~~[illegible]~~

Arithmetic Statistics

1. Introduction

Typical questions

- What is the probability that a random integer is even?
  $\mathbb{P}(x \text{ even} \mid x \in \mathbb{Z}) = \frac{1}{2}$ (?)

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

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

- For a fixed pol. $f \in \mathbb{Z}[X]$,
  $\mathbb{E}(\#\{x \in \mathbb{F}_p \mid f(x) = 0\} \mid p \text{ prime}) = ?$

- For a fixed ell. curve $E/\mathbb{Q}$,
  how does $\#E(\mathbb{F}_p)$ behave for random p?

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

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

- For a fixed number field K,
  $\mathbb{P}(\mathfrak{a} \text{ principal ideal} \mid \mathfrak{a} \subseteq \mathcal{O}_K \text{ ideal}) = ?$
  $\#\{\mathfrak{a} \subseteq \mathcal{O}_K \mid \mathrm{Nm}(\mathfrak{a}) \leq T\} \sim ?$ for $T \to \infty$

- $\mathbb{P}(\mathrm{Cl}(K) = 1 \mid K \text{ (random) number field of deg. } n) = ?$
  $\#\{K \text{ number field of deg. } n \mid |\mathrm{disc}(K)| \leq T\} \sim ?$ for $T \to \infty$

- $\mathbb{P}(\mathrm{Gal}(\text{Gal. cl. of } K/\mathbb{Q}) = S_n \mid K \text{ n.f. of deg. } n) = ?$

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

  ⋮

~~1.1. Statistics~~ 1.1. Statistics

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

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

Use e.g. the uniform prob. measure unless specified otherwise.

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

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

expected value of $f(x)$:

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

(We could also assign weights $w(x) \geq 0$ and let $\mathbb{P}(x \in A \mid x \in X) = \frac{\sum_{x \in A} w(x)}{\sum_{x \in X} w(x)}$.)

If X is countable (e.g. $X = \mathbb{N}, \mathbb{Z}, \{\text{primes}\}, \{\text{n.f.}\}, \ldots$):

Intuitively, we want $\mathbb{P}(x = 1 \mid x \in \mathbb{N}) = \mathbb{P}(x = 2 \mid x \in \mathbb{N}) = \ldots = 0$.

$\Rightarrow \mathbb{P}$ can't be given by a σ-additive probability measure.

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

$$\mathbb{P}(x \in A \mid x \in X) := \lim_{T \to \infty} \mathbb{P}(x \in A \mid x \in X_T)$$

$$\mathbb{P}^{\sup} \quad = \limsup$$

$$\mathbb{P}^{\inf} \quad = \liminf$$

$$\mathbb{E}(f(x) \mid x \in X) := \lim_{T \to \infty} \mathbb{E}(f(x) \mid x \in X_T)$$

(We could again use weights.)

Rmk If $\# X = \# \mathbb{N}$ (with weights 1), then removing finitely many elements from X doesn't change $\mathbb{P}, \mathbb{E}$.

Remark a) $\mathbb{P}$ is finitely additive:

$$\mathbb{P}(x \in A_1 \sqcup \dots \sqcup A_k) = \mathbb{P}(x \in A_1) + \dots + \mathbb{P}(x \in A_k)$$

if the RHS exists

b) $\mathbb{E}$ is finitely linear

$$\mathbb{E}(\lambda_1 f_1(x) + \dots + \lambda_k f_k(x)) = \lambda_1 \mathbb{E}(f_1(x)) + \dots + \lambda_k \mathbb{E}(f_k(x)).$$

if the RHS exists

We will order $\mathbb{Z}$ or $\mathbb{N} = \{1, 2, \dots\}$ by $\mathrm{inv}(x) = |x|$.

$$\mathbb{P}(x \text{ even} \mid x \in \mathbb{N} \text{ or } \mathbb{Z}) = \lim_{T \to \infty} \mathbb{P}(x \text{ even} \mid 1 \le x \le T) = \lim \frac{\lfloor \frac{T}{2} \rfloor}{T} = \frac{1}{2}$$

$$\mathbb{P}(x \text{ square}) = 0$$

$$\mathbb{P}(x \text{ prime}) = 0 \quad \text{by the prime number theorem}$$

$$\mathbb{E}((-1)^x) = 0$$

Remark For any ~~$a \in \mathbb{Z}/m\mathbb{Z}$~~ $f : \mathbb{Z}/m\mathbb{Z} \to \mathbb{R}$,

~~$\mathbb{E}(f(a \bmod n) \mid x \in \mathbb{Z}) = \mathbb{E}(f(x) \mid x \in \mathbb{Z}/n\mathbb{Z})$~~

~~$\mathbb{P}(x \equiv a \bmod m \mid x \in \mathbb{Z}) = \frac{1}{m}$.~~

$$\mathbb{E}(f(x \bmod m) \mid x \in \mathbb{Z}) = \mathbb{E}(f(x) \mid x \in \mathbb{Z}/m\mathbb{Z})$$

More generally, if we order $\mathbb{Z}^n$ by any norm on $\mathbb{R}^n$,

~~$\mathbb{P}(x$~~ for any ~~$a \in (\mathbb{Z}/m\mathbb{Z})^n$~~, $f : (\mathbb{Z}/m\mathbb{Z})^n \to \mathbb{R}$

~~$\mathbb{P}(x \equiv a \bmod m \mid x \in \mathbb{Z}^n) = \frac{1}{m^n}$.~~

$$\mathbb{E}(f(x \bmod m) \mid x \in \mathbb{Z}) = \mathbb{E}(f(x) \mid x \in (\mathbb{Z}/m\mathbb{Z})^n).$$

1.2. Squarefree integers

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

$$\left.\begin{aligned} \mathbb{P}(4 \nmid x) &= 1 - \tfrac{1}{4} \\ \mathbb{P}(9 \nmid x) &= 1 - \tfrac{1}{9} \end{aligned}\right\} \underset{\text{CRT}}{\Rightarrow} \mathbb{P}(4, 9 \nmid x) = (1 - \tfrac{1}{4})(1 - \tfrac{1}{9})$$

$$\mathbb{P}(4, 9, 25 \nmid x) = (1 - \tfrac{1}{4})(1 - \tfrac{1}{9})(1 - \tfrac{1}{25})$$

$\vdots$

~~This is calle~~

$\rightsquigarrow$ Guess:

Thm 1.2.1 $\mathbb{P}(x \text{ squarefree}) = \prod_p \left(1 - \frac{1}{p^2}\right) = \frac{1}{\zeta(2)} \approx 0.61$

Rmk This process ~~[illegible]~~, considering more and more primes is ~~The above~~ called a <u>sieve</u>.

The above argument shows "$\le$":

For any $B > 0$,

$$\mathbb{P}^{\sup}(x \text{ squarefree}) \le \mathbb{P}(p^2 \nmid x \ \forall p \le B) \underset{\text{CRT}}{=} \prod_{p \le B} \left(1 - \frac{1}{p^2}\right) \xrightarrow{B \to \infty} \prod_p \left(1 - \frac{1}{p^2}\right).$$

More generally:

Rmk 1.2.2 For every prime p, let $e_p \ge 0$ and $A_p \subseteq (\mathbb{Z}/p^{e_p}\mathbb{Z})^n$.

$$\Rightarrow \mathbb{P}^{\sup}(x \bmod p^{e_p} \in A_p \forall p \mid x \in \mathbb{Z}^n) \le \prod_p \mathbb{P}(x \in A_p \mid x \in (\mathbb{Z}/p^{e_p}\mathbb{Z})^n).$$

But "$\geq$" is tricky because ~~there is no~~ the CRT with ∞ many primes fails badly:

Exe (sieve theory nightmare: conspiracy of primes)

Let $p_1, p_2, \ldots$ be the prime numbers.

We'd expect $\mathbb{P}(x \not\equiv i \bmod p_i^2 \ \forall i) = \prod_i \mathbb{P}(x \not\equiv i \bmod p_i^2)$

$$= \prod \left(1 - \frac{1}{p_i^2}\right) \approx 0.61.$$

But actually there is no such $x \in \mathbb{N}$ because always $x \equiv x \bmod p_x^2$.

Proof 1 of "$\geq$"

$$\mathbb{P}^{\inf}(x \text{ squarefree}) \geq \mathbb{P}(p^2 \nmid x \ \forall p \leq B) - \mathbb{P}^{\sup}(p^2 \mid x \text{ for some } p > B)$$

$\mathbb{P}(p^2 \nmid x \ \forall p \leq B) \xrightarrow{B \to \infty} \prod_p \left(1 - \frac{1}{p^2}\right)$

$\mathbb{P}^{\sup}(p^2 \mid x \text{ for some } p > B) \xrightarrow{B \to \infty}$ Goal: 0

[Note: There are ∞ many $p > B$, so we can't use additivity on the RHS!]

Indeed,

$$\mathbb{P}^{\sup}(p^2 \mid x \text{ for some } p > B) = \limsup_{T \to \infty} \underbrace{\mathbb{P}(\cdots \mid 1 \leq x \leq T)}_{\leq \sum_{B < p \leq \sqrt{T}} \underbrace{\mathbb{P}(p^2 \mid x \mid 1 \leq x \leq T)}_{\frac{\lfloor T/p^2 \rfloor}{T} \leq \frac{1}{p^2} \text{ (careful!)}} \leq \sum_{B < p \leq \sqrt{T}} \frac{1}{p^2} \leq \frac{1}{B}} \leq \frac{1}{B} \xrightarrow{B \to \infty} 0$$

$\square$

Pf 2 of Thm

Use Möbius inversion:

$$\#\{x \le T \text{ sqfree}\} = \#\{x \le T\} - \#\{x \le T : 4 \mid x\} - \#\{x \le T \mid 9 \mid x\} - \dots + \#\{x \le T \mid 4 \cdot 9 \mid x\} + \dots \mp \dots$$

$$= \sum_{1 \le d \le \sqrt{T}} \mu(d) \cdot \underbrace{\#\{x : d^2 \mid x\}}_{\left\lfloor \frac{T}{d^2} \right\rfloor = \frac{T}{d^2} + O(1)}$$

$$= \dots = \underbrace{\left(\sum_{d \ge 1} \frac{\mu(d)}{d^2} \right)}_{\prod_p \left(1 - \frac{1}{p^2}\right)} \cdot T + O(T^{1/2})$$

□

Pf 3 of Thm

Let $a_n := \begin{cases} 1, & n \text{ sqfree} \\ 0, & \text{otherwise} \end{cases}$

$$\sum_{n \ge 1} \frac{a_n}{n^s} = \prod_p \left(1 + \frac{1}{p^s}\right) = \prod_p \frac{1 - \frac{1}{p^{2s}}}{1 - \frac{1}{p^s}} = \frac{\zeta(s)}{\zeta(2s)}$$ has rightmost pole

at $s = 1$ with residue $\frac{1}{\zeta(2)}$.

By Wiener–Ikehara, $\underbrace{\sum_{n \le T} a_n}_{= \#\{n \le T \text{ sqfree}\}} \sim \frac{1}{\zeta(2)} \cdot T$ for $T \to \infty$

□

<u>Conjecture</u>

Let $f \in \mathbb{Z}[x]$ be a nonconstant polynomial. Then,

$$\mathbb{P}_{x \in \mathbb{Z}}\left(f(x) \text{ squarefree}\right) = \prod_p \mathbb{P}_{x \in \mathbb{Z}/p^2\mathbb{Z}}\left(p^2 \nmid f(x)\right).$$

("$\leq$" is trivial)

This is known for:

$\deg(f) \leq 2$ (similar proof)

$\deg(f) = 3$ (Hooley, 1967)

$\deg(f)$ arbitrary assuming the ABC conjecture (Granville, 1998)

~~The upper bound is~~

Notation

$f(x, \varepsilon) \ll_\varepsilon g(x, \varepsilon)$

$\Leftrightarrow f(\ldots) = O_\varepsilon(\ldots)$

$\Leftrightarrow \exists C(\varepsilon) > 0 : \forall x : \ |f(x, \varepsilon)| \leq C(\varepsilon) \cdot g(x, \varepsilon).$

e.g. $100 T^{1/2} \ll T$ for large T

$\lfloor T \rfloor = T + O(1)$

$f \asymp g$ means: $f \ll g$ and $g \ll f$.

$f(x) \sim g(x)$ as $x \to \infty$ means: $\frac{f(x)}{g(x)} \xrightarrow{x \to \infty} 1$

$f(x) = o_{x \to \infty}(g(x))$ means: $\frac{f(x)}{g(x)} \xrightarrow{x \to \infty} 0$

2. Random primes

Thm 2.1
(PNT for arithmetic progressions)

For any $a \in (\mathbb{Z}/n\mathbb{Z})^\times$,

$$\mathbb{P}_{p \text{ prime}}(p \equiv a \bmod n) = \frac{1}{\varphi(n)} = \frac{1}{\#(\mathbb{Z}/n\mathbb{Z})^\times}.$$

~~Thm 2.2 (Chebotarev density thm)~~

Let $L|K$ be a fin. Gal. ext. with Gal group G.

~~For any unram. primes $\mathfrak{P}|\mathfrak{p}$ of $L|K$, Frob~~
~~we have a~~

For any unram. prime $\mathfrak{p}$ of K,

$$\mathrm{Frob}(\mathfrak{p}) := \{\mathrm{Frob}(\mathfrak{P}|\mathfrak{p}) : \mathfrak{P}|\mathfrak{p} \text{ prime of } L\}$$

is a conj. class of G.

Thm 2.2 (Chebotarev density theorem)

For any conj. cl. C,

$$\mathbb{P}_{\mathfrak{p} \text{ prime of } K}(\mathrm{Frob}(\mathfrak{p}) = C) = \frac{\#C}{\#G}$$

(unram.)

if we order the $\mathfrak{p}$ by $\mathrm{inv}(\mathfrak{p}) := \mathrm{Nm}(\mathfrak{p})$.

Informally: pick $\mathfrak{p}$ and then pick a random $\mathfrak{P}|\mathfrak{p}$

$$\mathbb{P}(\mathrm{Frob}(\mathfrak{P}|\mathfrak{p}) = g) = \frac{1}{\#G}.$$

Rmk If $K = \mathbb{Q}$, $L = \mathbb{Q}(\zeta_n)$, $\mathrm{Gal}(L|K) \cong (\mathbb{Z}/n\mathbb{Z})^\times$,
$(\zeta_n \mapsto \zeta_n^a) \leftrightarrow a$

then $\mathrm{Frob}(p) = (p \bmod n)$, so Thm 2.1 is a special case.

Def ~~Let L/K be an ext. of number field~~ ~~Let $f \in K$ ...~~

a) A (sqfree) pol. $f \in K[X]$ of deg. n has *splitting type* $(k_1, \dots, k_r)$ if $f = f_1 \cdots f_r$ for distinct irreducible $f_1, \dots, f_r \in K[X]$ of degrees $k_1, \dots, k_r$.

b) An unram. prime $\mathfrak{q}$ of a number field K has *splitting type* $(k_1, \dots, k_r)$ in a degree n ext. $L|K$ if $\mathfrak{q}\mathcal{O}_L = \mathfrak{P}_1 \cdots \mathfrak{P}_r$ for distinct primes $\mathfrak{P}_1, \dots, \mathfrak{P}_r$ of inertia degrees $k_1, \dots, k_r$.

Rmk splitting type (n): a) irreducible b) inert
$(1, \dots, 1)$: splits completely

Thm 2.3 Let K be a n.f., $f \in \mathcal{O}_K[X]$ a monic irred. pol, $\alpha \in \overline{K}$ a root of f, $L = K(\alpha)$, $\mathfrak{q}$ a prime of K $\nmid [\mathcal{O}_L : \mathcal{O}_K[\alpha]]$.
Then, $(f \bmod \mathfrak{q}) \in (\mathcal{O}_K/\mathfrak{q})[X]$ has spl. type $(k_1, \dots, k_r)$ iff $\mathfrak{q}$ has spl. type $(k_1, \dots, k_r)$ in L.

Def A permutation $\pi \in S_n$ has *cycle type* $(k_1, \dots, k_r)$ if it consists of cycles of lengths $k_1, \dots, k_r$ (with $k_1 + \dots + k_r = n$).

Exe $(1\,2\,3)(4\,5)(6\,7)(8) \in S_8 \rightsquigarrow (3,2,2,1)$.

Rmk cycle type (n): single n-cycle
$(1, \dots, 1)$: identity

Lemma 2.4 Let $k_1+\dots+k_r=n$ and let c_l the nr. of times l occurs among $k_1,\dots,k_r$.

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

Ex $\mathbb{P}(\pi \text{ is } n\text{-cycle}) = \frac{1}{n}$, $\mathbb{P}(\pi = id) = \frac{1}{n!}$

Pf The perm. with cycle type $(k_1,\dots,k_r)$ form a conj. cl. of S_n, i.e. an orbit of the conj. action $G \curvearrowright G$.

$$\Rightarrow \mathbb{P}(\dots) = \frac{\#\text{the orbit}}{\#G} = \boxed{\frac{1}{\#\text{Stab}}} = \frac{1}{\prod l^{c_l}\cdot c_l!}$$

This will keep coming up!

How many ways to renumber without changing perm.?
can rotate each cycle $\rightsquigarrow l^{c_l}$
can permute cycles $\rightsquigarrow c_l!$

$\square$

The splitting type of $\mathfrak{q}$ can be determined from $\mathrm{Frob}(\mathfrak{q})$:

Lemma 2.5 Let $M|L|K$ be n.f., $M|K$ Galois, $n=\deg(L|K)$, $G=\mathrm{Gal}(M|K)$, $H=\mathrm{Gal}(M|L)$.

G acts on G/H (the n-element set) by left mult., so interpret el. of G as permutations in S_n.

$\Rightarrow$ splitting type of unram. prime $\mathfrak{q}$ of K in L = cycle type of $\mathrm{Frob}(\mathfrak{q})$.
(only depends on conj. cl!)

The Chebotarev density thm then implies:

<u>Thm 2.6</u> Let $f \in \mathcal{O}_K(x)$ be a monic {irreducible} pol. of degree n with Galois group $G \hookrightarrow S_n$ (the embedding is given by the action of G on the n roots of f).

$$\mathbb{P}_{\mathfrak{p}}\left(f \bmod \mathfrak{p} \text{ has splitting type } (k_1,\dots,k_r)\right)$$

$$= \mathbb{P}_{\pi \in G}\left(\pi \text{ has cycle type } (k_1,\dots,k_r)\right).$$

<u>Cor 2.7</u>

$$\mathbb{E}_{\mathfrak{p}}(\#\text{ roots of } f \bmod \mathfrak{p}) = 1$$

<u>Pf</u> HW $\square$

3. Random polynomials

3.1. Over finite fields

~~[illegible]~~

~~For a random pol.~~

~~fixed q and~~

~~For a fixed finite field $\mathbb{F}_q$ and a random monic pol. $f \in \mathbb{F}_q[X]$~~

~~of degree n, one can ask~~

Thm 3.1.1 (Chebotarev's baby sibling)

$$\underbrace{\lim_{q \to \infty} \mathbb{P}_{\substack{f \in \mathbb{F}_q[X] \\ \text{monic} \\ \text{of degree } n}} \left(f \text{ has splitting type } (k_1, \dots, k_r) \right)}$$

One can certainly compute this, but the answer gets cleaner in the limit $q \to \infty$

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

~~First~~ [We first show two examples:]

Ex A $\lim \mathbb{P}$ (f splits completely) $= \frac{1}{n!}$

Pf of Ex s.c.: $f(X) = (X-a_1) \cdots (X-a_n)$ with $a_1, \dots, a_n \in \mathbb{F}_q$

$$\mathbb{P}(\dots) = \frac{\binom{q}{n}}{q^n} = \underbrace{\frac{q}{q} \cdot \frac{q-1}{q} \cdots \frac{q-n+1}{q}}_{\xrightarrow{q \to \infty} 1} \cdot \frac{1}{n!}$$

$\square$

Exe[B] $\lim \mathbb{P}(f \text{ irreducible}) = \frac{1}{n}$

Pf of Exe Let $I_n := \{\text{irred. monic deg } n \text{ pol}\}$

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

$$\Rightarrow \quad q^n = \sum_{d \mid n} d \cdot \# I_d$$

$$\Rightarrow \quad 1 = \sum_{d \mid n} d \cdot \underbrace{\frac{\# I_d}{q^n}}_{\substack{\to 0 \text{ unless } d = n \\ (\text{because } \# I_d \leq q^d)}} \xrightarrow{q \to \infty} n \cdot \underbrace{\frac{\# I_d}{q^n}}_{\mathbb{P}(\cdots)}$$

$\square$

Rmk $n \cdot \# I_n = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) \cdot q^d$ by Möbius inversion.

[You can see in those two exe that things are uglier before the limit.]

Pf of Thm ~~...~~

With the notation from Lemma 2.4:

$\mathbb{P}($ splitting type $(k_1,\dots,k_r))$

$$\underset{\substack{\uparrow \\ \text{need to choose } c_\ell \\ \text{irreducible factors of} \\ \text{degree } \ell}}{=} \frac{1}{q^n} \prod_{\ell=1}^{n} \binom{\# I_\ell}{c_\ell} \underset{\substack{\uparrow \\ n = k_1+\dots+k_r \\ = \sum \ell c_\ell}}{=} \prod_{\ell=1}^{n} \frac{1}{q^{\ell c_\ell}} \binom{\# I_\ell}{c_\ell}$$

$$= \prod_\ell \underbrace{\frac{\# I_\ell}{q^\ell}}_{\substack{\downarrow \text{ by Ex B} \\ \frac{1}{\ell}}} \cdots \underbrace{\frac{\# I_\ell - c_\ell + 1}{q^\ell}}_{\substack{\downarrow \\ \frac{1}{\ell}}} \cdot \frac{1}{c_\ell!} \longrightarrow \prod_\ell \frac{1}{\ell^{c_\ell} c_\ell!} = \mathbb{P}(\text{cycle type}(k_1,\dots,k_r))$$

$\square$

Cor 3.1.2 $\lim \mathbb{P}(f \text{ squarefree}) = 1$

Pf $\mathbb{P}(\text{squarefree}) = \sum_{(k_1,\dots,k_r)} \mathbb{P}(\text{splitting type}(k_1,\dots,k_r))$

$$= \sum_{(k_1,\dots,k_r)} \mathbb{P}(\text{cycle type}(k_1,\dots,k_r)) = 1$$ $\square$

[another ~~...~~ pf: f sqfree $\Leftrightarrow$ $\mathrm{disc}(f) \neq 0$]

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

3.2. Over $\mathbb{Z}$

~~Identify monic pol. $f \in \mathbb{Z}[X]$ of degree n with vectors in~~

Identify $\{\text{monic deg. } n \text{ pol. } f \in \mathbb{Z}[X]\}$ with $\mathbb{Z}^n$

$$X^n + a_{n-1}X^{n-1} + \dots + a_0 \qquad (a_{n-1}, \dots, a_0)$$

and order them by any norm on $\mathbb{R}^n$.

