iwasawa decomp. of $SL_n(\mathbb{R})$) (A5,85)

With $A_1 = \{ a \in A \mid \det(a) = 1 \}$ and $K_1 = SO_n(\mathbb{R}) = \{ k \in K \mid \det(k) = 1 \}$,

we obtain a diffeom.

$$\begin{aligned} N \times A_1 \times K_1 &\longrightarrow SL_n(\mathbb{R}) \\ (n, a, k) &\longmapsto nak. \end{aligned}$$

Siegel sets

AS, 86

~~Def A matrix $g \in GL_n(\mathbb{R})$ is Siegel reduced if its Iwasawa decomp.~~
~~$g = nak$ with $n = \begin{pmatrix} 1 & & & 0 \\ n_{21} & 1 & & \\ n_{31} & n_{32} & \ddots & \\ & & \ddots & 1 \end{pmatrix}$ and $a = \begin{pmatrix} a_1 & & \\ & \ddots & \\ & & a_n \end{pmatrix}$~~
~~satisfies~~

Def Let $N' = \left\{ n = \begin{pmatrix} 1 & & & 0 \\ n_{21} & 1 & & \\ n_{31} & n_{32} & 1 & \\ \cdots & & \ddots & 1 \end{pmatrix} \in N \;\middle|\; n_{ij} \in \left[-\tfrac{1}{2}, \tfrac{1}{2}\right] \ \forall i > j \right\} \subseteq N$

and $A' = \left\{ a = \begin{pmatrix} a_1 & & \\ & \ddots & \\ & & a_n \end{pmatrix} \in A \;\middle|\; a_{i+1} \geq \frac{\sqrt{3}}{2} \cdot a_i \text{ for } i = 1, \dots, n-1 \right\} \subseteq A.$

Thm The Siegel set $\widetilde{\mathcal{F}}_{\text{Siegel}} = N'A'K \subseteq GL_n(\mathbb{R})$ is a (measurable) almost fund. dom. for $GL_n(\mathbb{Z}) \backslash GL_n(\mathbb{R})$. Furthermore, if $g = nak \in N'A'K$ and $\lambda_1 \leq \dots \leq \lambda_n$ are the (Euclidean) successive minima of the lattice corr. to g, then $a_i \asymp_n \lambda_i$ for $i = 1, \dots, n$.

End of lecture 11

~~Idea of pf To show that each full lattice Λ has a basis $(b_1, \dots, b_n)$ with $g = \begin{pmatrix} -b_1- \\ \vdots \\ -b_n- \end{pmatrix} \in \widetilde{\mathcal{F}}_{\text{Siegel}}$, look at a basis whose Iwasawa decomp. lexicographically minimizes $(a_1, \dots, a_n)$. It's easy to make $n \in N'$ by applying a lower triangular integer matrix. If $a_{i+1} < \frac{\sqrt{3}}{2} a_i$, then exchanging b_i and b_{i+1} reduces $(a_1, \dots, a_n)$ lexicographically.~~ $\}$

~~For $a_i \asymp \lambda_i$: Note that $a_1 \ll a_2 \ll \dots \ll a_n$.~~
~~We have $|b_i| \leq a_i + \sum_{j=1}^{i-1} \frac{1}{2} a_j \ll a_i$. $\Rightarrow \lambda_i \ll a_i$~~
~~But by Minkowski's second thm, $\lambda_1 \cdots \lambda_n \asymp \det(g) = a_1 \cdots a_n$. $\Rightarrow$ asymp. eq. $\lambda_i \asymp a_i$.~~ □

Cor (HW, Mahler's criterion) (AS, 87)

A closed subset X of $GL_n(\mathbb{Z})\backslash GL_n(\mathbb{R})$ (with the quot. top. induced by the standard top. on $GL_n(\mathbb{R}) \subseteq M_{n\times n}(\mathbb{R}) = \mathbb{R}^{n^2}$) is compact if and only if there exist $0 < C \le C' < \infty$ such that the succ. min. of any lattice Λ in X satisfy

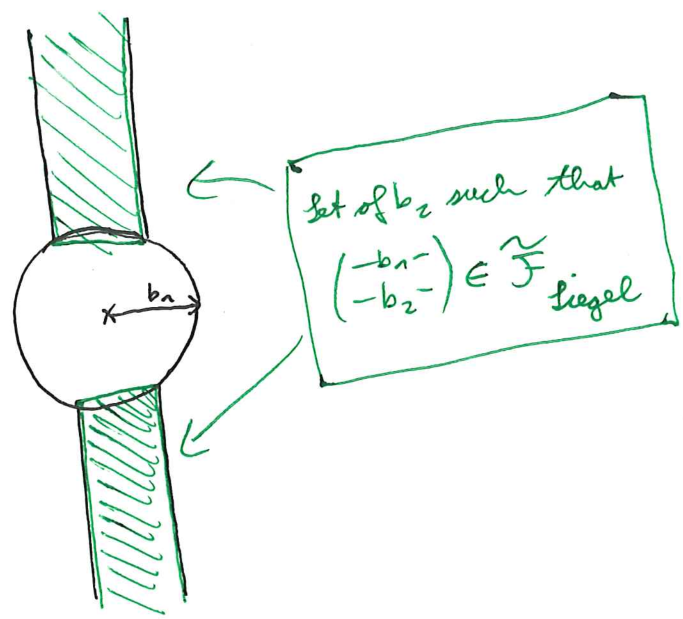
$$C \le \lambda_1 \le \dots \le \lambda_n \le C'.$$

SKIP

Rmk For $n = 2$, we have $\tilde{\mathcal{F}}_{Siegel} \supseteq \tilde{\mathcal{F}}_{Mink}$.

[This is a little false for $n = 3, 4$ and horribly false for $n \ge 5$.]

[The diagonal of a 5-dim. hypercube is more than twice as long as its sides.]



AS, 88

Idea of Pf

3) Each full lattice Λ has a basis $(b_1, \dots, b_n)$ with $g = \begin{pmatrix} - b_1 - \\ \vdots \\ - b_n - \end{pmatrix} \in \widetilde{\mathfrak{F}}_{\text{Siegel}}$

Consider a basis that lexicographically minimises $(a_1, \dots, a_n)$.
[Explain why there is a minimum!]
Applying an element of $N \cap M_n(\mathbb{Z})$, we can make

$|n_{ij}| \leq \frac{1}{2}$, so $n \in N$! If $a \notin A$, say $a_{i+1} < \frac{\sqrt{3}}{2} a_i$,

do this part last

exchange b_i and b_{i+1}:

$\tilde{b}_j = b_j$ for $j \neq i, i+1$

$\tilde{b}_i = b_{i+1}$

$\tilde{b}_{i+1} = b_i$

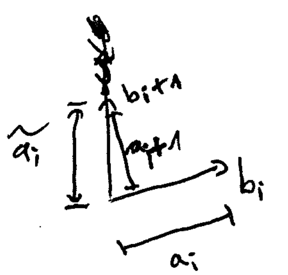
[After projecting onto the orth. complement of the subspace spanned by $b_1, \dots, b_{i-1}$, we're left with the 2-dimensional case!]

The corr. Iwasawa decomp. has

$$\tilde{a}_j = a_j \text{ for } j \neq i, i+1$$

$$\tilde{a}_i = \sqrt{a_{i+1}^2 + (n_{i+1,i}\, a_i)^2} < \sqrt{\tfrac{3}{4} a_i^2 + \tfrac{1}{4} a_i^2} = a_i.$$

$\Rightarrow$ not lexicographically minimal!



1) We have $|b_i| \asymp a_i \asymp \lambda_i$

Clearly, $a_1 \ll \dots \ll a_n \Rightarrow |b_i| = \sqrt{a_i^2 + \sum_{j=1}^{i-1} (n_{ij} a_j)^2} \ll a_i$ for all i

$\Rightarrow \lambda_i \ll a_i$

But by Minkowski's second theorem,

$$\lambda_1 \cdots \lambda_n \asymp \det(g) = \det(n\, a\, k) = \det(a) = a_1 \cdots a_n.$$

$\Rightarrow$ The asymp. ineq. $\ll$ must be asymp. eq. $\asymp$.

2) Each full lattice has only fin. many bases $(b_1, \dots, b_n)$ with $\begin{pmatrix} -b_1- \\ \vdots \\ -b_n- \end{pmatrix} \in \widehat{\mathfrak{S}}_{\text{Siegel}}$ (AS, 83)

There are only fin. many bases with $|b_i| \asymp \lambda_i$.

$\square$

Haar measures

AS, 90

Let G be a locally compact Hausdorff topological group.

mult $\cdot : G\times G \to G$ and inv. $\cdot^{-1}: G \to G$ are continuous

Thm G has a left Haar measure, and a right Haar measure, unique up to mult. by a positive constant.

Def G is unimodular if a left Haar measure is also a right Haar measure.

Rmk Any commutative group is unimodular. We'll now fix normalizations of Haar measures of some groups.

Thm + Def $(\mathbb{R}^n, +)$ is unimod, with the Lebesgue Haar measure $dx = d^+x$

Thm + Def $\mathbb{R}^\times$ is unimod., with Haar measure $d^\times x = \frac{d^+x}{|x|}$

Pf $d^+(\lambda x) = |\lambda| d^+x$, so $d^\times(\lambda x) = \frac{|\lambda| d^+x}{|\lambda x|} = \frac{d^+x}{|x|} = d^\times x$ for any $\lambda \in \mathbb{R}^\times$.

Lemma If G is a d-dim. Lie group and ω is a (left) G-inv. d-form, then $|\omega|$ is a (left) Haar measure on G.

Lemma If G is an open subset of $\mathbb{R}^n$, then $d^\times g = \frac{d^+g}{|\varphi(g)|}$ is a left Haar measure, where $\varphi(g)$ is the Jacobian determinant of the left mult. by g map $G \to G$ at the identity.

Just explain the technique of "fixing" a measure to become a Haar measure.

Ex

Thm + Def $GL_n(\mathbb{R}) \subset M_{n\times n}(\mathbb{R}) = \mathbb{R}^{n^2}$ is unimodular, with Haar measure

$$d^\times g = \frac{d^+g}{|\det(g)|^n}.$$

AS, 91

~~Haar measure on $N \cdot A \subset GL_n(\mathbb{R})$~~

Haar measure on $GL_n(\mathbb{R})$

Thm + Def $\quad d^\times n \overset{=dn=}{} \prod_{i>j} dn_{ij}$ is a Haar measure on N.

$$N = \left\{ \begin{pmatrix} 1 & & \\ n_{ij} & 1 & \\ \vdots & \ddots & 1 \end{pmatrix} \right\}$$

Thm + Def Consider the set $N \cdot A = \left\{ \begin{pmatrix} >0 & & 0 \\ & \ddots & \\ * & & >0 \end{pmatrix} \right\}$. The following is (the pull-back of) a left Haar measure on $N \cdot A$ (along the diffeom. $N \times A \to N \cdot A$):

$$\prod_{i>j} \frac{a_j}{a_i} dn_{ij} \prod_i d^\times a_i = \prod_i a_i^{n+1-2i} \, d^\times n \, d^\times a$$

Rmk The following is a right Haar measure: $d^\times n \, d^\times a$

Pf of Thm It is clearly left N-invariant because $d^\times n$ is.

For left A-invariance, let $t = \begin{pmatrix} t_1 & & \\ & \ddots & \\ & & t_n \end{pmatrix} \in A$. Left mult. by $t \in A$ is given by

$$\begin{array}{ccc} G & \xrightarrow{t} & G \\ \uparrow & & \uparrow \\ N \times A & \longrightarrow & N \times A \\ (n, a) & \longmapsto & (n', a') \end{array}, \quad \text{where } a' = ta$$

and $n'_{ij} = \frac{t_i}{t_j} n_{ij}$ for $i > j$ (so $t n a = n' a'$).

$$\left[\Rightarrow \prod_{i>j} \frac{a_j}{a_i} dn_{ij} \prod_i d^\times a_i = \prod_{i>j} \frac{t_j a_j}{t_i a_i} d\left(\frac{t_i}{t_j} n_{ij}\right) \prod_i d^\times (t a_i) = \prod_{i>j} \frac{a'_j}{a'_i} dn'_{ij} \prod_i d^\times a'_i \right].$$

$\square$

(AS, 92)

Def Let V_d $\left[= \dfrac{2\pi^{\frac{d}{2}}}{\Gamma(\frac{d}{2})}\right]$ be the volume of the $(d-1)$-dimensional unit sphere S^{d-1}. Normalize the Haar measure $d^\times k$ on the <u>compact</u> group $K = O_n(\mathbb{R})$ so that $\mathrm{vol}^\times(K) = \int_K d^\times k = V_1 \cdots V_n$.

Rmk $O_1(\mathbb{R}) = \{\pm 1\}$ has volume $V_1 = 2$. (The 0-sphere S^0 consists of two points.)

$O_2(\mathbb{R})$ is a double cover of $SO_2(\mathbb{R}) = \{\text{rot. by } 0 \leq \alpha < 2\pi\}$ and has volume $V_1 V_2 = 2 \cdot 2\pi$. (The 1-sphere has circumference 2π.)

Rmk embed $O_{n-1}(\mathbb{R})$ into $O_n(\mathbb{R})$ by fixing the n-th standard basis vector e_n. We get a bijection

$$O_n(\mathbb{R})/O_{n-1}(\mathbb{R}) \longleftrightarrow S^{n-1} \subset \mathbb{R}^n.$$

$$[M] \longmapsto M e_n \in \mathbb{R}^n$$

(AS,93)

<u>Thm</u> The pull-back of the Haar measure $d^\times g$ on $GL_n(\mathbb{R})$ along $N \times A \times K \to GL_n(\mathbb{R})$ [with the normalisations chosen above] is

$$\prod_i a_i^{n+1-2i} \, d^\times n \, d^\times a \, d^\times k .$$

Neglecting normalisations, this follows from:

<u>Lemma</u> Let G be unimodular and let $A, B \subset G$ be closed subgroups such that

$$\begin{aligned} A \times B &\to G \\ (a,b) &\mapsto ab \end{aligned}$$ is a diffeomorphism.

Let dg be a Haar measure on G, $d_l a$ be a left Haar measure on A, and $d_r b$ be a right Haar measure on B. Then, (the pullback of) dg is a constant multiple of $d_l a \, d_r b$.

<u>Pf</u> The pullback along $$\begin{aligned} A \times B &\to G \\ (a,b) &\mapsto ab^{-1} \end{aligned}$$ is by definition left $A \times B$-invariant, so it's a left Haar measure on $A \times B$, so proportional to $d_l a \, d_l b$, where $d_l b$ is the left Haar measure on B defined by $\int_B f(b) d_l b = \int_B f(b^{-1}) d_r b$.

$\square$

Haar measure on $SL_n(\mathbb{R})$

The map
$$\begin{aligned} \mathbb{R}^{>0} \times SL_n(\mathbb{R}) &\longrightarrow GL_n^+(\mathbb{R}) := \{ g \in GL_n(\mathbb{R}) \mid \det(g) > 0 \} \\ (\lambda, h) &\longmapsto \lambda h \end{aligned}$$
is a diffeomorphism and a group isomorphism.

$\Rightarrow$ $SL_n(\mathbb{R})$ is unimodular and if $d^\times h$ is a Haar measure on $SL_n(\mathbb{R})$, then (the pushforward of) $d^\times \lambda \, d^\times h$ is a Haar measure on $GL_n^+(\mathbb{R})$.

<u>Def</u> We normalise the Haar measure $dh^\times$ on $SL_n(\mathbb{R})$ so that $d_g^\times = n \, d^\times \lambda \, d^\times h$ is the Haar measure on $GL_n(\mathbb{R})$ defined earlier.

<u>Lemma</u> The pullback of $d_g^\times$ along the diffeomorphism
$$\begin{aligned} SL_n(\mathbb{R}) \times \mathbb{R}^\times &\longrightarrow GL_n(\mathbb{R}) \\ (h, \; t) &\longmapsto h \cdot \begin{pmatrix} 1 & & \\ & \ddots & \\ & & t \end{pmatrix} \end{aligned}$$
is the measure $d^\times h \, d^\times t$ (normalised as above).

Pf The pullback is a Haar measure on $SL_n(\mathbb{R}) \times \mathbb{R}^\times$. To show that the normalisation is correct, compute the Jacobian at the identity of the composition
$$SL_n(\mathbb{R}) \times \mathbb{R}^{>0} \longrightarrow GL_n^+(\mathbb{R}) \longrightarrow \mathbb{R}^{>0} \times SL_n(\mathbb{R}).$$

$\square$

AS, 95

Thm Identify $A_1 = \left\{ a \;\middle|\; a = \begin{pmatrix} a_1 & & \\ & \ddots & \\ & & a_n \end{pmatrix},\ a_1, \dots, a_n > 0,\ \det(a) = 1 \right\}$

with $B = (\mathbb{R}^{>0})^{n-1}$ by

$$A_1 \longleftrightarrow B$$

$$(a_i)_i \longleftrightarrow (b_i)_i \text{ with } b_i^n = \frac{a_{i+1}}{a_i}$$

$$\text{and } a_i = \frac{(b_1 \cdots b_{i-1})^n}{b_1^{n-1} b_2^{n-2} \cdots b_{n-1}}.$$

The Haar measure $d^\times h$ on $SL_n(\mathbb{R})$ pulls back, along $N \times A_1 \times K_1 \to SL_n(\mathbb{R})$, $N \times B \times K_1$, to the measure

$$n^{n} \cdot \prod_{i \le j < k} \hat{b}_j^{n} \cdot d^\times n\, d^\times b\, d^\times k = n^{n} \prod_j b_j^{-nj(n-j)}\, d^\times n\, d^\times b\, d^\times k.$$

Volume of $SL_n(\mathbb{Z})\backslash SL_n(\mathbb{R})$

(AS, 96)

Thm Let $\mathcal{F}$ be a (measurable) fund. domain for $SL_n(\mathbb{Z})\backslash SL_n(\mathbb{R})$. Then,

$$\mathrm{vol}^\times(\mathcal{F}) \left[= \int_{\mathcal{F}} d^\times h = \int_{SL_n(\mathbb{R})} \chi_{\mathcal{F}}(h)\, d^\times h\right] = \zeta(2)\cdots\zeta(n),$$

where $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$ is the Riemann zeta function. [Surprise!!]

for $\zeta(2) = \frac{\pi^2}{6}$.

Rmk All measurable fund. dom. have the same volume because the action of $SL_n(\mathbb{Z})$ on $SL_n(\mathbb{R})$ is measure-preserving.

Rmk You can easily show that $0 < \mathrm{vol}^\times(\mathcal{F}_{Siegel} \cap SL_n(\mathbb{R})) < \infty$, which implies that $0 < \mathrm{vol}^\times(\mathcal{F}) < \infty$.

Rmk $\mathcal{F}_{Siegel}$ is a fund. dom. for $GL_n(\mathbb{Z})\backslash GL_n(\mathbb{R})$. $id, \begin{pmatrix} -1 & & \\ & \ddots & \\ & & 1 \end{pmatrix}$ are rep. of cosets of $SL_n(\mathbb{Z})\backslash GL_n(\mathbb{Z})$.

$\Rightarrow \mathcal{F}_{Siegel} \sqcup \begin{pmatrix} -1 & & \\ & \ddots & \\ & & 1 \end{pmatrix} \mathcal{F}_{Siegel} = \mathcal{F}_{Siegel}^{\sqcup 2}$ is a fund. dom. for $SL_n(\mathbb{Z})\backslash GL_n(\mathbb{R})$.

$\Rightarrow \mathcal{F} = \mathcal{F}_{Siegel}^{\sqcup 2} \cap SL_n(\mathbb{R})$ is a fund. dom. for $SL_n(\mathbb{Z})\backslash SL_n(\mathbb{R})$.

Pf with a gap

Note that $\mathbb{R}^{>0} \cdot \mathcal{F} \subset GL_n^+(\mathbb{R})$ is a fund. dom. for $SL_n(\mathbb{Z})\backslash GL_n^+(\mathbb{R})$.

For any $T > 0$, let $GL_n^T(\mathbb{R}) := \{g \in GL_n(\mathbb{R}) \mid 0 < \det(g) \le T\}$, and $M_n^T(\mathbb{Z}) := \{g \in M_n(\mathbb{Z}) \mid 0 < \det(g) \le T\}$.

$$\Rightarrow \mathcal{F}_T := (\mathbb{R}^{>0} \cdot \mathcal{F}) \cap GL_n^T(\mathbb{R}) = (0, T^{\frac{1}{n}}] \cdot \mathcal{F}$$

is a fund. dom. for $SL_n(\mathbb{Z})\backslash GL_n^T(\mathbb{R})$.

(with $\mathcal{F}_T = T^{\frac{1}{n}} \cdot \mathcal{F}_1$).

A 5,97

Now, count integral orbits / points in $\mathcal{F}_T$:

$$\#\left(SL_n(\mathbb{Z})\backslash M_n^T(\mathbb{Z})\right)$$

$$= \#\left(\mathcal{F}_T \cap M_n(\mathbb{Z})\right)$$

Lebesgue measure on $M_n(\mathbb{R})$

$$\sim \mathrm{vol}^+(\mathcal{F}_T) \qquad (\text{for } T \to \infty)$$

Gap (to be proven later)

$$= \mathrm{vol}^+(T^{\frac{1}{n}}\mathcal{F}_1)$$

$$= T^n \cdot \mathrm{vol}^+(\mathcal{F}_1)$$

$M_n(\mathbb{R})$ is n^2-dimensional

$$= T^n \cdot \int_{\mathcal{F}_1} d^+g = T^n \cdot \int_{\mathcal{F}_1} |\det(g)|^n \, d^\times g$$

$$= T^n \cdot \int_0^1 \int_{\mathcal{F}\subset SL_n(\mathbb{R})} \underbrace{|\det(\lambda h)|^n}_{\lambda^{n^2}} \, n \, d^\times h \, d^\times \lambda$$

$\mathcal{F}_1 = (0,1]\cdot \mathcal{F}$, $d^\times g = n\, d^\times\lambda\, d^\times h$

end of lecture 12

$$= T^n \cdot n \cdot \underbrace{\int_0^1 \lambda^{n^2} d^\times \lambda}_{1/n^2} \cdot \int_{\mathcal{F}} d^\times h = T^n \cdot \frac{1}{n} \cdot \mathrm{vol}^\times(\mathcal{F}).$$

Reminder: $M_n^T(\mathbb{Z}) = \{ g \in M_n^T(\mathbb{Z}) \mid 0 < \det(g) \le T \}$ (AS 98)

$\Rightarrow$ It remains to prove:

Lemma $\#\left(SL_n(\mathbb{Z})\backslash M_n^T(\mathbb{Z})\right) \sim \frac{1}{n}\zeta(2)\cdots\zeta(n)\cdot T^n$ for $T\to\infty$.