Thm 3.2.1

$$\mathbb{P}_{\substack{f \in \mathbb{Z}[X] \\ \text{monic} \\ \text{degree } n}} (f \text{ has Galois group } S_n) = 1$$

i.e.: f is irred. and the Galois closure of $\mathbb{Q}[X]/f(X)$ over $\mathbb{Q}$ has group S_n

Lemma 3.2.2

$$\mathbb{P}(f \bmod p \text{ doesn't have splitting type } (k_1, \dots, k_r) \text{ for any } p) = 0$$

[as long as $k_1 + \dots + k_r = n$]

Pf $\quad \text{LHS} \leq \prod_p (1 - \underbrace{\mathbb{P}(\text{has splitting type } (k_1, \dots, k_r) \bmod p)}_{\xrightarrow{p \to \infty} \mathbb{P}_{\pi \in S_n}(\text{cycle type } (k_1, \dots, k_r)) > 0}) = 0$

(by Thm 3.1.1)

$\square$

Pf of Thm

~~G must contain~~

Recall:
If $f \bmod p$ has splitting type $(k_1, \dots, k_r)$, then $\mathrm{Frob}(p) \in \mathrm{Gal}(f)$ has cycle type $(k_1, \dots, k_r)$.

$\Rightarrow$ With prob. 1, $\mathrm{Gal}(f) \subseteq S_n$ contains an element of every cycle type.

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

Rmk Using the large sieve (cf. Serre: Lectures on the Mordell–Weil Theorem, Chapter 12), one can show:

$$\#\{ f \in \mathbb{Z}[x] \text{ monic deg } n \mid f \text{ has Gal. grp. } \neq S_n \text{ and } \|f\| \leq T \}$$

$$\ll T^{n-\frac{1}{2}} \log T,$$

whereas

$$\#\{ f \in \mathbb{Z}[x] \text{ monic deg } n \mid \|f\| \leq T \} \asymp T^n .$$

<u>Rmk</u> Using the Lang-Weil bound / étale cohomology, one can

Chebotarev's sister

also deal with families of special polynomials.

For example: (you can show this without Lang-Weil!)
The pol. $f_T(X) = X^3 - TX + (T-3)X + 1$ has Gal. grp. $A_3 \subseteq S_3$ over $\mathbb{Q}(T)$.
For any $t \in \mathbb{F}_q$, the pol. $f_t(X) = X^3 - tX + (t-3)X + 1$ has

Galois group 1 (=splits completely) or A_3 (irreducible), if f_t

is sqfree.

$$\lim_{q\to\infty} \mathbb{P}_{t\in\mathbb{F}_q}(f_t \text{ splits completely}) = \mathbb{P}_{\pi\in A_3}(\pi = id) = \frac{1}{3}$$

$$\lim_{q\to\infty} \mathbb{P}\,(f_t \text{ irreducible}) = \mathbb{P}(\pi \neq id) = \frac{2}{3}.$$

$$\mathbb{P}_{t\in\mathbb{Z}}(f_t \text{ irred. with Gal. grp } A_3) = 1$$

4. Lattices

~~4.1. Successive minima~~

Def A rank r lattice in $\mathbb{R}^n$ is a subgr. Λ generated by r linearly indep. vectors $\underbrace{b_1,\dots,b_r}_{\text{basis of } \Lambda} \in \mathbb{R}^n$.

A full lattice in $\mathbb{R}^n$ is a rank n lattice.

The covolume of a full lattice is $\mathrm{covol}(\Lambda) = \left|\det\begin{pmatrix} -b_1- \\ \vdots \\ -b_n- \end{pmatrix}\right|$

$$= \mathrm{vol}\Big(\underbrace{\{x_1 b_1 + \dots + x_n b_n \mid 0 \le x_i < 1\ \forall i\}}_{\text{a fundamental cell of } \Lambda}\Big)$$

4.1. Successive minima

Let $D(R) := \{x \in \mathbb{R}^n : |x| \le R\}$.

Def Fix a norm $|\cdot|$ on $\mathbb{R}^n$. For $i = 1, \dots, r$, the <u>i-th successive minimum</u> of a rank r lattice Λ is $\lambda_i(\Lambda) := \min\{t \geq 0 \mid \exists\, v_1, \dots, v_i \in \Lambda$ linearly indep. of norm $\le t\}$.

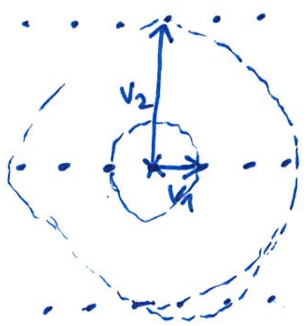
(w.r.t. $|\cdot|$)

Rmk a) $0 < \lambda_1 \le \dots \le \lambda_n$

b) There are lin. indep. vectors $v_1, \dots, v_n \in \Lambda$ with $|v_i| = \lambda_i \quad \forall i$.
(Such a basis $(v_1, \dots, v_n)$ is a <u>directional basis</u> w.r.t. $\Lambda, |\cdot|$.)

c) If $\lambda'_1, \dots, \lambda'_n$ are the succ. min. w.r.t. $|\cdot|'$, then $\lambda_i \asymp_{|\cdot|, |\cdot|'} \lambda'_i \ \forall i$ by the equivalence of norms.

<u>Warning</u> For $n \ge 3$, there might be no directional basis that spans Λ! (HW)



Let $K = D(1)$.

Rmk a) K is compact convex centrally symmetric set.

b) For any cpt. conv c.s. set $K \subset \mathbb{R}^n$, there is a norm:
$|v| := \min\{t \ge 0 \mid v \in tK\}$.

[Well-known:]

Thm 4.1.1 (Minkowski's first ~~theorem~~) Let Λ be a full lattice.

If $\dfrac{\mathrm{vol}(K)}{2^n \cdot \mathrm{covol}(\Lambda)} \geq 1$, then $\lambda_1(\Lambda) \leq 1$.

(i.e. $\exists\, 0 \neq v \in \Lambda \cap K$)

This is a corollary of:

Thm 4.1.2 (Minkowski's second) Let Λ be a full lattice.

$$\frac{1}{n!} \leq \lambda_1 \cdots \lambda_n \cdot \frac{\mathrm{vol}(K)}{2^n \cdot \mathrm{covol}(\Lambda)} \leq 1.$$

In particular, $\lambda_1 \cdots \lambda_n \asymp_n \dfrac{\mathrm{covol}(\Lambda)}{\mathrm{vol}(K)}$. ["nearly orthogonal vectors"]

Pf $\frac{1}{n!} \leq \ldots$

Let $v_1, \ldots, v_n$ be a directional basis.

$\Lambda \supseteq \Lambda' :=$ lattice spanned by $v_1, \ldots, v_n$.

$\mathrm{covol}(\Lambda) \leq \mathrm{covol}(\Lambda')$

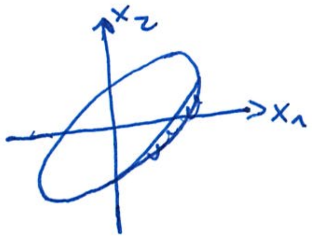
$K \supseteq K' :=$ convex hull of $\pm \frac{v_1}{\lambda_1}, \ldots, \pm \frac{v_n}{\lambda_n}$.

$$\mathrm{vol}(K) \geq \mathrm{vol}(K') = \frac{2^n}{n!} \cdot \det \begin{pmatrix} - v_1/\lambda_1 - \\ \vdots \\ - v_n/\lambda_n - \end{pmatrix} = \frac{2^n\, \mathrm{covol}(\Lambda')}{n!\, \lambda_1 \cdots \lambda_n} \geq \frac{2^n\, \mathrm{covol}(\Lambda)}{n!\, \lambda_1 \cdots \lambda_n}$$

$\ldots \leq 1$

W.l.o.g. $v_1, \ldots, v_n$ are the standard basis of $\mathbb{R}^n$.

Let $U = B(1) = \{v \in \mathbb{R}^n : |v| < 1\}$.



We might try to scale U by a factor λ_i in the i-th coordinate direction, but that won't quite work! Instead, we apply an ingenious nonlinear transformation h.

Claim There is a cont. fct. $h : U \to \mathbb{R}^n$ such that for $i = 1, \ldots, n$:

a) The i-th coord. of $h(x_1, \ldots, x_n)$ is $\lambda_i x_i + g_i(x_{i+1}, \ldots, x_n)$ for some fct. $g_i : \mathbb{R}^{n-i} \to \mathbb{R}$.

b) $h(x_1, \ldots, x_n) \in \lambda_i U + g_i'(x_{i+1}, \ldots, x_n)$ for some fct. $g_i' : \mathbb{R}^{n-i} \to \mathbb{R}^n$.

This suffices:

a) $\Rightarrow \operatorname{vol}(h(U)) = \lambda_1 \cdots \lambda_n \cdot \operatorname{vol}(U) = \lambda_1 \cdots \lambda_n \operatorname{vol}(K)$.

Let $a \neq b \in U$, say $a_i \neq b_i$, $a_{i+1} = b_{i+1}, \ldots, a_n = b_n$.

$$\left.\begin{array}{l} \text{By a), the } i\text{-th coord. of } p(a,b) := \dfrac{h(a) - h(b)}{2} \\ \quad \text{is } \lambda_i(a_i - b_i) \neq 0. \\ \text{By b) and the triangle ineq., } |p(a,b)| < \lambda_i \end{array}\right\} \Rightarrow p(a,b) \notin \Lambda \text{ by def. of succ. min.}$$

$\Rightarrow$ No two points in $U' := \frac{h(U)}{2}$ differ by an el. of Λ.

$$\Rightarrow \operatorname{vol}(U') \leq \operatorname{covol}(\Lambda)$$

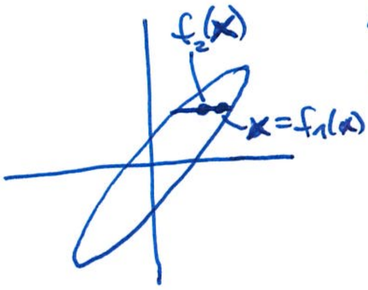
$$\operatorname{vol}(U') = \frac{\lambda_1 \cdots \lambda_n}{2^n} \cdot \operatorname{vol}(K)$$

To prove the claim:

Let $S_i := \mathbb{R}v_1 + \dots + \mathbb{R}v_i$.

Let $f_i : U \longrightarrow U$

$x \longmapsto$ centroid of the convex set $U \cap (x + S_{i-1})$



$f_i(a)$ only depends on $a_i, \dots, a_n$ and the last coord of $f_i(a)$ are $a_i, \dots, a_n$.

Let $h : U \longrightarrow \mathbb{R}^n$

$x \longmapsto \lambda_1 f_1(x) + (\lambda_2 - \lambda_1) f_2(x) + \dots + (\lambda_n - \lambda_{n-1}) f_n(x)$

The last $n-i$ summands only depend on $x_{i+1}, \dots, x_n$.

a): The i-th coord. of the first i summands sum to

$$\lambda_1 x_i + (\lambda_2 - \lambda_1) x_i + \dots + (\lambda_i - \lambda_{i-1}) x_i = \lambda_i x_i$$

b): The sum of the first i summands has norm

$< \lambda_1 + (\lambda_2 - \lambda_1) + \dots + (\lambda_i - \lambda_{i-1}) = \lambda_i$ by the triangle inequality because $|x| < 1$ (as $x \in U$). $\square$

Lemma 4.1.3 Let $\Lambda' \subseteq \Lambda$ be the lattice spanned by a directional basis $(v_1, \dots, v_n)$ of Λ.

Then, $[\Lambda : \Lambda'] \leq n!$

Pf HW $\square$

Lemma 4.1.4 There is a basis $(b_1,\dots,b_n)$ of Λ with $|b_i| \asymp_n \lambda_i(\Lambda)$.

Pf Construct $b_1,\dots,b_n$ iteratively. Assume we've constructed $b_1,\dots,b_{i-1}\in\Lambda$ so that the rank $i-1$ lattice $\Lambda\cap(\mathbb{R}b_1+\dots+\mathbb{R}b_{i-1})$ is spanned by $b_1,\dots,b_{i-1}$. ~~Let $b_1,\dots,b_i$ be a basis of~~

Let $v\in\Lambda$ be lin. indep. from $b_1,\dots,b_{i-1}$ with $|v|=\lambda_i$.

Let $b_1,\dots,b_i$ be a basis of $\Lambda\cap(\mathbb{R}b_1+\dots+\mathbb{R}b_{i-1}+\mathbb{R}v)$

Write $b_i = x_1b_1+\dots+x_{i-1}b_{i-1}+yv$.

$$\left.\begin{array}{l}\text{W.l.o.g. } 0\le x_i<1.\\ v\in\Lambda \Rightarrow \frac{1}{y}\in\mathbb{Z}\Rightarrow |y|\le 1\end{array}\right\}\Rightarrow |b_i|\le|b_1|+\dots+|b_{i-1}|+|v|$$
$$=\lambda_1+\dots+\lambda_{i-1}+\lambda_i\le i\cdot\lambda_i\ll_n\lambda_i.$$

□

Lemma 4.1.5 Let $(v_1,\dots,v_n)$ be a ~~directional~~ basis of Λ with $|b_i|\asymp\lambda_i$.

Let $w=x_1v_1+\dots+x_nv_n$ $\quad(x_1,\dots,x_n\in\mathbb{R})$.

Then, $\cancel{|x_i|\ll_n \frac{|w|}{\lambda_i}}$ $|w|\asymp_{n,|\cdot|}\max(|x_1|\lambda_1,\dots,|x_n|\lambda_n)$
$\asymp_n |x_1|\lambda_1+\dots+|x_n|\lambda_n$.

Pf "$\ll$": triangle inequality
"$\gg$": Cramer's rule:

$$x_i=\frac{\det\begin{pmatrix}| & & | & | & | & & |\\ v_1 & \cdots & v_{i-1} & w & v_{i+1} & \cdots & v_n\\ | & & | & | & | & & |\end{pmatrix}}{\det\begin{pmatrix}| & & |\\ v_1 & \cdots & v_n\\ | & & |\end{pmatrix}}$$

$$\Rightarrow |x_i|\le\frac{|v_1|\cdots|v_{i-1}|\,|w|\,|v_{i+1}|\cdots|v_n|}{\operatorname{covol}(\Lambda)}=\underbrace{\frac{\lambda_1\cdots\lambda_n}{\operatorname{covol}(\Lambda)}}_{\asymp 1}\cdot\frac{|w|}{\lambda_i}$$

□

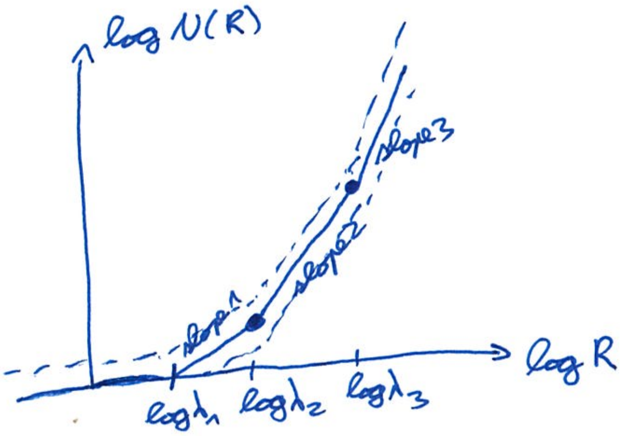
4.2. Counting lattice points

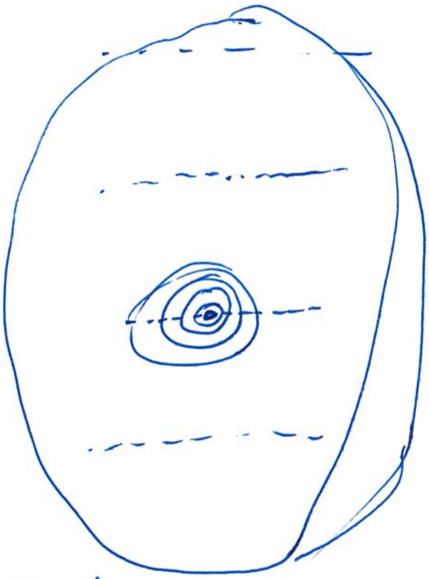
Thm 4.2.1.

For any $R \geq 0$:

$$N(R) := \#(\Lambda \cap B(R)) \asymp_{n,|\cdot|} \max_{0 \leq i \leq n} \left(\frac{R}{\lambda_1} \cdots \frac{R}{\lambda_i} \right)$$

$$= \begin{cases} 1, & R < \lambda_1 \\ \frac{R}{\lambda_1} \cdots \frac{R}{\lambda_i}, & \lambda_i \leq R < \lambda_{i+1} \\ \frac{R}{\lambda_1} \cdots \frac{R}{\lambda_n}, & \lambda_n \leq R \end{cases}$$





Pf Choose a basis $(b_1, \ldots, b_n)$ as before and write $w = x_1 b_1 + \ldots + x_n b_n$.

$$\left(|w| \leq R \Rightarrow |x_i| \ll \frac{R}{\lambda_i} \ \forall i \right) \Rightarrow \#\{w\} \ll \left(\frac{R}{\lambda_1}+1\right) \cdots \left(\frac{R}{\lambda_n}+1\right)$$

$$\left(|x_i| \ll \frac{R}{\lambda_i} \ \forall i \Rightarrow |w| \leq R \right) \Rightarrow \#\{w\} \gg \left(\frac{R}{\lambda_1}+1\right) \cdots \left(\frac{R}{\lambda_n}+1\right)$$

$$\boxed{\#\{x_i \in \mathbb{Z} \mid |x_i| \leq r\} \asymp 1 + r \text{ for all } r \geq 0}$$

$$\asymp \max_{0 \leq i \leq n} \left(\frac{R}{\lambda_1} \cdots \frac{R}{\lambda_i} \right) \quad \square$$

Thm 4.2.2 (Davenport's Lemma)

[Reference: Davenport: On a principle of Lipschitz
(+ corrigendum)]

(Let $C \geq 1$.) Let $A \subseteq \mathbb{R}^n$ be a (semialgebraic) set defined by at most C polynomial inequalities $F_i(x_1, \dots, x_n) \geq 0$, each of (total) degree $\leq C$.

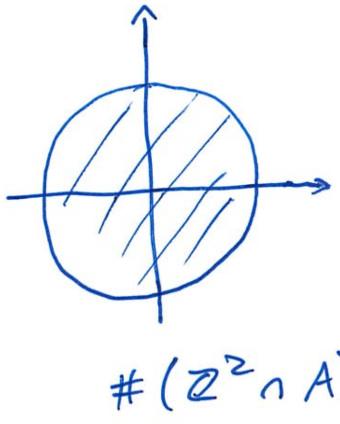
For every subset $S = \{i_1, \dots, i_k\}$ of $\{1, \dots, n\}$, let

$$\pi_S : \mathbb{R}^n \longrightarrow \mathbb{R}^k, \quad (x_1, \dots, x_n) \longmapsto (x_{i_1}, \dots, x_{i_k})$$

[the proj. that forgets the coordinates not in S]

Then,
$$\#(\mathbb{Z}^n \cap A) = \mathrm{vol}_n(A) + O_C\Big(\sum_{\substack{S \subsetneq \{1,\dots,n\} \\ \#S = k}} \mathrm{vol}_k(\pi_S(A))\Big).$$

Ese $A = \{(x, y) \mid x^2 + y^2 \leq R^2\}$



$\mathrm{vol}_2(A) = \mathrm{area}(A) = \pi R^2$

$\pi_{\{1\}}(A) = [-R, R] \subseteq \mathbb{R}^1 \rightarrow O(R)$

$\pi_{\{2\}}(A) = [-R, R] \subseteq \mathbb{R}^1 \rightarrow O(R)$

$\pi_{\emptyset}(A) = \{*\} \subseteq \mathbb{R}^0 \rightarrow O(1)$

$$\#(\mathbb{Z}^2 \cap A) = \pi R^2 + O(R+1)$$

important if $R \to 0$.

Idea of proof, illustrated by this example

Let $I_{x_1} = \{ y \in \mathbb{R} \mid x_1^2 + y^2 \leq R^2 \}$

$$\#(\mathbb{Z}^2 \cap A) = \sum_{\substack{x_1 \in \mathbb{Z}: \\ |x_1| \leq R}} \#(I_{x_1} \cap \mathbb{Z})$$

$$= \sum_{\substack{x \in \mathbb{Z}: \\ |x| \leq R}} \left(\int_{I_x} dy + O(1) \right)$$

$$= \sum_x \int_{I_x} dy + O(R+1)$$

$$= \int_{-R}^{R} \int_{I_x} dy\,dx + O(R+1)$$

$$= \pi R^2 + O(R+1).$$

□

Rmk The general proof uses induction over n and a cell decomposition argument (real algebraic geometry).

Rmk Another interesting point-counting lemma can be found in Widmer: Counting primitive points of bounded height (section 5)

Instead of counting lattice points in a region, one often obtains better error bounds when counting with a smooth weight.

$\cancel{\#(I\cap\mathbb{Z}) = \text{length}(I) + O(1)}$

I.e.: instead of $\#(A\cap\mathbb{Z}^n) = \sum_{x\in\mathbb{Z}^n} 1_A(x)$ $(\approx \mathrm{vol}(A))$

estimate $\sum_{x\in\mathbb{Z}^n} f(x)$ $\left(\approx \int_{\mathbb{R}^n} f(x)\,dx\right)$ for a smooth compactly supported function $f:\mathbb{R}^n\to\mathbb{R}_{\geq 0}$ approximating 1_A (from above or below).

1_I

To estimate $\sum_{x\in\mathbb{Z}^n} f(x)$, one uses:

Thm 4.2.3 (Poisson summation) For any Schwartz function $f:\mathbb{R}^n\to\mathbb{C}$, we have

$$\sum_{x\in\mathbb{Z}^n} f(x) = \sum_{t\in\mathbb{Z}^n} \hat{f}(t).$$

Here, $\hat{f}(0) = \int_{\mathbb{R}^n} f(x)\,dx$ and the remaining terms produce the error term.

Thm 4.2.4 If $f:\mathbb{R}^n \to \mathbb{C}$ is a Schwartz fct. (e.g. smooth and compactly supported) then $\hat{f}:\mathbb{R}^n \to \mathbb{C}$ is a Schwartz fct. (in part., $\hat{f}(t) \ll_{f,k} |t|^{-k}$ $\forall t \in \mathbb{R}^n$, $\forall k \geq 0$).

Let $GL_n(\mathbb{R})$ act on functions $f:\mathbb{R}^n \to \mathbb{C}$ by $(Mf)(x) = f(M^{-1}x)$.

Rule: $\widehat{Mf} = |\det(M)| \cdot (M^T)^{-1} \hat{f}$.

Thm 4.2.5 Let $f:\mathbb{R}^n \to \mathbb{C}$ be smooth and compactly supported, and $k \geq 1$. Let $f_R(x) = f\left(\frac{x}{R}\right)$ $(I_R f)(x)$, $\begin{pmatrix} R & & 0 \\ & \ddots & \\ 0 & & R \end{pmatrix}$. Then

$$\sum_{x \in \mathbb{Z}^n} f_R(x) = R^n \cdot \int_{\mathbb{R}^n} f(x)\,dx + O_{f,k}(R^{-k}) \text{ for } R \to \infty.$$

the error goes to 0 !!!

SKIP

Pf $\hat{f}_R(t) = R^n \cdot \hat{f}(Rt)$

$$\sum_{0 \neq t \in \mathbb{Z}^n} \hat{f}(Rt) \ll R^{-k} \underbrace{\sum_{0 \neq t \in \mathbb{Z}^n} |t|^{-k}}_{\text{indep. of } R,\ <\infty \text{ for large enough } k} \ll R^{-k}$$

$$\Rightarrow \sum f_R(x) = R^n \underbrace{\hat{f}(0)}_{\int f(x)dx} + O(R^{n-k}). \quad \square$$

More generally, we can count on any lattice:

Thm 4.2.6 Let f be smooth and cpt supp. and $k \geq 1$. Let Λ be a full lattice in $\mathbb{R}^n$ with succ. min. $\lambda_1, \dots, \lambda_n$. Then,

$$\sum_{x \in \Lambda} f(x) = \cancel{\boxed{\frac{\int_{\mathbb{R}^n} f(x)\,dx}{\mathrm{covol}(\Lambda)} + O_{f,k}(\lambda_n^k)}} \quad \text{as } \lambda_n \to 0.$$

$$\frac{1}{\mathrm{covol}(\Lambda)} \left(\int_{\mathbb{R}^n} f(x)\,dx + O_{f,k}(\lambda_n^k) \right)$$

Pf. Let $v_1, \dots, v_n$ be a basis of Λ with $|v_i| \asymp \lambda_i$.

$$M = \begin{pmatrix} - v_1 - \\ \vdots \\ - v_n - \end{pmatrix}. \qquad \Rightarrow \Lambda = M^T \mathbb{Z}^n$$

$$LHS = \sum_{x \in M^T \mathbb{Z}^n} f(x) = \sum_{x \in \mathbb{Z}^n} \underbrace{f(M^T x)}_{((M^T)^{-1} f)(x)} = \sum_{0 \neq t \in \mathbb{Z}^n} \underbrace{|\det(M)|^{-1}}_{\frac{1}{\mathrm{covol}(\Lambda)}} \hat{f}(M^{-1} t)$$

$$\text{Main term} = \frac{1}{\mathrm{covol}(\Lambda)} \int f(x)\,dx.$$

The entries of M are $\ll \lambda_n$.

$$\Rightarrow 1 \leq |t| \ll \lambda_n \cdot |M^{-1} t|$$

$$\Rightarrow \text{error term} \ll \frac{1}{\mathrm{covol}} \sum_{0 \neq t \in \mathbb{Z}^n} \lambda_n^k |t|^{-k} \ll \frac{\lambda_n^k}{\mathrm{covol}}$$

↑ suff. large k

$\square$

Rmk

$\boxed{\text{The previous theorem follows by letting } \Lambda = \frac{1}{R} \mathbb{Z}^n.}$

Rmk A useful way to approximate a fct. f by a smooth fct. is to consider the convolution $f * g$ with a smooth fct. $g: \mathbb{R}^n \to \mathbb{R}$ with (small) cpt. support and with $\int g(x)dx = 1$.

$$(f*g)(x) = \int f(x-y)g(y)dy = \int f(y)g(x-y)dy$$

Rmk Let $f, g \in L^1(\mathbb{R}^n)$. Then:

a) $f*g \in L^1(\mathbb{R}^n)$

b) $\widehat{f*g}(t) = \hat{f}(t) \cdot \hat{g}(t)$

c) $\operatorname{supp}(f*g) \subseteq \operatorname{supp}(f) \cdot \operatorname{supp}(g)$

d) If g is smooth, then $f*g$ is smooth.

4.3. Rings of integers

If K is a number field of degree n with r_1 real emb. and r_2 pairs of complex emb., combine them to $K \hookrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \cong \mathbb{R}^n$

as $\mathbb{R}$-vector spaces using $\mathbb{C} \cong \mathbb{R}^2$, $a+bi \leftrightarrow (a,b)$

$\mathcal{O}_K$ is a full lattice in $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ with

$$\operatorname{covol}(\mathcal{O}_K) = 2^{-r_2} \cdot |\operatorname{disc}(K)|^{1/2}.$$

Any fractional ideal $\mathfrak{a}$ is a full lattice with

$$\operatorname{covol}(\mathfrak{a}) = \operatorname{Nm}(\mathfrak{a}) \cdot \operatorname{covol}(\mathcal{O}_K).$$

We use the norm

$$\|(a_1, \ldots, a_{r_1}, b_1, \ldots, b_{r_2})\| = \max(|a_1|, \ldots, |a_{r_1}|, |b_1|, \ldots, |b_{r_2}|)$$

on $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$.

Rmk 4.3.1 $\|xy\| \leq \|x\| \cdot |y|$

Lemma 4.3.2 $\lambda_1(\mathcal{O}_K) = 1$

Pf "$\leq$": $\|\underset{\mathcal{O}_K}{\underset{\Uparrow}{1}}\| = 1$. "$\geq$": For any $0 \neq x \in \mathcal{O}_K$, $1 \leq |\operatorname{Nm}(x)| = \prod_{\sigma : K \hookrightarrow \mathbb{C}} |\sigma(x)|$.

$\Rightarrow |\sigma(x)| \geq 1$ for some σ $\Rightarrow \|x\| \geq 1$. $\square$

<u>Exe</u> Let $K=\mathbb{Q}(\sqrt{p},\sqrt{q})$ for primes $p<q$.

Then,

$$\lambda_2(\mathcal{O}_K) \asymp \sqrt{p},$$
$$\lambda_2(\mathcal{O}_K) \asymp \sqrt{q},$$
$$\lambda_3(\mathcal{O}_K) \asymp \sqrt{pq}.$$

<u>Pf</u> "$\ll$" $1,\sqrt{p},\sqrt{q},\sqrt{pq} \in \mathcal{O}_K$ lin. indep.

"$\gg$" follows because $\lambda_1\lambda_2\lambda_3\lambda_4 \asymp \text{covol} \asymp |\mathrm{disc}(K)|^{1/2} \underset{\text{HW}}{\asymp} pq$. $\square$

~~Exe picked a random monic pol. $f \in \mathbb{Z}[X]$ of deg. 3~~

<u>Rmk</u> If you order degree n number fields K (with Galois group S_n) by $|\mathrm{disc}(K)|$, it is expected that $\mathbb{P}_K(\lambda_n(\mathcal{O}_K)/\lambda_2(\mathcal{O}_K) \le c) \xrightarrow{c\to\infty} 1$.
(known for $n \le 5$ by Bhargava, Harron: The equidist. of lattice shapes of rings of int. in cubic, quartic, quintic.

<u>Def</u> A number field K is <u>primitive</u> if there is no field $\mathbb{Q} \subsetneq F \subsetneq K$.

<u>Exe</u> a) A number field of prime degree.

b) A number field of degree n with Galois group (of the Galois closure) S_n.

<u>Thm 4.3.3</u> If K is primitive, then

$$\lambda_{i+j-1}(\mathcal{O}_K) \le \lambda_i(\mathcal{O}_K)\lambda_j(\mathcal{O}_K) \quad \forall\, 1 \le i,j \le n \text{ with } i+j-1 \le n.$$

This follows from:

<u>Lemma 4.3.4</u> (Multiplicative Kneser's Theorem:
Hou, Leung, Xiang: A generalisation of an addition theorem of Kneser)
Let K be primitive, consider $\mathbb{Q}$-vector spaces $0 \neq A, B \subseteq K$.

$$\Rightarrow \dim(\underbrace{A\cdot B}_{\substack{\mathbb{Q}\text{-vector space}\\ \text{spanned by } a\cdot b \text{ for } a\in A,\, b\in B}}) \ge \min(\dim(A)+\dim(B)-1, \dim(K)).$$

Pf of Thm: Let $v_1, v_2, \ldots, v_n$ be a directional basis,

$A_i = \langle v_1, \ldots, v_i \rangle$.

By the lemma, $\dim(A_i \cdot A_j) \geq i+j-1$.

$A_i \cdot A_j$ is spanned by elements $v_r v_s \in \mathcal{O}_K$ with $r \leq i$, $s \leq j$.

$$|v_r v_s| \underset{\text{Annle 4.3.1}}{\leq} |v_r| \cdot |v_s| = \lambda_r \lambda_s \leq \lambda_i \lambda_j.$$

$\Rightarrow \lambda_{i+j-1} \leq \lambda_i \lambda_j$ $\square$

Pf of Lemma: by induction over $\dim(A)$.

$\dim(A) = 1$ is clear, so assume $\dim(A) \geq 2$. Fix $a, a' \in A$ lin. indep.

For $0 \neq b \in B$, let $V_{ab} = Ab \cap aB$,
$W_{ab} = Ab + aB$.

Case 1: $V_{a,b} = Ab$. $\forall 0 \neq b \in B$

$\Rightarrow Ab \subseteq aB \quad \forall 0 \neq b \in B$

$\Rightarrow A \cdot B \subseteq aB$. $\Rightarrow \frac{a'}{a} \cdot B \subseteq B \Rightarrow \underbrace{\mathbb{Q}\left(\frac{a}{a'}\right)}_{= K \text{ because } \frac{a}{a'} \notin \mathbb{Q},\ K \text{ primitive}} \cdot B \subseteq B \Rightarrow B = K \Downarrow A \cdot B = K$

~~Let $a' \in A$ lin. indep. from~~

Case 2: $V_{a,b} \subsetneq Ab$ for some $0 \neq b \in B$

Apply the ind. hypothesis to $\underset{\substack{\neq \\ 0}}{V_{a,b}} \ni ab$ and $ab \in \underset{\substack{\neq \\ 0}}{W_{a,b}}$:

$$\dim(A \cdot B) \geq \dim(\underbrace{V_{ab} \cdot W_{ab}}_{\subseteq abA\cdot B}) \geq \min(\underbrace{\dim(V_{ab}) + \dim(W_{ab})}_{\substack{= \dim(Ab) + \dim(aB) \\ = \dim(A) + \dim(B)}} - 1, \dim(K))$$

$\square$

Reference: Vemulapalli: Bounds on succ. min. of orders in n. f. and scalar invariants of curves

5. Fundamental domains

We will want to count orbits of an action $G \circlearrowright X$.

For example: $\mathcal{O}_K^\times \circlearrowright \mathcal{O}_K$ by left mult.

$GL_2(\mathbb{Z}) \circlearrowright \{$binary forms $f(x,y)$ of degree n with integer coefficients$\}$

Idea: count lattice points in a fundamental domain.
We'll use weighted fund. dom.
Let G act on fct. $f: X \to \mathbb{R}_{\geq 0}$ by $(gf)(x) = f(g^{-1}x)$.

(so $g 1_A = 1_{gA}$.)

Def A fund. dom. for $G \circlearrowright X$ is a fct. $f: X \to \mathbb{R}_{\geq 0}$ s.t.

$$\sum_{g \in G} gf = 1.$$

[only allow nonneg. values to avoid issues with conditional convergence]

Ex If G is finite, $f(x) = \frac{1}{\# G}$ is the trivial fund. dom.

Ex $f = 1_{[0,1)}$ fund. dom. for $\mathbb{Z} \circlearrowright \mathbb{R}$ (addition)

~~f = 1 fund. cell for~~

Ex Λ full lattice in $\mathbb{R}^n$ with fund. cell C

1_C fund. dom. for $\Lambda \circlearrowright \mathbb{R}^n$ (addition)

Ex $f(x) = \begin{cases} 1 & , x > 0 \\ 1/2 & , x = 0 \\ 0 & , x < 0 \end{cases}$ for $\{\pm 1\} \underset{\text{mult.}}{\circlearrowright} \mathbb{R}$.

Ex $1_{\text{squarefree int.}}$ fund. dom. for $\mathbb{Q}^{\times 2} \underset{\text{mult.}}{\circlearrowright} \mathbb{Q}^\times$

Rmk a) If $\#\mathrm{Stab}(x) < \infty$ $\forall x$, and $S \subseteq X$ is a set containing exactly one el. of each orbit, ~~then f is a fund. dom. if and only if~~

then $f(x) := \begin{cases} 1/\#\mathrm{Stab}(x), & x \in S \\ 0, & x \notin S \end{cases}$

is a fund. dom.

b) Otherwise, there is no fund. dom.

Lemma 5.1 All fund. dom. f_1, f_2 for $G \curvearrowright X$ have the same size: $\sum_{x \in X} f_1(x) = \sum_{x \in X} f_2(x)$.

Cor $\sum_{x \in X} f(x) = \sum_{\text{orbit } Gx} \frac{1}{\#\mathrm{Stab}(x)} \underbrace{= \frac{\#X}{\#G}}_{\text{if } G \text{ is finite}}$

Rmk a) If f is a fund. dom. for $G \curvearrowright X$,

then $f \cdot 1_A$ is a fund. dom. for $G \curvearrowright A \subseteq X$.

b) If f is a fund. dom. for $G \curvearrowright X$,

then gf — " — — " — for all $g \in G$.

Generalising Lemma 5.1 :

Lemma 5.2 Let G be a countable group with a measure-preserving action on a measure space X. $(vol(gA) = vol(A))$

Then, any two fund. dom. f_1, f_2 have the same volume:

measurable

$$\int_X f_1(x)dx = \int_X f_2(x)dx$$

Pf HW $\square$

We call this integral (if there is a measurable fund. dom.) the volume of $G\backslash X$:

$$vol(G\backslash X) = \int_X f(x)dx$$

[Lemma is the case of the counting measure]

Ex: Any two fund. cells for Λ have the same volume.

[Often, it's not so easy to pick a single repr. of each orbit. Easier to construct:]

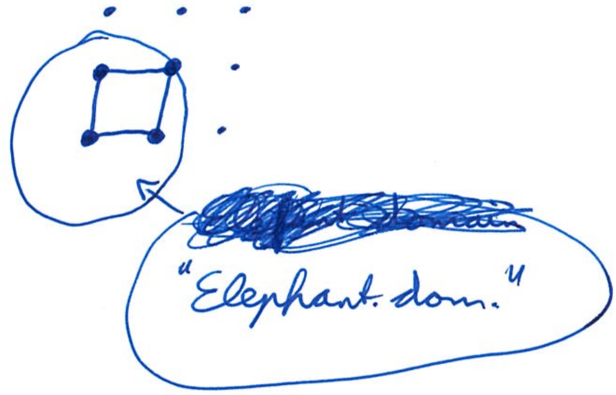
Def An almost fund. dom. (elephund. dom.) for $G \curvearrowright X$ is a set $S \subseteq X$ such that $1 \leq \#\{g \in G \mid gx \in S\} < \infty$ for all $x \in X$.

Rmk This is equiv. to $\#Stab(x) < \infty$ and $1 \leq \#(S \cap Gx) < \infty$.

Def The associated fund. dom. is

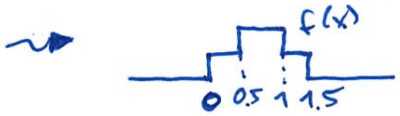
$$f(x) = \begin{cases} 1/\#\{g \in G \mid gx \in S\} & , x \in S \\ 0 & , x \notin S. \end{cases}$$

<u>Exe</u> For any full lattice Λ, a suff. large ball $D(R)$ is an almost fund. dom. for $\Lambda \curvearrowright \mathbb{R}^n$.



<u>Exe</u> $\mathbb{Z} \curvearrowright \mathbb{R}$

$S = [0, 1.5]$



<u>Lemma 5.3</u> Let G be countable, with a measure-preserving action on X. If S is a measurable almost fund. dom., then f is measurable.

the assoc. f.d.

<u>Pf</u> For any finite $I \subseteq G$, $A_I := \bigcap_{g \in I} gS$ is measurable.

$\Rightarrow$ For any $k \geq 0$, $B_k := \bigcup_{\substack{id \in I \subseteq G \\ \# I = k}} A_I$ is measurable.

$\Rightarrow \{x \in X \mid f(x) = \frac{1}{k}\} = B_k \setminus B_{k+1}$ is measurable.

$\Rightarrow f$ is measurable. $\square$

We can smoothen fund. dom.:

anything $*$ smooth = smooth

fund. dom. $*$ vol. 1 = fund. dom.

<u>Lemma 5.4</u> Let G be a locally compact Hausdorff group with left Haar measure $d_\ell g$ and right Haar measure $d_r g = d_\ell g^{-1}$. Let $H \leq G$ a subgroup and $f \in L^1(G)$ an integrable fund. dom. for $H \curvearrowright G$ (left mult.).

Let $\eta \in L^1(G)$ with $\int_G \eta(g)\, d_r g = 1$.

Then,

$$\cancel{= \int_G f(g) \cdot g\eta \, d_\ell g = \int_G}$$

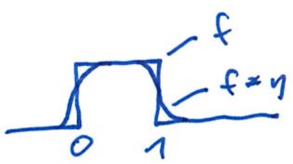
$$\cancel{(f*\eta)(g) = \int_G f(t)\cdot \eta(t^{-1}g)\, dt}$$

$$(f*\eta)(a) = \int_G f(b)\cdot \eta(b^{-1}a)\, d_\ell b \underset{b = ac^{-1}}{=} \int_G f(ac^{-1})\cdot \eta(c)\, d_r c$$

is also a fund. dom. for $H \curvearrowright G$.

Intuition: $f*\eta = \int_G f(b)\cdot \underbrace{b\eta}_{\substack{\text{left } b \text{ translate of } \eta \\ \text{(hopefully easy to count lattice points in here)}}} d_\ell b = \int_G \underbrace{fc}_{\substack{\text{right } c \text{ translate of } f \\ \text{(also a fund. dom.)}}} \cdot\, \eta(c)\, d_r c$.

<u>Ex</u> $\mathbb{Z} \curvearrowright \mathbb{R}$



<u>Pf</u> $\sum_{h\in H} (f*\eta)(ha) = \int_G \underbrace{\sum_{h\in H} f(hac^{-1})}_{1}\, \eta(c)\, d_r c = \int_G \eta(c)\, d_r c = 1.$ $\square$

6. The class number formula

~~Reminder~~

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

$$K \hookrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$$

Define the hom. $l: \mathbb{R}^\times \longrightarrow \mathbb{R}$, $x \longmapsto \log|x|$

and $l: \mathbb{C}^\times \longrightarrow \mathbb{R}$, $x \longmapsto 2\log|x| = \log(x\bar{x})$

combine them to $l: (\mathbb{R}^{r_1} \times \mathbb{C}^{r_2})^\times \longrightarrow \mathbb{R}^{r_1+r_2}$.

Let $s: \mathbb{R}^{r_1+r_2} \longrightarrow \mathbb{R}$, $(t_1, \dots, t_{r_1+r_2}) \longmapsto t_1 + \dots + t_{r_1+r_2}$.

<u>Note</u> $s(l(x)) = \log|N_m(x)|$

In particular, $l(\mathcal{O}_K^\times) \subseteq H := \ker(s)$.

~~Reminder~~

We identify $H \xrightarrow{\sim} \mathbb{R}^{r_1+r_2-1}$, $(t_1, \dots, t_{r_1+r_2}) \mapsto (t_1, \dots, t_{r_1+r_2-1})$.

[This defines a measure on H!]

<u>Reminder</u> The kernel of $l: \mathcal{O}_K^\times \longrightarrow H$ is the group (μ_K) of roots of unity in K.

The image is a full lattice in H, whose covolume is the <u>regulator</u> R_K.

Let $C \subseteq H$ be a fundamental cell.

<u>Lemma 6.1</u> For any proj. $\pi : \mathbb{R}^{r_1+r_2} \twoheadrightarrow H$,

$$f(x) = \frac{1}{\#\mu_K} \cdot \mathbb{1}_C(\pi(\ell(x)))$$

is a fund. dom. for $\mathcal{O}_K^\times \underset{\text{mult.}}{\curvearrowright} (\mathbb{R}^{r_1} \times \mathbb{C}^{r_2})^\times$.

<u>Pf</u> $\displaystyle\sum_{u \in \mathcal{O}_K^\times} f(ux) = \sum_{v \in \ell(\mathcal{O}_K^\times)} \frac{\cancel{\#\mu_K}}{\cancel{\#\mu_K}} \cdot 1_C(v + \pi(\ell(x))) = 1$

$\displaystyle\sum_{u \in \mathcal{O}_K^\times} \frac{1}{\#\mu_K} \cdot 1_C(\pi(\ell(u)) + \pi(\ell(x)))$

C is fund. cell for $\ell(\mathcal{O}_K^\times) \subseteq H$

$\square$

<u>Lemma 6.2</u> Let $S(T) = \{a \in (\mathbb{R}^{r_1} \times \mathbb{C}^{r_2})^\times \mid |\mathrm{Nm}(a)| \leq T\}$.

Then, $f_T(x) := f(x) \cdot 1_{S(T)}(x)$ is a fund. dom. for $\mathcal{O}_K^\times \curvearrowright S(T)$

with volume $\displaystyle\int_{S(T)} f_T(x)\,dx = \frac{2^{r_1}(2\pi)^{r_2} R_K}{\#\mu_K} \cdot T$.

<u>Pf</u> $f_T(x) = f_1(x/T^{1/n})$. $\Rightarrow \int f_T = (T^{1/n})^n \cdot \int f_1 = T \cdot \int f_1$.

$\Rightarrow$ It suffices to consider $T = 1$.
All fund. dom. have same vol. $\Rightarrow$ w.l.o.g., π is the proj. ignoring the last coor
We perform a change of variables on $(\mathbb{R}^{r_1} \times \mathbb{C}^{r_2})^\times$:

Write elements of $\mathbb{R}^\times$ as $x = \pm e^z$ $(z \in \mathbb{R})$
and elements of $\mathbb{C}^\times$ as $x = e^{\frac{z}{2} + it}$ $(z \in \mathbb{R},\ 0 \leq t < 2\pi)$.

Let $E = \{z \in \mathbb{R}^{r_1+r_2} \mid s(z) \leq 0\}$.

Then,

$$\int_{S(T)} f(x)\,dx = \frac{2^{r_1}\pi^{r_2}}{\#\mu_K} \cdot \int_{E\cap\pi^{-1}(C)} \exp(z_1+\dots+z_{r_1+r_2})\,dz$$

$$= \frac{2^{r_1}\pi^{r_2}}{\#\mu_K} \cdot \int_C \int_{-\infty}^{0} \exp(r)\,dr\; d(z_1,\dots,z_{r_1+r_2-1})$$

$C \subseteq H \cong \mathbb{R}^{r_1+r_2-1}$

$$= \frac{2^{r_1}\pi^{r_2} R_K}{\#\mu_K}.$$

□

Thm 6.3 $\#\{\mathfrak{a} \subseteq \mathcal{O}_K \text{ principal ideal},\ \mathfrak{a} \neq 0 \mid \mathrm{Nm}(\mathfrak{a}) \le T\} \sim_K \dfrac{2^{r_1}(2\pi)^{r_2} R_K T}{\#\mu_K |\mathrm{disc}(K)|^{1/2}}$

for $T \to \infty$.

Pf $\mathrm{LHS} = \#\,\mathcal{O}_K^\times \backslash (\mathcal{O}_K \cap S(T))$

$$= \sum_{x\in\mathcal{O}_K} f_T(x)$$

If we use the projection $\pi(z) = z - \frac{s(z)}{n}\cdot(\underbrace{1,\dots,1}_{r_1},\underbrace{2,\dots,2}_{r_2})$,

then $f(\lambda x) = f(x)\ \forall \lambda \in \mathbb{R}^\times$.