There's a better fund. dom. for [the action on integral matrices] $SL_n(\mathbb{Z})\backslash M_n^+(\mathbb{Z})$:

Any $SL_n(\mathbb{Z})$-orbit contains exactly one matrix $g\in M_n^+(\mathbb{Z})$ of the form
$$g = \begin{pmatrix} a_1 & b_{12} & \cdots & b_{1n} \\ & a_2 & \ddots & b_{2n} \\ & & \ddots & \vdots \\ 0 & & & a_n \end{pmatrix} \quad \text{with } a_1,\dots,a_n \ge 1$$
and $0 \le b_{ij} < a_j$ for all $i<j$. (Hermite normal form)

[Construct it column by column, from left to right. In the i-th column, first use the Euclidean algorithm to make rows $i,\dots,n$ look right. (a_i is the gcd of the original entries in these $n-i+1$ places.) Then subtract/add row i from/to rows $1,\dots,i-1$ to make them correct.]

$$\Rightarrow \#\left(SL_n(\mathbb{Z})\backslash M_n^T(\mathbb{Z})\right) = \sum_{\substack{a_1,\dots,a_n\ge 1\\ a_1\cdots a_n \le T}} \underbrace{a_2^1 a_3^2 \cdots a_n^{n-1}}_{\text{number of possible values of } b_{ij}}$$

The Dirichlet series of $c_k := \sum_{a_1\cdots a_n = k} a_1^0 a_2^1 \cdots a_n^{n-1}$ is $\zeta(s)\zeta(s-1)\cdots\zeta(s-n+1)$.
Its rightmost pole is at $s=n$, of order 1, with residue $\zeta(n)\cdots\zeta(2)$.

$$\Rightarrow \sum_{k\le T} c_k \sim \frac{1}{n}\zeta(2)\cdots\zeta(n)\cdot T^n \quad \text{for } T\to\infty.$$

Wiener-Ikehara HW?

$\square$

[We still need to show that the number of int. matrices in a (measurable) fund. dom. $\mathcal{F}$ is asymptotic to vol($\mathcal{F}$). Problem: counting int. pts. in measurable sets can go horribly wrong!]

(AS, 99)

Convolution

[Don't panic. Convolve!]

Def Let G be a unimodular group with Haar measure dg. The convolution of two measurable sets A, B on G is the set $A * B$ with char. fct.

$$\chi_{A*B}(g) = \int_G \chi_A(s)\chi_B(s^{-1}g)\,ds \quad \left[= \int_A \chi_{sB}(g)\,ds\right]$$

$$= \int_G \chi_A(gt^{-1})\chi_B(t)\,dt \quad \left[= \int_B \chi_{At}(g)\,dt\right]$$

$t = s^{-1}g$

Haar measure is inv. under right mult. by g and under inversion by unimodularity

Shorthand: $\chi_{A*B} = \int_A \{sB\}\,ds = \int_B \{At\}\,dt$.

Rmk ~~$A*B$ is well-defined if and only if~~

$A * B$ well-defined

$\Leftrightarrow \int_G \chi_A(s)\chi_B(s^{-1}g)\,ds < \infty$ for all $g \in G$

$\Leftrightarrow \int_G \chi_A(gt^{-1})\chi_B(t)\,dt < \infty$ for all $g \in G$

~~Exe If χ_A is bounded (e.g. A is a set) and vol(B) < ∞, then $A*B$ is well-defined.~~

~~Rmk Since $\chi_B(s^{-1}g) = \chi_{sB}(g)$ and $\chi_A(gt^{-1}) = \chi_{At}(g)$, it's reasonable to write $A*B = \int_A (sB)\,ds = \int_B (At)\,dt$.~~

Exe If the char. fct. χ_A is bounded (e.g. if A is a set) and vol(B) < ∞, then $A * B$ is well-defined.

AS,100

Rmk $A * B$ is measurable and

$$\mathrm{vol}(A * B) = \mathrm{vol}(A) \cdot \mathrm{vol}(B)$$

Pf $\int_G \chi_{A*B}(g)\,dg = \int_G \int_G \chi_A(s)\chi_B(s^{-1}g)\,ds\,dg = \int_G \chi_A(s) \underbrace{\int_G \chi_B(s^{-1}g)\,dg}_{\mathrm{vol}(B)}\,ds = \mathrm{vol}(A)\cdot \mathrm{vol}(B).$ $\square$

Rmk $B * A = (A^{-1} * B^{-1})^{-1}$

Rmk If G is commutative, then $B * A = A * B$.

Rmk $A * (B * C) = (A * B) * C$

Idea

a) horrible $*$ nice $=$ nice, where "nice" means e.g. "smooth" or "easy to count lattice points in"

"Convolving with an interval fills in small holes."

[See problem 2 on PSet 3 and problem 1 on PSet 4.]

"It also thickens cusps, making them easier to understand."

b) (fund. dom.) $*$ (set of volume 1) $=$ (fund. dom.)

[The combination of these two facts is very powerful!]

Thm Let A, B be so that $A * B$ is well-defined and let C be another set on G. Then,

$$\#((A*B)\cap C) = \int_A \underbrace{\#((sB)\cap C)}_{\text{Independent of } A!}\,ds.$$

Pf $\chi_{(A*B)\cap C}(g) = \chi_{A*B}(g)\cdot\chi_C(g) = \int_A \chi_{sB}(g)\chi_C(g)\,ds$

$$= \int_A \chi_{(sB)\cap C}(g)\,ds$$

$\square$

(AS, 101)

Thm Let H be a subgroup of the unimodular group G. Let $\mathcal{F}$ be a fund. dom. for $H\backslash G$ and let A be a set on G of volume 1. Then, $\mathcal{F} * A$ is a well-defined fund. dom. for $H\backslash G$.

Rmk If $0 < vol(A) < \infty$, use $A' = A^{\sqcup \frac{1}{vol(A)}}$. $\rightsquigarrow \mathcal{F} * A' = (\mathcal{F} * A)^{\sqcup \frac{1}{vol(A)}}$.

~~Pf~~ ~~$\mathcal{F}$ fund. dom. $\Leftrightarrow \sum_{h\in H} h\mathcal{F} = G$~~

~~well-def.: $\chi_{\mathcal{F}}(g) \leq 1 \, \forall g \in G \Rightarrow \chi_{\mathcal{F}}$ bounded $+ vol(A) < \infty \Rightarrow$ well-def. [and $vol(\mathcal{F} * A) = vol(\mathcal{F})$]~~

$$\Downarrow \qquad \Downarrow$$

~~$\mathcal{F}t$ fund. dom. $\forall t \in G \Leftrightarrow \sum_{h\in H} h\mathcal{F}t = G$~~

$$\Downarrow \qquad \Downarrow$$

~~"average" $\mathcal{F} * A = \int_A (\mathcal{F}t)\,dt$ fund. dom. $\Leftrightarrow \sum_{h\in H} \int_A (h\mathcal{F}t)\,dt$~~

$$\int_A \underbrace{\Big(\sum_{h\in H} h\mathcal{F}t\Big)}_{G} dt = G$$

vol(A) = 1 □

Pf Well-definedness:

$\mathcal{F}$ fund. dom. $\Rightarrow \chi_{\mathcal{F}}(g) \leq 1 \ \forall g$ and $vol(A) < \infty$.

Fund. dom.:

Idea: $\mathcal{F}t$ is a fund. dom. for any $t \in G$.

$\Rightarrow$ The "average" $\mathcal{F} * A = \int_A \mathcal{F}t\,dt$ is a fund. dom.

Formally: Let $g \in G$. $\Rightarrow \sum_{h\in H} \chi_{\mathcal{F}*A}(hg) = \sum_{h\in H} \int_G \chi_{\mathcal{F}}(hgt^{-1})\chi_A(t)\,dt$

$$= \int_G \sum_{h\in H} \chi_{\mathcal{F}}(hgt^{-1})\chi_A(t)\,dt = \int_G \chi_A(t)\,dt = vol(A) = 1. \qquad \square$$

Before continuing with the computation of vol(fund. dom. of $SL_n(\mathbb{Z})\backslash SL_n(\mathbb{R})$) AS, 102

Lemma Fix some $n \geq 1$. Let $Q \subset SL_n(\mathbb{R})$ be a compact and let $C > 0$ be a constant. For any $q \in Q$ and $a \in A$ with ($a_i > 0$ and) $a = \begin{pmatrix} a_1 & & \\ & \ddots & \\ & & a_n \end{pmatrix}$, $a_{i+1} \geq C a_i$ for $i = 1, \dots, n-1$, $[a_1 \ll_C \dots \ll_C a_n]$ consider the full lattice $\Lambda = (qa)^{-1}\mathbb{Z}^n = a^{-1}q^{-1}\mathbb{Z}^n$. Its Euclidean succ. min. $\lambda_1 \leq \dots \leq \lambda_n$ satisfy $\lambda_i \asymp_{Q,C} a_{n+1-i}^{-1}$ for $i = 1, \dots, n$.

indep. of q, a

$$(\lambda_1 \asymp a_n^{-1}, \dots, \lambda_n \asymp a_1^{-1}).$$

Pf By Minkowski's second thm,

$$\lambda_1 \cdots \lambda_n \asymp_n \operatorname{covol}(\Lambda) = |\det(a^{-1}q^{-1})| = a_1^{-1} \cdots a_n^{-1}.$$

$\Rightarrow$ It suffices to show $\lambda_i \ll a_{n+1-i}^{-1}$. Since $Q \subset SL_n(\mathbb{R})$ is compact, the i-th row vector of q^{-1} has length $O_Q(1)$. $\Rightarrow$ The i-th row vector of $a^{-1}q^{-1}$ has length $O_Q(a_i^{-1})$. $\Rightarrow$ After reordering, the result then follows from $a_n^{-1} \ll_C \dots \ll_C a_1^{-1}$.

The n row vectors are of course linearly independent.

□

To complete the computation of the volume of a fund. dom. of $SL_n(\mathbb{Z})\backslash SL_n(\mathbb{R})$, it remains to prove the following thm:

Thm Let $\mathcal{F}$ be a measurable fund. dom. for $SL_n(\mathbb{Z})\backslash SL_n(\mathbb{R})$. For $T>0$, let $\mathcal{F}_T = (0, T^{\frac{1}{n}}]\cdot\mathcal{F} \subset GL_n^+(\mathbb{R})$. Then,

$$\#(\mathcal{F}_T \cap M_n(\mathbb{Z})) \sim \mathrm{vol}^+(\mathcal{F}_T) \quad \text{for } T \to \infty.$$

Lebesgue!

Pf

Thm Let $\mathcal{F}$ be a measurable fund. dom. for $SL_n(\mathbb{Z})\backslash GL_n^+(\mathbb{R})$. det>0

For $T>0$, consider the fund. dom. $\mathcal{F}_T = \mathcal{F} \cap GL_n^T(\mathbb{R})$ of $SL_n(\mathbb{Z})\backslash GL_n^T(\mathbb{R})$. $0<\det\leq T$ Then,

$$\#(\mathcal{F}_T \cap M_n(\mathbb{Z})) \sim \mathrm{vol}^+(\mathcal{F}_T) \quad \text{for } T \to \infty.$$

Lebesgue

Pf Both sides are independent of the choice of the fund. dom. $\mathcal{F}_T$. $\Rightarrow$ We may w.l.o.g. assume that the support of $\mathcal{F}_T$ is contained in $\tilde{\mathcal{F}}_{\text{Siegel}} \subset GL_n(\mathbb{R})$.

Let S

(AS, 104)

<u>Thm</u> Let $\mathcal{F}$ be a measurable fund. dom. for $SL_n(\mathbb{Z})\backslash SL_n(\mathbb{R})$.

For $T>0$, consider the fund. dom. $\mathcal{F}_T = (0,T]\cdot\mathcal{F}$
for $SL_n(\mathbb{Z})\backslash GL_n^{T^n}(\mathbb{R})$. $\leftarrow$ ($0 < \det \le T^n$)

Then,

Lebesgue!

$$\#(\mathcal{F}_T \cap M_n(\mathbb{Z})) \sim \mathrm{vol}^+(\mathcal{F}_T) \quad \text{for } T\to\infty.$$

<u>Pf</u> Both sides are indep. of the choice of fund. dom. $\mathcal{F}_T$. (The action of $SL_n(\mathbb{R})$ preserves the Lebesgue measure.)
Assume w.l.o.g. that $\mathrm{supp}(\mathcal{F}) \subset \widetilde{\mathcal{F}}_{\text{Siegel}}^{\wedge SL_n(\mathbb{R})} = N' A_1' K_1$.

[Now, use convolution to make $\mathcal{F}$ nicer!]

Fix any subset $S \subset SL_n(\mathbb{R})$ of volume 1 whose boundary is Lipschitz.

$\Rightarrow$ $\mathcal{F} * S$ is also a fund. dom. for $SL_n(\mathbb{Z})\backslash SL_n(\mathbb{R})$,

$(\mathcal{F}*S)_T = (0,T]\cdot(\mathcal{F}*S)$ is also a fund. dom. for $SL_n(\mathbb{Z})\backslash GL_n^{T^n}(\mathbb{R})$,

with $\mathrm{vol}^+((\mathcal{F}*S)_T) = \mathrm{vol}^+(\mathcal{F}_T)$.

$\Rightarrow$ It suffices to prove

$$\#((\mathcal{F}*S)_T \cap M_n(\mathbb{Z})) \sim \mathrm{vol}^+(\mathcal{F}_T) \quad \text{for } T\to\infty.$$

But $$\mathrm{LHS} = \int_{\mathcal{F}} \underbrace{\#(((0,T]\cdot g S) \cap M_n(\mathbb{Z}))}_{f(g)}\, dg = \int_{\mathcal{F}} f(g)\, dg.$$

Now, we want to apply Widmer's Thm. to the integrand.
Write $g = n a k$ with $n \in N'$, $a = \begin{pmatrix} a_1 & & \\ & \ddots & \\ & & a_n \end{pmatrix} \in A_1'$,

$k \in K_1 = SO_n(\mathbb{R})$. The set gS could be narrow and long if a_1 is small and a_n is large!

$\leadsto$ It'll be better to rescale the lattice $M_n(\mathbb{Z})$ than the set S.

$$f(g) = \#((0,T]\cdot \underset{nak}{g} S \cap M_n(\mathbb{Z})) = \#((0,T]\cdot k S \cap (na)^{-1} M_n(\mathbb{Z}))$$

End of lecture 13

(AS, 105)

Since K_1 is compact, $\partial(k\cdot S)$ is $(O_s(1), O_s(1))$-Lipschitz.

$\Rightarrow \partial((0,T]\cdot k S)$ is $(O_s(1), O_s(T))$-Lipschitz.

Also, $kS \subset M_n(\mathbb{R})$ is contained in a ball of radius $O_s(1)$,
so $(0,T]\cdot kS$ is contained in a ball of radius $O_s(T)$.

Since $N' \subset SL_n(\mathbb{R})$ is compact and any $a \in A'$ satisfies $a_1 \ll \dots \ll a_n$, the previous lemma shows that the succ. min. $\lambda_1 \leq \dots \leq \lambda_n$ of $\Lambda = (n\,a)^{-1}\mathbb{Z}^n$ satisfy $\lambda_i \asymp a_{n+1-i}^{-1}$.

Note that $(n\,a)^{-1} M_n(\mathbb{Z}) \cong \Lambda^n$ consists of the matrices whose columns lie in Λ.

Λ^n has the same succ. min. as Λ, with each λ_i occuring n times. [could apply Widmer for $f(g)$, but the integral of the error term would be ∞!]

If $f(g) = \#(\underbrace{(0,T]\cdot kS}_{\subset GL_n(\mathbb{R})} \cap (n\,a)^{-1} M_n(\mathbb{Z})) \neq 0$, there must be n linearly independent vectors in Λ of length $O_s(T)$.

$\Rightarrow T \gg_s \lambda_n \asymp a_1^{-1} \gg \dots \gg a_n^{-1}$.

$\rightsquigarrow$ Cut off cusp: Let $\mathcal{F}^{(T)} = \mathcal{F} \cap \{ g = n\,a\,k \mid a_1^{-1} \ll_s T \}$.

$\Rightarrow$ LHS $= \int_{\mathcal{F}^{(T)}} f(g)\,dg$.

$\mathcal{F}^{(T)} \to \mathcal{F}$ (monotonically) for $T \to \infty$

RHS $= \mathrm{vol}^+(\mathcal{F}_T) = \mathrm{vol}^+((0,T]\cdot\mathcal{F}) \sim \mathrm{vol}^+((0,T]\cdot\mathcal{F}^{(T)})$

AS, 106

Let $g = nak \in \mathrm{supp}(\mathcal{F}^{(T)})$. By Widmer's theorem,

$$f(g) = \frac{\mathrm{vol}^+((0,T]\cdot kS)}{\mathrm{covol}(\Lambda^n)} + \sum_{l=0}^{n^2-1} \mathcal{O}_S\left(\frac{T^l}{\text{prod. of } l \text{ smallest succ. min. of } \Lambda^n}\right)$$

$xa_1^{-1}, \dots, xa_n^{-1}$, each n times

$g, k \in SL_n(\mathbb{R})$ preserve Lebesgue measure

$T \gg a_1^{-1} \gg \dots \gg a_n^{-1}$ and $\prod a_i = 1$

$$= \frac{\mathrm{vol}^+((0,T]\cdot S)}{1} + \mathcal{O}_S\left(\frac{T^{n^2-1}\cdot a_1^{-1}}{1}\right)$$

$$\Rightarrow \int_{\mathcal{F}^{(T)}} f(g)\,dg = \int_{\mathcal{F}^{(T)}} \left(\mathrm{vol}^+((0,T]\cdot S) + \mathcal{O}_S\left(\frac{T^{n^2-1}}{a_1}\right)\right) dg$$

$$\text{main term} = \int_{\mathcal{F}^{(T)}} \mathrm{vol}^+((0,T]\cdot S)\,dg = \mathrm{vol}^\times(\mathcal{F}^{(T)})\cdot \mathrm{vol}^+((0,T]\cdot S)$$

$$= \frac{T^n}{n}\mathrm{vol}^\times(\mathcal{F}^{(T)})\cdot \mathrm{vol}^\times(S) = \mathrm{vol}^+((0,T]\cdot \mathcal{F}^{(T)})\cdot \underbrace{\mathrm{vol}^\times(S)}_{1} \times T^{n^2}$$

[We did this computation last time.] ✓

$$\frac{\text{error term}}{\text{main term}} \ll \int_{\mathcal{F}^{(T)}} \frac{1}{Ta_1}\,dg \ll \int_{\mathrm{supp}(\mathcal{F}^{(T)})} \frac{1}{Ta_1}\,dg$$

$$\leq \int_{N'A'_1K_1} \frac{1}{Ta_1}\,dg = \int_{N'}\int_{A'_1}\int_{K_1} \frac{1}{Ta_1}\,dk\,da\,dn$$

AS, 107

$$\int_{N'} \int_{\left[\frac{\sqrt{3}}{2},\infty\right]^{n-1} \subset \underset{\substack{\| \\ (\mathbb{R}^{>0})^{n-1}}}{B}} \int_{K_1} \frac{b_1^{n-1}\cdots b_{n-1}}{T} \, \frac{d^\times k \, d^\times b \, d^\times n}{\prod_{i=1}^{n-1} b_i^{ni(n-i)}} \ll \frac{1}{T} \xrightarrow{T\to\infty} 0 \checkmark$$

Formula for Haar measure on $SL_n(\mathbb{R})$,

$$\frac{a_{i+1}}{a_i} = b_i^n,$$

$$a_1 = \frac{1}{b_1^{n-1}\cdots b_1}$$

$\square$

AS, 108

p-adic Haar measure.

Let k be a non-arch. local field with ring of integers $\mathcal{O}_k$, prime $\mathfrak{p} = (\pi)$, valuation v, residue field $\kappa = k/\mathfrak{p}$ of order q, norm $|x| = q^{-v(x)}$ for $x \in k^\times$.

We normalize the Haar measure $dx = d^+x$ on k by $\mathrm{vol}^+(\mathcal{O}_k) = 1$ (compact).

$\rightsquigarrow$ The restriction to $\mathcal{O}_k$ is a probability measure.

Rmk For $\lambda \in k^\times$, we have $d(\lambda x) = |\lambda|\, dx$.

Pf $d(\lambda x)$ is also a Haar measure on k.

By uniqueness of Haar measures, it suffices to show that

$$\mathrm{vol}(\lambda \mathcal{O}_k) = |\lambda|\, \mathrm{vol}(\mathcal{O}_k).$$

Since $k^\times = \mathcal{O}_k^\times \times \pi^{\mathbb{Z}}$, it suffices to prove this for $\lambda \in \mathcal{O}_k^\times$ and $\lambda = \pi$.

For $\lambda \in \mathcal{O}_k^\times$, $\lambda\mathcal{O}_k = \mathcal{O}_k$ and $|\lambda| = 1$.

For $\lambda = \pi$, note that $\mathcal{O}_k$ is the disjoint union of q translates of $\mathfrak{p} = \pi\mathcal{O}_k$ (residue classes), so $\mathrm{vol}(\pi\mathcal{O}_k) = \frac{1}{q}$, and $|\pi| = q^{-1}$.

$\square$

$\rightsquigarrow$ We get a mult. Haar measure $d^\times x = \frac{dx}{|x|}$ on $k^\times$.

Rmk For $A \subseteq \mathcal{O}_k/\mathfrak{p}^e$, we have

$$\underbrace{\mathbb{P}\big((x \bmod \mathfrak{p}^e) \in A \mid x \in \mathcal{O}_k\big)}_{=\ \mathrm{vol}(\{x \in \mathcal{O}_k : (x \bmod \mathfrak{p}^e) \in A\})} = \mathbb{P}(x \in A \mid x \in \mathcal{O}_k) = \frac{\#A}{q^e}.$$

Rmk Let $S \subset \mathcal{O}_k$ be a set of representatives for the q residue classes.

We can write any $x \in \mathcal{O}_k$ uniquely as $x = \sum_{i=0}^{\infty} c_i \pi^i$ with $c_i \in S$. ("digits")

$\rightsquigarrow$ bijection $\mathcal{O}_k \longleftrightarrow \prod_{i=0}^{\infty} S$.

The Haar measure on $\mathcal{O}_k$ is (on Borel sets) the product measure, where we endow S with the uniform probability measure.

[Roll dice for each digit.]