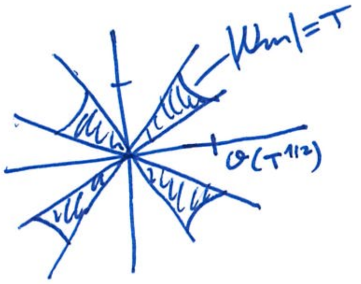
Rmk For $K = \mathbb{Q}(i)$, this is $\{x+iy \in \mathbb{Z}[i] \mid x^2+y^2 \le T\}$

($\rightsquigarrow$ Gauß circle problem)

We can use Davenport's lemma (after replacing by a semialgebraic approximation!)

$$\Rightarrow \text{LHS} = \frac{\int f_T(x)\,dx}{\mathrm{covol}(\mathcal{O}_K)} + O\left(T^{n-1}\right) \text{ for } T \to \infty.$$

the proj. of supp(f_T) onto each axis in $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \cong \mathbb{R}^n$ has length $O(T^{1/n})$.



□

Pf 2 Using lemma 5.4, replace $1_C : H \to \{0,1\}$ by $1_C \underset{H}{*} \eta$ for a smooth compactly supported function $\eta : H \to \mathbb{R}_{\geq 0}$ with $\int_H \eta(z)\,dz = 1$.

Also, replace $1_{[0,T]}(|Nm(x)|) = 1_{S(T)}(x)$ by a smooth compactly supported approximation $\tau(|Nm(x)|/T)$.

$$\sum_{\substack{0 \neq \mathfrak{a} \subseteq \mathcal{O}_K \\ \text{principal}}} \tau(\mathfrak{a}) = \sum_{x \in \mathcal{O}_K} \frac{1}{\#\mu_K} (1_C * \eta)(\pi(L(x))) \cdot \tau(Nm(x)/T)$$

$$= \int_H \frac{1_C(h)}{\#\mu_K} \underbrace{\sum_{x \in \mathcal{O}_K} \eta(\pi(L(x)) - h)\, \tau(|Nm(x)|/T)}\, dh$$

smooth function of x; the parameter T scales the fct. by a factor of $T^{1/n}$

$$\underset{\text{Thm 4.2.6}}{\uparrow}= \int_H \frac{1_C(h)}{\#\mu_K \cdot \mathrm{covol}(\mathcal{O}_K)} \left[\int_{\mathbb{R}^{r_1}\times\mathbb{C}^{r_2}} \eta(\pi(L(x))-h)\, \tau(|N_m(x)|/T)\, dx + \mathcal{O}_K(T^{-k}) \right] dh$$

$$= \frac{1}{\mathrm{covol}(\mathcal{O}_K)} \int_{\mathbb{R}^{r_1}\times\mathbb{C}^{r_2}} \underbrace{\frac{(1_C * \eta)(\pi(L(x)))}{\#\mu_K}}_{\substack{(\text{fund. dom.})(x) \\ \text{for } \mathcal{O}_K^\times \circlearrowright \mathbb{R}^{r_1}\times\mathbb{C}^{r_2}}} \underbrace{\tau(|N_m(x)|)}_{\substack{\text{approx.} \\ \text{to } 1_{(0,1]}(|N_m(x)|) \\ \shortparallel \\ 1_{S(1)}(x)}} dx \cdot T + \mathcal{O}_K(T^{-k})$$

As you let τ go to $1_{(0,1]}$, (say monotonely ptwise a.e.) ~~this goes to~~ the integral goes to $\int f_T(x)\,dx$ by monotone convergence. $\square$

Thm 6.4 (class number formula)

$$\#\{0 \neq \mathfrak{a} \in \mathcal{O}_K \text{ ideal} \mid \mathrm{Nm}(\mathfrak{a}) \leq T\} \sim \frac{2^{r_1}(2\pi)^{r_2} R_K h_K}{\#\mu_K |\mathrm{disc}(K)|^{1/2}} \cdot T$$

__Pf__ Consider an ideal class $c \in \mathcal{Cl}(K)$. Let $\mathfrak{b} \in c$ be a fractional ideal.

$$\{0 \neq \mathfrak{a} \text{ ideal in } c\} \longleftrightarrow \mathcal{O}_K^\times \backslash \mathfrak{b}^{-1}$$

$$x \cdot \mathfrak{b} \longleftarrow\!\shortmid \; x$$

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

As in the prev. Thm.,

$$\#\left(\mathcal{O}_K^\times \backslash \{x \in \mathfrak{b}^{-1} \mid |\mathrm{Nm}(x)| \leq \tfrac{T}{\mathrm{Nm}(\mathfrak{b})}\}\right)$$

$$\sim \frac{2^{r_1}(2\pi)^{r_2} R_K}{\#\mu_K \underbrace{\mathrm{covol}(\mathfrak{b}^{-1})}_{\frac{|\mathrm{disc}(K)|^{1/2}}{2^{r_2} \cdot \mathrm{Nm}(\mathfrak{b})}}} \cdot \frac{T}{\mathrm{Nm}(\mathfrak{b})}$$

$\square$

7. GL_n and SL_n

7.1. Haar measures

Prop 7.1.1 Any locally cpt. Hausdorff ~~top.~~ group G has a left Haar measure $d_l g$ and a right Haar measure $d_r g$, unique up to mult. by a number in $\mathbb{R}_{>0}$.

Def G is unimodular if we can take $d_l g = d_r g = dg$. Then, dg is called a Haar measure on G.

Rmk We can take $d_r g = d_l(g^{-1})$.

Ex $K, K^\times, K^n, GL_n(K), SL_n(K)$ for any local field K.

We'll use the following Haar measures:

Ex Lebesgue measure $dx = d^+x$ on $\mathbb{R}$ $\qquad d(t+x) = dx$

$$d^\times x = |x|^{-1} dx \quad \text{on } \mathbb{R}^\times \qquad d^\times(tx) = |tx|^{-1} d(tx) = d^\times x$$

Ex

Ex K nonarch. loc. field with prime ideal $\mathfrak{q}_K$, residue field $\mathbb{F}_{q_K}$, normalised valuation v_K, norm $|x|_K = q_K^{-v_K(x)}$. Normalize the Haar measure dx on K so that $\mathrm{vol}(\mathcal{O}_K) := \int_{\mathcal{O}_K} dx = 1$.

Rmk For any subset A of $\mathcal{O}_K/\mathfrak{q}_K^n$,

$$\mathrm{vol}(\{x \in \mathcal{O}_K \mid (x \bmod \mathfrak{q}_K^n) \in A\}) = \mathbb{P}_{x \in \mathcal{O}_K/\mathfrak{q}_K^n}(x \in A).$$

Rmk $d(tx) = |t|_K dx$ for $t \in K$.

Ex $d^\times x = |x|_K^{-1} dx$ on $K^\times$

Ex If da, db are our Haar measures on A, B, use the prod. measure on $A \times B$.

<u>Ex</u> Let K be any local field. The Lebesgue measure d^+g on $GL_n(K) \subset M_n(K)$ is not a (mult.) Haar measure:

$$d^+(ag) = |\det(a)|_K^n \, d^+g \quad \text{for } a \in GL_n(K).$$

Left mult. by a on a column has determinant det(a). There are n columns.

$$\Rightarrow \quad d^\times g = |\det g|_K^{-n} \, d^+g \text{ is a Haar measure}$$

<u>Ex</u> The map

$$K^\times \times SL_n(K) \longrightarrow GL_n(K)$$
$$(t, h) \longmapsto \begin{pmatrix} 1 & & \\ & \ddots & \\ & & t \end{pmatrix} h = t h = g$$

is a homeomorphism (in fact a diffeomorphism). We normalize the Haar measure $d^\times h$ on $SL_n(K)$ so that $d^\times t \, d^\times h$ is the pull-back of $d^\times g$.

The pull-back must be left invariant because $d^\times g$ is a Haar measure!

<u>Remk</u> $\mathbb{R}_{>0} \times SL_n(\mathbb{R}) \to GL_n(\mathbb{R})$ is a homeom. and isom.

$$(\lambda, h) \mapsto \lambda h$$

The pull-back of $d^\times g$ is $n \, d^\times \lambda \, d^\times h$.

7.2. Minkowski sets ~~Recall: Elements of~~

~~Thm 7.2.1 S^{Mink}~~

Recall: Elements of $GL_n(\mathbb{R})$ corr. to bases $(b_1, \dots, b_n)$ of $\mathbb{R}^n$.

Two matrices lie in the same $GL_n(\mathbb{Z})$-orbit iff their bases span the same lattice.

~~$GL_n(\mathbb{R})$~~

$\rightsquigarrow$ An almost fund. dom. for $GL_n(\mathbb{Z}) \curvearrowright GL_n(\mathbb{R})$ corr. to an almost unique choice of basis of each full lattice $\Lambda \subseteq \mathbb{R}^n$.

Def ~~Thm 7.2.1~~ The Minkowski set S^{Mink} is the set of matrices $\begin{pmatrix} - b_1 - \\ \vdots \\ - b_n - \end{pmatrix} \in GL_n(\mathbb{R})$ so that $(b_1, \dots, b_n)$ is a directional basis for the lattice Λ spanned by $b_1, \dots, b_n$.

Thm 7.2.1 S^{Mink} is a measurable almost fund. dom. for $GL_n(\mathbb{Z}) \curvearrowright GL_n(\mathbb{R})$

Pf "≥ 1 el. of each orbit": clear

"$< \infty$ —"— ": There are only fin. many $b_i \in \Lambda$ with $|b_i| = \lambda_i$. $\square$

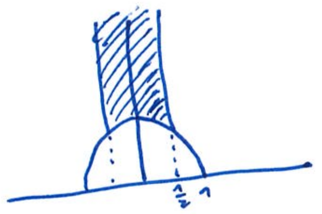
Rmk S^{Mink} is $\mathbb{R}^\times$-invariant and right $O_n(\mathbb{R})$-invariant

Ese ($n=2$, Euclidean norm) We have a bij.

$$\mathbb{R}^\times \backslash GL_2(\mathbb{R}) / O_2(\mathbb{R}) \longleftrightarrow \mathbb{H} = \{(x,y) \mid x \in \mathbb{R}, y \in \mathbb{R}_{>0}\}$$

$$\begin{pmatrix} 1 & 0 \\ x & y \end{pmatrix} \longleftarrow\!\shortmid \ (x,y)$$

The image of S^{Mink} is:



$$\boxed{\begin{pmatrix} -v_1- \\ -v_2- \end{pmatrix} \in S^{\text{Mink}} \Leftrightarrow |v_1| \leq |v_2| \text{ and } |v_1 \cdot v_2| \leq \tfrac{1}{2}|v_1|^2}$$

Rmk S^{Mink} is close to a fund. dom.: almost all lattices have exactly 2^n dir. bases (choices of signs of $\pm b_1, \ldots, \pm b_n$).

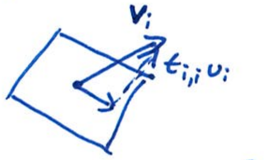
But it is difficult to check whether $M \in S^{\text{Mink}}$.

7.3. Iwasawa decomposition

Given a basis $(v_1, \dots, v_n)$ of $\mathbb{R}^n$, the Gram-Schmidt process produces the orth. basis $(u_1, \dots, u_n)$ s.t.

$$v_i = t_{i,1} u_1 + \dots + t_{i,i} u_i \quad \text{with } t_{ij} \in \mathbb{R},\ t_{ii} > 0.$$

Here, $v_i - t_{i,i} u_i$ is the orth. proj. of v_i onto the subspace $\langle v_1, \dots, v_{i-1} \rangle = \langle u_1, \dots, u_{i-1} \rangle$. t_{ii} is the length of the perpendicular vector $t_{ii} u_i$.



Let $T := \left\{ \begin{pmatrix} * & 0 & 0 \\ \vdots & \ddots & 0 \\ * & \cdots & * \end{pmatrix} \in GL_n(\mathbb{R}) \text{ lower triangular with positive entries on the diagonal} \right\}.$

Lemma 7.3.1

a) $T \times O_n(\mathbb{R}) \longrightarrow GL_n(\mathbb{R})$ is a homeomorphism.
$(t, k) \longmapsto tk$

b) The pullback of $d^\times g$ is ~~scalar multiple of~~ $d_l^\times t \, d^\times k$ for a left Haar measure $d_l^\times t$ on T and a (right) Haar measure $d^\times k$ on $O_n(\mathbb{R})$.

Remark: $O_n(\mathbb{R})$ is unimodular.

Pf a) follows from Gram-Schmidt process

b) The pull-back is left T and right $O_n(\mathbb{R})$-invariant.
(The pull-back along $(t,k) \mapsto tk^{-1}$ is left $T \times O_n(\mathbb{R})$-invariant, hence a multiple of $d_l^\times t \, d_l^\times k = d_l^\times t \, d_r^\times k^{-1}$.) $\square$

Let $N := \left\{ \begin{pmatrix} 1 & & 0 \\ * & \ddots & \\ * & * & 1 \end{pmatrix} \right\} \subset J$ be the group of lower triangular unipotent matrices. Lemma 7.3.2 $\prod_{i>j} dn_{ij}$ is a (left) Haar measure on N.
~~Pf left mult by~~ Pf HW $\square$

Let $A := \left\{ \begin{pmatrix} * & & 0 \\ & \ddots & \\ 0 & & * \end{pmatrix} \right\} \subset J$ be the group of diagonal matrices with positive entries on the diagonal. Write $a_1, \dots, a_n$ for the diagonal entries of $a \in A$.

Lemma 7.3.3

a) $N \times A \longrightarrow J$ is a homeom.
$(n, a) \longmapsto na$

b) The pullback of $d_i^\times t$ is a scalar multiple of

$$\prod_{i>j} \frac{a_j}{a_i} \, dn_{ij} \cdot \prod_i d^\times a_i = \prod_{i>j} dn_{ij} \cdot \prod_i a_i^{n+1-2i} \, d^\times a_i \qquad (I)$$

Pf a) is clear

b) ~~$\prod_{i>j} dn_{ij}$ is a left Haar measure on N:~~

~~Left mult. by n acts by a lower triangular unipotent matrix on the i-th column vector of the tangent space of N.~~ ~~$\mathbb{R}^{n-i}$~~

The measure (I) is left N-invariant by Lemma 7.3.2.

For left A-invariance, note that for $t \in A$,

$tna = n'a'$ with $n'_{ij} = \frac{t_i}{t_j} n_{ij}$, $a' = ta$. $\square$

Together:

Thm 7.3.4 (Iwasawa decomposition of $GL_n(\mathbb{R})$)

a) $$N \times A \times O_n(\mathbb{R}) \longrightarrow GL_n(\mathbb{R}) \text{ is a diffeomorphism.}$$
$$(n, a, k) \longmapsto nak$$

b) $\prod_{i>j} \frac{a_j}{a_i} \, du_{ij} \prod_i d^\times a_i \, d^\times k$ is the pullback of a Haar measure on $GL_n(\mathbb{R})$.

Cor 7.3.5 (Iwasawa decomp. of $SL_n(\mathbb{R})$)

Let $B = \{ a \in A \mid \underset{a_1 \cdots a_n}{\overset{\shortparallel}{\det(A)}} = 1 \} \cong (\mathbb{R}^{>0})^{n-1}$

$$a \longleftrightarrow (b_i)_{i=1,\dots,n-1} \text{ with } b_i = \frac{a_{i+1}}{a_i}$$

$$a_i = \frac{b_1 \cdots b_{i-1}}{(b_1^{n-1} \cdots b_{n-2}^2 \, b_1)^{1/n}}$$

a) $N \times B \times SO_n(\mathbb{R}) \longrightarrow SL_n(\mathbb{R})$ is a diffeom.

b) ~~The Haar measure~~

$\prod_{i>j} d n_{ij} \prod_i b_i^{-i(n-i)} \, d^\times b_i \, d^\times k$ is the pullback of a Haar measure on $SL_n(\mathbb{R})$.

7.4. Siegel sets

Def Let $N' = \{n \in N \mid |n_{ij}| \leq \frac{1}{2}\ \forall i > j\}$, $A' = \{a \in A \mid a_{i+1} \geq \frac{\sqrt{3}}{2} a_i\ \forall\ 1 \leq i \leq n-1\}$

The Siegel set S^{Siegel} is $N' \cdot A' \cdot O_n(\mathbb{R}) \subseteq GL_n(\mathbb{R})$

Thm 7.4.1 a) S^{Siegel} is a measurable almost fund. dom. for $GL_n(\mathbb{Z}) \curvearrowright GL_n(\mathbb{R})$.

b) If $nak \in N'A'O_n(\mathbb{R})$ corr. to the lattice Λ, then

$a_i \underset{\text{dim. } n, \|\cdot\|}{\asymp} \lambda_i(\Lambda)$ for $i = 1, \dots, n$.

Pf b) Let $nak = \begin{pmatrix} -v_1- \\ \vdots \\ -v_n- \end{pmatrix}$, $k = \begin{pmatrix} -u_1- \\ \vdots \\ -u_n- \end{pmatrix}$.

$$v_i = \sum_{j<i} n_{ij} a_j u_j + a_i u_i .$$

$$\Rightarrow |v_i| \leq \sum_{j<i} \underbrace{|n_{ij}|}_{\substack{\leq \frac{1}{2} \\ (n \in N')}} \cdot \underbrace{a_j}_{\substack{\ll a_i \\ (a \in A')}} + a_i \ll a_i$$

$$\Rightarrow \lambda_i \ll a_i$$

On the other hand,

$$a_1 \cdots a_n = |\det(nak)| = \operatorname{covol}(\Lambda) \underset{\substack{\uparrow \\ \text{Minkowski's} \\ \text{second theorem}}}{\asymp} \lambda_1 \cdots \lambda_n .$$

a) "$\leq \infty$ el. of each orbit": There are only finitely many $v_i \in \Lambda$ with $|v_i| \leq a_i \approx \lambda_i(\Lambda)$.

"≥ 1 el. of each orbit":

Construct $v_1, \dots, v_n$ inductively. To construct v_i:

Let $\tau_i : \mathbb{R}^n \to \mathbb{R}^n$ be the proj. onto the orth. complement of $\langle v_1, \dots, v_{i-1} \rangle$.

$\tau_i(\Lambda)$ is a lattice of rank $n-(i-1)$.

Choose $v_i \in \Lambda$ so that $a_i = \tau_i(v_i) \neq 0$ has minimal length and $|\mu_{ij}| \leq \frac{1}{2}$ $\forall j < i$. (This can be arranged by adding integer multiples of $v_1, \dots, v_{i-1}$ to v_i.)

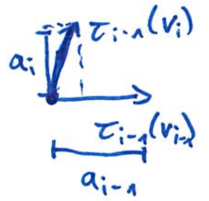
~~If we had a~~

~~Note that~~

If we had $a_i < \frac{\sqrt{3}}{2} a_{i-1}$, then

$$|\tau_{i-1}(v_i)|^2 < \left(\tfrac{1}{2} a_{i-1}\right)^2 + \left(\tfrac{\sqrt{3}}{2} a_{i-1}\right)^2 = a_{i-1}^2,$$

contradicting the minimality of $a_{i-1} = |\tau_{i-1}(v_{i-1})|$.



$\square$

7.5. Fundamental volume

Rmk W.r.t. Haar measure, $\mathrm{vol}(GL_n(\mathbb{Z})\backslash GL_n(\mathbb{R}))=\infty$.

Ex $(n=1)$ $GL_1(\mathbb{Z})\backslash GL_1(\mathbb{R}) = \{\pm 1\}\backslash \mathbb{R}^\times = \mathbb{R}_{>0}$. $\mathrm{vol}(\ldots)=\int_0^\infty x^{-1}dx=\infty$.

Thm 7.5.1 With respect to the Haar measure on $SL_n(\mathbb{R})$,

$$\mathrm{vol}(SL_n(\mathbb{Z})\backslash SL_n(\mathbb{R})) = \zeta(2)\zeta(3)\cdots\zeta(n).$$

Ex $(n=1)$ $SL_1(\mathbb{R})=\{1\}$ and the Haar measure is 1.

Ex $(n=2)$ can be shown using the explicit Minkowski set by integrating.

Rmk Let $B' = \{(b_i)_i \in B \mid b_i \geq \frac{\sqrt{3}}{2} \ \forall i\}$

$$\mathrm{vol}(SL_n(\mathbb{Z})\backslash SL_n(\mathbb{R})) \leq \mathrm{vol}(S^{\text{Siegel}} \cap SL_n(\mathbb{R}))$$

$$= \mathrm{vol}(N' \cdot B' \cdot SO_n(\mathbb{R}))$$

$$= \int_{N'\times B'\times SO_n(\mathbb{R})} \prod_{i>j} dn_{ij} \prod_i b_i^{-i(n-i)}\, d^\times b_i \, d^\times k$$

$$= \prod_{i>j} \underbrace{\int_{-1/2}^{1/2} dn_{ij}}_{1} \cdot \prod_{i=1}^{n-1} \underbrace{\int_{\sqrt{3}/2}^{\infty} b_i^{-i(n-i)} d^\times b_i}_{\left.\frac{b_i^{-i(n-i)}}{-i(n-i)}\right|_{b_i=\frac{\sqrt{3}}{2}}^{\infty} < \infty} \cdot \underbrace{\int_{SO_n(\mathbb{R})} d^\times k}_{<\infty}$$

because $SO_n(\mathbb{R})$ is compact

$< \infty$.

fund. dom. for SL_2

Better illustration for volume:

Pf of Thm. [Idea: approximate volume of fund. dom using "known" number of orbits.]

We estimate $N(T) := \# SL_n(\mathbb{Z}) \backslash \{ M \in M_{n\times n}(\mathbb{Z}) \mid 0 < \det(M) \leq T \}$.

in two ways:

a) directly

b) using the volume of a fund. dom.

$\boxed{a)}$ Let $M^+_{n\times n}(\mathbb{Z}) = \{ M \in M_{n\times n}(\mathbb{Z}) \mid 0 < \det(M) \}$.
Every $SL_n(\mathbb{Z})$-orbit in $M^+_{n\times n}(\mathbb{Z})$ contains exactly one matrix M in Hermite normal form:

$$M = \begin{pmatrix} a_1 & b_{1,2} & \cdots & b_{1,n} \\ & a_2 & \ddots & \vdots \\ & & \ddots & b_{n-1,n} \\ 0 & & & a_n \end{pmatrix} \quad \text{with } a_1, \dots, a_n \geq 1 \text{ and } 0 \leq b_{ij} < a_j \quad \forall i < j.$$

[You can use row transf. to put any matrix in this form: Go column by column. In column i, while two entries in rows $j_1, j_2 \geq i$ are $\neq 0$ (w.l.o.g. both >0), subtract the smaller from the larger. Make the remaining entry >0. Then, add multiples of row i to rows $1, \dots, i-1$.]

$$\Rightarrow N(T) = \sum_{\substack{a_1, \dots, a_n \geq 1: \\ a_1 \cdots a_n \leq T}} \underset{\substack{\uparrow \\ \#\{b_{1,2}\}}}{a_2} \; \underset{\substack{\uparrow \\ \#\{(b_{13}, b_{23})\}}}{a_3^2} \cdots a_n^{n-1}$$

$$= \sum_{m \leq T} \Big(m^{-s}\text{-coeff. in } \underbrace{\zeta(s)\zeta(s-1)\cdots\zeta(s-(n-1))}_{\substack{\text{rightmost pole at } s = n \\ \text{with residue } \zeta(2)\cdots\zeta(n)}} \Big)$$

$$\underset{\substack{\uparrow \\ \text{Wiener-Ikehara} \\ \text{(or compute}}}{\sim} \frac{1}{n} \zeta(2) \cdots \zeta(n) \cdot T^n$$

(b) Let f be a measurable fund. dom. for $SL_n(\mathbb{Z}) \curvearrowright SL_n(\mathbb{R})$.
(Any $M \in M_n^+(\mathbb{R})$ can be written uniquely as λg with $\lambda \in \mathbb{R}_{>0}$, $g \in SL_n(\mathbb{R})$.)
Let $f_T(\underbrace{\lambda g}_{\in M_n^+(\mathbb{R})}) = 1_{(0,T]}(\lambda^n) \cdot f(g)$ for $\lambda \in \mathbb{R}_{>0}$, $g \in SL_n(\mathbb{R})$.

$$\Rightarrow N(T) = \sum_{M \in M_n^+(\mathbb{Z})} f_T(M)$$

$\Rightarrow$ Naively, $N(T) \sim \displaystyle\int_{M_n^+(\mathbb{R}) \subset GL_n(\mathbb{R})} f_T(M) \underbrace{d^+M}_{\det(M)^n \cdot d^\times M}$

$$\underset{\substack{\uparrow \\ \text{def. of } d^\times g}}{=} \int_{\mathbb{R}_{>0}} \int_{SL_n(\mathbb{R})} f_T(\lambda g) \cdot \lambda^{n^2} \cdot n \, d^\times g \, d^\times \lambda$$

$$= \underbrace{\int_0^{T^{1/n}} n \lambda^{n^2} \underbrace{d^\times \lambda}_{\frac{d\lambda}{\lambda}}}_{\left[\frac{1}{n}\lambda^{n^2}\right]_{\lambda=0}^{T^{1/n}}} \cdot \underbrace{\int_{SL_n(\mathbb{R})} f(g) \, d^\times g}_{vol(SL_n(\mathbb{Z}) \backslash SL_n(\mathbb{R}))}$$

$$= \frac{1}{n} vol(\ldots) \cdot T^n.$$

Combining with a), the result would follow.

One way ~~to~~ make the estimate rigorous:

Thickening the cusp: ~~Replace f by~~ Smoothen f by replacing it by $f * \eta$ for $\eta : SL_n(\mathbb{R}) \to \mathbb{R}_{\geq 0}$ smooth and compactly supported with $\int \eta(g) d^\times g = 1$.

~~Replace $1_{[0,T]}$ by a smooth approximation $\tau : \mathbb{R}_{>0} \to$ (lower or upper bound) compactly supported~~

Let $\tau : \mathbb{R}_{>0} \to \mathbb{R}_{\geq 0}$ be smooth and compactly supported.

Let $\tilde{f}_T(\lambda g) = \tau(\lambda^n / T) \cdot (f * \eta)(g)$.

$$\Rightarrow \tilde{N}(T) := \sum_{M \in SL_n(\mathbb{Z}) \backslash M_n^+(\mathbb{Z})} \tau(\det(M)/T)$$

$$= \sum_{M \in M_n^+(\mathbb{Z})} \tilde{f}_T(M)$$

$$\underset{\substack{\uparrow \\ \text{def. of } f * \eta}}{=} \int_{SL_n(\mathbb{R})} f(h) \; S(T,h) \, d^\times h$$

~~with~~ $\cancel{S(g,T) := \sum_{M = \lambda g \in M_n^+(\mathbb{Z})}} \underbrace{\tau(\lambda^n/T)\eta(h^{-1}g)}_{\cancel{\text{smooth, cpt. supp. fct. of } M \text{, scaled by a factor of } T^{1/n} \text{ from } \tau(\lambda^n)\eta(h^{-1}g)}}$

with $S(T,h) := \sum_{M \in M_n^+(\mathbb{Z})} r_{T,h}(M)$,

$r_{T,h}(\lambda g) = \tau(\lambda^n/T)\eta(h^{-1}g)$.

Note that $r_{T,h}(M) = r_{1,id}(T^{-1/n} h^{-1} M) = (T^{1/n}h) r_{1,id}(M)$ and that $r_{1,id}$ is smooth and cpt. supp.

Assume f is Siegel's fund. dom., so $\mathrm{supp}(f) \subseteq S^{\text{Siegel}} = N' B' SO_n(\mathbb{R})$

Cutting off the cusp:

If $h = \underset{\substack{\cap \\ N'}}{n}\,\underset{\substack{\cap \\ B'}}{b}\,\underset{\substack{\cap \\ SO_n(\mathbb{R})}}{k}$, $T^{1/n} b = a \in A$, then any entry in the first row of a matrix in $\mathrm{supp}(r_{T,h}) = \underbrace{T^{1/n} h}_{\substack{n a k_{\in SO_n(\mathbb{R})} \\ \begin{pmatrix} 1 & 0 \\ * & 1 \end{pmatrix} \begin{pmatrix} a_1 & \\ & \ddots \end{pmatrix}}} \underbrace{\mathrm{supp}(r_{1,id})}_{\text{compact}}$ (compact) has entries $\ll a_1$.

$\Rightarrow$ If $a_1 \ll 1$ (for a suff. small constant), then there is no $M \in M_n^+(\mathbb{Z}) \cap \mathrm{supp}(r_{T,h})$, so $S(T,h) = 0$. (All entries in the first row would have to be 0.)

Otherwise (if $a_1 \gg 1$), we apply Poisson summation.

$$S(T,h) = \sum_{M \in \underbrace{(T^{-1/n} h^{-1}) M_n^+(\mathbb{Z})}} r_{1,id}(M)$$

lattice $\Lambda = \underbrace{\Lambda' \oplus \dots \oplus \Lambda'}_{n \text{ (columns)}}$
with Λ' spanned by the columns of $T^{-1/n} h^{-1}$

The lattice Λ' is the dual of the lattice Λ'' spanned by the rows of $T^{1/n} h$. $\overset{\text{Rat}}{\Longrightarrow}$ The succ. min. of Λ' are the inverses of the succ. min. of Λ'', which are $\asymp a_1, \dots, a_n$ by Thm 7.4.1 b).

The succ. min of Λ are those of Λ', repeated n times.

$$\overset{\text{Thm } 4.2.6}{\Longrightarrow} \quad S(T,h) = T^n \int r_{1,id}(M)\, dM + O(T^n a_1^{-k})$$

$$= \int r_{T,h}(M)\, dM + O(T^n a_1^{-k})$$

$$\Rightarrow \hat{N}(T) = \int_{N' \cdot B' \cdot SO_n(\mathbb{R})} f(h) \Big(\underbrace{\int r_{T,h}(M)\, dM}_{\int_0^\infty \int_{SL_n(\mathbb{R})} \tau(\lambda^n/T)\, \underbrace{\lambda^{n^2} u\, d^\times g\, d^\times \lambda}_{\eta(h^{-1} g)}} + O(T^n \underbrace{a_1^{-k}}_{\to 0 \text{ as } a_1 \to \infty}) \Big)\, d^\times h$$

$$\left(\frac{T^{1/n}}{(b_1^{n-1} \cdots b_{n-1})^{1/n}} \asymp a_1 \gg 1\right)$$

as $T \to \infty$, the set of such $h \in S^{\text{Siegel}}$ converges to S^{Siegel}

$$\| \quad T^n \int_{SL_n} \eta(h^{-1} g)\, d^\times g \cdot \int_0^\infty n\tau(\lambda^n)\, \lambda^{n^2}\, d^\times \lambda$$

$$= T^n \cdot \int_0^\infty n\tau(\lambda^n) \lambda^{n^2} d^\times \lambda \cdot \underbrace{\int (f * \eta)(g)\, d^\times g}_{\text{vol}(\dots)} + o_{T \to \infty}(T^n).$$

Approximate $1_{[1,2]}$ from above and below by functions τ.

$\rightsquigarrow$ upper and lower bound for $N(2T)-N(T)$.

The result follows by taking the limit $T\to\infty$ for better and better approximations. $\square$

We can also compute volumes over $\mathbb{Z}_p$:

Thm 7.5.2 $\operatorname{vol}(GL_n(\mathbb{Z}_p)) = \prod_{i=1}^{n} (1-p^{-i})$.

Pf $M \in M_n(\mathbb{Z}_p)$ lies in $GL_n(\mathbb{Z}_p)$ iff $(M \bmod p) \in GL_n(\mathbb{F}_p)$.

$$\mathbb{P}((M \bmod p) \in GL_n(\mathbb{F}_p)) \underset{\substack{\uparrow \\ \text{Write} \\ M \bmod p = \begin{pmatrix} -v_1- \\ \vdots \\ -v_n- \end{pmatrix}}}{=} \prod_{i=1}^{n} \underbrace{\mathbb{P}(v_i \text{ lin. indep. from } v_1,\dots,v_{i-1} \text{ assuming } v_1,\dots,v_{i-1} \text{ are lin. indep.})}_{1-p^{(i-1)-n}}$$

$\square$

Thm 7.5.3 $\operatorname{vol}(SL_n(\mathbb{Z}_p)) = \prod_{i=2}^{n} (1-p^{-i})$

Pf
$$\mathbb{Z}_p^\times \times SL_n(\mathbb{Z}_p) \longleftrightarrow GL_n(\mathbb{Z}_p)$$
$$(t, h) \longmapsto \begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \\ & & & t \end{pmatrix} h = g$$

$$d^\times t \, d^\times h = d^\times g$$

$$\Rightarrow \underset{\substack{\| \\ 1-p^{-1}}}{\operatorname{vol}(\mathbb{Z}_p^\times)} \cdot \operatorname{vol}(SL_n(\mathbb{Z}_p)) = \underset{\substack{\| \\ \prod_{i=1}^{n}(1-p^{-i})}}{\operatorname{vol}(GL_n(\mathbb{Z}_p))}$$

$\square$

<u>Cor 7.5.4</u> $\mathrm{vol}(SL_n(\mathbb{Z})\backslash SL_n(\mathbb{R}))\cdot\prod_p \mathrm{vol}(SL_n(\mathbb{Z}_p))=1.$

This is not a coincidence! It is closely related to the fact that $SL_n(\mathbb{Q})$ has Tamagawa number 1:

$$\mathrm{vol}(SL_n(\mathbb{Q})\backslash SL_n(\mathbb{A}(\mathbb{Q})))=1$$

8. Ideals in quadratic number fields

For any (comm.) ring R, let $V(R)$ be the set of binary quadr. forms with coeff. in R: $f(X,Y) = aX^2 + bXY + cY^2$ $(a,b,c \in R)$

~~The discriminant~~

Let $GL_2(R)$ act on $V(R)$ by

$$(Mf)(v) = \det(M)^{-1} \cdot f(M^T v) \quad \text{for } M \in GL_2(R),\ f \in V(R),\ v \in R^2.$$

Lemma 8.1 The discriminant $\operatorname{disc}(f) = b^2 - 4ac$ is an invariant:

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

Remark $\begin{pmatrix} \lambda & \\ & \lambda \end{pmatrix} f = f$, so the action factors through $PGL_2(R) = GL_2(R)/R^\times$

Let K be a field with $\operatorname{char}(K) \neq 2$. For any $D \in K^\times$, consider the K-algebra $L_D = K[X]/(X^2 - D)$ of degree 2. Rmk If $D \notin K^{\times 2}$, then $L_D \cong K(\sqrt{D})$.
$\alpha_D \leftrightarrow \sqrt{D}$

Otherwise, $L_D \cong K \times K$.
$\alpha_D \leftrightarrow (\sqrt{D}, -\sqrt{D})$

Let $\alpha_D \in L_D$ be the image of X.

Rmk $(1, \alpha_D)$ and $(1, \tau_D)$ are K-bases of L_D.

$$\tau_D = \frac{D + \alpha_D}{2}$$

Lemma 8.2 Let $K = \mathbb{Q}$. If L is ~~an étale ext. of $\mathbb{Q}$ of degree 2~~ a quadr. number field with discriminant D, then $L \cong L_D$ and $(1, \tau_D)$ is a $\mathbb{Z}$-basis of the ring of integers of L_D.

Pf ~~The min. pol. of $a + b\tau_D$ is~~

$$\cancel{\left(X - a - b\cdot\frac{D+\alpha_D}{2}\right)\left(X - a - b\cdot\frac{D-\alpha_D}{2}\right)}$$

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

$$\cancel{= X^2 + a^2 + b^2\frac{D^2}{4} - 2aX - bDX + abD - b^2\frac{D}{4}}$$

Let $L = \mathbb{Q}(\sqrt{t})$, $t \in \mathbb{Z}$ squarefree.

If $t \not\equiv 1 \bmod 4$, then $(1, \sqrt{t})$ is an integral basis and $D = 4t$

If $t \equiv 1 \bmod 4$, then $\left(1, \frac{1+\sqrt{t}}{2}\right)$ — " — $D = t$. □

Def Such a number $D \in \mathbb{Z}$ is a fundamental discriminant.

Rmks D is a fund. disc. if and only if

$D \neq 0, 1$ and: $D \equiv 1 \bmod 4$ is squarefree, or $\mathbb{Z} \ni \frac{D}{4} \not\equiv 1 \bmod 4$ is sqfree.

~~D is squarefree and~~

~~$D \equiv 1$~~

<u>Thm 8.3</u> We have a $GL_2(K)$-equivariant bijection

$$L_D^\times \backslash \{K\text{-basis } (\omega_1,\omega_2) \text{ of } L_D\} \xleftrightarrow{(*)} \{f \in V(K) \mid disc(f) = D\}$$

$$[(\omega_1,\omega_2)] \longmapsto \frac{Nm_{L_D|K}(X\omega_1 + Y\omega_2)}{Nm(\omega_1,\omega_2)}$$

$$\text{with } Nm(\omega_1,\omega_2) := \det_K \begin{pmatrix} 1 \mapsto \omega_1 \\ \tau_D \mapsto \omega_2 \end{pmatrix}$$

$$\left[\left(1, \frac{b+\alpha_D}{2a}\right)\right] \text{ if } a\neq 0 \longleftarrow\!\!\!\shortmid \quad aX^2 + bXY + cY^2$$

$$\dots \qquad \text{if } a=0$$

Here, $L_D^\times$ acts on {basis} by mult.: $s(\omega_1,\omega_2) = (s\omega_1, s\omega_2)$

and $GL_2(K)$ — " — by matrix mult., considering (ω_1,ω_2) a vector.

<u>Pf</u> The map $L_D^\times\backslash\{\text{basis}\} \to V(K)$ is well-def.:

If we apply $s \in L_D^\times$, then the numerator and denominator of the RHS are multiplied by $Nm(s) = \det_K(\text{mult. by } s)$.

The map is $GL_2(K)$-equivariant:

The RHS can be defined by

$$f(v) = \frac{Nm\left(\begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix} \cdot v\right)}{\det\begin{pmatrix} 1 \mapsto \omega_1 \\ \tau_D \mapsto \omega_2\end{pmatrix}}.$$

$\uparrow$ dot product

$\Rightarrow M(\omega_1,\omega_2) = (\omega_1',\omega_2')$ is sent to

$$\frac{Nm\left(M\begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix}\cdot v\right)}{\det\begin{pmatrix} 1 \mapsto \omega_1' \\ \tau_D \mapsto \omega_2'\end{pmatrix}} = \frac{Nm\left(\begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix} \cdot M^T v\right)}{\det\begin{pmatrix} 1 \mapsto \omega_1 \\ \tau_D \mapsto \omega_2\end{pmatrix} \cdot \det(M)} = (Mf)(v)$$

We have $disc(f) = D$:

Since $GL_2(K)$ acts transitively on {basis} and $disc(Mf) = disc(f)$, it suffices to check this for one basis $(1,\alpha_D)$, for which $f = \frac{X^2 - DY^2}{2}$.

That the maps are inverses can be checked directly. $\square$

Cor 8.4 a) $GL_2(K)$ acts transitively on $\{f \mid disc = D\}$.

b) $Stab_{GL_2(K)}(f) \cong L_D^\times$.

Pf a) $GL_2(K)$ acts transitively on {basis}.

b) we have

$Stab \longrightarrow L_D^\times$

$M \longmapsto s \in L_D^\times$ such that $M(\omega_1, \omega_2) = s(\omega_1, \omega_2)$. □

Thm 8.5 Let $K = \mathbb{Q}$ and let be a quadr. n.f. with discriminant D.

Then, (*) restricts to a $GL_2(\mathbb{Z})$-equivariant bijection

$L_D^\times \backslash \{\mathbb{Z}\text{-basis } (\omega_1, \omega_2) \text{ of a fractional ideal of } L_D\} \longleftrightarrow \{f \in V(\mathbb{Z}) \mid disc(f) = D\}$

Pf Let $\mathfrak{a} = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$.

"⇒" If $\mathfrak{a}$ is a fractional ideal, then

$x\omega_1 + y\omega_2 \in \mathfrak{a} \quad \forall x, y \in \mathbb{Z}$

$\Rightarrow Nm(x\omega_1 + y\omega_2)$ is divisible by $Nm(\mathfrak{a}) = |Nm(\omega_1, \omega_2)|$

$\Rightarrow f(x,y) \in \mathbb{Z} \quad \forall x, y \in \mathbb{Z}$

$\Rightarrow f \in V(\mathbb{Z})$.

"⇐" If $f \in V(\mathbb{Z})$, we can take $\omega_1 = 1$, $\omega_2 = \frac{b + \sqrt{D}}{2a}$.

(Note that $D = b^2 - 4ac \notin \mathbb{Q}^{\times 2}$, so $a \neq 0$.)

We need to check that $\underbrace{\mathbb{Z}[\tau_D]}_{= \mathcal{O}_L} \cdot \mathfrak{a} \subseteq \mathfrak{a}$, i.e. that $\tau_D \mathfrak{a} \subseteq \mathfrak{a}$:

$\tau_D \omega_1 = \tau_D = \frac{D-b}{2} \cdot \omega_1 + a \cdot \omega_2 \in \mathfrak{a}$ because $D \equiv b^2 - 4ac \equiv b \bmod 2$

$\tau_D \omega_2 = -c \cdot \omega_1 + \frac{D+b}{2} \cdot \omega_2 \in \mathfrak{a}$ □

Cor 8.6 a) We obtain a bijection

$$\mathcal{C}\ell(L) \longleftrightarrow GL_2(\mathbb{Z}) \backslash \{ f \in V(\mathbb{Z}) \mid \mathrm{disc} = D \}.$$

b) $\mathrm{Stab}_{GL_2(\mathbb{Z})}(f) \cong \mathcal{O}_L^\times$.

Pf a) $GL_2(\mathbb{Z})$ acts transitively on the $\mathbb{Z}$-bases of $\mathfrak{a}$.

b) If $M(\omega_1, \omega_2) = s(\omega_1, \omega_2)$ with $M \in GL_2(\mathbb{Z})$, then $\mathfrak{a} = s\mathfrak{a}$, so $s \in \mathcal{O}_L^\times$.

If $s \in \mathcal{O}_L^\times$, then $\mathfrak{a} = s\mathfrak{a}$, so there is a change of $\mathbb{Z}$-basis sending (ω_1, ω_2) to $s(\omega_1, \omega_2)$. $\square$

~~Remark In particular, $GL_2(\mathbb{Z}) \circlearrowleft \{ f \in V(\mathbb{Z}) \mid \mathrm{disc} = D \}$ has a fund. dom. if and only if $\mathcal{O}_L^\times$~~

Lemma 8.7 a) If $D > 0$, then $GL_2(\mathbb{Z}) \circlearrowleft \{ f \in V(\mathbb{Z}) \mid \mathrm{disc} = D \}$ has no fund. dom.

b) If $D < 0$, then

$S := \{ f \in V(\mathbb{Z}) \mid \mathrm{disc} = D, \ |b| \le a \le c \}$

is an almost fund. dom. The associated fund. dom. χ satisfies $\chi(f) = \frac{1}{2}$ for all f in the interior of S.

Pf a) $\mathrm{Stab} \cong \mathcal{O}_L^\times$ is infinite.

b) We have an $SL_2(\mathbb{R})$-equivariant

$$GL_2(\mathbb{R})/O_2(\mathbb{R}) \longleftrightarrow \{f \in V(\mathbb{R}) \mid \mathrm{disc}(f) < 0\}$$

$$M = \begin{pmatrix} - v_1 - \\ - v_2 - \end{pmatrix} \longmapsto \|Xv_1 + Yv_2\|^2$$

with $-4\det(M) = \mathrm{disc}(f)$.

Minkowski's almost fund. dom. $\{ \binom{v_1}{v_2} \mid \|v_1\| \le \|v_2\|, |v_1 \cdot v_2| \le \frac{1}{2}\|v_1\|^2 \}$ for $GL_2(\mathbb{Z}) \curvearrowright GL_2(\mathbb{R})/O_2(\mathbb{R})$ is mapped to $\{f \mid |b| \le a \le c\}$.

We have $GL_2(\mathbb{Z}) = SL_2(\mathbb{Z}) \cup \begin{pmatrix} -1 & \\ & 1 \end{pmatrix} SL_2(\mathbb{Z})$.

Think about how $\begin{pmatrix} -1 & \\ & 1 \end{pmatrix}$ acts on LHS and RHS ... "$\square$"

Thm 8.8 $\displaystyle\sum_{\substack{K \text{ imag. quadr. n.f.} \\ 0 < -\mathrm{disc}(K) \le T}} h_K \sim C \cdot T^{3/2}$

~~We thus conclude~~

~~Ingredients~~

1) $\displaystyle\sum_{\substack{K \text{ imaginary} \\ \text{quadr. n.f.} \\ 0 < -\mathrm{disc}(K) \le T}} h_K$ ~~$= \#\{f \in V(\mathbb{Z}) \mid |b| \le a \le c, -(b^2 - 4ac) \le T \text{ fundamental disc.}\}$~~

$$= \sum_{\substack{f \in V(\mathbb{Z}): \\ 0 < -\mathrm{disc}(f) \le T \\ \mathrm{disc}(f) \text{ fund. disc.}}} \chi(f) = \sum_{\substack{f \in V(\mathbb{Z}) \cap S \\ 4ac - b^2 \le T \\ -b^2 + 4ac \text{ fund. disc}}} \frac{1}{2} + O\Bigg(\sum_{\substack{f \in V(\mathbb{Z}) \cap \partial S \\ 4ac - b^2 \le T \\ -b^2 + 4ac \text{ f.d.}}} 1 \Bigg)$$

2) Cut off cusp: If $|a| < 1$, then $a = 0$, so $b = 0$, so $\mathrm{disc}(f) = b^2 - 4ac = 0$.

3) Davenport's lemma [Note: the region in $\mathbb{R}^3$ is scaled by a factor of $T^{1/2}$ $\Rightarrow \mathrm{vol} \sim T^{3/2}$]

4) Sieve for fund. disc.
(E.g. for any $p \neq 2$, remove $f \in V(\mathbb{Z})$ such that $p^2 \mid b^2 - 4ac$.)

Rmk $\sum_{K\ldots} 1 \sim C'' \cdot T$ by Pset 1

$\leadsto$ on average, $h_K R_K$ is $\asymp T^{1/2}$ for a q.n.f. of disc $\asymp T$.

~~Brauer-Siegel~~

We will also ~~show~~ sketch how to show:

Thm 8.9

$$\sum_{\substack{K \text{ real q.n.f.} \\ 0 < \operatorname{disc}(K) \leq T}} h_K R_K \sim C' \cdot T^{3/2}$$

Brauer-Siegel Theorem

Let K be a n.f. of degree n and let $\varepsilon > 0$.