Ese $\mathrm{vol}^+(\mathcal{O}_k^\times) = \mathrm{vol}^\times(\mathcal{O}_k^\times) = \mathrm{vol}^+(\mathcal{O}_k) - \mathrm{vol}^+(\mathfrak{p}) = 1 - q^{-1}$

$|x| = 1$ for $x \in \mathcal{O}_k^\times$

$= \mathbb{P}(x \neq 0 \mid x \in \kappa)$

Define Haar measures on $GL_n(k)$, $SL_n(k)$ as over $\mathbb{R}$.

Lemma $\mathrm{vol}^+(GL_n(\mathcal{O}_k)) = \mathrm{vol}^\times(GL_n(\mathcal{O}_k)) = \prod_{i=1}^{n} (1 - q^{-i})$

$|\det(g)| = 1$ for $g \in GL_n(\mathcal{O}_k)$

Pf LHS $= \mathbb{P}(g \in GL_n(\kappa) \mid g \in M_n(\kappa))$

$= \mathbb{P}(v_1, \dots, v_n \text{ lin. indep.} \mid v_1, \dots, v_n \in \kappa^n)$

look at col. of g

$= \mathbb{P}(v_1 \neq 0) \cdot \mathbb{P}(v_2 \notin \langle v_1 \rangle \mid v_1 \neq 0) \cdot \ldots \cdot \mathbb{P}(v_n \notin \langle v_1, \dots, v_{n-1} \rangle \mid v_1, \dots, v_{n-1} \text{ lin. indep.})$

$= (1 - q^{-n})(1 - q \cdot q^{-n}) \cdots (1 - q^{n-1} \cdot q^{-n})$

$= (1 - q^{-1})(1 - q^{-2}) \cdots (1 - q^{-n})$. $\square$

Lemma $\mathrm{vol}^+(SL_n(\mathcal{O}_k)) = \mathrm{vol}^\times(SL_n(\mathcal{O}_k)) = \prod_{i=2}^{n} (1 - q^{-i})$

Pf Under the homeomorphism $SL_n(\mathcal{O}_k) \times \mathcal{O}_k^\times \xrightarrow{\sim} GL_n(\mathcal{O}_k)$, $(h, t) \longmapsto h \begin{pmatrix} t & & 0 \\ & 1 & \\ 0 & & \ddots \\ & & & 1 \end{pmatrix}$, the Haar measure $d^\times g$ on $GL_n(\mathcal{O}_k)$ pulls back to $d^\times h \, d^\times t$.

$\Rightarrow \mathrm{vol}^\times(SL_n(\mathcal{O}_k)) \cdot \underbrace{\mathrm{vol}^\times(\mathcal{O}_k^\times)}_{1 - q^{-1}} = \underbrace{\mathrm{vol}^\times(GL_n(\mathcal{O}_k))}_{\prod_{i=1}^{n} (1 - q^{-i})}$. $\square$

Strong approximation + Tamagawa number / Let $\mathbb{A} = \mathbb{A}(\mathbb{Q}) = \prod_v{}' \mathbb{Q}_v = \mathbb{R} \times \prod_p{}' \mathbb{Q}_p$ be the ring of adeles and $\mathbb{A}_{fin} = \prod_p{}' \mathbb{Q}_p$. (AS, 110)

Thm (Strong approx. for $\mathbb{G}_a$ (over $\mathbb{Q}$, away from ∞))
The image of $\mathbb{Q}$ in $\mathbb{A}_{fin}$ is dense (in $\mathbb{A}_{fin}$).

Pf We need to show that every open set $U \subseteq \mathbb{A}_{fin}$ contains an element of $\mathbb{Q}$. It suffices to show this for basis open sets
$U = \prod_{p\in S} U_p \times \prod_{p\notin S} \mathbb{Z}_p$, where S is a finite set of primes and
$U_p \subseteq \mathbb{Q}_p$ is open. W.l.o.g. $U_p = y_p + p^{e_p}\mathbb{Z}_p$ with $y_p \in \mathbb{Q}_p$, $e_p \in \mathbb{Z}$.
Multiplying by large enough powers of $p \in S$, we can assume $y_p \in \mathbb{Z}_p$, $e_p \geq 0$.
By the CRT, there exists $x \in \mathbb{Z}$ s.t. $x \equiv y_p \mod p^{e_p}$ $\forall p$.
$\Rightarrow x \in U$. □

Cor For any $y = (y_p)_p \in \mathbb{A}_{fin}$, there is some $x \in \mathbb{Q}$ such that $x + y = (x + y_p)_p \in \prod_p \mathbb{Z}_p$.

Pf $U = \prod_p (\mathbb{Z}_p - y_p)$ is an open subset of $\mathbb{A}_{fin}$.
$\overset{SA}{\Rightarrow} \exists x \in \mathbb{Q}: x \in \mathbb{Z}_p - y_p \ \forall p$
$\Downarrow$
$x + y_p \in \mathbb{Z}_p$ □

Cor The set $[0,1) \times \prod_p \mathbb{Z}_p$ is a fund. dom. for $\mathbb{Q}\backslash\mathbb{A}$. Its volume (the Tamagawa number of $\mathbb{G}_a$ over $\mathbb{Q}$) is 1.

Pf By the prev. cor. every $\mathbb{Q}$-orbit contains some $y \in \mathbb{R} \times \prod_p \mathbb{Z}_p$.
$$\Rightarrow \sum_{x\in\mathbb{Q}} \chi_{[0,1)\times\prod_p\mathbb{Z}_p}(x+y) = \sum_{x\in\mathbb{Q}} \chi_{[0,1)}(x+y_\infty) \underbrace{\prod_p \underbrace{\chi_{\mathbb{Z}_p}(x+y)}_{=1 \Leftrightarrow x\in\mathbb{Z}_p}}_{=1 \Leftrightarrow x \in \mathbb{Z}} = \sum_{x\in\mathbb{Z}} \chi_{[0,1)}(x+y_\infty) = 1$$ □

$[0,1)$ is fund. dom. for $\mathbb{Z}\backslash\mathbb{R}$.

$\mathrm{vol}([0,1)) = 1$
$\mathrm{vol}(\mathbb{Z}_p) = 1$.

AS, 111

Thm (Strong approx. for SL_n)

The image of $SL_n(\mathbb{Q})$ in $SL_n(\mathbb{A}_{fin})$ is dense.

Pf By def. of the top. on $SL_n(\mathbb{A}_{fin})$, it suffices to prove that the closure of the image of $SL_n(\mathbb{Q})$ contains $SL_n(\mathbb{Q}_p)$ for every p. For $a \neq b$, consider the subgroup G_{ab} of SL_n consisting of matrices $(m_{ij})_{i,j}$ with $m_{ij} = 1$ for $i=j$, $m_{ij}=0$ for $i \neq j$ if $(i,j) \neq (a,b)$.

$$m = \begin{array}{cc} \begin{bmatrix} 1 & & 0 \\ & \ddots & \\ 0 & * & 1 \end{bmatrix} & \leftarrow a \\ \uparrow & \\ b & \end{array}$$

We have $G_{ab} \cong \mathbb{G}_a$ (i.e. $G_{ab}(R) = R$ for any ring R).

Now, $SL_n(\mathbb{Q}_p)$ is generated by the el. of the subgroups $G_{a,b}(\mathbb{Q}_p)$ for $a \neq b$. $\Rightarrow$ It suffices to prove that the closure of the image of $G_{a,b}(\mathbb{Q}) \subset SL_n(\mathbb{Q})$ contains $G_{a,b}(\mathbb{Q}_p) \subset SL_n(\mathbb{Q}_p)$. This follows from strong approx. for $\mathbb{G}_a$. $\square$

Cor Let F be a fund. dom. for $SL_n(\mathbb{Z}) \backslash SL_n(\mathbb{R})$. Then, $F \times \prod_p SL_n(\mathbb{Z}_p)$ is a fund. dom. for $SL_n(\mathbb{Q}) \backslash SL_n(\mathbb{A})$. Its volume (the Tamagawa number of SL_n over $\mathbb{Q}$) is 1.

Pf Fund. dom.: Follows from SA like for $\mathbb{G}_a$.

Volume: $\mathrm{vol}(F) = \zeta(2) \cdots \zeta(n)$

$\mathrm{vol}(SL_n(\mathbb{Z}_p)) = (1-p^{-2}) \cdots (1-p^{-n})$

$\prod \cdots = 1.$ $\square$

Weil's conjecture on Tamagawa numbers (known)

The Tamagawa number of a simply connected simple algebraic group over a number field is 1.

End of lecture 14

Field ext. of fixed degree

Two ways of counting degree n ext. of a fixed field K:

- count field ext. $L|K$ up to isom.
- count subfields $L \subseteq \overline{K}$

Lemma Any separable ext. $L|K$ of degree n is isomorphic to exactly $\frac{n}{\# \mathrm{Aut}(L)}$ subfields $L \subseteq K^{sep}$

aut. as K-algebra   separable closure

$$\text{“} \ \frac{1}{n} \sum_{L \subseteq K^{sep}} f(L) = \sum_{L/\cong} \frac{f(L)}{\# \mathrm{Aut}(L)} \ \text{”}$$

Pf There are n embeddings $L \hookrightarrow K^{sep}$. Two embeddings have the same image if and only if they differ by an automorphism of L.

$$\begin{tikzcd} L \arrow[r, hook] \arrow[d, "\wr"] & K^{sep} \\ L \arrow[ur, hook] & \end{tikzcd}$$

$\square$

Extensions of rings

<u>Def</u> Let R be a Dedekind dom. with field of fractions K.
An an R-<u>lattice</u> is a fin. gen. torsionfree R-module A. Its <u>rank</u> is the (finite!) dimension of the K-vector space $A \otimes_R K$.

<u>Rmk</u> $A \longrightarrow A \otimes_R K$ is injective for any R-lattice A.

<u>Rmk</u> Any free R-module is an R-lattice.

<u>Ex</u> If R is PID, any R-lattice is free.

<u>Def</u> Let R, K as above. A <u>degree n extension</u> of R is a (commutative, unitary) R-algebra S, which (as R-module) is an R-lattice of rank n.
Its <u>discriminant</u> is the ideal $\mathrm{disc}(S|R) \subseteq R$ gen. by the elements $\det((\mathrm{Tr}(w_i w_j))_{i,j}) \in R$ with $w_1, \dots, w_n \in S$.
It is <u>nondegenerate</u> if $\mathrm{disc}(S|R) \neq 0$.

<u>Ex</u> R is a deg. 1 ext. of R with disc $= (1)$.

Ex Let $L|K$ be a field ext. of deg. n. Then, $L|K$ is a deg. n ext. with

$$\operatorname{disc}(L|K) = \begin{cases} K = (1), & \text{if } L|K \text{ is separable} \\ (0), & \text{else.} \end{cases}$$

Ex If $f(X) \in R[X]$ is monic of degree n, then $S = R[X]/(f(X))$ is a deg. n ext. with $\operatorname{disc}(S|R) = (\operatorname{disc}(f))$.

Rmk (base change)

If S is a deg. n ext. of R and $R' \supseteq R$ is another Dedekind dom., then $S' = S \otimes_R R'$ is a deg. n ext. of R' with $\operatorname{disc}(S'|R') = \operatorname{disc}(S|R) \cdot R'$.

Rmk (cartesian product)

If $S_1, \dots, S_r$ are deg. $n_1, \dots, n_r$ ext. of R, then $S = S_1 \times \dots \times S_r$ is a deg. $n = n_1 + \dots + n_r$ ext. of R with $\operatorname{disc}(S|R) = \operatorname{disc}(S_1|R) \cdots \operatorname{disc}(S_r|R)$.

Ex $S = \underbrace{R \times \dots \times R}_{n}$ is a deg. n ext. of R with $\operatorname{disc}(S|R) = (1)$, called the trivial ext.

Thm The nondegenerate ext. of a field K (also called étale extensions) are exactly the K-algebras of the form $L = L_1 \times \dots \times L_r$ where $L_1, \dots, L_r$ are separable degree $n_1, \dots, n_r$ ext. of K.

Cor If K is separably closed, there is only the trivial nondeg. ext.

Cor For any nondeg. deg. n ext. $L|K$, there are exactly n ring hom. $L \longrightarrow K^{sep}$.

Pf There are n_i embeddings $L_i \hookrightarrow K^{sep}$.
Compose with proj. $L \twoheadrightarrow L_i$.
$\rightsquigarrow$ Total of n ring hom. $L \longrightarrow K^{sep}$.
All hom. are of this form. $\square$

<u>Lemma</u> Let L, K as above and assume that K is the field of fractions of a Dedekind dom. $\mathcal{O}_K$. Then, the ring of int. $\mathcal{O}_L$ $(=$(int. closure of $\mathcal{O}_K$ in $L) = \mathcal{O}_{L_1} \times \ldots \times \mathcal{O}_{L_r})$ is a deg. n ext. of $\mathcal{O}_K$ with

$\mathrm{disc}(\mathcal{O}_{L_i} | \mathcal{O}_K) = D_{L_i|K}$ (relative discriminant of $L_i|K$).

It is <u>maximal</u>: there is no deg. n ext. $S \supsetneq \mathcal{O}_L$ of $\mathcal{O}_K$.

Extensions of finite fields

Thm The number of nondeg. deg. n ext. of $\mathbb{F}_q$ up to isomorphism is the number of partitions of the integer n.

Pf The nondeg. ext. are

$$\mathbb{F}_{q^{n_1}} \times \dots \times \mathbb{F}_{q^{n_r}} \text{ with } n_1 + \dots + n_r = n. \qquad \square$$

We can do a weighted count:

Thm

$$\sum_{\substack{\text{nondeg. deg } n \\ \text{ext. } L \mid \mathbb{F}_q \\ \text{up to isom.}}} \frac{1}{\# \mathrm{Aut}_K(L)} = 1.$$

Pf Let $L = \mathbb{F}_{q^{n_1}} \times \dots \times \mathbb{F}_{q^{n_r}}$ with $n = n_1 + \dots + n_r$.

Let the number l occur c_l times in $(n_1, \dots, n_r)$.

$$\Rightarrow \# \mathrm{Aut}(L) = \prod_{l=1}^{n} l^{c_l} \cdot c_l!$$

each of the c_l factors $\mathbb{F}_{q^l}$ has l autom.

there are $c_l!$ permutations of the c_l factors $\mathbb{F}_{q^l}$

$$\Rightarrow \frac{1}{\# \mathrm{Aut}(L)} = \mathbb{P}(\pi \text{ has cycle type } (n_1, \dots, n_r) \mid \pi \in S_n).$$

$$\Rightarrow \sum_{L \dots} \frac{1}{\# \mathrm{Aut}(L)} = 1$$ (any $\pi \in S_n$ has exactly one cycle type).

$\square$

Extensions of local fields

(Serre, Sur une formule de masse ...)

Thm Let K be a local field with residue field $\mathbb{F}_q$, normalized val. v_K and norm $|x| = q^{-v_K(x)}$.
Consider the ~~totally~~ ramified (separable) degree n field ext. $L|K$. We have

$$\frac{1}{n} \sum_{L \subseteq K^{sep}} |D_{L|K}| = \sum_{\substack{L|K \\ \text{up to} \cong}} \frac{|D_{L|K}|}{\# \mathrm{Aut}(L)} = \frac{1}{q^{n-1}}.$$

Pf For any L as above, let
$U_L = \{ \pi \in \mathcal{O}_L \mid \underbrace{v_L(\pi)}_{= n \cdot v_K(\pi)} = 1 \}$ be the set of uniformizers of L.

Let $\sigma_1, \dots, \sigma_n$ be the embeddings $L \hookrightarrow K^{sep}$.

Identify monic deg. n pol. $f(X) = X^n + a_{n-1}X^{n-1} + \dots + a_0 \in \mathcal{O}_K[X]$ with vectors $(a_{n-1}, \dots, a_0) \in \mathcal{O}_K^n$.

Let $P_n \subseteq \mathcal{O}_K^n$ be the set of monic separable degree n Eisenstein pol. $f(X)$.

$v_K(a_{n-1}), \dots, v_K(a_1) \geq 1$, $v_K(a_0) = 1$

The min. pol. $f(X) = \prod_{i=1}^{n} (X - \sigma_i(\pi))$ of any $\pi \in U_L$ lies in P_n.

$\rightsquigarrow$ map $\varphi_L : U_L \longrightarrow P_n$
$\pi \longmapsto$ min. pol.

$\rightsquigarrow$ map $\varphi : \coprod_{\substack{L \subseteq K^{sep} \\ \text{as above}}} U_L \longrightarrow P_n$

(disjoint union because $L = K(\pi)$).

All n roots of any $f(X) \in P_n$ have $v_K(\pi) = \frac{1}{n}$, so they each generate a tot. ram. sep. deg. n ext. L/K, so lie in some U_L.

$\Rightarrow$ Any $f(X) \in P_n$ has exactly n preimages in $\coprod U_L$.

Endow K and L with Haar measures such that $\mathrm{vol}(\mathcal{O}_K) = \mathrm{vol}(\mathcal{O}_L) = 1$.

$$\mathrm{vol}(\underbrace{\{\text{mon. deg. } n \text{ Eisenstein pol.}\}}_{\subseteq \mathcal{O}_K^n})$$

$$= \mathrm{vol}(\{x \in \mathcal{O}_K \mid v_K(x) \geq 1\})^{n-1}$$ (coeff. $a_{n-1}, \dots, a_1$)

$$\cdot \mathrm{vol}(\{x \in \mathcal{O}_K \mid v_K(x) = 1\})$$ (coeff. a_0)

$$= (q^{-1})^{n-1} \cdot (q^{-1} \cdot (1 - q^{-1}))$$

$$= q^{-(n-1)} \cdot (q^{-1} - q^{-2}).$$

$$\mathrm{vol}(\underbrace{\{\text{mon. deg. } n \text{ inseparable pol.}\}}_{\subseteq \mathcal{O}_K^n})$$

$$= 0$$

$f(x)$ inseparable
$\Leftrightarrow \mathrm{disc}(f) = 0$
$\mathrm{disc}(f)$ is a polynomial $(\neq 0)$
in the coeff. of $f(x)$

$$\Rightarrow \mathrm{vol}(P_n) = q^{-(n-1)} \cdot (q^{-1} - q^{-2})$$

p-adic change of variables

(see Igusa: An introduction to the theory of local zeta functions, pg. 111
León-Cardenal, Zúñiga-Galindo: ... from scratch)

<u>Thm</u> (change of var. in dim. 1) Let K be a nonarch. local field and let $U \subset K$ be a compact open subset and $f(X) \in K[X]$. For any $y \in K$, let $m(y)$ be the number of $x \in U$ s.t. $f(x) = y$. Then,

$$\underbrace{\int_K m(y)\,dy}_{\text{vol}(\text{im}(f: U \to K) \text{ as a multiset})} = \int_U |f'(x)|\,dx$$

ASIDE

<u>Exe</u> Let $K = \mathbb{Q}_p$, $U = \mathbb{Z}_p^\times$, $f(x) = X^2$.

If $p \neq 2$: By Hensel's lemma, for $y \in \mathbb{Z}_p$,

$$m(y) = \begin{cases} 2, & (y \bmod p) \in \mathbb{F}_p^{\times 2} \quad (\text{quadr. res.}) \\ 0, & \text{else.} \end{cases}$$

$$\Rightarrow LHS = 2 \cdot \frac{\#\text{ nonzero quadr. res.}}{p} = \frac{p-1}{p} = 1 - \frac{1}{p}$$

$$v_p(f'(x)) = v_p(2x) = 0 \quad \forall x \in \mathbb{Z}_p^\times \Rightarrow |f'(x)| = 1 \; \forall x \in \mathbb{Z}_p^\times$$

$$\Rightarrow RHS = \int_{\mathbb{Z}_p^\times} 1\,dx = \text{vol}(\mathbb{Z}_p^\times) = 1 - \frac{1}{p} \quad \checkmark$$

If $p=2$: By Hensel's lemma, for $y \in \mathbb{Z}_2^\times$:

$$m(y) = \begin{cases} 2, & y \equiv 1 \bmod 8 \\ 0, & \text{else} \end{cases}$$

$$\Rightarrow LHS = 2 \cdot \frac{1}{8} = \frac{1}{4}$$

$v_2(f'(x)) = v_2(2x) = 1$, so $|f'(x)| = \frac{1}{2}$ $\forall x \in \mathbb{Z}_2^\times$

$$\Rightarrow RHS = \int_{\mathbb{Z}_2^\times} \frac{1}{2}\, dx = \frac{1}{2} \operatorname{vol}(\mathbb{Z}_2^\times) = \frac{1}{4} \quad \checkmark$$

Ex Let $K = \mathbb{F}_p((T))$, $U = \mathbb{F}_p[[T]] = \mathcal{O}_K$, $f(x) = X^p$.

For $y \in \mathbb{F}_p[[T]]$:

$$m(y) = \begin{cases} 1, & y = b_0 + b_p X^p + b_{2p} X^{2p} + \dots \text{ for some } b_0, b_p, \ldots \in \mathbb{F}_p \\ 0, & \text{else} \end{cases}$$

(∞ many digits have to be 0)

$$\Rightarrow LHS = 0$$

$$|f'(x)| = |pX^{p-1}| = 0$$

$$\Rightarrow RHS = 0 \quad \checkmark$$

Pf of Thm: Replace U by $\pi^a U$ and $\pi^b f\left(\frac{X}{\pi^a}\right)$.

$\Rightarrow$ we can assume that $U \subseteq \mathcal{O}_K$ and $f(X) \in \mathcal{O}_K[X]$.

The map $\begin{array}{l} U \to \mathbb{Z} \cup \{\infty\} \\ x \mapsto v(f'(x)) \end{array}$ is continuous.

You can show that $\mathrm{vol}(f(\{x \in \mathcal{O}_K \mid f'(x) = 0\})) = 0$.

(If the pol. $f'(X)$ is nonzero, it's a finite set.

Otherwise, $f(X)$ is constant or $\mathrm{char}(K) = p > 0$ and $f(X) = g(X^p)$ for some pol. $g(X) \in \mathcal{O}_K(X)$.

$$\begin{array}{ccccc} \mathcal{O}_K & \longrightarrow & \mathcal{O}_K & \longrightarrow & \mathcal{O}_K \\ x \mapsto x^p & & x \mapsto f(x) & & \end{array}$$

By the last exe. the image of $x \mapsto x^p$ has volume 0.

$\Rightarrow$ the image of $x \mapsto g(x^p)$ has volume 0.)

The sets $\{x \in U \mid v(f'(x)) = t\}$ for $t \in \mathbb{Z}$ are also compact and open. $\rightsquigarrow$ w.l.o.g. $v(f'(x)) = t \ \forall x \in U$.