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

[These keep showing up together and are difficult to separate!]

Reminder $\quad \operatorname{disc}(f) = D = \operatorname{disc}(L)$ (L quadr. n.f.) $\quad \rightsquigarrow L = \mathbb{Q}[X]/(X^2-D)$

$\cancel{\operatorname{Stab}_{GL_2(\mathbb{Z})}(f) \simeq \mathcal{O}_L^\times}$

$$L \otimes \mathbb{R} = \mathbb{R}[X]/(X^2-D) = \begin{cases} \mathbb{C}, & D<0 \\ \mathbb{R}\times\mathbb{R}, & D>0 \end{cases}$$

$\cancel{\operatorname{Stab}_{GL_2(\mathbb{R})}(f) \simeq}$

$$\begin{tikzcd} \operatorname{Stab}_{GL_2(\mathbb{Z})}(f) \arrow[r, "\sim"] \arrow[d, hook] & \mathcal{O}_L^\times \arrow[d, hook] \\ \operatorname{Stab}_{GL_2^{\pm 1}(\mathbb{R})}(f) \arrow[r, "\sim"] \arrow[d, hook] & (L\otimes\mathbb{R})^{\pm 1} \arrow[d, hook] \\ \operatorname{Stab}_{GL_2(\mathbb{R})}(f) \arrow[r, "\sim"] & (L\otimes\mathbb{R})^\times \end{tikzcd}$$

$Cl(L) \longleftrightarrow GL_2(\mathbb{Z})\backslash\{f \in V(\mathbb{Z}) \mid \operatorname{disc}(f)=D\}$

$\{*\} \longleftrightarrow GL_2^{\pm 1}(\mathbb{R})\backslash\{f \in V(\mathbb{R}) \mid \operatorname{disc}(f)=D\}$ [$\mathbb{R}^\times \subseteq GL_2(\mathbb{R})$ acts trivially]

$\{*\} \longleftrightarrow GL_2(\mathbb{R})\backslash\{f \in V(\mathbb{R}) \mid \operatorname{disc}(f)=D\}$

$$(L\otimes\mathbb{R})^\times = \begin{cases} \mathbb{C}^\times \\ \mathbb{R}^\times \times \mathbb{R}^\times \end{cases}$$

Let $GL_2^{\pm 1}(\mathbb{R}) = \{M \in GL_2(\mathbb{R}) \mid \det(M) = \pm 1\}$,

$$(L\otimes\mathbb{R})^{\pm 1} = \{x \in (L\otimes\mathbb{R})^\times \mid Nm(x) = \pm 1\} = \begin{cases} S^1 = \{x \in \mathbb{C}^\times \mid |x| = 1\} \\ \{(s,t) \in \mathbb{R}^\times \times \mathbb{R}^\times \mid st = \pm 1\} \cong \{\pm 1\}\times\mathbb{R}^\times \end{cases}$$

To prove this, we need a more general concept of fundamental domains. For motivation:

Lemma 8.10

Let G act transitively on X with finite stabilisers.
Let α be a fund. dom. for the left action of $H \subseteq G$ on G.
Let $x_0 \in X$. For any $x \in X$, let $\beta(x) = \sum_{\substack{g \in G: \\ x = g x_0}} \alpha(g)$.

Then, $\sum_{x \in Hy} \beta(x) = [\mathrm{Stab}_G(y) : \mathrm{Stab}_H(y)]$ for all $y \in \underset{\overset{\shortparallel}{G x_0}}{X}$.

Rmk If $\alpha = \mathbb{1}_A$ for some subset A of G, then β is the characteristic function of the multiset $A x_0$.

Rmk We'd like to apply this with $X = \{f \in V(\mathbb{R}) \mid \mathrm{disc}(f) = D\}$, $G = GL_2(\mathbb{R})$, $H = GL_2($

Pf of Lemma

Let $y = a x_0$, $a \in G$.

$$\sum_{x \in Hy} \beta(x) \underset{\underset{x = hy}{\uparrow}}{=} \frac{1}{\#\mathrm{Stab}_H(y)} \sum_{h \in H} \beta(hy)$$

$$= \text{—}\,''\,\text{—} \sum_{h \in H} \sum_{\substack{g \in G: \\ hy = g x_0 \\ \shortparallel \\ h a x_0}} \alpha(g)$$

$$\underset{\underset{g = has}{\uparrow}}{=} \text{—}\,''\,\text{—} \sum_{h \in H} \sum_{s \in \mathrm{Stab}_G(x_0)} \alpha(has)$$

$$\underset{\underset{(\alpha \text{ f.d. for } H \subseteq G)}{\uparrow}}{=} \frac{\#\mathrm{Stab}_G(x_0)}{\#\mathrm{Stab}_H(y)} = \frac{\#\mathrm{Stab}_G(y)}{\#\mathrm{Stab}_H(y)}. \qquad \square$$

We need to work with infinite stabilisers, though!

<u>Lemma 8.11</u>

Let G [redacted] act transitively on X.

Let α be a fund. dom. for the left action of a <u>countable</u> subgroup $H \subseteq G$ on G. [redacted]

[redacted] For each $x \in X$, [redacted]

assume $\mathrm{Stab}_G(x)$ is a topological group with Haar measure $d_x s$ and assume that they are compatible under the isomorphisms

$$\begin{aligned} \mathrm{Stab}_G(x) &\xrightarrow{\sim} \mathrm{Stab}_G(gx) . \\ s &\longmapsto g s g^{-1} \end{aligned}$$

(i.e. this [redacted] is a homeom. and $d_{gx}(gsg^{-1}) = d_x s$.)

Let $x_0 \in X$. For any $x \in X$, let $\beta(x) = \int_{\mathrm{Stab}_G(x_0)} \alpha(gs)\, d_{x_0} s = \int_{\mathrm{Stab}_G(x)} \alpha(sg)\, d_x s$.
$\quad x = g x_0$

(This is independent of the choice of g! [redacted])

Then, $\sum_{x \in Hy} \beta(x) = \mathrm{vol}(\mathrm{Stab}_H(y) \backslash \mathrm{Stab}_G(y))$ for all $y \in X$,

assuming there is a measurable fund. dom. σ for the left action of $\mathrm{Stab}_H(y)$ on $\mathrm{Stab}_G(y)$.

<u>Rmk</u> The previous lemma is the case where [redacted] $\mathrm{Stab}_G(x)$ has the discrete top. and counting measure (assuming H is countable).

Pf let $y = a x_0$, $a \in G$.

$$\sum_{x \in Hy} \beta(x) = \sum_{h \in H/\mathrm{Stab}_H(y)} \beta(\underbrace{hy}_{hax_0})$$

$$= \sum \int_{\mathrm{Stab}_G(hy)} \alpha(sha)\, d_{hy} s$$

$$\underset{s = hth^{-1}}{=} \sum \int_{\mathrm{Stab}_G(y)} \alpha(hta)\, d_y t$$

$$\underset{\substack{\sigma \text{ fund.} \\ \text{dom. for } \mathrm{Stab}_H(y) \curvearrowright \mathrm{Stab}_G(y)}}{=} \sum \int \sum_{u \in \mathrm{Stab}_H(y)} \sigma(u^{-1}t)\, \alpha(hta)\, d_y t$$

$$\underset{t = us}{=} \sum \int \sum \sigma(s)\, \alpha(husa)\, d_y s$$

$$= \sum_{h \in H} \int \sigma(s)\, \alpha(hsa)\, d_y s$$

$$\underset{\substack{\alpha \text{ fund. dom.} \\ \text{for } H \curvearrowright G}}{=} \int \sigma(s)\, d_y s$$

$$= \mathrm{vol}(\mathrm{Stab}_H(y) \backslash \mathrm{Stab}_G(y)).$$

$\square$

If $D<0$ (imaginary case), then

$$\mathrm{vol}\left(\mathrm{Stab}_{GL_2(\mathbb{Z})}\backslash \mathrm{Stab}_{GL_2^{\pm 1}(\mathbb{R})}\right) = \frac{1}{\# \mathcal{O}_L^\times} \cdot \underbrace{\mathrm{vol}(S^1)}_{2\pi\ (?)} .$$

$X := \{ f \in V(\mathbb{R}) \mid \mathrm{disc}(f) = D \}$

Taking $\alpha :=$ Minkowski's fund. dom (for $\|\cdot\|_2$),

$$x_0 := \frac{\sqrt{|D|}}{2}(X^2+Y^2) \in V(\mathbb{R})$$

$$\mathrm{Stab}_{GL_2^{\pm 1}(\mathbb{R})}(x_0) = O_2(\mathbb{R}),$$

one gets $\beta \simeq c \cdot 1_{\{|b| \le a \le c\}}$ ~~as before~~

(as last time).

<u>If $D>0$</u> (real case), then

$$\mathrm{vol}\left(\mathrm{Stab}_{GL_2(\mathcal{O})} \backslash \mathrm{Stab}_{GL_2^{\pm 1}(\mathbb{R})}\right) = R_K$$ (times a constant)

Take $x_0 = \sqrt{D}\, XY \in V(\mathbb{R})$.

$$\mathrm{Stab}_{GL_2^{\pm 1}(\mathbb{R})}(x_0) = \left\{ \begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix} \right\}$$

Cleaner example of fund. dom. α to use:

<u>Lemma 8.12</u> The set A of matrices $g = \begin{pmatrix} x_1 & y_1 \\ x_2 & y_2 \end{pmatrix} \in GL_2(\mathbb{R})$ such that

a) $x_2, y_1 \geq x_1, -y_2 \geq 0$

or

b) $x_2, -y_1 \geq x_1, y_2 \geq 0$

is an almost fundamental domain for $GL_2(\mathbb{Z}) \circlearrowleft GL_2(\mathbb{R})$.

Let α be the corr. fund. dom. If the strict inequalities are satisfied, then $\alpha(g) = 1$.

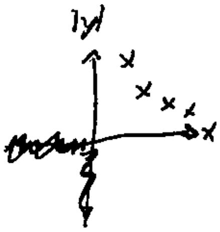
~~Pf~~ (sketch) Let Λ be a full lattice in $\mathbb{R}^2$. Assume Λ contains no nonzero vectors of the form $(x,0)$ or $(0,y)$.

Let $B = \{(x,y) \in \Lambda \mid x>0,\ \nexists (x',y') \in \Lambda : 0<x'<x,\ |y'| \le |y|\}$

Clearly, $B \neq \emptyset$.

$v_1, v_2 \in B$, $v_1=(x_1,y_1)$, $v_2=(x_2,y_2)$

If , then either



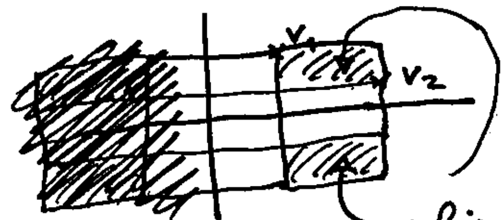
a) $\{x_1\} < \{x_2\}$ and $|y_1| > |y_2|$ (write this as $v_1 < v_2$)

or

b) $\{x_1\} > \{x_2\}$ and $|y_1| < |y_2|$ ($v_1 > v_2$)

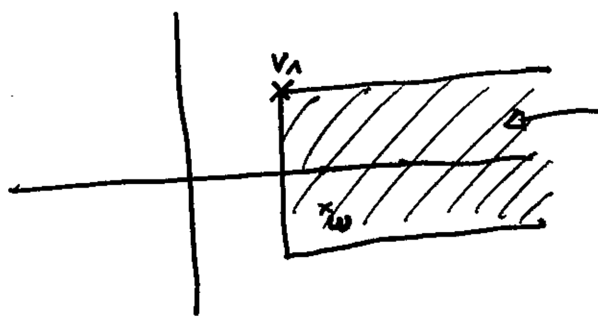
SKIP

For any $v_1, v_2 \in A$, there are only finitely many $w \in L$ with $v_1 < w < v_2$.



For every $v_1 \in A$, there exists a smallest $v_2 \in A$ with $v_2 > v_1$ and a largest $v_3 \in B$ with $v_3 < v_1$

~~(by Minkowski's first theorem)~~

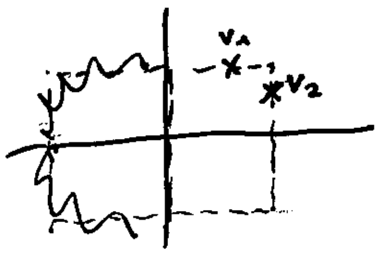


~~Say v, w have positive x-coordinates.~~
~~Then, their y-coordinates have opposite signs:~~
~~Otherwise, $w - v_1$ would have x-coord~~

~~Let~~ **Claim** $v_i = (x_i, y_i)$. Then, y_1, y_2 have opposite signs:

~~Say $x_1, x_2 > 0$. Then, y_1, y_2 have opposite signs~~

Pf Say $y_1, y_2 > 0$. Then, $v_2 - v_1 = (x_2 - x_1, y_2 - y_1) \in \Lambda$ has $0 < x_2 - x_1 < x_2$ and $|y_2 - y_1| \le y_1$. ↯

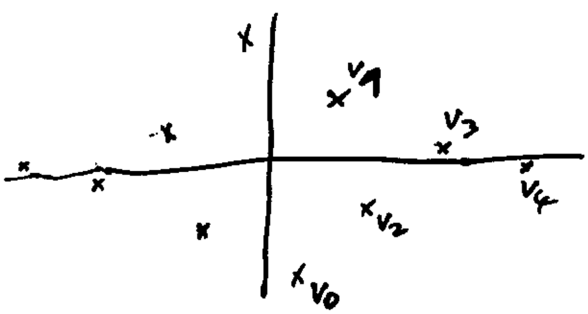


Claim v_1, v_2 form a basis of Λ. other

Pf The triangle $(0, v_1, v_2)$ contains no el. of Λ.
$\Rightarrow$ The parallelogram spanned by v_1, v_2 contains no lattice points besides $0, v_1, v_2, v_1 + v_2$. $\square$

Conclusion:

$B_\Lambda = \{\dots, v_{-1}, v_0, v_1, \dots\}$ with $\dots < v_{-1} < v_0 < v_1 < v_2 < \dots$ and, {assuming the x-coord. are > 0}, the y-coord. have alternating signs.

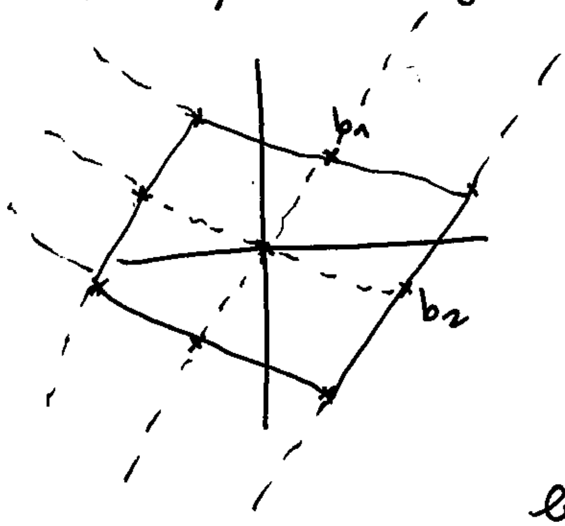


There is usually a unique index n such that v_n lies in $\{(x,y) \mid |x| \le |y|\}$ and v_{n+1} lies in $\{(x,y) \mid |x| \ge |y|\}$.

Then, $\begin{pmatrix} -v_n- \\ -v_{n+1}- \end{pmatrix}$ lies in A and in the $GL_2(\mathbb{Z})$-orbit corresponding to Λ.

Conversely, say (b_1, b_2) is a basis of Λ with $\begin{pmatrix} -b_1- \\ -b_2- \end{pmatrix} \in A_q$

~~The interior of the convex set spanned by $\pm b_1, \pm b_2$ contains no nonzero lattice points.~~



~~The parallelograms in this picture contain no lattice points in their interior.~~

Then, b_1, b_2 must be consecutive vectors in $\dots, v_0, v_1, \dots$

because there is no lin. combo $\underset{(0,0)\neq(x,y)}{=} c_1 b_1 + c_2 b_2 \in$

with $x < x_2$, $|y| < |y_1|$.

$\Downarrow$ c_1, c_2 have different signs

$\Downarrow$ c_1, c_2 have same sign

$\square$

Rmk You can compute v_{n+2} from v_n, v_{n+1} as follows:

$$v_{n+2} = v_n + k v_{n+1}, \quad \text{where } 1 \le k \in \mathbb{Z} \text{ is chosen so that}$$

y_{n+2} has the opposite sign as y_{n+1} and smaller magnitude:

~~If $y_n > 0$, $y_{n+1} < 0$, say, then $k = \left\lceil \frac{y_n}{-y_{n+1}} \right\rceil$~~

$$k = \left\lceil -\frac{y_n}{y_{n+1}} \right\rceil. \qquad \rightsquigarrow \frac{y_{n+2}}{y_{n+1}} = \frac{y_n}{y_{n+1}} + \left\lceil -\frac{y_n}{y_{n+1}} \right\rceil$$

~~(smells like continued fraction)~~

Rmk This gives you the "continued fraction" algorithm for computing a fund. unit of $\mathcal{O}_L$:

Start with a basis (v_0, v_1) of any fractional ideal $\mathfrak{a} \subseteq L \subseteq \mathbb{R}\times\mathbb{R}$.
$v_0, v_1 \in L$

Compute $v_2, v_3, \ldots$

If $u \in \mathcal{O}_L^\times$, then uv_0 must also lie in B ($\in u\mathfrak{a} = \mathfrak{a}$) ~~$(uv_0, uv_1)$ is also a reduced basis of $u\mathfrak{a} = \mathfrak{a}$.~~ $\Rightarrow uv_0 = v_p$ for some $p \in \mathbb{Z}$.

(and then $uv_i = v_{p+i} \ \forall i \in \mathbb{Z}$)

$\Rightarrow$ The first unit in the sequence $\frac{v_1}{v_0}, \frac{v_2}{v_0}, \ldots$ is a fund. unit.

__Lemma 8.13__ Let α be the corresponding fund. dom. for $GL_2(\mathbb{Z}) \curvearrowright GL_2^{\pm 1}(\mathbb{R})$ and define β as in Lemma 8.11. Let $f = aX^2 + bXY + cY^2 \in V(\mathbb{R})$ with $\operatorname{disc}(f) = D$. We have $\beta(f) \neq 0$ and only if $a \geq 0, c \leq 0, b \geq |a+c|$. Then, $\beta(f) = C \cdot \log \frac{\sqrt{D}+b}{\sqrt{D}-b}$. [This is ∞ if $ac = 0$, but then D is a square!]

__Pf__ Assume $a \neq 0$. Note that $f = g' \sqrt{D} XY$ for

$$g' = \begin{bmatrix} 1 & 1 \\ \frac{b \pm \sqrt{D}}{2a} & \frac{b \mp \sqrt{D}}{2a} \end{bmatrix} \in GL_2(\mathbb{R})$$

$$\Rightarrow f = g \sqrt{D} XY \text{ with } g = \frac{g'}{\sqrt{|\det(g')|}} \in GL_2^{\pm 1}(\mathbb{R}).$$

Recall: $\mathrm{Stab}_{GL_2^{\pm 1}(\mathbb{R})}(\sqrt{D} XY) = \{ \begin{pmatrix} s & \\ & t \end{pmatrix} \mid s, t \in \mathbb{R}^\times, st = \pm 1 \}$.

We have $g \begin{pmatrix} s & 0 \\ 0 & t \end{pmatrix} \in A$ if and only if

~~$s > 0$, $t \geq 0$, $t \geq s$, $(-b+\sqrt{D}) \cdot s \geq (b+\sqrt{D}) \cdot t$~~

~~$2a \leq -b+\sqrt{D}$, $b+\sqrt{D} \leq 2a$~~

~~$s > 0$, $s \leq |t|$, $(\sqrt{D}-b) \cdot |t| \leq (\sqrt{D}+b) \cdot s$,~~

~~$2a \leq b+\sqrt{D}$, $\sqrt{D}-b \leq 2a$.~~

$a \geq 0$, $c \leq 0$, $b \geq |a+c|$, $1 \leq \underbrace{\frac{|t|}{s}}_{= \frac{1}{s^2}} \leq \frac{\sqrt{D}+b}{\sqrt{D}-b}$

~~This is equiv. to~~

$$\cancel{|\sqrt{D}-2a| \leq b \leq \sqrt{D} \quad \text{and } s>0 \text{ and } \quad 1 \leq \underset{\overset{\parallel}{s^{-2} \text{ if } \begin{pmatrix} s & \\ & t \end{pmatrix} \in GL_2^{\pm 1}(\mathbb{R})}}{\frac{|t|}{s}} \leq \frac{\sqrt{D}+b}{\sqrt{D}-b}}.$$

$$\int\limits_{\substack{GL_2^{\pm 1}(\mathbb{R}) \\ s>0, \\ 1 \leq \frac{|t|}{s} \leq \frac{\sqrt{D}+b}{\sqrt{D}-b}}} d^{\times}\begin{pmatrix} s & \\ & t \end{pmatrix} = C \cdot \log \frac{\sqrt{D}+b}{\sqrt{D}-b}.$$

The cases $a=0$ works similarly... (?) $\square$

<u>Summary</u> If $D > 0$ is the disc. of a q.r.f. L, then

$$h_L R_L = C' \sum_{\substack{f \in V(\mathbb{Z}) \\ \mathrm{disc}(f)=D}} \beta(f) = C'' \sum_{\substack{f \in V(\mathbb{Z}) \\ \mathrm{disc}(f)=D \\ |\sqrt{D}-2a| \leq b \leq \sqrt{D} \\ a \geq 0}} \log \frac{\sqrt{D}+b}{\sqrt{D}-b}.$$

This can be used to show Thm 8.9:

$$\sum_{0<\mathrm{disc}(L) \leq T} h_L R_L \sim C''' T^{3/2}.$$

(For example, use a variant of Davenport's Lemma.)

~~[illegible]~~ Let $G, H, X, \alpha, \beta, \ldots$ as in Lemma 8.11. Assume X is a ~~[illegible]~~ measure ~~[illegible]~~ space with measure dx

Let dg be a measure on G such that

$$\int_G \rho(g)\,dg = \int_X \int_{\mathrm{Stab}_G(x_0)} \rho(gs)\,d_{x_0}s\,dx$$ for all reasonable g and all $x_0 \in X$.

where we write $x = g x_0$

$\rightsquigarrow$ In particular, $\int_X \beta(x)\,dx = \int_G \alpha(g)\,dg$.

Each base point $x_0 \in X$ gives you a function $\beta = \beta_{x_0}$ such that $\sum_{z \in Hy} \beta_{x_0}(z) = \mathrm{vol}(\mathrm{Stab}_H(y) \backslash \mathrm{Stab}_G(y))$ $\forall y \in X$.

Idea: To smoothen β, average over $x_0 \in X$ using a smooth weight $\eta(x_0)$:

$$\tilde{\beta}(z) := \int_X \beta_{x_0}(z)\, \eta(x_0)\, dx_0$$

$$= \int_X \int_{\mathrm{Stab}_G(x_0)} \alpha(gs)\, dx_{0s}\, \eta(x_0)\, dx_0$$

with $z = g x_0$

$$\underset{g' = g^{-1}}{=} \int_G \alpha(g'^{-1})\, \eta(g'^{-1} z)\, dg'$$

= average over g' in fund. domain of $\underbrace{g' \text{ translates of } \eta}_{\text{count points in here!}}$.