For large enough e, we have $a + \pi^e \subseteq U \ \forall a \in U$ (because U is compact and open) and $f(a + \pi^e) = f(a) + \pi^{t+e}$ and each $y \in f(a) + \pi^{t+e}$ has exactly one preimage in $a + \pi^e$ (by Hensel's lemma). We have

$$\int_{a+\pi^e} \underbrace{|f'(x)|}_{q^{-t}} dx = q^{-e-t} = \int_{f(a)+\pi^{e+t}} 1 \, dy.$$

$\Rightarrow$ The result follows by splitting up U into sets of the form $a + p^e$ for $a \in U$. $\square$

More generally:

<u>Thm</u> Let $U \subset K^n$ be a cpt. open set and $f_1(x), \dots, f_n(x) \in K[X_1, \dots, X_n]$. For any $y \in K^n$, let $m(y)$ be the number of $x \in K^n$ s.t. $f(x) = y$.

Then,
$$\int_K m(y)\, dy = \int_U |\det \mathrm{Jac}(f)(x)|\, dx,$$
where $\mathrm{Jac}(f)(x) = \left(\dfrac{\partial f_i(x)}{\partial x_j}\right)_{i,j}$.

<u>Pf</u> "as in the real case". $\square$

Fixing an $\mathcal{O}_K$-basis $(\omega_1, \ldots, \omega_n)$ of $\mathcal{O}_L$, we can identify $\mathcal{O}_L$ with $\mathcal{O}_K^n$.

$$b_1\omega_1 + \ldots \longleftrightarrow (b_1, \ldots, b_n)$$

The Haar measures on $\mathcal{O}_L$ and $\mathcal{O}_K^n$ agree.

The map

$$\begin{array}{c} \varphi : \mathcal{O}_L \longrightarrow \mathcal{O}_K^n \\ \cong \\ \mathcal{O}_K^n \end{array}$$

$$(b_1, \ldots, b_n) \longmapsto \prod_{i=1}^{n} (X - \sigma_i(b_1\omega_1 + \ldots + b_n\omega_n))$$

sending $\alpha \in \mathcal{O}_L$ to its min. pol. is given by n polynomials in $b_1, \ldots, b_n$.

<u>Claim</u> The Jacobian det. at $\pi \in U_L \subseteq \mathcal{O}_L \cong \mathcal{O}_K^n$ is $|D_{L|K}|$.

$$\underset{\substack{\uparrow \\ \text{change of var.}}}{\Longrightarrow} \mathrm{vol}(\varphi(U_L) \text{ as a multiset}) = \mathrm{vol}(U_L) \cdot |D_{L|K}|$$

$$= q^{-1}(1 - q^{-1}) \cdot |D_{L|K}|.$$

Since $\varphi : \bigsqcup U_L \longrightarrow P_n$ is an n-cover,

$$\sum_{L \subseteq K^{sep}} \mathrm{vol}(\varphi(U_L) \text{ as multiset}) = n \cdot \mathrm{vol}(P_n)$$

$$\| \qquad\qquad\qquad\qquad \|$$

$$\sum_L q^{-1}(1 - q^{-1}) \cdot |D_{L|K}| \qquad\qquad n \cdot q^{-(n-1)} \cdot q^{-1}(1 - q^{-1})$$

$$\Longrightarrow \frac{1}{n} \sum_L |D_{L|K}| = \frac{1}{q^{n-1}}.$$

$\square$

Pf of claim W.l.o.g. the basis of $\mathcal{O}_L$ is given

$w_i = \pi^{i-1}$ $(i=1,\dots,n)$. The map φ is the

composition of

$$\begin{aligned} \mathcal{O}_K^n \cong \mathcal{O}_L &\longrightarrow \mathcal{O}_L^n \\ \alpha &\longmapsto (\sigma_j(\alpha))_j \\ (b_1,\dots,b_n) &\longmapsto \Big(\sum_i b_i\, \sigma_j(\pi^{i-1})\Big)_j \end{aligned}$$

and

$$\begin{aligned} \mathcal{O}_L^n &\longrightarrow \mathcal{O}_K^n \\ (c_j)_j &\longmapsto \prod_j (x - c_j) \end{aligned}$$

The first map has Jacobian matrix $\left(\sigma_j(\pi^{i-1})\right)_{i,j}$.

at π.

The second map has Jacobian determinant at $(\sigma_j(\pi))_j$

$$\pm \prod_{i<j} \left(\sigma_i(\pi) - \sigma_j(\pi)\right) = \pm \det\left(\left(\sigma_j(\pi^{i-1})\right)_{i,j}\right)$$

by problem 3a on PSet 3.

$\Rightarrow$ The absolute Jacobian det. of φ at π is

$$\left|\det\left(\sigma_j(\pi^{i-1})\right)_{i,j}\right|^2 = |D_{L|K}| .$$

$(\pi^{i-1})_i$ is a basis of $\mathcal{O}_L$ over $\mathcal{O}_K$

$\square$

Thm Let K be a nonarch. local field. Consider the (separable) deg. n field ext. $L|K$ with ram. index e and res. field ext. deg. f $(n = e \cdot f)$. We have

$$\frac{1}{n} \sum_{L \subseteq K^{sep}} |D_{L|K}| = \sum_{\substack{L \text{ up} \\ \text{to isom.}}} \frac{|D_{L|K}|}{\# \mathrm{Aut}_K(L)} = \frac{1}{f \cdot q^{n-f}} .$$

Pf

$$\begin{tikzcd} L \arrow[d, dash, "\text{deg. } e \text{ tot. ram.}"] \\ L^{I(L|K)} = F \arrow[d, dash, "\text{deg. } f \text{ unram.}"] \\ K \end{tikzcd}$$

There is exactly one unram. deg. f ext. $F|K$.

By the rel. disc. formula,

$$D_{L|K} = \mathrm{Nm}_{F|K}(D_{L|F}) \cdot \underbrace{D_{F|K}}_{\substack{(1) \text{ because} \\ F|K \text{ is unram.}}} = \mathrm{Nm}_{F|K}(D_{L|F})$$

$$\Rightarrow |D_{L|K}|_K = |\mathrm{Nm}_{F|K}(D_{L|F})|_K = |D_{L|F}|_F$$

$$\Rightarrow \frac{1}{n} \sum_{L \subseteq K^{sep}} |D_{L|K}|_K$$

$$= \frac{1}{n} \sum |D_{L|F}|_F$$

$$= \frac{1}{f \cdot e} \sum |D_{L|F}|_F$$

$$= \frac{1}{f} \cdot \frac{1}{(q^f)^{e-1}} = \frac{1}{f q^{n-f}}. \qquad \square$$

res. field of F is $\mathbb{F}_{q^f}$

Thm Let K be a nonarch. local field. Consider the nondeg. deg. n ext. $L|K$. We have

$$a_n := \sum_{\substack{L \text{ up to} \\ \text{isom.}}} \frac{|D_{L|K}|}{\# \mathrm{Aut}_K(L)} = \sum_{k=0}^{n} \frac{P(n,k)}{q^{n-k}},$$

where $P(n,k)$ is the number of partitions of the integer n into k positive summands (modulo order).

(Bhargava: Mass formulae for ext. of local fields (Thm 1.1)
Kedlaya: Mass formulas for local Galois repr. (–"–))

Ex $a_0 = 1$ $(L = 1)$

$a_1 = 1$ $(L = K)$

$a_2 = 1 + q^{-1}$ (if $2 \nmid q$, then the ext. are

$L = K \times K, K(\sqrt{a}), K(\sqrt{\pi}), K(\sqrt{a\pi})$

where $a \in \mathcal{O}_K^\times$ is a quadr. nonresidue, all have 2 automorphisms, the disc. are $1, 1, q, q$)

$a_3 = 1 + q^{-1} + q^{-2}$

$a_4 = 1 + q^{-1} + 2q^{-2} + q^{-3}$

Pf We can write $L = L_1 \times \dots \times L_r$ with $D_{L|K} = D_{L_1|K} \cdots D_{L_r|K}$

and $n = [L_1 : K] + \dots + [L_r : K]$.

Consider the permutation action of S_r on the set of tuples $(L_1, \dots, L_r)$.

isom. classes

$$\# \mathrm{Aut}(L) = \# \mathrm{Aut}(L_1) \cdots \# \mathrm{Aut}(L_r) \cdot \# \mathrm{Stab}_{S_r}((L_1, \dots, L_r))$$

$$\mathrm{Aut}(L) = (\mathrm{Aut}(L_1) \times \dots \times \mathrm{Aut}(L_r)) \rtimes \mathrm{Stab}_{S_r}((L_1, \dots, L_r)).$$

$$\Rightarrow a_n = \sum_{L \text{ deg. } n} \frac{|D_{L|K}|}{\# \mathrm{Aut}(L)}$$

$$= \sum_{r \geq 0} \sum_{\substack{S_r\text{-orbit} \\ [(L_1, \dots, L_r)] \\ \text{with } n = \sum_{i=1}^{r} [L_i : K]}} \frac{|D_{L_1|K}| \cdots |D_{L_r|K}|}{\# \mathrm{Aut}(L_1) \cdots \# \mathrm{Aut}(L_r)} \cdot \frac{1}{\# \mathrm{Stab}_{S_r}((L_1, \dots))}$$

$$\underset{\substack{\uparrow \\ \text{orbit-stab. thm.}}}{=} \sum_{r \geq 0} \frac{1}{r!} \sum_{\substack{(L_1, \dots, L_r) \\ \dots = n}} \frac{|D_{L_1|K}| \cdots |D_{L_r|K}|}{\# \mathrm{Aut}(L_1) \cdots \# \mathrm{Aut}(L_r)}$$

Use generating function:

$$\sum_{n\geq 0} a_n (qX)^n = \sum_{r\geq 0} \frac{1}{r!}\Bigg(\sum_{\substack{L \text{ field ext.} \\ (\text{up to } \cong)}} \frac{|D_{L|K}|}{\# \mathrm{Aut}(L)} \cdot (qX)^{[L:K]} \Bigg)^r$$

$$= \sum_{r\geq 0} \frac{1}{r!}\Bigg(\sum_{e,f\geq 1} \frac{1}{f\, q^{ef-f}} \cdot (qX)^{ef} \Bigg)^r$$

$$= \exp\Bigg(\sum_{e,f\geq 1} \underbrace{\frac{1}{f\, q^{ef-f}} \cdot (qX)^{ef}}_{\frac{q^f \cdot X^{ef}}{f} = \frac{(qX^e)^f}{f}} \Bigg)$$

$$= \exp\Bigg(\sum_{e\geq 1} \log \frac{1}{1-qX^e} \Bigg)$$

$$= \prod_{e\geq 1} \frac{1}{1-qX^e} = \prod_{e\geq 1} \sum_{t\geq 0} (qX^e)^t$$

$$= \sum_{t_1,t_2,\ldots\geq 0} q^{t_1+t_2+\ldots} X^{1\cdot t_1+2\cdot t_2+3\cdot t_3+\ldots}$$

$$\overset{?}{=} \sum_{n\geq 0} \sum_{k\geq 0} P(n,k)\, q^k X^n \implies a_n q^n = \sum_{k\geq 0} P(n,k)\, q^k .$$

write a part. of n into k summands

$n = 1\cdot t_1 + 2\cdot t_2 + \ldots$

$k = t_1 + t_2 + \ldots$

$\square$

Global fields

Binary cubic forms

Let R be an int. dom. with field of fractions K.
Let $V(R)$ be the set of binary cubic forms with coeff. in R:
pol. $f(X,Y) = aX^3 + bX^2Y + cXY^2 + dY^3 \in R[X]$

The discriminant is

$$\mathrm{disc}(f) = b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^2 + 18abcd$$

$$\underset{\text{if } a\neq 0}{=} \mathrm{disc}(f(X,1))$$

$$\underset{\text{if } d\neq 0}{=} \mathrm{disc}(f(1,X)),$$

Let $M = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in GL_2(R)$ act on $f \in V(R)$

by $(Mf)(v) = \dfrac{f(M^T v)}{\det(M)}$, $\quad \left(v = \begin{pmatrix} X \\ Y \end{pmatrix}\right)$

i.e. $(Mf)(X,Y) = \dfrac{f(pX + rY,\ qX + sY)}{\det(M)}$

Exe $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} f = \lambda \cdot f$

Lemma 1 a) $\mathrm{disc}(Mf) = \det(M)^2 \cdot \mathrm{disc}(f)$

b) The linear map $\varphi_M : V(K) \longrightarrow V(K)$
$f \longmapsto Mf$

has determinant $\det(\varphi_M) = \det(M)^2$.

Pf $GL_2(K)$ is gen. by matrices of the form

$\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ * & 1 \end{pmatrix}, \begin{pmatrix} * & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & * \end{pmatrix}$.

$\Rightarrow$ suffices to check the claims for matrices M of these forms.

a) $\left(\begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix} f\right)(x,1) = f(x+t,1)$

$\Rightarrow \left(\begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix} f\right)(x,1)$ and $f(x,1)$ have same leading coeff.

and roots are shifted by t.

$\Rightarrow$ same disc.

...

$\square$

Lemma 2 Let $f \in V(K)$. The abs. value of the Jacobian determinant of $\eta_f : GL_2(K) \to V(K)$

$$M \mapsto Mf$$

at $M \in GL_2(K)$ w.r.t.

the standard 4-form on $M_2(K) \cong K^4$ ($\rightsquigarrow$ Lebesgue measure)

$\begin{pmatrix} p & q \\ r & s \end{pmatrix} \leftrightarrow (p, \ldots)$

and the standard 4-form on $V(K) \cong K^4$

$aX^3 + \ldots \leftrightarrow (a, \ldots)$

is $|\det \mathrm{Jac}(\eta_f)(M)| = |\mathrm{disc}(f)|$.

Pf Let $\rho_M : GL_2(K) \to GL_2(K)$ be the right mult. by M map.

Let $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. $\Rightarrow \eta_{Mf} = \eta_f \circ \rho_M$

$$\underset{\text{chain rule}}{\Rightarrow} \mathrm{Jac}(\eta_{Mf})(I) = \mathrm{Jac}(\eta_f)(M) \cdot \mathrm{Jac}(\rho_M)(I)$$

$$\Rightarrow \underbrace{|\det \text{''} \text{---}|}_{\overset{!}{=} |\mathrm{disc}(Mf)|} = \underbrace{|\det \text{''} \text{---}|}_{\overset{?}{=} |\mathrm{disc}(f)|} \cdot \underbrace{|\det \text{''} \text{---}|}_{|\det(M)|^2}$$

$\Rightarrow$ By Lemma 1a, it suffices to check the claim for $M = I$ and all $f \in V(R)$.

$$\frac{\partial}{\partial t}\left(\left(\begin{pmatrix} 1 & t \\ 0 & 1\end{pmatrix} f\right)(x,y)\right)\Big|_{t=0} = bx^3 + 2cx^2y + 3dxy^2$$

$$\frac{\partial}{\partial t}\left(\left(\begin{pmatrix} 1 & 0 \\ t & 1\end{pmatrix} f\right)(x,y)\right)\Big|_{t=0} = 3ax^2y + 2bxy^2 + cy^3$$

$$\frac{\partial}{\partial t}\left(\left(\begin{pmatrix} 1+t & 0 \\ 0 & 1\end{pmatrix} f\right)(x,y)\right)\Big|_{t=0} = 2ax^3 + bx^2y - dy^3$$

$$\frac{\partial}{\partial t}\left(\left(\begin{pmatrix} 1 & 0 \\ 0 & 1+t\end{pmatrix} f\right)(x,y)\right)\Big|_{t=0} = -ax^3 + cxy^2 + 2dy^3.$$

$$\Rightarrow \left|\det \mathrm{Jac}(\eta_f)(I)\right| = \left|\det\begin{pmatrix} b & 2c & 3d & 0 \\ 0 & 3a & 2b & c \\ 2a & b & 0 & -d \\ -a & 0 & c & 2d\end{pmatrix}\right| = |\mathrm{disc}(f)|,$$

$\square$

3 points in $\mathbb{P}^1$

Let $V_{disc \neq 0} = \{ f \in V \mid disc(f) \neq 0 \}$.

The following bij. is helpful in understanding the action of $GL_2(\bar{K})$ on $V_{disc\neq 0}(\bar{K})$:

$$V_{disc\neq 0}(\bar{K})/\bar{K}^\times \longleftrightarrow \{\text{sets } S \text{ of three (dist.) pts. on } \mathbb{P}^1(\bar{K})\}$$

$$[f] \longmapsto \text{roots } [x:y] \in \mathbb{P}^1(\bar{K}) \text{ of } f$$

$$\left[\prod_{i=1}^{3}(b_i X - a_i Y)\right] \longleftarrow \{(a_i : b_i) \mid i = 1,2,3\}$$

Let $PGL_2(\bar{K})$ act on $\mathbb{P}1(\bar{K})$ by $M(x:y] = [x':y']$
$\quad\;\; \Psi \qquad\qquad\qquad\quad\; \Psi$
$\quad [M] \qquad\qquad\quad\;\; [x:y]$

with $\begin{pmatrix} x' \\ y' \end{pmatrix} = (M^T)^{-1}\begin{pmatrix} x \\ y \end{pmatrix}$, This makes the bijection $PGL_2(\bar{K})$-equivariant.

It turns out that $PGL_2(\bar{K})$ acts simply transitively on the set of (ordered!) tuples (P_1, P_2, P_3) of three distinct points $P_1, P_2, P_3 \in \mathbb{P}^1(\bar{K})$.

$\Rightarrow Stab_{PGL_2(\bar{K})}([f]) = Stab_{PGL_2(\bar{K})}(\text{set of roots of } f) \cong S_3$

perm. of the roots

Since $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} f = \lambda \cdot f$, it follows that:

__Lemma 3__ $\quad \mathrm{Stab}_{GL_2(\bar{K})}(f) \cong S_3 \quad$ (for $f \in V(K)$)

$$\begin{array}{c} \mathrm{Stab}_{GL_2(\bar{K})}(f) \\ \cup\!\mid \\ \mathrm{Stab}_{GL_2(K)}(f) \end{array}$$

Cubic extensions

Consider a cubic (= degree 3) ext. S of a PID R with field of fractions K.

__Lemma__ $\quad S$ has an R-basis of the form $(1, \omega_1, \omega_2)$.

(In part., S/R is a free R-mod. of rank 2.)

__Pf__ Since S is an R-lattice of rank 3 and R is a PID, S is free of rank 3.

Consider the embedding

$$\begin{array}{ccc} S & \hookrightarrow & S \otimes_R K \\ \uparrow & & \uparrow \\ R & \hookrightarrow & K \end{array}.$$

Every $x \in S$ is integral over R (it's a root of the char. pol. of the mult. by x map $S \to S$).

$\Rightarrow S \cap K = R$

$\Rightarrow 1 \in S$ is a primitive vector in the lattice S.

$\Rightarrow$ S has a basis of the form $(1, \omega_1, \omega_2)$. $\square$

<u>Rmk</u> Let (θ_1, θ_2) be a basis of the R-module S/R. Then, there is a unique basis $(1, \omega_1, \omega_2)$ of S with $\omega_i \equiv \theta_i \mod R$ such that $\omega_1\omega_2 \in R$.

<u>Pf</u> Take any $\omega_1' \equiv \theta_1$, $\omega_2' \equiv \theta_2 \mod R$. Then, $(1, \omega_1', \omega_2')$ is a basis of S.

$\Rightarrow$ We can write

$$\omega_1'\omega_2' = n \cdot 1 + p \cdot \omega_1' + q \cdot \omega_2' \text{ with } n, p, q \in R.$$

Write $\omega_1 = \omega_1' + \delta_1$, $\omega_2 = \omega_2' + \delta_2$ with $\delta_1, \delta_2 \in R$.

$$\Rightarrow \omega_1\omega_2 = (n + \delta_1\delta_2) \cdot 1 + (p + \delta_2) \cdot \omega_1' + (q + \delta_1)\omega_2' \in R$$

if and only if $p + \delta_2 = q + \delta_1 = 0$. $\square$

(Davenport, Heilbronn: On the density of disc. of cubic fields I + II

Bhargava, Shankar, Tsimerman:
On the Davenport-Heilbronn theorem
and second-order terms.)

<u>Thm</u> Define a commutative R-bilinear mult. op. on a free R-module $S = \langle 1, \omega_1, \omega_2 \rangle$ as follows, with $a, b, c, d, n, m, l \in R$:

$$\omega_1 \omega_2 = n$$
$$\omega_1^2 = m - b\omega_1 + a\omega_2$$
$$\omega_2^2 = l - d\omega_1 + c\omega_2$$
$$\begin{pmatrix} 1\cdot 1 = 1 \\ 1\cdot\omega_1 = \omega_1 \\ 1\cdot\omega_2 = \omega_2 \end{pmatrix}$$

This mult. op. is associative (so we obtain a cubic ext. S of R) if and only if

$$n = -ad, \quad m = -ac, \quad l = -bd.$$

<u>Pf</u> associative $\iff$ $\omega_1(\omega_2^2) = (\omega_1\omega_2)\omega_2$ and $(\omega_1^2)\omega_2 = \omega_1(\omega_1\omega_2)$

$$\omega_1(\omega_2^2) = l\omega_1 - dm + bd\omega_1 - ad\omega_2 + cn$$
$$(\omega_1\omega_2)\omega_2 = n\omega_2$$

$\Updownarrow$ ...

$\Updownarrow$

$$-dm + cn = 0 \text{ and } l + bd = 0 \text{ and } -ad = n$$

$\square$

Cor Consider the set of $(S,(\theta_1,\theta_2))$, where S is a cubic ext. of R and (θ_1,θ_2) is a basis of S/R.

Identify $(S,(\theta_1,\theta_2))$ with $(S',(\theta_1',\theta_2'))$ if there is an isom. $S\to S'$ of R-alg. that sends θ_1 to θ_1' and θ_2 to θ_2'. We get a bijection

$$\{(S,(\theta_1,\theta_2))\}/\cong \;\longleftrightarrow\; V(R)$$

$$(S,(\theta_1,\theta_2)) \longmapsto f(x,y)=ax^3+bx^2y+cxy^2+dy^3$$

with a,b,c,d as in the prev. Thm.

Thm With S,θ_1,θ_2, f as above, let $\varphi_{\theta_1,\theta_2}: S/R\to R$ be the composition of

$$S/R \longrightarrow \Lambda^2(S/R)$$

$$[\alpha] \longmapsto \underbrace{[\alpha]\wedge[\alpha^2]}$$

indep. of the rep. α:

$$[\alpha+r]\wedge[(\alpha+r)^2]$$

$$=[\alpha]\wedge[\alpha^2+2\alpha r\cancel{+r^2}]$$

$$=([\alpha]\wedge[\alpha^2])+\cancel{(2r[\alpha]\wedge[\alpha])}$$

and $\Lambda^2(S/R) \longrightarrow R$

$$\theta_1 \wedge \theta_2 \longmapsto 1 .$$

We have $f(X,Y) = \varphi_{\theta_1,\theta_2}([X\theta_1 + Y\theta_2])$.