9. Counting algebraic integers

~~Let $\overline{\mathbb{Z}} \subset \overline{\mathbb{Q}}$ be the set of alg. integers.~~

<u>Def</u> $\deg(\alpha) = \deg(\text{min. pol. of } \alpha)$ for $\alpha \in \overline{\mathbb{Q}}$.

<u>Def</u> The <u>length</u> of $\alpha \in \overline{\mathbb{Q}}$ is

$$|\alpha| = \max_{\sigma : \overline{\mathbb{Q}} \to \mathbb{C}} \underbrace{|\sigma(\alpha)|}_{\substack{\text{the usual} \\ \text{absolute value (magnitude)} \\ \text{on } \mathbb{C}}} .$$

<u>Rmk</u> This agrees with the def. of $|\alpha|$ for $\alpha \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ in section 4.3.

<u>Def</u> Let $\overline{\mathbb{Z}}$ be the set of alg. integers in $\overline{\mathbb{Q}}$.

Let $\overline{\mathbb{Z}}_n = \{\alpha \in \overline{\mathbb{Z}} \text{ of degree } n\}$.

<u>Goal</u> Count $\alpha \in \overline{\mathbb{Z}}_n$ with $|\alpha| \leq T$.

<u>Idea</u> Count minimal polynomials.

<u>Def</u> Let $\pi : \mathbb{C}^n \longrightarrow \left\{ \substack{f \in \mathbb{C}[X] \\ \text{monic deg. } n} \right\} \cong \mathbb{C}^n$.

$$(\alpha_1, \dots, \alpha_n) \mapsto \prod_{i=1}^{n} (X - \alpha_i) \qquad X^n + a_{n-1}X^{n-1} + \dots + a_0 \mapsto (a_0, \dots, a_{n-1})$$

Thm 9.1 For any $n \geq 1$, there is a constant $C_n > 0$ such that $\#\{\alpha \in \overline{\mathbb{Z}}_n \mid |\alpha| \leq T\} \underset{n}{\sim} C_n T^{n(n+1)/2}$.

Ex $n = 1 \Rightarrow \overline{\mathbb{Z}}_n = \mathbb{Z}$

$LHS \sim 2T$.

More precisely:

Thm 9.2 For any $r_1, r_2 \geq 0$ with $r_1 + 2r_2 = n$, there is a constant $C_{r_1,r_2} > 0$ s.t. $\#\{\alpha \in \overline{\mathbb{Z}}_n$ of signature $(r_1,r_2) \mid |\alpha| \leq T\} \sim C_{r_1,r_2} T^{n(n+1)/2}$

Pf

$\boxed{\text{let } A = \{ a \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \mid \underset{\rho_i(a) \neq \rho_j(a)\, \forall i \neq j}{|a| \leq 1} \},\ A_T = T \cdot A = \{ a \mid \underset{\rho_i(a) \neq \rho_j(a)\, \forall i \neq j}{|a| \leq T} \}.}$

let $\rho_1, \dots, \rho_n$ be the $\underbrace{\text{hom.}}_{n\ \mathbb{R}\text{-algebra}}$ $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \to \mathbb{C}$ and let

$$\rho : \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \to \mathbb{C}^n, \quad a \mapsto (\rho_1(a), \dots, \rho_n(a)).$$

Let $\psi : \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \longrightarrow \{ f \in \mathbb{R}[x] \text{ monic, deg. } n \} \cong \mathbb{R}^n$,

$\psi(a) = \chi(\rho(a))$.

We obtain an n-to-1 map

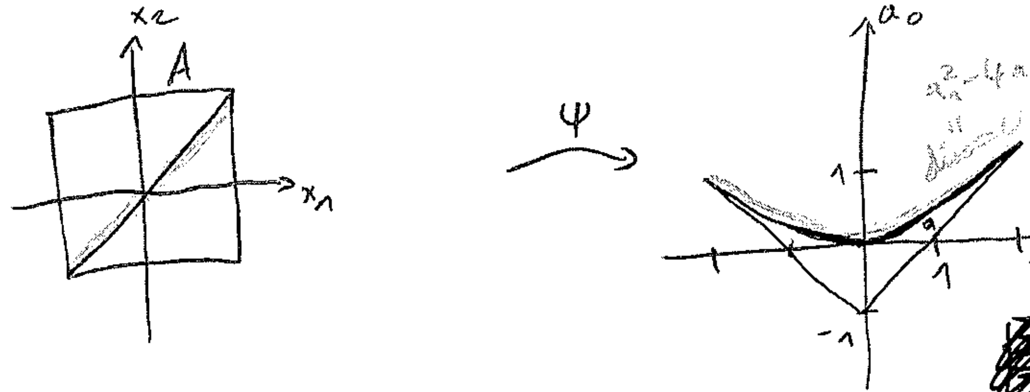
$$\{\alpha \in \overline{\mathbb{Z}} \text{ of signature } (r_1,r_2) \text{ with } |\alpha| \leq T\} \longrightarrow \{ f \in \mathbb{Z}[x] \cap \psi(A_T) \text{ irreducible} \}$$

Note: If $\psi(a) = (c_{n-1}, \dots, c_0)$, then $\psi(Ta) = (Tc_{n-1}, \dots, T^n c_0)$.

$$\Rightarrow \psi(A_T) = \underbrace{\begin{pmatrix} T & & \\ & \ddots & \\ & & T^n \end{pmatrix}}_{D_T} \psi(A).$$

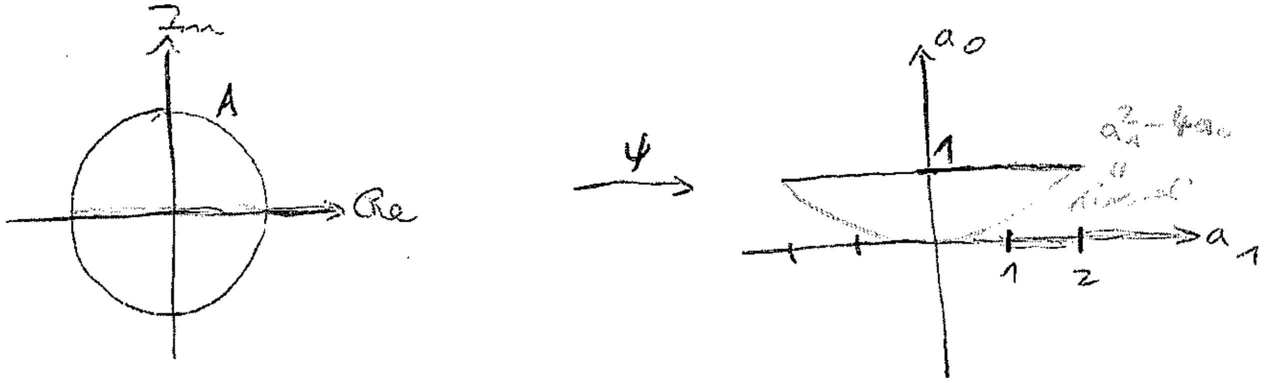
<u>Exe</u> Signature (2,0):

The Jacobian of $\psi : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$, $(x_1,x_2) \longmapsto (-(x_1+x_2),\, x_1x_2)$ has absolute determinant $|x_1 - x_2|$. We have $\mathrm{vol}(\psi(A)) = \frac{4}{3}$, so $C_{2,0} = \frac{8}{3}$.



<u>Exe</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 $C_{0,1} = \frac{16}{3}$.



<u>Exe</u> $C_2 = 8$

$\Rightarrow \#\{\alpha \in \overline{\mathbb{Z}} \text{ of signature } (r_1,r_2) \text{ with } |\alpha| \le T\}$

$$= \frac{1}{n} \cdot \#\{ f \in \mathbb{Z}[x] \cap D_T\,\psi(A) \text{ irreducible}\}$$

We have $\#\{f \in \mathbb{Z}[x] \cap D_T\,\psi(A)\} \sim T^{1+\dots+n} \cdot \mathrm{vol}(\psi(A))$. (I)

By the sieve theory argument in Thm 3.2.1,

$$\#\{\underset{x^n + c_{n-1}x^{n-1} + \dots + c_0}{\overset{\shortparallel}{f}} \in \mathbb{Z}[x] \mid c_{n-i} \ll T^i \ \forall i\} = o(T^{1+\dots+n}).$$

$\square$

To prove (I), you can use for example Davenport's Lemma or:

<u>Lemma 9.3</u> Let $A \subseteq \mathbb{R}^n$ be bounded with $vol(int(A)) = vol(\overline{A}) = V$.

Let Λ be a full lattice in $\mathbb{R}^n$ with (Euclidean) succ. min. $\lambda_1, \dots, \lambda_n$. Then,

$$\#(\Lambda \cap A) \underset{n,A}{\sim} \frac{V}{\mathrm{covol}(\Lambda)} \quad \text{as } \lambda_n \to 0.$$

<u>Pf</u> ~~For the lower bound, approximate~~
Approximate 1_A from below and above by smooth compactly supported functions and apply Poisson summation (Thm 4.2.6).

To do this, fix a sm. fct. $\eta : \mathbb{R}^n \to \mathbb{R}_{\geq 0}$ with $\mathrm{supp}(\eta) \subseteq D(1)$ and $\int \eta(x)dx = 1$.

Let $\eta_\delta(x) = \delta^n \eta(x/\delta)$. $\Rightarrow \mathrm{supp}(\eta_\delta) \subseteq D(\delta)$, $\int \eta_\delta(x) dx = 1$.

For any $\delta > 0$, let

$$U_\delta = \{ x \in \mathbb{R}^n \mid x + D(\varepsilon) \subseteq int(A) \}$$

$$K_\delta = \overline{A} + D(\varepsilon).$$

$$\Rightarrow 0 \leq 1_{U_\delta} * \eta_\delta \leq 1_A \leq 1_{K_\delta} * \eta_\delta \,,$$

$1_{U_\delta} \xrightarrow{\delta \to 0} 1_{int(A)}$ ptwise, increasin[g]
$1_{K_\delta} \xrightarrow{\delta \to 0} 1_{\overline{A}}$ ptwise, decreasin[g]

By Thm 4.2.6,

$$\sum_{x \in \Lambda} (1_{U_\delta} * \eta_\delta)(x) \sim \frac{\int 1_{U_\delta} * \eta_\delta}{\mathrm{covol}(\Lambda)} = \frac{vol(U_\delta)}{\mathrm{covol}(\Lambda)} \xrightarrow{\delta \to 0} \frac{vol(i\dots}{\mathrm{covol}\dots}$$

by monotone convergence

$$\sum (1_{K_\delta} * \eta_\delta)(x) \sim \dots \frac{vol(K_\delta)}{\mathrm{covol}(\Lambda)} \longrightarrow \frac{vol(\overline{A})}{\mathrm{covol}(\Lambda)}.$$

You can show that $\varphi(A)$ satisfies the conditions of Lemma 9.3 and compute its volume using:

<u>Lemma 9.4</u> The Jacobian determinant of $\mathcal{V}: \mathbb{C}^n \to \mathbb{C}^n$ is $\pm \prod_{i<j} (a_i - a_j)$.

<u>Pf</u> Let $\partial_i = \frac{\partial}{\partial a_i}$.

The i-th row of the Jacobian $J_n(a_1, \dots, a_n)$ is the coefficient vector of the polynomial

$$\frac{\partial \mathcal{V}}{\partial a_i}(a) = -\prod_{j \neq i} (X - a_j) \text{ of degree } n.$$

Subtract the n-th row from all other rows.

$$\frac{\partial \mathcal{V}}{\partial a_i}(a) - \frac{\partial \mathcal{V}}{\partial a_n}(a) = -(a_n - a_i) \cdot \underbrace{\prod_{j \neq i,n} (X - a_j)}_{\text{pol. of degree } n-2}.$$

Then, divide the i-th row by $a_n - a_i$.

The X^{n-1}-coeff. of $\frac{\partial \mathcal{V}}{\partial a_n}(a)$ is -1.

$\Rightarrow$ The resulting matrix looks like

$$\begin{bmatrix} 0 & & & \\ \vdots & & \boxed{J_{n-1}(a_1, \dots, a_{n-1})} & \\ 0 & & & \\ -1 & * & * & * \end{bmatrix}.$$

$\Rightarrow \det(J_n(a_1, \dots, a_n)) = \pm \prod_{i<n} (a_i - a_n) \cdot \det(J_{n-1}(a_1, \dots, a_{n-1}))$.

$\square$

Lemma 9.5 The Jacobian determinant of $\rho : \underset{\underset{\mathbb{R}^n}{\parallel}}{\mathbb{R}^{r_1}\times\mathbb{C}^{r_2}} \to \mathbb{C}^n$

is $\pm 2^{r_2}$.

Pf $\begin{array}{c}\mathbb{R} \to \mathbb{R} \\ a \mapsto a\end{array}$ has det 1.

$\begin{array}{c}\mathbb{C} \to \mathbb{C}^2 \\ a \mapsto (a,\bar{a})\end{array}$ has det 2.

$\square$

Cor 9.6 $$\mathrm{vol}(\psi(A)) = \frac{\cancel{2^{r_2}}}{r_1!\cdot\cancel{2^{r_2}}\, r_2!}\cdot\int_A \prod_{i<j} |\rho_i(a)-\rho_j(a)|\, da.$$

Pf $A \to \psi(A)$ is a $r_1!\cdot 2^{r_2} r_2!$-to-1 map, so the result follows from change of variables. $\square$

AS, 39

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

<u>Thm</u> 9.7 Fix some $n \geq 2$. There is a constant $C_n' > 0$ such that for all $t \in \mathbb{Z}$,

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

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

10. Counting number fields with a short generator

Let C_n' as in section 9.

<u>Def</u> An <u>order</u> in a number field L (of degree n) is a subring $\mathcal{O} \ni 1$ of $\mathcal{O}_L$ ~~which has rank n~~ such that $\mathbb{Q} \cdot \mathcal{O} = L$.

(equivalently: which has rank n as a $\mathbb{Z}$-module).

<u>Def</u> $\overline{\mathbb{Z}}_n' := \{ \alpha \in \overline{\mathbb{Z}}_n \mid tr(\alpha) = 0 \}$. ~~And Every $[\alpha] \in \overline{\mathbb{Z}}_n / \mathbb{Z}$ has exactly one representative in $\overline{\mathbb{Z}}_n'$~~

$\alpha - \frac{1}{n} tr(\alpha)/n$

$$\begin{tikzcd}
\{ \alpha \in \overline{\mathbb{Z}}_n' \} \arrow[r, "\text{not surjective}"] \arrow[dr, two heads] & \{ \mathcal{O} \subseteq \overline{\mathbb{Z}} \text{ order in deg. } n \text{ number field} \} \arrow[d, two heads] \\
& \{ L \text{ deg. } n \text{ number field} \}
\end{tikzcd}$$

$\alpha \longmapsto \mathbb{Z}[\alpha]$

$\alpha \longmapsto \mathbb{Q}(\alpha)$

$\mathcal{O} \longmapsto \mathbb{Q} \cdot \mathcal{O}$

Thm 10.1 $\#\{\mathcal{O} \subseteq \overline{\mathbb{Z}} \text{ as above s.t. } \mathcal{O} = \mathbb{Z}[\alpha] \text{ for some } \alpha \in \overline{\mathbb{Z}}_n' \text{ with } |\alpha| \leq T\}$

$$\sim \frac{1}{2} C_n' \cdot T^{(n-1)(n+2)/2}.$$

Pf "$\leq$" $\mathbb{Z}[\alpha] = \mathbb{Z}[-\alpha]$.

"$\geq$" We need to show that if we order the elements $\alpha \in \overline{\mathbb{Z}}_n'$ by $|\alpha|$, then

$$\mathbb{P}_\alpha\big(\exists \underset{\alpha, -\alpha}{\underset{\neq}{\beta}} \in \overline{\mathbb{Z}}_n' : \mathbb{Z}[\alpha] = \mathbb{Z}[\beta],\ |\beta|_2 \leq |\alpha|_2\big) = 0.$$

Euclidean norm on $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \cong \mathbb{R}^n$

$$LHS \leq \mathbb{P}_\alpha\big(\exists \beta \in \mathbb{Z}[\alpha] \cap \{tr = 0\} \text{ lin. indep. from } \alpha : |\beta|_2 \leq |\alpha|_2\big)$$

Call α bad if there is such a β.

$\mathbb{Z}[\alpha] \cap \{tr = 0\} \subseteq$ lattice $\Lambda = \Lambda(\alpha)$ spanned by $y_1, \ldots, y_{n-1}$,

where $y_i = y_i(\alpha) = \alpha^i - \frac{1}{n} tr(\alpha^i)$

Fix a signature (r_1, r_2).

Let $H = \{x \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \mid tr(x) = 0\}$.

For $i=1,\dots,n-1$, let $g_i(x)\geqslant 0$ be the (Euclidean) distance of $y_i(x)\in\mathbb{R}^{r_1}\times\mathbb{C}^{r_2}\cong\mathbb{R}^n$ from the subspace spanned by $y_1(x),\dots,y_{i-1}(x)$. (as in Gram–Schmidt)

If $\rho_i(x)\neq\rho_j(x)$ $\forall i\neq j$ for the n maps $\rho_1,\dots,\rho_n:\mathbb{R}^{r_1}\times\mathbb{C}^{r_2}\to\mathbb{C}$,

then $1,x,\dots,x^{n-1}$ are lin. indep. and hence $y_1,\dots,y_{n-1}$ are lin. indep.

Then, $g_i(x)>0$ $\forall i$. Let $h(x)=\min\limits_{2\leq i\leq n}\dfrac{g_i(x)}{g_{i-1}(x)}$.

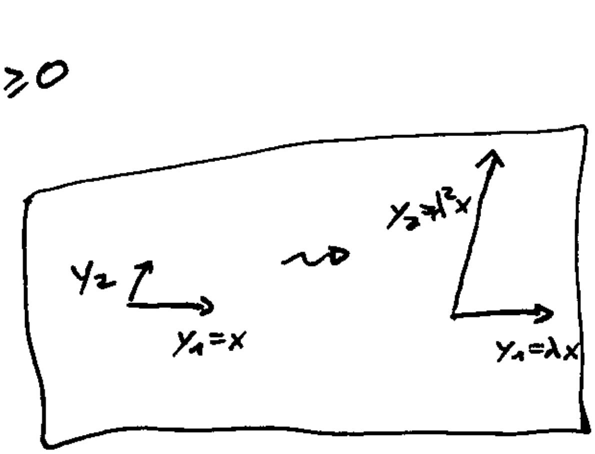
Claim: If x is bad, then $h(x)\leq 1$.

Pf: If $h(x)>1$, then any vector in $\Lambda(x)$ lin. indep. from $y_1^{(x)}=x$ has distance $>g_1(x)=|x|_2$ from some subspace, and in particular has length $>|x|_2$. $\square$ (claim)

Note: $y_i(\lambda x)=\lambda^i y_i(x)$ $\quad\forall\lambda\geqslant 0$

$\Rightarrow g_i(\lambda x)=\lambda^i g_i(x)$

$\Rightarrow h(\lambda x)=\lambda h(x)$



Let $B_\varepsilon = \{ x \in H \mid |x| \leq 1,\ h(x) \leq \varepsilon \}$.

For all $T \geq \frac{1}{\varepsilon}$, $\quad T \cdot B_\varepsilon$ contains all $\underbrace{x}_{\text{bad}} \in H$ with $|x| \leq T$.

$\Rightarrow$ The fraction of bad x goes to 0 as $T \to \infty$ because

B_ε goes monotonically to $\emptyset$ as $\varepsilon \to 0$.

$\square$

Bror
10.2

$\#\{K \subseteq \overline{\mathbb{Q}} \text{ as above s.t. } K = \mathbb{Q}(\alpha) \text{ for some } \alpha \in \mathbb{Z}_n' \text{ with } |\alpha| \leq T\}$

$\asymp T^{(n-1)(n+2)/2}$

To prove "$\gg$", one can use a (difficult!) sieve to show that $\mathcal{O}_{\mathbb{Q}(\alpha)} = \mathbb{Z}[\alpha]$ for a positive proportion of α.

In fact, $\mathbb{Z}[\alpha]$ has squarfree discriminant for a positive proportion of α.
(See Bhargava, Shankar, Wang: Squarefree values of polynomial discriminants.)

11. Counting number fields of small discriminant

Conjecture 11.1 (Folklore, Malle) Let $n \geq 2$. Let K be any n.f.

There are constants $C_{n,K}, C'_{n,K} > 0$ s.t.

a) $\# \{ L \subseteq \overline{\mathbb{Q}}$ of degree n $\mid$ $|disc(L)| \leq T \} \sim C_{n,K} T$
ext. of K

b) $\# \{$ $\quad$ - - " $\quad$ - - - and Galois group $S_n \} \sim C'_{n,K} T$.

Conj. 11.2 (Malle) We have $C_{n,K} = C'_{n,K}$ if and only if n is prime.

Known cases:

$n=2$: Cost 1 (for $K = \mathbb{Q}$), Datskovski–Wright (any K)

$n=3$: Davenport–Heilbronn (using a parametrisation, for $K=\mathbb{Q}$), Bhargava–Shankar–Wang (any K)

$n=4,5$: Bhargava ($\quad$ – " – $\quad$, for $K=\mathbb{Q}$), $\quad$ – " –

Lower bound:

Thm 11.3 (B-S-W)

$$\# \{ L \subseteq \overline{\mathbb{Q}} \text{ ext. of } \mathbb{Q} \text{ of degree } n, \ |disc(L)| \leq T, \ Gal = S_n \} \gg T^{\frac{1}{2} + \frac{1}{n}}.$$

Pf If $\alpha \in \overline{\mathbb{Z}}$ generates L, then

$$disc(L) \leq disc(\mathbb{Z}[\alpha]) = \det\left((\rho_i(\alpha^j))_{\substack{i=1,\dots,n \\ 0 \leq j \leq n-1}} \right)^2$$

$$\ll |\alpha|^{2(0+1+\dots+(n-1))} = |\alpha|^{n(n-1)}.$$

$$\Rightarrow LHS \gg \# \{ L \text{ gen. by } \alpha \text{ with } |\alpha| \ll T^{1/n(n-1)} \text{ with } Gal = S_n \} \gg T^{(n+2)/2n}$$
Prop 10.2

$\square$

Upper bound:

Thm 11.4 (Schmidt) Let $n \geq 2$.

$$\#\{L \subseteq \overline{\mathbb{Q}} \text{ ext. of } \mathbb{Q} \text{ of degree } n,\ |\mathrm{disc}(L)| \leq T\} \ll_n T^{(n+2)/4}.$$

(Recall: conjectured to be $\asymp T$.)

Pf that $\#\{L \text{ as above}, \nexists \underset{\text{(primitive)}}{\text{subext.}}\ \mathbb{Q} \subsetneq F \subsetneq L\} \ll T^{(n+2)/4}$

Let $1 = \lambda_1 \leq \lambda_2 \leq \ldots \leq \lambda_n$ be the succ. min. of $\mathcal{O}_L$.

$\lambda_2 \cdots \lambda_n \asymp \mathrm{covol}(\mathcal{O}_L) \asymp |\mathrm{disc}(L)|^{1/2} \leq T^{1/2}$

$\Rightarrow \lambda_2 \ll \quad |^{1/2(n-1)}$.