<u>Pf</u> Let $\alpha = X\theta_1 + Y\theta_2$.

$$\Rightarrow \alpha^2 \equiv -(bX^2 + dY^2)\theta_1 + (aX^2 + cY^2)\theta_2 \mod R$$

$$\Rightarrow [\alpha] \wedge [\alpha^2] = f(X,Y)(\theta_1 \wedge \theta_2) .$$ $\square$

<u>Lemma</u> The (transitive) action of $GL_2(R)$ on the set of bases (θ_1, θ_2) of S/R (for fixed S) corresponds to the action of $GL_2(R)$ on $V(R)$.

<u>Pf</u> This follows from the previous Thm.

$$(Mf)(v) = \frac{f(M^T v)}{\det(M)} \begin{array}{l} \leftarrow \text{"from the first map"} \\ \leftarrow \text{"from the second map"} \end{array}$$

$\square$

Cor We get a bij.

$$\{\text{cubic ext.s of } R\} \longleftrightarrow GL_2(R) \backslash V(R).$$

Cor Let S corr. to $f \in V(R)$. Then,

$$\mathrm{Stab}_{GL_2(R)}(f) \cong \mathrm{Aut}_R(S).$$

Pf aut. of S

$\|$

R-lin. map $S \to S$ fixing $1 \in S$ and commuting with mult.

$\|$

change of basis $(1, \omega_1, \omega_2)$ that fixes a, b, c, d

$\|$

change of bases (θ_1, θ_2) that fixes a, b, c, d
($\Leftrightarrow$ fixes f)

$\|$

el. of $GL_2(R)$ that fixes f.

$\square$

Exe Consider the triv. eset. $L = K \times K \times K$ of K.

Take $\omega_1 = (1,0,0)$, $\omega_2 = (0,1,0)$. $(1 = (1,1,1))$

This corresponds to

$$f(X,Y) = X^2Y + XY^2 = XY(X+Y).$$

$$\mathrm{Stab}_{GL_2(K)}(f) \cong \mathrm{Aut}_K(L) \cong S_3.$$

Lemma Let $f(X,Y) = aX^3 + bX^2Y + cXY^2 + dY^3 \in V(K)$ with $a \neq 0$. Then, the corr. cubic eset. of K

$$L \cong K[X]/(f(X,1)).$$

Pf The isom. is given by $\omega_1 \mapsto aX$

$\omega_2 \mapsto aX^2 + bX + c$. $\square$

Warning This works only over fields!

<u>Cor</u> The cubic ext. L of K corr. to $f \in \mathcal{V}(K)$ is an int. dom. if and only if f is irreducible.

<u>Pf</u> If $a \neq 0$, then $L \cong K[X]/(f(X,1))$ is an int. dom.

$\iff f(X,1)$ irred.

$\iff f(X,Y)$ irred.

If $a=0$, then $\omega_1 \omega_2 = 0$ ($\Rightarrow$ not int. dom.)

and $f(X,Y) = Y(bX^2 + cXY + dY^2)$

is not irred. $\square$

<u>Rmk</u> Let $f \in \mathcal{V}(K)$ with $\mathrm{disc}(f) \neq 0$ corr. to the nondeg. cubic ext. L of K. Then, $\mathrm{Gal}(K^{sep}|K)$ acts on the 3 roots $P_1, P_2, P_3 \in \mathbb{P}^1(K^{sep})$ of f exactly like it acts on the three K-alg. hom. $\rho_1, \rho_2, \rho_3 : L \to K^{sep}$ (by right composition).

Thm Let R be a PID. If S corr. to $f \in \mathcal{V}(R)$, then

$$\operatorname{disc}(S) = (\operatorname{disc}(f)).$$

Pf just compute... "$\square$"

Maximal extensions

Def We call a nondegenerate deg. n ext. S of a Dedekind dom. R with field of fractions K <u>maximal</u> if S is the int. closure of R in the nondeg. deg. n ext. $S \otimes_R K$ of K.

We call it <u>maximal at a prime $\mathfrak{q}$</u> of R if the nondeg. deg. n ext. $S \otimes_R R_{\mathfrak{q}}$ of $R_{\mathfrak{q}}$ is maximal.

completion of R at $\mathfrak{q}$

Rmk A nondeg. deg. n ext. S of R is max. if and only if there is no deg. n ext. $S' \supsetneq S$ of R.

Key facts

a) Every nondeg. deg. n ext. L of K corresponds to exactly one max. deg. n ext. S of R,

b) rel. disc. $D_{L|K} = \operatorname{disc}(S|R)$

c) $\operatorname{Aut}_K(L) = \operatorname{Aut}_R(S)$

d) Maximality is a local cond. (cf. next page)

Thm Let S be a nondeg. deg. n sset. of a Dedekind dom. R. Then:

S maximal $\Leftrightarrow$ S maximal at every $\mathfrak{p}$

Pf "$\Leftarrow$" $S = \{x \in \underbrace{S \otimes K}_{L} \mid x \in S \otimes R_{\mathfrak{p}} \ \forall \mathfrak{p}\}$

$$= \text{"} \bigcap_{\mathfrak{p}} (S \otimes R_{\mathfrak{p}}) \text{"}$$

+ Rmk

"$\Rightarrow$" R is dense in $R_{\mathfrak{p}}$

$\Rightarrow$ $S = S \otimes_R R$ is dense in $S \otimes R_{\mathfrak{p}}$

+ Rmk $\square$

Rmk

$$\begin{array}{ccc} \text{max.} & \Longleftrightarrow & \text{max. at every } \mathfrak{p} \\ \Uparrow & & \Uparrow \\ \text{disc. sqfree} & \Longleftrightarrow & \text{disc. sqfree at every } \mathfrak{p} \\ & & (\mathfrak{p}^2 \nmid \text{disc}) \end{array}$$

(Reiner, Maximal orders)

For cubic ext., denote by $V^{max}(R)$ the set of $f \in V_{disc \neq 0}(R)$ corr. to max. ext. S of R.

Big goal

<u>Thm</u> $$N(T) := \sum_{\substack{\text{deg. 3 } \underline{\text{field}} \\ \text{ext. } L|\mathbb{Q} \\ \text{with } |D_L| \leq T}} \underbrace{\frac{1}{\# \mathrm{Aut}(L)}}_{\substack{=1 \text{ } \cancel{\text{for}} \\ 100\% \text{ of } L}} \sim \frac{1}{3\zeta(3)} \cdot T$$ for $T \to \infty$.

In part. $\#\{\text{deg. 3 field ext. } L|\mathbb{Q} \text{ with } |D_L| \leq T\} \sim \frac{1}{3\zeta(3)} \cdot T$ for $T \to \infty$.

<u>Pf</u> Overview:

$$N(T) = \sum_{\substack{[f] \in GL_2(\mathbb{Z}) \backslash V^{irred, max}(\mathbb{Z}) \\ |disc(f)| \leq T}} \frac{1}{\# \mathrm{Stab}_{GL_2(\mathbb{Z})}(f)}$$

Let $\mathcal{F}_T$ be a fund. dom. for $GL_2(\mathbb{Z})\backslash V_{0\neq|\mathrm{disc}|\leq T}(\mathbb{R})$.

$\Rightarrow N(T) = \#(\mathcal{F}_T \cap V^{\mathrm{irred,\,max}}(\mathbb{Z}))$

Basically, this is a lattice-point counting problem. To reduce $V(\mathbb{Z})$ to $V^{\mathrm{irred,\,max}}(\mathbb{Z})$, use a sieve.

<u>Step 1: Construct a nice fund. dom. $\mathcal{F}_T$ for $GL_2(\mathbb{Z})\backslash V_{0\neq|\mathrm{disc}|\leq T}(\mathbb{R})$</u>

Recall the bij.

$$GL_2(\mathbb{R})\backslash V_{0\neq\mathrm{disc}}(\mathbb{R}) \longleftrightarrow \{\text{nondeg. cubic ext. of } \mathbb{R}\}$$
$$\| $$
$$\{\mathbb{R}\times\mathbb{R}\times\mathbb{R},\ \mathbb{R}\times\mathbb{C}\}$$

Let $f_1, f_2 \in V(\mathbb{R})$ correspond to $\mathbb{R}\times\mathbb{R}\times\mathbb{R}$, $\mathbb{R}\times\mathbb{C}$,

$$\Rightarrow \#\mathrm{Stab}_{GL_2(\mathbb{R})}(f_1) = \#\underbrace{\mathrm{Aut}(\mathbb{R}\times\mathbb{R}\times\mathbb{R})}_{S_3} = 6$$

$$\#\mathrm{Stab}_{GL_2(\mathbb{R})}(f_2) = \#\mathrm{Aut}(\mathbb{R}\times\mathbb{C}) = 2$$

W.l.o.g. $|\mathrm{disc}(f_1)| = |\mathrm{disc}(f_2)| = 1$.

(E.g. $f_1 = XY(X+Y)$, $f_2 = \frac{1}{\sqrt{2}} X(X^2+Y^2)$.)

Now, $\mathcal{F}^{\mathbb{R}} := \{f_1\}^{\sqcup \frac{1}{6}} \sqcup \{f_2\}^{\sqcup \frac{1}{2}}$ is a

fund. dom. for $GL_2(\mathbb{R}) \backslash V_{\mathrm{disc} \neq 0}(\mathbb{R})$. (I)

Let $\mathcal{F}^{SL}$ be a fund. dom. for $SL_2(\mathbb{Z}) \backslash SL_2(\mathbb{R})$.

$\Rightarrow \mathcal{F}^{GL^{\pm 1}} := \left(\mathcal{F}^{SL} \sqcup \mathcal{F}^{SL}\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}\right)^{\sqcup \frac{1}{2}}$

is a fund. dom for $GL_2(\mathbb{Z}) \backslash \underbrace{GL_2^{\pm 1}(\mathbb{R})}_{\{M \in GL_2(\mathbb{R}) : \det(M) = \pm 1\}}$.

$\Rightarrow \mathcal{F}^{GL}_T := (0, T^{1/4}] \cdot \mathcal{F}^{GL^{\pm 1}}$ is a fund.

dom. for $GL_2(\mathbb{Z}) \backslash \underbrace{GL_2^{|\det| \leq T^{1/2}}(\mathbb{R})}_{\{M \in GL_2(\mathbb{R}) \mid |\det(M)| \leq T^{1/2}\}}$.

(II)

$(\mathrm{I}),(\mathrm{II}) \Rightarrow \mathcal{F}_T := \mathcal{F}_T^{GL} \cdot \mathcal{F}^{\mathbb{R}}$

$$:= \bigsqcup_{M \in \mathcal{F}_T^{GL}} M \cdot \mathcal{F}^{\mathbb{R}}$$

$$= \bigsqcup_{M \in \mathcal{F}_T^{GL}} \{M f_1\}^{\sqcup \frac{1}{6}} \sqcup \{M f_2\}^{\sqcup \frac{1}{2}}$$

is a fund. dom. for $GL_2(\mathbb{Z}) \backslash V_{0 \neq |\mathrm{disc}| \leq T}^{(\mathbb{R})}$

(because $|\mathrm{disc}(Mf)| = |\det(M)|^2 \cdot |\mathrm{disc}(f)|$
and $|\mathrm{disc}(f_1)| = |\mathrm{disc}(f_2)| = 1$).

Note: weight of f in $\mathcal{F}_T$:

$$\chi_{\mathcal{F}_T}(f) = \frac{1}{6} \# \{M \in \mathcal{F}_T^{GL} \mid M f_1 = f\}$$

$$+ \frac{1}{2} \# \{M \in \mathcal{F}_T^{GL} \mid M f_2 = f\}.$$

(at least one of these is 0)

Step 2: $\mathrm{vol}(\mathcal{F}_T) = \frac{1}{3}\zeta(2)\cdot T$

We've shown that the maps

$$\eta_{f_1}, \eta_{f_2} : GL_2(\mathbb{R})^{\subset \mathbb{R}^4} \longrightarrow V(\mathbb{R}) = \mathbb{R}^4$$
$$M \longmapsto Mf_1,\ Mf_2$$

have abs. Jac. det. $|\mathrm{disc}(f_1)|, |\mathrm{disc}(f_2)| = 1$ at M.

$$\Rightarrow \mathrm{vol}(\mathcal{F}_T) = \frac{1}{6}\mathrm{vol}(\eta_{f_1}(\mathcal{F}^{GL}_T) \text{ as a multiset})$$
$$+ \frac{1}{2}\mathrm{vol}(\eta_{f_2}(\mathcal{F}^{GL}_T) \text{ as a multiset})$$

$$\underset{\text{change of variables}}{=} \left(\frac{1}{6}+\frac{1}{2}\right)\cdot \int_{\mathcal{F}^{GL}_T} 1\, d^+M$$

$$\underset{d^\times M = \frac{d^+M}{|\det(M)|^2}}{=} \frac{2}{3}\cdot \int_{\underbrace{\mathcal{F}^{GL}_T}_{(0,T^{1/4}]\cdot \mathcal{F}^{GL^{\pm 1}} = (0,T^{1/4}]\cdot\left(\mathcal{F}^{SL} \sqcup \mathcal{F}^{SL}\begin{pmatrix}-1&0\\0&1\end{pmatrix}\right)^{\sqcup\frac{1}{2}}}} |\det(M)|^2\, d^\times M$$

$$= \frac{2}{3} \cdot \int_0^{T^{1/4}} \int_{\mathcal{F}^{SL}} \underbrace{|\det(\lambda h)|^2}_{\lambda^4} \cdot 2\, d^\times h \, d^\times \lambda$$

$M = \lambda h$

$\rightsquigarrow d^\times M = 2\, d^\times \lambda \, d^\times h$

was the def. of our Haar measure $d^\times h$ on $SL_2(\mathbb{R})$

$$= \frac{2}{3} \cdot 2 \cdot \int_0^{T^{1/4}} \lambda^4 \, d^\times \lambda \cdot \int_{\mathcal{F}^{SL}} 1 \, d^\times h$$

$$= \frac{2}{3} \cdot 2 \cdot \frac{(T^{1/4})^4}{4} \cdot \mathrm{vol}(\mathcal{F}^{SL})$$

fund. dom. for $SL_2(\mathbb{Z}) \backslash SL_2(\mathbb{R})$

$$= \frac{1}{3} \cdot T \cdot \zeta(2).$$

Step 3: Cut off cusp

Note: Take $n\,a\,k \in \mathcal{F}_{\text{Siegel}}$

$$\underset{\substack{\cap \\ N' \\ \uparrow \\ \text{cpt.}}}{n}\ \underset{\substack{\cap \\ A' \\ \| \\ \left\{\begin{pmatrix} t^{-1} & 0 \\ 0 & t\end{pmatrix} \,\middle|\, t \geq \underbrace{\sqrt{\frac{\sqrt{3}}{2}}}_{?}\right\}}}{a}\ \underset{\substack{\cap \\ K \\ \uparrow \\ \text{cpt.}}}{k}$$

Fix $f = aX^3 + bX^2Y + cXY^2 + dY^3$.

$$\Rightarrow \begin{pmatrix} t^{-1} & 0 \\ 0 & t\end{pmatrix} f = \underbrace{t^{-3}}_{\to 0 \text{ for } t \to \infty} aX^3 + t^{-1}bX^2Y + tcXY^2 + t^3dY^3$$

Let $f = aX^3 + \dots + dY^3 \in V^{\text{irred}}(\mathbb{Z})$.

Then, $a \neq 0$ (since f is irreducible, hence not divisible by X).

$\Rightarrow |a| \geq 1$ (since $a \in \mathbb{Z}$).

Let $V^{|a|\geq 1} = \{ f = aX^3 + \dots \in V \mid |a| \geq 1 \}$.

Let $(\mathcal{F}^{GL}_T)' = \mathcal{F}^{GL}_T \cap \{ M \in GL_2(\mathbb{R}) \mid Mf_1 \text{ or } Mf_2 \in V^{|a|\geq 1}(\mathbb{R}) \}$.

Let $\mathcal{F}^!_T = (\mathcal{F}^{GL}_T)' \cdot \mathcal{F}^{\mathbb{R}}$ as before.

$$\Rightarrow N(T) = \#\left(\mathcal{F}_T \cap V^{\text{irred, max}}(\mathbb{Z})\right)$$

$$= \#\left(\mathcal{F}_T' \cap V^{\text{irred, max}}(\mathbb{Z})\right).$$

<u>Step 4: For any full lattice $\Lambda \subset V(\mathbb{R}) \cong \mathbb{R}^4$, we have $\#(\mathcal{F}_T' \cap \Lambda) \sim \frac{\mathrm{vol}(\mathcal{F}_T)}{\mathrm{covol}(\Lambda)}$ for $T \to \infty$.</u>

As the fund. dom. for $SL_2(\mathbb{Z}) \backslash SL_2(\mathbb{R})$, use the convolution

$\mathcal{F}^{SL} :=$ (Siegel's fund. dom.) $*$ (subset A of $SL_2(\mathbb{R})$ of volume 1 such that $\partial((0,1] \cdot A) \subset SL_2(\mathbb{R})$ is Lipschitz).

As when we computed the volume of a fund. dom. for $SL_n(\mathbb{Z}) \backslash SL_n(\mathbb{R})$, you can apply Widmer's theorem and bound the error term (since we've cut off the cusp!).

Also, $\mathrm{vol}(\mathcal{F}'_T) \sim \mathrm{vol}(\mathcal{F}_T)$ for $T \to \infty$.

("fraction of volume in cusp $\to 0$").

<u>Note</u>: This implies that

$$N(T) = \#\left(\mathcal{F}'_T \cap V^{\text{irred, max}}(\mathbb{Z})\right)$$

$$\leq \#\Big(\mathcal{F}'_T \cap \underbrace{V(\mathbb{Z})}_{\cong \mathbb{Z}^4 \text{ full lattice of covolume } 1}\Big)$$

$$\sim \mathrm{vol}(\mathcal{F}_T) = \frac{1}{3}\zeta(2)\cdot T.$$

To get the correct constant, we'll use a sieve.

$$\frac{1}{3\zeta(3)}$$

Step 5: $V^{\max}(\mathbb{Z}_p)$ is a compact open subset of $V(\mathbb{Z}_p) \cong \mathbb{Z}_p^3$ of volume $(1-p^{-3})(1-p^{-2})$.

Recall the bij.

$$GL_2(\mathbb{Z}_p)\backslash V^{\max}(\mathbb{Z}_p) \longleftrightarrow \{\text{nondeg. cubic ext. } L \text{ of } \mathbb{Q}_p\}$$

$$\mathrm{Stab}_{GL_2(\mathbb{Z}_p)}(f) \cong \mathrm{Aut}_{\mathbb{Q}_p}(L)$$

$$(\mathrm{disc}(f)) = D_{L|\mathbb{Q}_p}$$

For any $f \in V^{\max}(\mathbb{Z}_p)$ corr. to L, consider the map

$$\eta_f : \underset{\subset \mathbb{Z}_p^4}{GL_2(\mathbb{Z}_p)} \to \underset{\subset \mathbb{Z}_p^4}{V^{\max}(\mathbb{Z}_p)}$$
$$M \mapsto Mf$$

Its abs. Jac. det. at any M is $|\mathrm{disc}(f)| = |D_{L|\mathbb{Q}_p}|$.
Any element of the image of η_f has exactly $\#\mathrm{Stab}_{GL_2(\mathbb{Z}_p)}(f) = \#\mathrm{Aut}(L)$ preimages.

$\Rightarrow$ By change of variables, the image (= the orbit $GL_2(\mathbb{Z}_p)\cdot f$) has volume

$$\mathrm{vol}(GL_2(\mathbb{Z}_p)\cdot f \text{ as a set})$$

$$= \frac{1}{\# \mathrm{Aut}(L)} \cdot \int_{GL_2(\mathbb{Z}_p)} |D_{L|\mathbb{Q}_p}| \, d^+ M$$

$$= \frac{|D_{L|\mathbb{Q}_p}|}{\# \mathrm{Aut}(L)} \cdot \mathrm{vol}^+(GL_2(\mathbb{Z}_p))$$

$$= \frac{|D_{L|\mathbb{Q}_p}|}{\# \mathrm{Aut}(L)} \cdot (1-p^{-2})(1-p^{-1})$$

Since $V^{\max}(\mathbb{Z}_p) = \bigsqcup_L$ (orbit corr. to L),

we get

$$\mathrm{vol}(V^{\max}(\mathbb{Z}_p)) = \sum_L \frac{|D_{L|\mathbb{Q}_p}|}{\# \mathrm{Aut}(L)} \cdot (1-p^{-2})(1-p^{-1})$$

$$= (1+p^{-1}+p^{-2}) \cdot (1-p^{-2})(1-p^{-1})$$

Bhargava, Kedlaya's mass formula

$$= (1-p^{-3})(1-p^{-2}).$$

Each orbit (corr. to L) is compact because it is the image of the compact set $GL_2(\mathbb{Z}_p)$ under the cont. map η_f (where $f \in V^{\max}(\mathbb{Z}_p)$ corr. to L). Since there are only fin. many such L (see PSet 6), this implies that $V^{\max}(\mathbb{Z}_p)$ is compact. ∎

Since the Jacobian of η_f is invertible everywhere, η_f is an open map. $\Rightarrow$ The orbit (= image of the open set $GL_2(\mathbb{Z}_p)$) is open.

$\Rightarrow V^{\max}(\mathbb{Z}_p)$ is open.

<u>Note:</u> A subset A of $\mathbb{Z}_p^n$ is compact and open if and only if A is the preimage of some subset A' of $(\mathbb{Z}/p^e\mathbb{Z})^n$ for some $e \geq 0$.
("Whether $x \in A$ depends only on $x \bmod p^e$.")

<u>Pf</u> "$\Rightarrow$" Since sets of the form $x + p^e \cdot \mathbb{Z}_p^n$ form a basis of open sets, A can be covered by sets of this form. Since A is cpt., it can be covered by finitely many.

"$\Leftarrow$" The projection $\mathbb{Z}_p^n \longrightarrow (\mathbb{Z}/p^e\mathbb{Z})^n$ is continuous. Any A' is open and closed.

$\Rightarrow$ $A \subseteq \mathbb{Z}_p^n$ open and closed

$\Downarrow$ $\mathbb{Z}_p^n$ compact

A compact

$\square$

$\Rightarrow$ Whether $f \in V(\mathbb{Z}_p)$ lies in $V^{max}(\mathbb{Z}_p)$ only depends on $f \bmod p^{e_p}$ for some fixed e_p. The volume $vol(V^{max}(\mathbb{Z}_p))$ is the fraction of residue classes belonging to $V^{max}(\mathbb{Z}_p)$.

Step 6: "Almost all $f \in \mathcal{F}'_T \cap V(\mathbb{Z})$ are irreducible":

$$\#\left(\mathcal{F}'_T \cap \left(V(\mathbb{Z}) \setminus V^{\text{irred}}(\mathbb{Z})\right)\right) = o(T) \quad \text{for } T \to \infty$$

f reducible over $\mathbb{Z}$

$\Rightarrow$ f reducible over $\mathbb{Z}_p$ $\forall p$

$\Rightarrow$ f corresponds to a product of ≥ 2 field ext. of $\mathbb{Q}_p$ (not integral domain) $\forall p$

$\Leftrightarrow$ f doesn't corr. to a field ext. of $\mathbb{Q}_p$ $\forall p$

$\Rightarrow$ f doesn't corr. to the unramified cubic field ext. $L_p = \mathbb{Q}_p(\zeta_{p^3-1})$ of $\mathbb{Q}_p$ $\forall p$

$\Leftrightarrow$ $f \notin$ ($GL_2(\mathbb{Z}_p)$-orbit in $V^{\max}(\mathbb{Z}_p)$ corr. to L_p). $\forall p$.

Let $M \geq 2$.

$\Rightarrow \#\left(\mathcal{F}'_T \cap \left(V(\mathbb{Z}) \setminus V^{\text{irred}}(\mathbb{Z})\right)\right)$

$\leq \#\{f \in \mathcal{F}'_T \cap V(\mathbb{Z}) \mid f \notin (\text{orbit corr. to } L_p) \ \forall p \leq M\}$

In step 5, we've seen that the orbit corr to L_p is a cpt. open subset of $V^{\max}(\mathbb{Z}_p)$ of volume

$$\text{vol}(\text{orbit corr. to } L_p) = \frac{|D_{L_p}|_{\mathbb{Q}_p}|}{\# \text{Aut}(L_p)} \cdot (1-p^{-2})(1-p^{-1})$$

$$= \frac{1}{3} \cdot (1-p^{-2})(1-p^{-1}).$$

$\Rightarrow$ By applying step 4 to every residue class mod $\prod_{p \le M} p^{e_p}$, you see that

$$\#\{f \in \mathfrak{F}_T' \cap V(\mathbb{Z}) \mid f \notin (\text{orbit corr. to } L_p)\ \forall p \le M\}$$

$$\underset{M}{\sim} \mathrm{vol}(\mathfrak{F}_T') \cdot \prod_{p \le M} (1 - \mathrm{vol}(\text{orbit corr. to } L_p))$$

$$= \frac{1}{3} \zeta(2) \cdot T \cdot \prod_{p \le M} \Big(1 - \underbrace{\tfrac{1}{3}(1-p^{-2})(1-p^{-1})}_{\xrightarrow[p \to \infty]{} \frac{1}{3}}\Big)$$

But $\prod_{p \le M} \left(1 - \frac{1}{3}(1-p^{-2})(1-p^{-1})\right) \xrightarrow[M \to \infty]{} 0.$

Step 7: "Sieve for max. est."

$$\#\left(\mathcal{F}^1_T \cap V^{\text{irred},\max}(\mathbb{Z})\right) \sim \frac{1}{3\zeta(3)} \cdot T$$

Remember that

$$f \in V^{\max}(\mathbb{Z})$$

$$\iff f \in V^{\max}(\mathbb{Z}_p) \quad \forall p$$

Let $M \geq 2$.

$$\Rightarrow 0 \leq \#\{f \in \mathcal{F}^1_T \cap V^{\text{irred}}(\mathbb{Z}) : f \in V^{\max}(\mathbb{Z}_p)\ \forall p \leq M\}$$

main term

$$- \#\left(\mathcal{F}^1_T \cap V^{\text{irred},\max}(\mathbb{Z})\right)$$

$$\leq \#\{f \in \mathcal{F}^1_T \cap V^{\text{irred}}(\mathbb{Z}) : f \notin V^{\max}(\mathbb{Z}_p) \text{ for some } p > M\}$$

error term $\to$

$$\leq \sum_{p > M} \#\{f \in \mathcal{F}^1_T \cap V^{\text{irred}}(\mathbb{Z}) : f \notin V^{\max}(\mathbb{Z}_p)\}.$$

By step 4 and the CRT,

$$\#\{f \in \mathcal{F}^1_T \cap V^{\text{irred}}(\mathbb{Z}) : f \in V^{\max}(\mathbb{Z}_p)\ \forall p \leq M\}$$

$$\underset{M}{\sim} \operatorname{vol}(\mathcal{F}^1_T) \cdot \prod_{p \leq M} \operatorname{vol}\left(V^{\max}(\mathbb{Z}_p)\right)$$

$$= \frac{1}{3}\zeta(2)\cdot T \cdot \prod_{p\le M}(1-p^{-3})(1-p^{-2})$$

step 2,5

But

$$\frac{1}{3}\zeta(2)\cdot \prod_{p\le M}(1-p^{-3})(1-p^{-2}) \xrightarrow[M\to\infty]{} \frac{1}{3\zeta(3)}.$$

By step 8, we have

$$\sum_{p>M} \# \{ f\in \mathcal{F}^1_T \cap V^{\mathrm{irred}}(\mathbb{Z}) : f\notin V^{\max}(\mathbb{Z}_p)\}$$

$$\ll \sum_{p>M} \frac{T}{p^2} \ll \frac{T}{M} = o_{M\to\infty}(T).$$

<u>Step 8:</u> $\#\left(GL_2(\mathbb{Z})\backslash \{f\in V^{\mathrm{irred}}_{0\ne|\mathrm{disc}|\le T}(\mathbb{Z}) \mid f\notin V^{\max}(\mathbb{Z}_p)\right)$

$$\ll \frac{T}{p^2}.$$

doesn't depend on T, p

Claim 1 Let S be a nondeg. cubic ext. of $\mathbb{Z}$ which is not maximal at p. Then, S is a subext. of some cubic ext. S' of $\mathbb{Z}$

of type I: $S/\mathbb{Z} = p\cdot(S'/\mathbb{Z})$:

if (θ_1', θ_2') is a basis of $S'/\mathbb{Z}$, then $(p\theta_1', p\theta_2')$ is a basis of $S/\mathbb{Z}$.

$$(\Rightarrow [S':S] = p^2)$$

of type II: there is a basis (θ_1', θ_2') of $S'/\mathbb{Z}$ such that $(p\theta_1', \theta_2')$ is a basis of $S/\mathbb{Z}$ and the cubic form $f' \in V(\mathbb{Z})$ corr. to $(S', (\theta_1', \theta_2'))$ is not divisible by p.

$$(\Rightarrow [S':S] = p).$$

Pf We know that S is a subext. of some cubic ext. S' of $\mathbb{Z}$ of index p^k for some $k \geq 1$.

Let (θ_1, θ_2) of $S/\mathbb{Z}$ and let (θ_1', θ_2') of $S'/\mathbb{Z}$. We obtain a base change matrix $M \in M_2(\mathbb{Z}) \cap GL_2(\mathbb{Q})$ sending θ_1' to θ_1 and θ_2' to θ_2, with

$$|\det(M)| = [S':S] = p^k.$$

We can put M in Smith normal form:

$$M = A\begin{pmatrix} p^r & 0 \\ 0 & p^s \end{pmatrix} B \quad \text{with } A, B \in GL_2(\mathbb{Z}) \text{ and}$$

$r \geq s \geq 0$. The matrices A, B corr. to changing the bases $(\theta_1, \theta_2), (\theta_1', \theta_2')$.

$\rightsquigarrow$ W.l.o.g. $A = B = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, so $M = \begin{pmatrix} p^r & 0 \\ 0 & p^s \end{pmatrix}$.

Note $r + s = k \geq 1$.

Let $(S, (\theta_1, \theta_2))$ corr. to $f \in V(\mathbb{Z})$.

$$f = aX^3 + bX^2Y + cXY^2 + dY^3$$

$\Rightarrow (S', (\theta_1', \theta_2'))$ corr. to $M^{-1} f \in V(\mathbb{Z})$

$$M^{-1}f = p^{-2r+s} aX^3 + p^{-r} bX^2Y + p^{-s} cXY^2 + p^{r-2s} dY^3$$

$\Rightarrow p^{-2r+s} a,\ p^{-r} b,\ p^{-s} c,\ p^{r-2s} d \in \mathbb{Z}$

If $p^{-1}a, p^{-1}b, p^{-1}c, p^{-1}d \in \mathbb{Z}$, we could take $r = s = 1$,

so $\theta_1 = p\theta_1'$, $\theta_2 = p\theta_2'$ (Type I).

Assume not. $\Rightarrow$ We can't have $r = s \geq 1$.

$\Rightarrow r \geq s + 1 \geq 1$. $\Rightarrow p^{-2}a, p^{-1}b, c, pd \in \mathbb{Z}$.

$\rightsquigarrow$ We could take $r = 1$, $s = 0$, so

$\theta_1 = p\theta_1'$, $\theta_2 = \theta_2'$. (Type II) $\square$ (claim 1)

<u>Claim 2</u> For fixed p, any nondeg. cubic ext. S' of $\mathbb{Z}$

has a) exactly 1 subext. S of type I (and index p^2)

b) at most 3 subext. S of type II (and index p).

<u>Pf</u> a) clear

b) The subext. S depends on the choice of basis (θ_1', θ_2'), but it only depends on $\theta_1' \bmod \theta_2'$ and $\theta_2' \bmod p \cdot \theta_1'$.

Let $\underset{\substack{\shortparallel \\ aX^3 + \dots + dY^3}}{f'} \in V(\mathbb{Z}_p)$ corr. to $(S', (\theta_1', \theta_2'))$.

$$\Rightarrow \underset{\substack{\shortparallel \\ p^2 aX^3 + pbX^2Y + cXY^2 + p^{-1}dY^3}}{\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} f'} \in V(\mathbb{Z}_p) \text{ corr. to } (S, (\theta_1, \theta_2))$$

$$\Rightarrow 0 \equiv d \equiv f'(0,1) \bmod p.$$

The cubic form f' has at most 3 zeroes in $\mathbb{P}^1(\mathbb{F}_p)$ (corr. to valid choices of θ_2'.)

$\square$ (Claim 2)

(cf. section 3 of Bhargava, Shankar, Tsimerman).

This implies step 8:

$$\#\left(GL_2(\mathbb{Z}) \backslash \{f \in V^{\text{irred}}_{0 \neq |\text{disc}| \leq T}(\mathbb{Z}) \mid f \notin V^{\text{max}}(\mathbb{Z}_p)\}\right)$$

$$\leq 1 \cdot \#\left(GL_2(\mathbb{Z}) \backslash \{f \in V^{\text{irred}}_{0 \neq |\text{disc}| \leq \frac{T}{p^4}}(\mathbb{Z})\}\right) \quad (\text{type I})$$

$p^4 \leftarrow$ index p^2

$$+ 3 \cdot \#\left(GL_2(\mathbb{Z}) \backslash \{f \in V^{\text{irred}}_{0 \neq |\text{disc}| \leq \frac{T}{p^2}}(\mathbb{Z})\}\right) \quad (\text{type II})$$

$p^2 \leftarrow$ index p

$$\ll \frac{T}{p^4} + \frac{T}{p^2} \ll \frac{T}{p^2}.$$

$\uparrow$ steps 2, 4

$\Rightarrow$ This finishes the proof of the "big goal" theorem!!! $\square$

G-extensions

Let G be a finite group.

Def A <u>G-ext.</u> L of a field K is a degree $|G|$ ext. of K with a left action of G on the K-algebra L (fixes $1 \in L$, satisfies $g(x+y) = gx + gy$, $g(x \cdot y) = (gx)\cdot(gy)$, $g(\lambda x) = \lambda g x$ for $\lambda \in K$), which has a <u>normal basis</u>: a K-basis of the form

$(g\alpha)_{g \in G}$ for some $\alpha \in L$.

An <u>isom. of G-ext.</u> is a G-equivariant isom. $L_1 \xrightarrow{\sim} L_2$ of K-algebras.

Rmk (base change)
If L is a G-ext. of K and $K'|K$ is any field ext., then $L \otimes_K K'$ is a G-ext. of K'.

Rmk We can regard L a left $K[G]$-module.

Then, $\exists$ normal basis $(g\alpha)_{g\in G} \iff L \cong K[G]$ as a left $K[G]$-module, $g\alpha \leftrightarrow g$

Ex The <u>trivial G-ext.</u> $L = \prod_{g \in G} K = K \times \dots \times K$

with G-action $g(x_{g'})_{g' \in G} = (x_{g^{-1}g'})_{g' \in G}$.

Equivalently: $L = K(G)$ with mult. in L given by

$$\Big(\sum_g x_g g\Big) \cdot_L \Big(\sum_g y_g g\Big) = \sum_g x_g y_g g.$$

Thm (Normal basis theorem)

A Galois ext. $L|K$ with Galois group G has a normal basis (i.e. is a G-ext.)

Pf (when $|K| = \infty$)

Let $G = \{g_1, \dots, g_n\}$.

$L \otimes K^{sep}$ is a nondeg. deg. $|G|$ ext. of K^{sep}.

$$\Rightarrow \begin{tikzcd} L \otimes K^{sep} \arrow[r, phantom, "\cong"] & \underbrace{K^{sep} \times \dots \times K^{sep}}_{|G|} \\ L \arrow[u, hook] \end{tikzcd}$$

$\rightsquigarrow$ We obtain n distinct embeddings $L \hookrightarrow K^{sep}$, corr. to the n aut. of $L \subseteq K^{sep}$.

$$\Rightarrow \quad L \hookrightarrow K^{sep} \times \dots \times K^{sep}$$
$$y \mapsto (g_1 y, \dots, g_n y)$$

$\Rightarrow$ $L \otimes K^{sep}$ is the triv. G-ext of K^{sep}

Now, fix a K-basis $\omega_1, \dots, \omega_n$ of L.

Consider the pol.

$$f(X_1,\dots,X_n) = \det\left(g_i g_j (X_1 w_1 + \dots + X_n w_n)\right)_{i,j}$$
$$= \det\left(X_1 g_i g_j w_1 + \dots + X_n g_i g_j w_n\right)_{i,j}.$$

For $a_1,\dots,a_n \in K$, $\alpha = a_1 w_1 + \dots + a_n w_n \in L$, the following are equivalent:

$(g_i \alpha)_i$ is a basis of L

$\Leftrightarrow$ The image $\left((g_j g_i \alpha)_j\right)_i$ is a basis of $K^{sep} \times \dots \times K^{sep}$.

$\Leftrightarrow$ $\det(g_i g_j \alpha)_{i,j} \neq 0$

$\Leftrightarrow$ $f(a_1,\dots,a_n) \neq 0$.

Hence,

L has a normal basis

$\Leftrightarrow$ $f(a_1,\dots,a_n) \neq 0$ for some $a_1,\dots,a_n \in K$

$\Leftrightarrow$ pol. $f(X_1,\dots,X_n) \neq 0$

$|K| = \infty$

$\Leftrightarrow$ $f(a_1,\dots,a_n) \neq 0$ for some $a_1,\dots,a_n \in K^{sep}$

$\Leftrightarrow$ $L \otimes_K K^{sep}$ has a normal basis (true!)

same argument as before

$\square$

Def Let L be an H-ext. of K for some $H \leq G$.

Define the <u>induced G-ext</u> $\mathrm{Ind}_H^G L = K[G] \otimes_{K[H]} L$

with G-action $g(a \otimes b) = (ga) \otimes b$ and with

mult. given by

$$(g \otimes b) \cdot (g \otimes b') = g \otimes (b b')$$
$$(g \otimes b) \cdot (g' \otimes b') = 0 \quad \text{when } gH \neq g'H.$$

$$\left[(g \otimes b) \cdot \underbrace{(gh \otimes b)}_{(g \otimes hb)} = g \otimes (b \cdot h b') \right]$$

Rmk $\mathrm{Ind}_H^G L \cong \underbrace{L \times \ldots \times L}_{r := [G:H]}$ as a K-algebra.

Pf Choose repr. $g_1, \ldots, g_r$ of the cosets in G/H.

$g_1 \otimes b_1 + \ldots + g_r \otimes b_r \longmapsto (b_1, \ldots, b_r)$. $\square$

Ex $\mathrm{Ind}_1^G K \cong K \times \ldots \times K$ is the triv ext.

Ex $\mathrm{Ind}_G^G L = L$

Thm $\mathrm{Ind}_H^G L$ is a G-ext.

Pf $\mathrm{Ind}_H^G L = K(G) \otimes_{K(H)} L \underset{\substack{\uparrow \\ L \text{ is } H\text{-ext}}}{\cong} K(G) \otimes_{K(H)} K(H) \cong K[G]$

as a left $K[G]$-module. + check that you get a left action of G on the K-algebra! $\square$

Thm (Classification)

The nondeg. G-ext. of K can be written as $L = \mathrm{Ind}_H^G F$, where $H \subseteq G$ and where F is a Galois ext. of K with Galois group H. The automorphism group is

$$\mathrm{Aut}_{G\text{-ext.}}(L) \cong C_G(H) = \{ g \in G \mid \forall h \in H : gh = hg \},$$

the centralizer of H in G.

(Pf. skipped!)

Another way to look at G-extensions:

<u>Def</u> Let $\Gamma_K := \mathrm{Gal}(K^{sep} | K)$ be the absolute Gal. group of K. To any continuous surjective hom. $f : \Gamma_K \twoheadrightarrow G$, we associate the Galois ext. $L_f = (K^{sep})^{\ker(f)}$ of K with Galois group G.

More generally, to any cont. hom. $f : \Gamma_K \to G$, we associate the G-ext. $L = \mathrm{Ind}_H^G \underbrace{(K^{sep})^{\ker(f)}}_{\substack{\text{Gal. ext. with} \\ \text{Gal. group } H}}$

where $H = \mathrm{im}(f)$.

<u>Thm</u> Let G act on $\mathrm{Hom}_{cont}(\Gamma_K \to G)$ by conjugation. We get a bij.

$$G \backslash \mathrm{Hom}_{cont}(\Gamma_K \to G) \longleftrightarrow \{\text{nondeg. } G\text{-ext. of } K \text{ (up to isom.)}\}$$

$$f \longmapsto L_f$$

Furthermore $\mathrm{Stab}_G(f) = C_G(\mathrm{im}(f)) \cong \mathrm{Aut}_{G\text{-ext}}(L_f)$.

Also, f is surjective if and only L_f is a field (= Gal. ext. of K).

Rmk If $K'|K$ is a separable field ext. and L is a G-ext. of K corr. to $f: \Gamma_K \to G$, then the G-ext. $L \otimes_K K'$ of K' corr. to $f': \Gamma_{K'} \subseteq \Gamma_K \to G$.

Rmk Let G_1, G_2 be finite groups. We obtain a bij.

$$\{\text{nondeg. } G_1\text{-ext. of } K\} \times \{\text{nondeg. } G_2\text{-ext. of } K\} \leftrightarrow \{\text{nondeg. } G_1 \times G_2\text{-ext. of } K\}$$

$$(L_1, L_2) \longmapsto L_1 \otimes_K L_2$$

If L_i corr. to $f_i : \Gamma_K \to G_i$, then $L_1 \otimes L_2$ corr. to

$$\Gamma_K \longrightarrow G_1 \times G_2$$
$$\sigma \longmapsto (f_1(\sigma), f_2(\sigma)).$$

$$\mathrm{Aut}_{G_1\text{-ext}}(L_1) \times \mathrm{Aut}_{G_2\text{-ext}}(L_2) \cong \mathrm{Aut}(L_1 \otimes L_2)$$

If $L_1, L_2 \subseteq K^{sep}$ are fields, then

$$L_1 \otimes L_2 \cong \mathrm{Ind}_H^{G_1 \times G} (\underbrace{L_1 \cdot L_2}_{\text{compositum}}),$$

where $H = \mathrm{Gal}(L_1 \cdot L_2 | K) \subseteq G_1 \times G_2$.

Rmk Let $n \geq 1$. We obtain a bij.

$$\{\text{nondeg. deg. } n \text{ eset. of } K\} \longleftrightarrow \{\text{nondeg. } S_n\text{-eset. of } K\}$$
$$F = L^T \longleftarrow\!\!\shortmid \quad L$$

where $T < S_n$ is the set of perm. of $\{1, \dots, n\}$ that fix 1 and $L^T = \{x \in L \mid \forall g \in T : gx = x\}$.

[For the '$\longrightarrow$' map, see Bhargava, Satriano: On a notion of "Galois closure" for extensions of rings.]

Let $\sigma_1, \dots, \sigma_n$ be the K-algebra homomorphisms $F \longrightarrow K^{sep}$.

Then, the map $f : \Gamma_K \longrightarrow S_n$ corr. to the S_n-est. L represents the action of Γ_K on the set $\{\sigma_1, \dots, \sigma_n\}$ of n hom. (by composition).

$$\mathrm{Aut}_{K\text{-alg.}}(F) \cong \mathrm{Aut}_{S_n\text{-eset}}(L)$$

F is a field if and only if the action of Γ_K on $\{1, \dots, n\}$ (induced by $f : \Gamma_K \to S_n$) is transitive. Then, $(K^{sep})^{\ker(f)}$ is Galois closure of F/K.

Decomposition, ramification

Let $\mathcal{O}_K$ be a Dedekind dom. with field of fractions K, let $L|K$ be a nondeg. deg. n ext. and let $\mathcal{O}_L$ be the int closure of $\mathcal{O}_K$ in L.

<u>Def</u> A <u>prime</u> of L is a max. ideal $\mathfrak{q} \subseteq \mathcal{O}_L$.

<u>Rmk</u> If $L = L_1 \times \dots \times L_r$. The primes of L are the ideals of the form $\mathfrak{q} = \mathcal{O}_{L_1} \times \dots \times \mathcal{O}_{L_{i-1}} \times \mathfrak{q} \times \mathcal{O}_{L_{i+1}} \times \dots \times \mathcal{O}_{L_r}$, where $\mathfrak{q}$ is a prime of L_i.

"$\{\text{primes of } L\} = \bigsqcup_i \{\text{primes of } L_i\}$"

<u>Rmk</u> If $\mathfrak{P}$ is a prime in L, then $\mathfrak{p} = \mathfrak{P} \cap K$ is a prime of K.

<u>Def</u> Assume that $L|K$ is a nondeg. G-ext.
Let $\mathfrak{P}$ be a prime of L and $\mathfrak{p} = \mathfrak{P} \cap K$.
We define the

<u>decomposition group</u> $D(\mathfrak{P}|\mathfrak{p}) = \{ g \in G \mid g\mathfrak{P} = \mathfrak{P} \}$.

<u>inertia group</u> $I(\mathfrak{P}|\mathfrak{p}) = \{ g \in D(\mathfrak{P}|\mathfrak{p}) \mid gx \equiv x \bmod \mathfrak{P} \ \forall x \in \mathcal{O}_L \}$

<u>higher ramification group</u> $(s \geq 0)$
$$I_s(\mathfrak{P}|\mathfrak{p}) = \{ g \in D(\mathfrak{P}|\mathfrak{p}) \mid gx \equiv x \bmod \mathfrak{P}^{s+1} \ \forall x \in \mathcal{O}_L \}.$$

<u>Rmk</u> $G \supseteq D \supseteq I = I_0 \supseteq I_1 \supseteq I_2 \supseteq \dots$
and $I_s = 1$ for sufficiently large s.

Rmk G acts transitively on the set of primes $\mathfrak{P}$ above a fixed prime $\mathfrak{p}$ of K.

Rmk
$$D(g\mathfrak{P}|\mathfrak{p}) = g\, D(\mathfrak{P}|\mathfrak{p})\, g^{-1}$$
$$I_s(g\mathfrak{P}|\mathfrak{p}) = g\, I_s(\mathfrak{P}|\mathfrak{p})\, g^{-1}$$

Rmk If $\kappa(\mathfrak{p}) = \mathcal{O}_K/\mathfrak{p}$ is a finite field, then $\kappa(\mathfrak{P})|\kappa(\mathfrak{p})$ is a Galois ext. with Galois group

$$D/I.$$

...

The discriminants of all subext. are determined by the higher ramification groups:

Thm Let K be a global or local field.
$$v_{\mathfrak{p}}(D_{L|K}) = \frac{|G|}{|I|} \cdot \sum_{s=0}^{\infty} (|I_s| - 1)$$

More ~~generally~~, for any $H \subseteq G$,

$$v_{\mathfrak{p}}(D_{L^H|K}) = \sum_{s=0}^{\infty} \left(\frac{[G:H]}{[I:I_s]} - \frac{1}{|I|} \cdot \sum_{g \in I_s} \#\{r \in G/H : gr = r\} \right)$$

Tamely ramified extensions

Def $L|K$ is <u>tamely ramified</u> at $\mathfrak{P}$ if $I_1(\mathfrak{P}|\mathfrak{p}) = 1$.
$$\shortparallel$$
$$I_2 = \dots$$

Rmk $L|K$ is tamely ramified if and only if (the residue field characteristic p of) $\mathfrak{P}$ doesn't divide $|I|$.

In particular, $L|K$ is tamely ramified whenever $p \nmid |G|$.

Cor If K is a local field with res. field char. $p \nmid |G|$, then every cont hom. $\Gamma_K \longrightarrow G$ factors through

$$\Gamma_K^{tame} := Gal(\underset{\substack{\uparrow \\ \text{max. tamely} \\ \text{ramified ext.}}}{K^{tame}} | K).$$

$$\Gamma_K \twoheadrightarrow \Gamma_K^{tame} \longrightarrow G$$

We get a bij.

$$\{\text{cont. hom. } \Gamma_K \to G\} \leftrightarrow \{\text{cont. } \Gamma_K^{tame} \to G\}.$$

Thm The max. tamely ramified field extension of a local field K with residue field $\mathbb{F}_q$ is

$$K^{tame} = \bigcup K(\zeta_m, \pi^{1/m}$$

Cor of Thm

If $L|K$ is tamely ramified at $\mathfrak{P}$ and $I(\mathfrak{P}|\mathfrak{q}) \leq G$ is generated $\tau \in G$, then

$$v_{\mathfrak{q}}(D_{L|K}) = |G| - \frac{1}{\mathrm{ord}(\tau)}$$

and for any $H \leq G$,

$$v_{\mathfrak{q}}(D_{L^H|K}) = [G:H] - \frac{1}{\mathrm{ord}(\tau)} \cdot \sum_{k=0}^{\mathrm{ord}(\tau)-1} \#\{r \in G/H : \tau^k r = r\}$$

$= [G:H] - \#($cycles of the permutation representing left mult. by τ on $G/H)$.

$$\boxed{\begin{array}{l} \Gamma_k = \mathrm{Gal}(K^{sep}|K) \\ \quad \downarrow \\ \Gamma_k^{tame} = \mathrm{Gal}(K^{tame}|K) \end{array}}$$

Thm The max. tamely ramified field ext. of a local field K with residue field $\mathbb{F}_q$ is

$$K^{tame} = \bigcup_{\substack{m\geq 1 \\ \gcd(m,q)=1}} K(\zeta_m, \pi_K^{1/m}) = \bigcup_{t\geq 0} K(\zeta_{q^t-1}, \pi_K^{1/(q^t-1)}).$$

Its Galois group Γ_K^{tame} contains the following dense (finitely presented) subgroup:

$$\langle \varphi, \tau \mid \varphi\tau\varphi^{-1} = \tau^q \rangle,$$

where τ is given by $\tau(\zeta_m) = \zeta_m$, $\tau(\pi_K^{1/m}) = \zeta_m \pi_K^{1/m}$
and φ is given by $\varphi(\zeta_m) = \zeta_m^q$, $\varphi(\pi_K^{1/m}) = \pi_K^{1/m}$

(lift of Frobenius).

Also $\langle\tau\rangle \overset{\mathbb{Z}}{\cong}$ is a dense subgroup of $I(K^{tame}/K)$

and $\langle\varphi\rangle \cong \mathbb{Z}$ is a dense subgroup of Γ_K^{tame}/I.

$$\begin{array}{c} K^{tame} \\ |I \\ K^{nr} \\ | \\ K \end{array}$$

$\cong Gal(K^{nr}/K)$
$\cong Gal(\overline{\mathbb{F}}_q/\mathbb{F}_q)$
$\cong \hat{\mathbb{Z}}$

Any subgroup of $Gal(K^{tame}/K)$ of finite index is open.

Cor We obtain a bij.

$$\{\text{cont. hom. } \Gamma_k^{tame} \longrightarrow G\} \longleftrightarrow \{(\bar\varphi, \bar\tau) \in G \times G \mid \bar\varphi \bar\tau \bar\varphi^{-1} = \bar\tau^q\}$$

$$f \longmapsto (f(\varphi), f(\tau))$$

If f corresponds to the (tamely ramified) G-extension $L|K$, then $I(L|K)$ is generated by $\bar\tau = f(\tau)$.

Lemma Let C be a conjugacy class in G. Then,

$$\frac{1}{|G|} \cdot \#\{\text{cont. } f : \Gamma_k^{tame} \to G : f(\tau) \in C\}$$

$$= \begin{cases} 1, & \text{if } C = C^q, \\ 0, & \text{if } C \neq C^q. \end{cases}$$

Pf $\mathrm{LHS} = \frac{1}{|G|} \cdot \#\{(\bar\varphi, \bar\tau) \in G \times C \mid \bar\varphi \bar\tau \bar\varphi^{-1} = \bar\tau^q\}$.

Since $\bar\tau, \bar\varphi \bar\tau \bar\varphi^{-1} \in C$, the LHS is 0 if $C \neq C^q$.

If $C = C^q$, fix any of the $|C|$ elements $\bar\tau$ of C.

Since $\bar\tau^q \in C^q = C$, there exists some $\bar\varphi_0 \in G$ s.t. $\bar\varphi_0 \bar\tau \bar\varphi_0^{-1} = \bar\tau^q$.

We have $\bar{\varphi}\,\bar{\tau}\,\bar{\varphi}^{-1} = \bar{\tau}\,? = \bar{\varphi}_0\,\bar{\tau}\,\bar{\varphi}_0^{-1}$ if and only if $\bar{\varphi}_0^{-1}\bar{\varphi}$ commutes with (= lies in the centralizer of) $\bar{\tau}$. By the orbit-stabilizer theorem (applied to the action of G on C by conjugation), the centralizer has size $\frac{|G|}{|C|}$.

$\Rightarrow$ $|C| \cdot \frac{|G|}{|C|} = |G|$ such pairs $(\bar{\varphi}, \bar{\tau})$ in total.

$\square$

G-extensions of number fields (Malle's conjecture)

Let K be a number field and $G \neq 1$ be a nontrivial finite group. Consider a function $d : G \longrightarrow \mathbb{R}^{\geq 0} \cup \{\infty\}$ satisfying the following properties:

a) $d(hgh^{-1}) = d(g)$ $\forall g, h \in G$

(so d is a class function $\{\text{conj. classes}\} \to \mathbb{R}^{\geq 0} \cup \{\infty\}$)

b) $d(g^n) = d(g)$ $\forall g \in G$, $n \in (\mathbb{Z}/|G|\mathbb{Z})^\times$

c) $d(g) = 0$ if and only if $g = id \in G$.

For any ~~place~~ place v of K, consider a <u>local invariant</u>

$\mathrm{inv}_v : \{\text{nondeg. } G\text{-ext. of } K_v\} \longrightarrow \mathbb{R}^{>0} \cup \{\infty\}$

such that for all but finitely many nonarchimedean $v = \mathfrak{q}$ with residue field char. $p \nmid |G|$ and any G-ext. L of K_v, we

$\mathrm{inv}_v(L) = \mathrm{Nm}(\mathfrak{q})^{d(\bar{\tau})}$, where $\bar{\tau} \in G$ generates the inertia group $I(L|K_v)$ (or $\bar{\tau} = f(\tau)$, where $f : \Gamma_u^{\mathrm{tame}} \to G$ corresponds to the G-ext. L of K_v).

<u>Rmk</u> This is well-def. according to a), b).

G-extensions of number fields

Existence

Of course, any field K has a G-ext. L, namely the triv ext. But the following question is open.

<u>Question</u> (Inverse Galois problem)
Is every finite group G the Galois grp. of some Galois ext. (= field G-ext.) $L|\mathbb{Q}$?

<u>Rmk</u> known for S_n, A_n, abelian groups, solvable groups, all sporadic finite simple groups except M_{23}, ...

<u>Rmk</u> Any fin. group G embeds into $S_{|G|}$. Therefore, G is the Galois group of some Galois ext. $L|K$:

$$\begin{tikzcd}
L \arrow[dr, dash, "G"] \arrow[dd, dash, "S_{|G|}"'] & \\
& K \arrow[dl, dash] \\
\mathbb{Q} &
\end{tikzcd}$$

Counting

Fix a field K and a finite group G. For any fct. $\mathrm{inv} : \{\text{nondeg. } G\text{-ext. of } K\} \to \mathbb{R} \cup \{\infty\}$, let

$$N_{\mathrm{inv}}(T) = \#\{\underline{\text{field}}\ G\text{-ext. } L/K : \mathrm{inv}(L) \leq T\}.$$

[$\mathrm{inv}(L) = \infty$ means that L is ignored/forbidden.]

<u>Question</u> How does $N_{\mathrm{inv}}(T)$ grow as $T \to \infty$?

We need to restrict the set of allowed invariant functions to make sense of this!

<u>Def</u> An <u>invponent</u> is a fct. $d : G \to \mathbb{R}^{\geq 0} \cup \{\infty\}$ satisfying the following properties:

a) $d(hgh^{-1}) = d(g)$ $\forall g, h \in G$ (so d is a class function $d : \{\text{conj. cl. of } G\} \to \mathbb{R}^{\geq 0} \cup \{\infty\}$)

b) $d(g^n) = d(g)$ $\forall g \in G$ $\forall n \in (\mathbb{Z}/|G|\mathbb{Z})^\times$
(if $\langle g \rangle = \langle g' \rangle$, then $d(g) = d(g')$)

c) $d(g) = 0$ if and only if $g = id$

Def Let d be an invponent and let k be a nonarch. local field with residue field $\mathbb{F}_q$ of characteristic $p \nmid |G|$. Every nondeg. G-ext. $L|k$ is tamely ramified, so $I(L|k) \subseteq G$ is cyclic. Define the <u>invariant associated to d</u> by

$$\mathrm{inv} : \{\text{nondeg. } G\text{-ext. of } k\} \longrightarrow \mathbb{R} \cup \{\infty\}$$
$$L \longmapsto q^{d(g)}, \text{ where } I(L|k) = \langle g \rangle.$$

Ex $\mathrm{inv}(L) = 1 \underset{c)}{\Longleftrightarrow} \tau = \mathrm{id} \Leftrightarrow I(L|k) = 1 \Leftrightarrow L|k$ unram.

Def Let K be a number field. We say that an invariant inv of nondeg. G-ext. of K is <u>compatible with</u> an invponent d if for each place v of K, there is a <u>local invariant</u> inv_v of nondeg. G-ext. of K_v such that

i) For any nondeg. G-ext. $L|K$,
$$\mathrm{inv}(L) = \prod_v \mathrm{inv}_v(L \otimes_K K_v).$$

ii) For all but fin. many ("<u>exceptional</u>") places v, the local invariant inv_v is the invariant associated to d.

<u>Rmk</u> Since any L is ramified only at fin. many places v, $\prod_v \mathrm{inv}_v(L \otimes_K K_v)$ is really a finite product.

Def The a-number of d is

$$a = a(d) = \min_{id \neq g \in G} d(g) > 0.$$

Let $\zeta = \zeta_{|G|}$, $U [= U(K)] = Gal(K(\zeta)|K) \leq (\mathbb{Z}/|G|\mathbb{Z})^\times$

$$(\zeta \mapsto \zeta^r) \mapsto r$$

Consider the action of $U \leq (\mathbb{Z}/|G|\mathbb{Z})^\times$ on the set of conjugacy classes C of G given $r . C = C^r$. (Note that $d(r.C) = d(C)$ by property b).)

The b-number is

$$b = b(d, K) = \begin{cases} 1, & a = \infty \\ \#(U \backslash \{\text{conj. cl. } C : d(C) = a\}), & a < \infty. \end{cases}$$

Malle's conjecture on steroids (MCS)

Let K be a number field with invariant inv compatible with invponent d. Then, there is a constant $C = C_{inv} \geq 0$ such that

$$N_{inv}(T) \sim C \cdot T^{\hat{a}(d)} \cdot (\log T)^{b(d,K)-1}$$

for $T \to \infty$.

<u>Exe A</u> MCS is true when $a(d)=\infty$ (i.e. $d(g)=\infty$ for all $g\neq id$):

$N_{inv}(T) \sim C\cdot T^0 \cdot (\log T)^0 = C$ for $T\to\infty$,

i.e. there are only fin. many field G-ext. $L|K$ s.t. $inv(L)<\infty$.

<u>Pf</u> For all nonexceptional places v, we have $inv_v(L\otimes_K K_v)<\infty$ only if L is unram. at v.

Hence, any L with $inv(L)<\infty$ can be ramified at only the fin. many exceptional v. For each exceptional v, there are only fin. many nondeg. G-ext. of K_v.

$\Rightarrow$ The disc. D_L is bounded.

$\Rightarrow$ There are only fin many possible L. $\square$

Exe B Assume $G \neq 1$.

$$\operatorname{disc}(L) := \left| \operatorname{Nm}_{K|\mathbb{Q}} D_{L|K} \right| = \frac{|D_L|}{|D_K|^{[L:K]}}$$

rel. disc. formula

is compatible with

$$d(g) = |G| \cdot \left(1 - \frac{1}{\operatorname{ord}(g)}\right)$$

(cf. computation of discr. of tamely ramified ext. of local fields).

$a(d) = |G| \cdot \left(1 - \frac{1}{p}\right)$ where p is the smallest prime factor of $|G|$.

$$b(d, K) = \begin{cases} 1, & G = C_p,\ K = \mathbb{Q} \quad \left(U = (\mathbb{Z}/p\mathbb{Z})^\times \circlearrowright \{0 \neq a \in \mathbb{Z}/p\mathbb{Z}\}\right) \\ p-1, & G = C_p,\ K = \mathbb{Q}(\zeta_p) \quad \left(U = 1 \circlearrowright \{0 \neq a \in \mathbb{Z}/p\mathbb{Z}\}\right) \\ \left[\frac{n}{2}\right], & G = S_n,\ K \text{ arbitrary} \\ & (U \text{ acts trivially on } \{\text{conj. cl. } C \text{ of order } 2\}) \\ \vdots & \end{cases}$$

Ese C   Let $H \leq G$. Then,

$$\mathrm{disc}^H(L) := \mathrm{disc}(L^H) = |N_{K|\mathbb{Q}} D_{L^H|K}| = \frac{|D_{L^H}|}{|D_K|^{[L:K]}}$$

is compatible with

$d(g) = [G:H] - \#$(cycles in the perm. representing left-mult by g in G/H)

Ese C.1   Let $n \geq 2$, $G = S_n$, $H = \mathrm{Stab}(1) \leq S$

set of perm. of $\{1, \dots, n\}$ fixing 1

We obtain a natural identification

$G/H \Longleftrightarrow \{1, \dots, n\}$, which is S_n-equivariant.

$\Rightarrow d(g) = n - \#(\text{cycles in } g \in S_n)$

$\Rightarrow a(d) = 1$ (and $d(g) = 1 \Leftrightarrow g$ has cycle type $(2, 1, \dots, 1)$ $\Leftrightarrow g$ is a transposition)

$b(d, k) = 1$ (all transpositions in S_n lie in the same conjugacy class).

Hence $MCS \Rightarrow N_{\mathrm{disc}\, H}(T) \sim C_n \cdot T$ for $T \to \infty$.

$$\begin{aligned} &\quad \parallel \\ &\#\{\text{deg. } n \text{ field ext. } L'|K \\ &\quad \text{whose Galois closure has} \\ &\quad \text{Galois group } S_n \\ &\quad \text{and s.t. } \mathrm{disc}(L') \leq T\} \end{aligned}$$

<u>Ex C.2</u> Let $n \geq 2$, G any transitive subgr. of S_n,

$H = G \cap \mathrm{Stab}(1) \subseteq G$.

We again obtain the G-equiv. bij.:

$G/H \longleftrightarrow \{1, \dots, n\}$.

$\Rightarrow d(g) = n - \#(\text{cycles in } g \in S_n)$.

<u>If G contains a transposition</u>:

$a(d) = 1$

Any two transp. in a transitive subgr. G of S_n are conjugate.

$\Rightarrow b(d, K) = 1$.

Hence, $MCS \Rightarrow N_{\mathrm{disc}\, H}(T) \sim C_{n,G} \cdot T$ for $T \to \infty$

$$\begin{aligned} &\quad \parallel \\ &\#\{\text{deg. } n \text{ field ext. } L'|K \text{ whose Gal. closure} \\ &\quad \text{has Gal. grp. } G \subseteq S_n \text{ (up to conj.)} \\ &\quad \text{and } \mathrm{disc}(L') \leq T\} \end{aligned}$$

If G contains no transp.:

$a(d) \geq 2$

Hence, MCS $\Rightarrow$

$$N_{\mathrm{disc}\, H}(T) \ll T^{\frac{1}{2}} (\log T)^{b-1} \text{ for } T \to \infty.$$

$$\parallel$$

$\#\{$deg. n field ext. $L'|K$
whose Gal. closure
has Galois group $G \leq S_n$
and $\mathrm{disc}(L') \leq T\}$

Cor of ex. C.1, C.2

MCS $\Rightarrow \#\{$deg. n field ext. $L'|K$ s.t. $\mathrm{disc}(L') \leq T\} \sim c_n' \cdot T$
for $T \to \infty$

Furthermore, ordering L' by $\mathrm{disc}(L')$,

$\mathbb{P}($Gal. cl. of $L'|K$ has Gal. grp. S_n $|$ L' as above$) = 1$

if and only if n is prime.

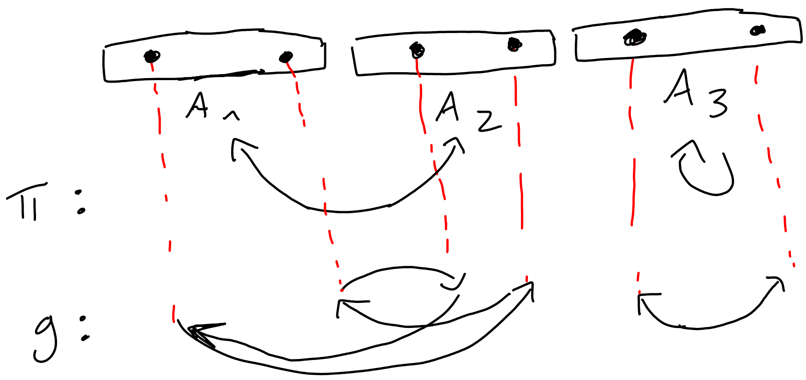
Pf $\mathbb{P} = 1 \Leftrightarrow \nexists$ transitive subgr. $G \subsetneq S_n$ containing
a transposition

$\Leftrightarrow$ n prime. $\square$

Ex If $n = r \cdot s$ with $r, s \geq 2$, partition $\{1, \dots, n\}$ into r sets $A_1, \dots, A_r$ of size s. Then,

$$G := \{ g \in S_n \mid \exists \pi \in S_r : \forall 1 \leq t \leq r : \forall i \in A_t : g(i) \in A_{\pi(t)} \}$$

is a transitive proper subgroup of S_n and contains a transposition.



MCS is a statement about the number of <u>field</u> extensions:

Rmk Let $d : G \to \mathbb{R}^{\geq 0} \cup \{\infty\}$. Denote the restriction to $H \subseteq G$ by $d|_H$.

Always $a(d|_H) \geq a(d)$.

But sometimes $a(d|_H) = a(d)$ and $b(d|_H, K) > b(d, K)$.

$\Rightarrow$ By MCS,

grows more slowly

$$\#\{\text{field } G\text{-ext. } L|K : \mathrm{inv}(L) \leq T\} \sim C_1 \cdot T^{\frac{1}{a}} (\log T)^{b(d)-1}$$

$$\#\{\text{field } H\text{-ext. } L'|K : \mathrm{inv}(L') \leq T\} \sim C_2 \cdot T^{\frac{1}{a}} (\log T)^{b(d|_H)-1}$$

$$\wedge \leftarrow L := \mathrm{Ind}_H^G L'$$

$$\#\{\text{nondeg. } G\text{-ext. } L|K : \mathrm{inv}(L) \leq T\}$$

grows more quickly

Ex There are $\sim C_1 \cdot T$ deg. 4 field ext. $L|\mathbb{Q}$ with $\mathrm{disc}(L) \leq T$. $(G = S_4)$

There are $\sim C_2 \cdot T(\log T)$ products L of two degree 2 field ext. of $\mathbb{Q}$ with $\mathrm{disc}(L) \leq T$. $(H = S_2 \times S_2 \subseteq S_4)$.

Heuristic for MCS

(cf. Malle: On the distribution of Galois groups,
— " — , II)

Assume there exists a field G-ext. $L|K$
with $\mathrm{inv}(L) < \infty$,

Basic assumption: For a finite set of places S
and nondeg. G-ext. L_v of K_v $(v \in S)$, the
number of field G-ext. L of K that are
unramified at all $v \notin S$ and such that
$L \otimes_K K_v \cong L_v$ for all $v \in S$
is "on average" $C_1 \cdot \prod_v \frac{1}{\# \mathrm{Aut}_{G\text{-ext}}(L_v)}$

for some constant $C_1 > 0$.
["local-global principle"]

In terms of Dirichlet series:
let $$D(s) = \sum_{\substack{L|K \text{ field} \\ G\text{-ext.}}} \frac{\mathrm{inv}(L)^{-s}}{\# \mathrm{Aut}(L)}$$

and $$D'_v(s) = \sum_{\substack{L_v|K_v \text{ nondeg.} \\ G\text{-ext.}}} \frac{\mathrm{inv}_v(L_v)^{-s}}{\# \mathrm{Aut}(L_v)} .$$

$\leadsto$ Basic assumption (basically by Tauberian thm / Wiener–Ikehara)

$$D(s) \approx \prod_v D_v'(s)$$

both sides have rightmost pole at the same positions and of the same order

$$\Rightarrow D(s) \approx \prod_v D_v'(s)$$

$$\approx \prod_{\substack{\mathfrak{q}=v \\ \text{not exceptional}}} D_v'(s)$$

not exceptional [i.e., $\mathfrak{q} \nmid |G|$, inv$_v$ given by d]

each $D_v'(s)$ is a finite sum and therefore entire

$$\approx \prod_{\mathfrak{q} \nmid |G|} \sum_{\substack{\text{conj. cl. } C: \\ C = C^{\mathrm{Nm}(\mathfrak{q})}}} (\mathrm{Nm}(\mathfrak{q})^{d(C)})^{-s}$$

cf. counting tamely ram. ext. of local fields

$$\approx \prod_{\mathfrak{p} \nmid |G|} \Big(\underset{\substack{\uparrow \\ C = \{id\} \\ (\text{unram. ext. of } K_v)}}{1} + \sum_{\substack{C: \\ C = C^{Nm(\mathfrak{p})}, \\ d(C) = a}} Nm(\mathfrak{p})^{-as} \Big)$$

$$\approx \prod_{\mathfrak{p} \nmid |G|} \prod_{\substack{C: \\ C = C^{Nm(\mathfrak{p})} \\ d(C) = a}} \left(1 + Nm(\mathfrak{p})^{-as}\right).$$

The Frobenius automorphism in

$U = Gal(K(\zeta_{|G|})|K) \subseteq (\mathbb{Z}/|G|\mathbb{Z})^\times$

of $\mathfrak{p} \nmid |G|$ with residue field $\mathbb{F}_q$ $(q = Nm(\mathfrak{p}))$

is $(q \bmod |G|)$. Hence,

$C = C^{Nm(\mathfrak{p})} \iff C = C^q \iff (q \bmod |G|) \in Stab_U(C)$

$\iff Frob(\mathfrak{p}) \in Stab_U(C)$

$\iff Frob(\mathfrak{p})$ maps to id in $U/Stab_U(C) \cong Gal(K(\zeta)_C | K)$,

where $K(\zeta)_C := K(\zeta)^{Stab_U(C)}$

$(\Leftrightarrow)$ y splits completely in $K(\zeta)_C$.

Therefore,

$$D(s) \approx \prod_{\substack{C:\\ d(C)=a}} \; \prod_{\substack{y \nmid |G| \\ \text{splitting} \\ \text{completely} \\ \text{in } K(\zeta)_C}} \left(1 + \mathrm{Nm}(y)^{-as}\right)$$

$$= \prod_{\substack{U\text{-orbit}[C]:\\ d(C)=a}} \; \prod_{\substack{y \nmid |G| \\ \text{s.c. in} \\ K(\zeta)_C}} \left(1 + \mathrm{Nm}(y)^{-as}\right)^{[U:\,\mathrm{Stab}_U(C)]}$$

U abelian, so every el. of an orbit has the same stabilizer

$$= \qquad \cdot \qquad - \Big(\qquad \Big)^{[K(\zeta)_C\,:\,K]}$$

$$\underbrace{= \prod_{\substack{U\text{-orbit}[C]:\\ d(C)=a}} \underbrace{\zeta_{K(\zeta)_C}(as)}_{\text{rightmost: simple pole at } s=\frac{1}{a}}}_{\text{order } b\,(=\#U\text{-orbits}) \text{ pole at } s=\frac{1}{a}}$$

Dedekind zeta function .

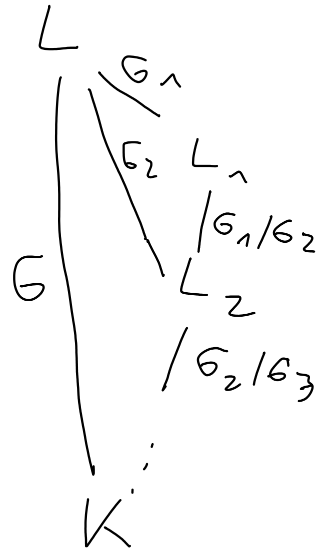
$\Rightarrow$ By Tauberian theorems / Wiener-Ikehara,

$$\sum_{\substack{L|K \text{ field} \\ G\text{-ext.} \\ \mathrm{inv}(L) \le T}} \underbrace{\frac{1}{\# \mathrm{Aut}(L)}}_{\substack{\shortparallel \\ \frac{1}{\#(\text{center of } G)}}} \sim C \cdot T^{\frac{1}{a}} (\log T)^{b-1}.$$

"$\Box$"

Strategies for proving (special cases of) MCS

1. Understand quotients of Γ_K.
   E.g. classfield theory description of the abelianization Γ_K^{ab}, dealing with abelian groups G
   (Wright: Distribution of discriminants of abelian extensions,
   Wood: On the probabilities of local behaviors in abelian field extensions)
2. Induction along chains of normal subgroups $1 \leq G_1 \leq G_2 \leq \dots \leq G_n = G$.

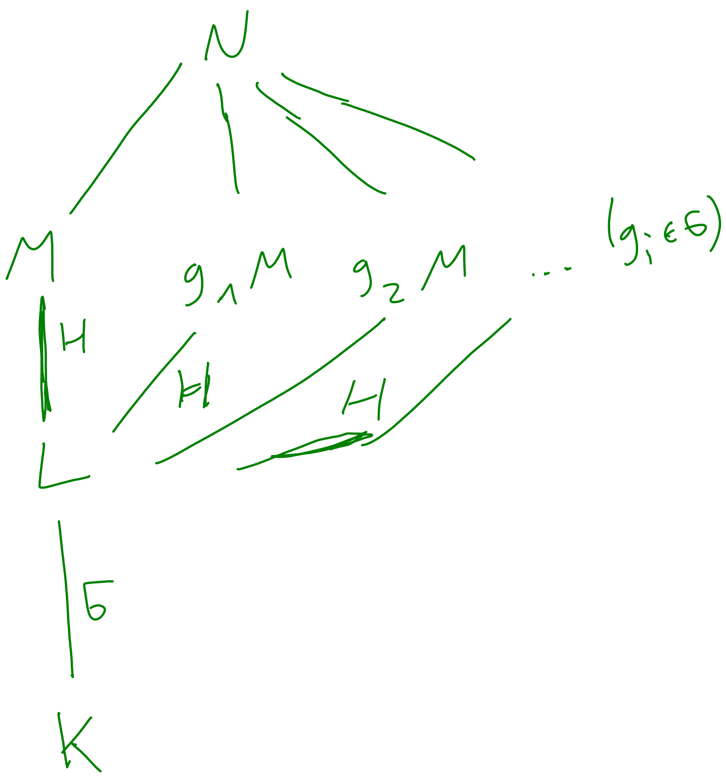


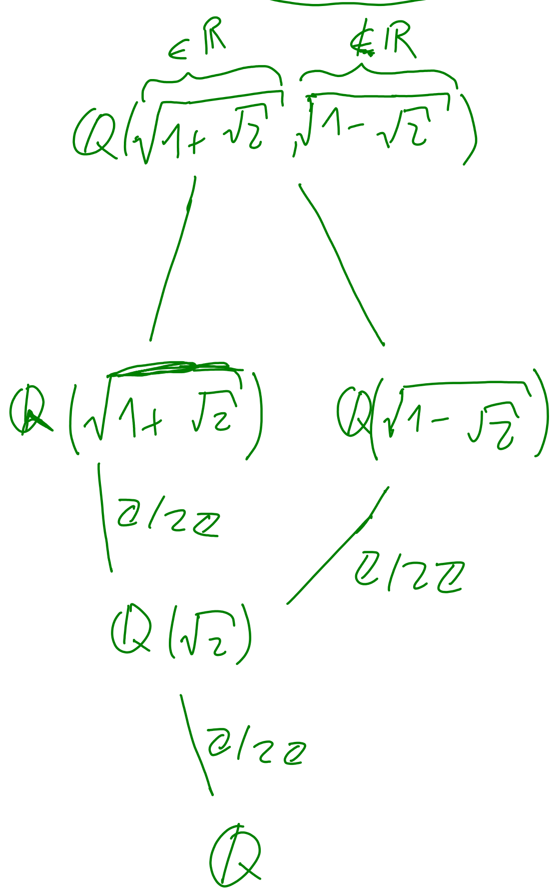
Try solving the problem for all G_{i+1}/G_i, then using induction.

Klüners proved MCS for nilpotent G when inv = disc in his habilitation: "Über die Asymptotik von Zahlkörpern mit vorgegebener Galoisgruppe".

Side remark:

Let $L|K$ be a Gal. ext. with Galois group G and let $M|L$ be a Gal. ext. with Galois group H. Let N be the Galois closure of $M|K$. Then, $\mathrm{Gal}(N|K)$ is a subgroup of the <u>wreath product</u> $H \wr G = \left(\prod_{g \in G} H\right) \underset{\text{permutation action}}{\rtimes} G$.





It is in fact a <u>transitive</u> subgroup:

The composition

$\mathrm{Gal}(N|K) \hookrightarrow H \wr G \twoheadrightarrow G$ is surjective.

(This is analoguous to the fact that the Galois group of the Galois closure of a degree n field extension is a transitive subgroup of S_n).

3. Analyze the mult. table of a G-ext. w.r.t. a normal basis (similar to what we did for cubic ext.)

(cf. Bhargava: The density of discriminants of quartic/quintic rings and fields)

4. Generalized Kummer theory

(cf. Wright-Yukie: Prehomogeneous vector spaces and field extensions)

Nonabelian group cohomology

Def Let G be a finite group. A G-group is a group A with a left action of G.

Define the group
$$H^0(G,A) = A^G = \{a \in A \mid ga = a \ \forall g \in G\}.$$

Let $Z^1(G,A)$ be the set of 1-cocycles: maps $\varphi : G \to A$ s.t. $\varphi(gh) = \varphi(g) \cdot g\varphi(h)$ $\forall g, h \in G$.

Define an action of A on $Z^1(G,A)$ by
$$(a\varphi)(g) = a \cdot \varphi(g) \cdot g a^{-1} \text{ for } a \in A, \varphi \in Z^1(G,A), g \in G.$$

The set $B^1(G,A)$ of 1-coboundaries is the A-orbit consisting of maps φ of the form $(g \mapsto a \cdot g^{-1}a)$ for some $a \in A$.

Define the pointed set $H^1(G,A) = A \backslash Z^1(G,A)$ with base point $1 = B^1(G,A)$.

[$H^2, H^3, \dots$ are problematic!]

Rmk If G acts trivially on A ($ga = a \; \forall g, a$),

then $H^0(G, A) = A$,

$$Z^1(G, A) = \mathrm{Hom}_{\text{group}}(G, A)$$

and A acts on $Z^1(G, A)$ by conjugation:

$$(a\varphi)(g) = a\,\varphi(g)\,a^{-1}.$$

$$H^1(G, A) = {}_{A}\backslash \mathrm{Hom}(G, A).$$

Rmk

You get functoriality, "truncated long exe. seq.", etc.

cf. Milne: Algebraic groups, Lie groups, and their arithmetic subgroups, chapter VI.

Nonabelian Galois cohomology

Def Let $L|K$ be a Galois ext. with Galois group G and A be a G-group such that

$$A = \bigcup_{\substack{F \subseteq L \\ \text{fin. subext. of } K}} A^{\mathrm{Gal}(L|F)} .$$

Write $H^0(L|K, A) = H^0(G, A) = A^G$.

If $L|K$ is a fin. ext., let

$$H^1(L|K, A) = H^1(G, A).$$

For infinite extensions, let

$$H^1(L|K, A) = \varinjlim_{\substack{F \subseteq L \\ \text{fin. Gal. ext. of } K}} H^1(F|K, A^{\mathrm{Gal}(L|F)}),$$

or define cocycles requiring that the map $\varphi : G \to A$ is continuous, where G comes with the Krull topology and A comes with the discrete topology.

Thm $H^1(L|K, L^\times) = 1$ (Hilbert 90)

$H^1(L|K, L) = 0$ (additive Hilbert 90)

$H^1(L|K, GL_n(L)) = 1$

(idea: $GL_n(L) = \mathrm{Aut}_L(L^n)$

$\rightsquigarrow$ el. of $H^1(L|K, GL_n(L))$ are in bij. with (n-dim.) K-vector spaces V (up to isom.) such that $V \otimes_K L \cong L^n$. But of course there is only one n-dimensional K-vector space!)

$$\boxed{\begin{array}{l} 1 \to SL_n(L) \to GL_n(L) \to L^\times \to 1 \\ 1 \to SL_n(K) \to GL_n(K) \to K^\times \\ \to H^1(SL_n(L)) \to H^1(GL_n(L)) = 1 \end{array}}$$

$\hookrightarrow H^1(L|K, SL_n(L)) = 1$

$H^1(L|K, L[G]^\times) = 1$

(idea: $L[G]^\times = \mathrm{Aut}_{\text{left } L[G]\text{-mod.}}(L[G])$

$\rightsquigarrow$ el. of $H^1(L|K, L[G]^\times)$ are in bij. with left $K[G]$-mod. V such that $V \otimes_K L \cong L[G]$. But there is only one such V, namely $V = K[G]$, by an argument similar to our pf of the normal basis thm).

Thm (Generalized Kummer Theory, cf. Wright-Yukie Prehomogeneous vector spaces and field extensions)

Let $L|K$ be a Galois ext.

Let $\mathcal{G}$ be an algebraic group defined over K

$$\left(\text{e.g. } \mathcal{G} = GL_n, SL_n, \underset{\substack{\uparrow \\ \mathbb{G}_m(K) = K^\times}}{\mathbb{G}_m}, \ldots \right)$$

let V be a variety defined over K

$$\left(\text{e.g. } V = \underset{\substack{\uparrow \\ \mathbb{A}^n(K) = K^n}}{\mathbb{A}^n} \right)$$

and consider an algebraic action of $\mathcal{G}$ on V defined over K. Assume that $H^1(L|K, \mathcal{G}(L)) = 1$. Let $v_0 \in V(K)$. Then, we obtain a bijection

$$H^1(L|K, \mathrm{Stab}_{\mathcal{G}(L)}(v_0)) \longleftrightarrow \mathcal{G}(K) \backslash \left(\mathcal{G}(L).v_0 \cap V(K) \right)$$

$$\left(\underset{\substack{\uparrow \\ \mathrm{Gal}(L|K)}}{\sigma} \longmapsto g^{-1} \sigma(g) \right) \longleftrightarrow \underset{(g \in \mathcal{G}(L))}{\mathcal{G}(K)\, g.v}$$

<u>Rmk</u> If $F := \mathrm{Stab}_{\mathcal{G}(L)}(v_0)$ is contained in $\mathcal{G}(K)$,

then $H^1(L|K, \underset{\substack{\uparrow \\ \text{trivial action} \\ \text{of } \mathrm{Gal}(L|K)}}{F}) = G \backslash \mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(L|K) \longrightarrow F)$.

If $L = K^{sep}$, then RHS $\leftrightarrow$ {nondeg. F-ext. of K}.

<u>Pf of Thm</u>

Every el. of $H^1(L|K, \mathrm{Stab})$ is of the form $(\sigma \mapsto g^{-1}\sigma(g))$ with $g \in \mathcal{G}(L)$ because the image in $H^1(L|K, \mathcal{G}(L)) = 1$ is trivial, so a 1-coboundary in $B^1(L|K, \mathcal{G}(L))$.

We have

$$\mathcal{G}(K)\, g \cdot v_0 = \mathcal{G}(K)\, g' \cdot v_0$$

$$\Updownarrow$$

$$\mathcal{G}(K)\, g\, \mathrm{Stab} = \mathcal{G}(K)\, g'\, \mathrm{Stab}$$

$$\Updownarrow$$

$$\exists\, h \in \mathcal{G}(K),\ s \in \mathrm{Stab} : g' = h g s$$

$$\Updownarrow$$

$$\exists\, s \in \mathrm{Stab} : g' s^{-1} g^{-1} \in \mathcal{G}(K).$$

$$\Updownarrow$$

$$\exists\, s \in \mathrm{Stab} : \forall \sigma : g' s^{-1} g^{-1} = \sigma(g' s^{-1} g^{-1})$$

$$\Updownarrow$$

$$\exists\, s \in \mathrm{Stab} : \forall \sigma : s^{-1} g^{-1} \sigma(g) \sigma(s) = g'^{-1} \sigma(g')$$

$$\Updownarrow$$

$$(\sigma \mapsto g^{-1}\sigma(g)) = (\sigma \mapsto g'^{-1}\sigma(g')) \text{ in } H^1(L|K, \mathrm{Stab})$$

...

$\square$

Example (Kummer Theory)

K field of $\mathrm{char}(K) \nmid n$ and $\zeta_n \in K$.

$\mathcal{G} = \mathbb{G}_m \rightsquigarrow \mathcal{G}(L) = L^\times \rightsquigarrow H^1(\Gamma_{L|K}, \mathcal{G}(L)) = 1$ by H 90

$\mathcal{V} = \mathbb{G}_m$

$\mathcal{G} \curvearrowright \mathcal{V}: \quad x \cdot y = x^n y$

$v_0 = 1 \in K^\times = \mathcal{V}(K)$

$$\mathrm{Stab}_{\mathcal{G}(K^{sep})}(v_0) = \langle \zeta_n \rangle \underset{\substack{\uparrow \\ \zeta_n \in K}}{\subseteq} \mathcal{G}(K)$$

$$\langle \zeta_n \rangle \cong C_n \quad \mathrm{char}(K) \nmid n$$

$$\mathcal{G}(K^{sep}) \cdot v_0 = (K^{sep})^{\times n} \underset{\substack{\uparrow \\ \mathrm{char}(K) \nmid n}}{=} (K^{sep})^\times .$$

Hence,

$$\{C_n\text{-ext. of } K\} \longleftrightarrow \mathcal{G}(K) \backslash \left((K^{sep})^\times \cap K^\times\right) .$$

$$= \mathcal{G}(K) \backslash K^\times$$

$$= K^{\times n} \backslash K^\times$$

Example (cubic ext.)

K any field of $\mathrm{char}(K) \neq 6$.

$\mathcal{G} = GL_2$

$\mathcal{V} = \{$ binary cubic forms $f(x,y)\}$

action $\mathcal{G} \circlearrowright \mathcal{V}$ as before:

$$(M.f)(v) = \frac{f(M^T v)}{\det(M)}$$

$v_0 = XY(X-Y)$

$$\mathrm{Stab}_{GL_2(K^{sep})}(v_0) = \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix} \right\rangle \subseteq GL_2(K)$$

$$\cong S_3$$

$$GL_2(K^{sep}).v_0 = \mathcal{V}^{disc \neq 0}(K^{sep})$$

$= \{ f \in \mathcal{V}(K^{sep}) \mid disc(f) \neq 0 \}$ is a dense subset of $\mathcal{V}(K^{sep})$. (Note that $\dim(GL_2) = 4 = \dim(\mathcal{V})$.) Hence,

$$\{S_3\text{-ext. of } K\} \leftrightarrow GL_2(K) \backslash \mathcal{V}^{disc \neq 0}(K).$$

Example (deg. 4 ext.)

k any field of char$(k) \nmid 4!$.

$\mathcal{G}' = GL_2 \times GL_3$

$$V(L) = L^2 \otimes \underbrace{Sym^2(L^3)}_{\{\text{symm. } 3\times 3\text{-matrices}\}}$$

$\mathcal{G}' \curvearrowright V$: $(M,N).(a \otimes B) = (Ma) \otimes (N B N^T)$.

This action has kernel

$$T = \{(\lambda^2 I_2, \lambda^{-1} I_3) \mid \lambda \in \mathbb{G}_m\}.$$

Let $\mathcal{G} = \mathcal{G}'/T$. $\rightsquigarrow$ $\mathcal{G} \curvearrowright V$

$$v_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 & 0 & -1 \\ 0 & 0 & 1 \\ -1 & 1 & 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & -1 \\ 0 & -1 & 0 \end{pmatrix}$$

$$\underset{\substack{\cong \\ S_4}}{\mathrm{Stab}_{\mathcal{G}(k^{sep})}(v_0)} \subseteq \mathcal{G}(k)$$

$\mathcal{G}(k^{sep}).v_0$ is a dense subset of $V(k^{sep})$

(Note that $\dim(\mathcal{G}) = 4 + 9 - 1 = 12 = 2 \cdot 6 = \dim(V)$.)

$$\{S_4\text{-ext. of } k\} \longleftrightarrow \mathcal{G}(k) \backslash \underbrace{\left(\mathcal{G}(k^{sep}).v_0 \cap V(k)\right)}_{\approx V(k)}.$$

Example (deg. 5 ext.)

$$\mathcal{G}' = GL_4 \times GL_5$$

$$V(L) = L^4 \otimes \underbrace{\mathrm{Alt}^2(L^5)}_{\{\text{skew-symm. } 5\times 5\text{-matrices}\}}$$

$\mathcal{G}' \curvearrowright V$: $(M,N).(a \otimes B) = (Ma) \otimes (NBN^T)$.

$\mathcal{G} := \mathcal{G}'/T$ where $T = \{(\lambda^2 I_4, \lambda^{-1} I_5) \mid \lambda \in \mathbb{G}_m\}$.

$$\begin{array}{c}\mathcal{G}(K)\\ \cup|\\ \mathrm{Stab}\end{array} \cong S_5$$

$$\dim(\mathcal{G}) = 16 + 25 - 1 = 40 = 4 \cdot 10 = \dim(V)$$

THE END