There is a number $\alpha \in \mathcal{O}_L$ with $|\alpha| \asymp \lambda_2$, $\alpha \notin \mathbb{Z}$.

~~and $\mathrm{Tr}_{L|\mathbb{Q}}(\alpha) = 0$ (replace α by $n \cdot \alpha -$ $\mathrm{Tr}(\alpha)$ if necessary).~~

$\mathbb{Q} \subsetneq \mathbb{Q}(\alpha) \subseteq L$, so $\mathbb{Q}(\alpha) = L$.

By Thm 10.1/Prop 10.2,

$$\#\{L \text{ gen. by some } \alpha \in \mathcal{O}_L \text{ with } |\alpha| \ll T^{1/2(n-1)}\} \ll T^{(n+2)/4}.$$

$\square$

This shows the Thm when n is prime. For the general statement, Schmidt ~~uses induction over~~ proves the following more general statement by induction over n:

SKIPPED **Thm 11.5** (Schmidt) For any number field $K \subseteq \overline{\mathbb{Q}}$ ~~of~~ degree m and any $n \geq 2$,

$$\#\{L \subseteq \overline{\mathbb{Q}} \text{ ext. of } K \text{ of degree } n,\ |\mathrm{disc}(L)| \leq T\} \ll_{n,m} |\mathrm{disc}(K)|^{-\frac{1}{2}} \cdot \left(\frac{T}{|\mathrm{disc}(K)|}\right)^{(n+}$$

For the general (nonprimitive) case:

$$\#\{L\} = \sum_{\substack{K \text{ ext. of } \mathbb{Q} \\ \text{of degree } m \mid n}} \underbrace{\#\{L \text{ ext. of } K \text{ of deg. } \tfrac{n}{m} \text{ s.t. } \nexists\, K \subsetneq F \subsetneq L\}}_{\text{count these using a similar strategy as before}}$$

↑ count these (by $|\mathrm{disc}(K)|$) using induction

For details, see Schmidt: Number fields of given degree and bounded discriminant

Rmk We expect

$$\lim_{\varepsilon \to 0} \mathbb{P}_K \left(\lambda_2(\mathcal{O}_K) < \varepsilon \, |\mathrm{disc}(K)|^{1/2(n-1)} \right) = 0.$$

The reason the upper and lower bounds are so far off is that $\mathbb{Z}[\alpha]$ usually has discriminant much larger than T (about $T^{n/2}$) for random $\alpha \in \overline{\mathbb{Z}}_n$ with $|\alpha| \asymp T^{1/2(n-1)}$.

Shankar–Tsimerman (2020) analyse how often $[\mathcal{O}_{\mathbb{Q}(\alpha)} : \mathbb{Z}[\alpha]] = k$ and therefore how often $|\mathrm{disc}(K)| \asymp \frac{T^{n/2}}{k^2}$. Assuming a sufficiently (outrageously!) small error bound in the "sieve", they justify Conjecture 11.1.

Also see Bhargava–Shankar–Wang (2022) and Anderson–Gafni–Hughes–Lemke Oliver–Lowry-Duda–Thorne–Wang–Zhang (2022).

We can do better than Schmidt:

<u>Idea</u> (Ellenberg–Venkatesh, 2006)

Instead of writing down the min. pol. of one el. $\alpha \in \mathcal{O}_L$ (generating L), pick $1 \le r \le n$ generators $\omega_1, \dots, \omega_r \in \mathcal{O}_L$ and for some $d \ge 1$, write down the integers

$\mathrm{Tr}(\omega_1^{i_1} \cdots \omega_r^{i_r})$ for $i_1, \dots, i_r \ge 0$, $i_1 + \dots + i_r = d$.

[For large enough d these numbers should determine $\omega_1, \dots, \omega_r$ and therefore the field L.]

If $\rho_1, \dots, \rho_n$ are the embeddings $L \to \mathbb{C}$, each ω_i corr. to a vector $\underset{\rho(\omega_i)}{} = (\rho_j(\omega_i))_{j=1,\dots,n} \in \mathbb{C}^n$.

The map $(\omega_1, \dots, \omega_r) \longmapsto (\mathrm{Tr}(\omega_1^{i_1} \cdots \omega_r^{i_r}))_{i_1 + \dots + i_r = d}$

corr. to a map $\varphi_{nrd} : \mathbb{C}^{rn} \longrightarrow \mathbb{C}^{E_{r,d}}$ $\quad \left(E_{r,d} = \#\{(i_1, \dots, i_r)\} = \binom{r+d-1}{d}\right)$

$$(X_{pq})_{\substack{p \le r \\ q \le n}} \longmapsto \left(\sum_q X_{1q}^{i_1} \cdots X_{rq}^{i_r} \right)_{i_1 + \dots + i_r = d}$$

<u>Lemma 11.6</u> If $d \ge 1$, $n \ge r \ge 6$ [and in many other cases], we have

$$\dim(\mathrm{im}(\varphi_{nrd})) = \min(rn, E_{r,d}).$$

<u>Idea of pf</u> It suffices to show that the Jacobian has full rank at some point.

$$\frac{\partial \varphi_{nrd}}{\partial X_{pq}} = \Bigg(\underbrace{\frac{\partial X_{1q}^{i_1} \cdots X_{rq}^{i_r}}{\partial X_{pq}}}_{\substack{\text{deriv. of hom.} \\ \text{deg. } d \text{ pol. evaluated at } (x_{1q}, \dots, x_{rq}) =: P_q}} \Bigg)_{i_1 + \dots + i_r = d}$$

This is the Alexander–Hirschowitz theorem.
(Proven by induction, specialising some of the n points $P_1, \ldots, P_n$ to lie on a hyperplane.)

"$\square$"

<u>Cor 11.7</u> If $d \geq 1$, $n \geq r \geq 6$, $rn \in E_{r,d}$, then there is a projection $\pi : \mathbb{C}^{E_{rd}} \to \mathbb{C}^{rn}$ such that $\pi \circ \varphi_{nrd} : \mathbb{C}^{rn} \to \mathbb{C}^{rn}$ is dominant and therefore we have $|(\pi \circ \varphi)^{-1}((\pi \circ \varphi)(P))| < \infty$ (and hence $\ll_{n,r,d} 1$) for <u>generic</u> points $P = (x_{pq})_{p,q} \in \mathbb{C}^{rn}$.

not satisfying a certain pol. equality

<u>Pf</u> AG … "$\square$"

<u>Thm 11.8</u> (Lemke Oliver – Thorne, 2020)

If $d \geq 1$, $n \geq r \geq 6$, $rn \in E_{rd}$, then
$\#\{L \text{ number field of degree } n \mid |\mathrm{disc}(L)| \leq T\} \ll T^{rd}$.

<u>Pf</u> Let $\alpha_1, \ldots, \alpha_n$ form a basis of $\mathcal{O}_L$ with $\alpha_i \asymp \lambda_i$. We have $\lambda_i \leq \lambda_n \ll T^{1/n}$ (HW).

Since $\rho(\alpha_1), \ldots, \rho(\alpha_n)$ form a $\mathbb{C}$-basis of $\mathbb{C}^n$, there is a <u>generic</u> point $(\omega_1, \ldots, \omega_r) \in \mathbb{C}^{rn}$ given by $\omega_p = \sum_j m_{pj} \alpha_j$ with $m_{pj} \in \mathbb{Z}$, $|m_{pj}| \ll_{n,r,d} 1$ such that ω_1 doesn't lie in any subfield $F \subsetneq K$. Pick one!

Only $\ll_{n,r,d} 1$ fields L produce the same point

$\varphi_{n,r,d}(\omega_1, \dots, \omega_r) \in \mathbb{Z}^{rn}$, whose coordinates are

$\ll \max(|\omega_1|, \dots, |\omega_r|)^d \ll \lambda_n^d \ll T^{d/n}$.

The number of such points is $\ll (T^{d/n})^{rn} = T^{rd}$. $\square$

Minimising rd subject to the cond. $d \geq 1$, $n \geq r \geq 6$, $rn \leq \binom{r+d-1}{d}$,

shows: $\#\{L\} \ll T^{O((\log n)^2)}$.

(You can take $d, r \asymp \log n$.)

12. Étale algebras

Let K be a field.

<u>Def</u> An <u>étale K-algebra</u> is a product ($L = L_1 \times \dots \times L_r$) of finitely many separable field extensions L_i of K.

The <u>degree</u> is
$$[L:K] = \dim_K(L) = \sum_i [L_i:K].$$

<u>Ese</u> The trivial degree n ext. $L = K^n = K \times \dots \times K$.

~~Ese If K is alg. closed, there is exactly one étale K ext of degree~~ n,
~~namely~~.

<u>Rmk</u> This is the only one if K is separably closed (or algebraically).

<u>Rmk</u> If $f \in K[X]$ is separable (of degree n), then $L = K[X]/(f(X))$ is an étale K-alg. of degree n.

<u>Rmk</u> The étale $\mathbb{R}$-algebras are $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ of degree $r_1 + 2r_2$.

<u>Rmk</u> A finite-dimensional K-algebra L is étale if and only if the trace form on L is nondegenerate.

<u>Rmk</u> Let $K'|K$ be any field extension.

L étale K-alg. of degree n

$$\Downarrow$$

$L \otimes_K K'$ étale K'-alg. of degree n

<u>Ese</u> For $K = \mathbb{Q}$ a) the factors of $L \otimes_{\mathbb{R}} \mathbb{C}$ corr. to the real/complex emb. of L.

b) the factors of $L \otimes_{\mathbb{Q}} \mathbb{Q}_p$ corr. to the primes of L above p.

<u>Lemma 12.1</u> If L is an étale K-alg. of degree n, there are exactly n K-algebra homomorphisms $L \to K^{sep}$.

<u>Pf</u> Write $L = L_1 \times \dots \times L_r$. Let $d_i = [L_i : K]$. There are d_i hom. $L_i \to K^{sep}$.
$L_1 \times \dots \times L_r$
Each hom. $L \to K^{sep}$ must factor <u>through</u> some L_i. $\square$

~~Defn 12.1 Let L as above, $\sigma_1, \dots, \sigma_n : L \to K$ the K-alg hom~~

Let $\Gamma_K = Gal(K^{sep}|K)$.

To any L as above with the K-alg. hom. $\rho_1, \dots, \rho_n : L \to K^{sep}$,

we can associate a continuous

group hom. $f : \underbrace{Gal(K^{sep}|K)}_{=\Gamma_K} \to S_n$

$\sigma \mapsto \pi$ such that $\sigma \circ \rho_i = \rho_{\pi(i)}$

Note that relabeling $\rho_1, \dots, \rho_n$ conjugates by an element of S_n.

<u>Rmk</u> If L is the subfield of K^{sep} fixed by $H \leq \Gamma_K$, then this corr. to the action of Γ_K on the n-element set Γ_K/H.

<u>Thm 12.2</u> This gives rise to a bijection

$$\left\{ \begin{array}{l} L \text{ étale deg. } n \text{ alg.} \\ (\text{up to isomorphism}) \end{array} \right\} \longleftrightarrow \underbrace{S_n \backslash Hom_{cont}(\Gamma_K, S_n)}_{\text{orbits of conjugation action}}.$$

<u>Rmk</u> If L corr. to $f : \Gamma_K \to S_n$
and L' corr. to $f' : \Gamma_K \to S_{n'}$,
then $L \times L'$ corr. to $\Gamma_K \xrightarrow{f \times f'} S_n \times S_{n'} \xhookrightarrow[\text{incl.}]{\text{nat.}} S_{n+n'}$.

<u>Rmk</u> {The action of Γ_K (on $\{1, \dots, n\}$) corr. to $L = L_1 \times \dots \times L_r$ has exactly r orbits.}

<u>Exe</u> $L = K^n$ corr. to the trivial map $\sigma \mapsto id$.

Pf of Thm

To construct the inverse, let $f : \Gamma_K \to S_n$.

This corr. to an action of Γ_K on $\{1, \dots, n\}$.

Assume there are r orbits, with representatives $t_1, \dots, t_r \in \{1, \dots, n\}$.

Then, the preimage of f is $L = L_1 \times \dots \times L_r$ with

L_i = subfield of K^{sep} fixed by $\mathrm{Stab}_{\Gamma_K}(t_i)$.

... □

Thm 12.3

If L corr. to f, then

$$\begin{aligned} \mathrm{Aut}_{K\text{-alg}}(L) &\xrightarrow{\sim} \mathrm{Stab}_{S_n}(f) = \text{centralizer of } \mathrm{im}(f) \le S_n \\ \tau &\longmapsto \text{the perm. } \alpha \in S_n \text{ such that } \rho_i \circ \tau^{-1} = \rho_{\alpha(i)} \end{aligned}$$

Pf HW □

Cor 12.4

$$\frac{1}{\#\mathrm{Aut}(L)} = \frac{\#\{f : \Gamma_K \to S_n \text{ corr. to } L\}}{\#S_n}$$

Pf Orbit-stabilizer theorem □

Lemma 12.5 Consider the étale degree n extensions L of $\mathbb{R}$, up to isomorphism.

a) $\#\{L\} = \left\lfloor \frac{n}{2} \right\rfloor + 1$

b) $\displaystyle\sum_L \frac{1}{\#\mathrm{Aut}(L)} = \mathbb{P}_{\pi \in S_n}(\pi^2 = id)$

Pf a) $L = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ with $n = r_1 + 2r_2$

$(0 \leq r_2 \leq \frac{n}{2})$

b) $\displaystyle LHS = \frac{1}{\#S_n} \cdot \#\{f : \Gamma_{\mathbb{R}} \longrightarrow S_n\}$

$\Gamma_{\mathbb{R}} = \{e, \sigma\} = C_2$ (cyclic group of order 2)

$$\{f : C_2 \to S_n\} \longleftrightarrow \{\pi \in S_n \mid \pi^2 = id\}$$

$$f \longmapsto f(\sigma)$$

$\square$

Rmk $\#\mathrm{Aut}(\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}) = r_1! \cdot r_2! \cdot 2^{r_2}$.

__Lemma 12.6__ Consider the étale degree n extensions L of $\mathbb{F}_q$, up to $\cong$.

a) $\#\{L\}$ = number of partitions of the integer n (ignoring order)

b) $$\sum_L \frac{1}{\#\mathrm{Aut}(L)} = 1$$

__Pf__ a)

$$L = \mathbb{F}_{q^{k_1}} \times \dots \times \mathbb{F}_{q^{k_r}} \quad \text{with } n = k_1 + \dots + k_r$$

b) $$\Gamma_{\mathbb{F}_q} = \hat{\mathbb{Z}}$$

$$\{f : \hat{\mathbb{Z}} \xrightarrow[\text{(cont.)}]{} S_n\} \longleftrightarrow \{f : \mathbb{Z} \longrightarrow S_n\} \longleftrightarrow S_n$$

$$\Rightarrow \text{LHS} = \frac{1}{\#S_n} \cdot \#S_n = 1$$

$\square$

13. p-adic integration

References:

- Igusa: An introduction to the theory of local zeta functions
- Popa: p-adic integration (lecture notes on his webpage)

Let K be a nonarch. local field with residue field $\mathbb{F}_q$, uniformizer π_K, normalized valuation v_K, norm $|x| = q^{-v_K(x)}$,

Haar measure dx normalised so $\underbrace{\int_{\mathcal{O}_K} 1\,dx}_{\mathrm{vol}(\mathcal{O}_K)} = 1$.

Lemma 13.1 Let $A \subseteq K$ be a measurable subset.

For any $t \in K$,

$$\mathrm{vol}(t \cdot A) = |t| \cdot \mathrm{vol}(A).$$

Rmk That's like for $K = \mathbb{R}$, Lebesgue measure.

Pf $t = 0$: clear

$t \in \mathcal{O}_K^\times$: The isom. $K \to K$, $x \mapsto tx$ sends $\mathcal{O}_K$ to $\mathcal{O}_K$.

~~$\Rightarrow$ It must send the Haar measure dx to itself.~~

~~$\Rightarrow \mathrm{vol}(tA) = \mathrm{vol}(A)$.~~

$\Rightarrow$ The pushforward of dx is dx.

$\Rightarrow \mathrm{vol}(f^{-1}(f(A))) = \mathrm{vol}(f(A))$.

$\underline{t=\pi}$: The isom. $f: K \to K$, $x \mapsto tx$ sends $\mathcal{O}_K$ to the ~~prime~~ prime ideal $\pi\mathcal{O}_K$.

Let $r_1, \dots, r_q \in \mathcal{O}_K$ be representatives of the residue classes mod π.

$$\Rightarrow \mathcal{O}_K = \bigsqcup_{i=1}^{q} (r_i + \pi\mathcal{O}_K)$$

$$\Rightarrow vol(\mathcal{O}_K) = \sum vol(r_i + \pi\mathcal{O}_K) \underset{\text{Haar measure}}{\overset{\uparrow}{=}} \sum vol(\pi\mathcal{O}_K) = q \cdot vol(\pi\mathcal{O}_K)$$

$$\Rightarrow vol(\pi\mathcal{O}_K) = \frac{1}{q} \cdot vol(\mathcal{O}_K) = |\pi| \cdot vol(\mathcal{O}_K).$$

The pushforward of the Haar measure dx with $vol(\mathcal{O}_K) = 1$ must be a Haar measure with $vol(\pi\mathcal{O}_K) = 1$.

$\Rightarrow$ It is $|\pi|^{-1} \cdot dx$.

$$\Rightarrow vol(A) = vol(f^{-1}(f(A)))$$

$= \text{volume of } f(A) \text{ w.r.t. pushforward}$

$= |\pi|^{-1} \cdot vol(f(A))$ $\square$

Thm 13.2 Let $A \subseteq K$ be compact and open (or more generally measurable).

Let $f \in K[x]$ be a polynomial (or more generally a K-analytic function). For any $y \in K$, let $m(y) := \#\{x \in A \mid f(x) = y\}$.

Then,
$$\underbrace{\int_K m(y)\,dy}_{\text{vol}(f(A) \text{ as a multiset})} = \int_A |f'(x)|\,dx .$$

<u>Ex</u> $K = \mathbb{Q}_p$, $A = \mathbb{Z}_p^\times$, $f(x) = x^2$

Case $p \neq 2$:

By Hensel's lemma,
$$m(y) = \begin{cases} 2, & (y \bmod p) \in \mathbb{F}_p^{\times 2} \text{ (quadr. res.)} \\ 0, & \text{otherwise} \end{cases}$$

$$\Rightarrow LHS = 2 \cdot \frac{\#\text{nonzero quadr. res.}}{p} = \frac{p-1}{p} = 1 - \frac{1}{p} .$$

$$v_p(f'(x)) = v_p(2x) = 0 \quad \forall x \in \mathbb{Z}_p^\times$$
$$\Downarrow$$
$$|f'(x)| = 1$$

$$\Rightarrow RHS = \int_{\mathbb{Z}_p^\times} 1\,dx = \text{vol}(\mathbb{Z}_p^\times) = 1 - \frac{1}{p} .$$

Case $p=2$:

By Hensel's lemma,

$$m(y) = \begin{cases} 2, & y \equiv 1 \bmod 8, \\ 0, & \text{otherwise.} \end{cases}$$

$$\Rightarrow LHS = 2 \cdot \frac{1}{8} = \frac{1}{4}$$

$$v_2(f'(x)) = v_2(2x) = 1 \quad \forall x \in \mathbb{Z}_2^\times$$

$$\Downarrow$$

$$|2x| = \frac{1}{2}$$

$$\Rightarrow RHS = \int_{\mathbb{Z}_2^\times} \frac{1}{2}\,dx = \frac{1}{2}\,\mathrm{vol}(\mathbb{Z}_2^\times) = \frac{1}{4}$$

Ex: $K = \mathbb{F}_p((T))$, $A = \mathcal{O}_K = \mathbb{F}_p[[T]]$, $f(x) = X^p$.

$(a_0 + a_1 X + a_2 X^2 + \dots)^p = a_0 + a_1 X^p + a_2 X^{2p} + \dots$

$$\Rightarrow m(y) = \begin{cases} 1, & y = b_0 + b_p X^p + b_{2p} X^{2p} + \dots \text{ for some } b_0, b_p, \ldots \in \mathbb{F}_p \\ & (\infty \text{ many "digits" of } Y \text{ have to be } 0\ldots) \\ 0, & \text{otherwise} \end{cases}$$

$$\Rightarrow LHS = 0$$

$$|f'(x)| = |pX^{p-1}| = 0$$

$$\Rightarrow RHS = 0$$

Pf of Thm

Replacing A by $\pi^a A$, f by $\pi^b f\left(\frac{x}{\pi^a}\right)$ for large a, b,

we can arrange $A \subseteq \mathcal{O}_K$, $f \in \mathcal{O}_K[X]$.

$$\begin{aligned} A &\longrightarrow \mathbb{Z} \cup \{\infty\} \quad \text{is continuous.} \\ x &\longmapsto v(f'(x)) \end{aligned}$$

Claim Let $B = \{x \in \mathcal{O}_K \mid f'(x) = 0\}$.

We have $\mathrm{vol}(f(B)) = 0$.

Pf If $f' \neq 0$, then $\# B < \infty$. (✓)

If $f' = 0$, then $f =$ constant (✓)

or $\mathrm{char}(K) = p$, $f = g(x^p)$ for some $g \in \mathcal{O}_K[x]$.

By the last example, $C = \{x^p \mid x \in \mathcal{O}_K\}$ has volume 0.

$\Rightarrow$ $f(B) = g(C)$ has volume 0.

f cont.

$\square$

For any $t \in \mathbb{Z}$, $\{x \in A \mid v(f'(x)) = t\}$ is compact and open.

w.l.o.g. $v(f'(x)) = t \quad \forall x \in A$.

Let $a \in A$ and let $e > 2t$. By Hensel's lemma,

we have $f(a + \mathfrak{p}^e) = f(a) + \mathfrak{p}^{t+e}$ and

each $y \in f(a) + \mathfrak{p}^{t+e}$ has exactly one preimage

in $a + \mathfrak{p}^e$.

We have $\displaystyle\int_{a+\mathfrak{p}^e} \underbrace{|f'(x)|}_{q^{-t}} dx = q^{-e-t} = \int_{f(a)+\mathfrak{p}^{e+t}} 1\, dy.$

The result follows by splitting up A into (finitely many) disjoint sets of the form $a+\ell^e$. $\square$

We discussed integration by substitution over nonarchimedean local fields last time. More generally, one can perform a change of variables in any dimension:

Theorem 13.3. *Let A be a compact open subset of K^n. Let $f_1, \ldots, f_n \in K[X_1, \ldots, X_n]$. For any $y \in K^n$, let $m(y) = \#\{x \in A \mid f(x) = y\}$. Then,*

$$\int_{K^n} m(y)\mathrm{d}y = \int_A |\det \mathrm{Jac}(f)(x)|\mathrm{d}x,$$

where $\mathrm{Jac}(f)(x) = (\frac{\partial f_i(x)}{\partial x_j})_{i,j}$ *is the Jacobian matrix.*

We skip the proof, which works similarly to Theorem 13.2, but using an n-dimensional form of Hensel's lemma.

Remark 13.4. *There is a good notion of manifolds over K. One can integrate real-valued functions over manifolds, and there is a corresponding change of variables formula. (See the two references mentioned last time: [Pop] and [Igu00].)*

14 Some mass formulas

One can either count isomorphism classes of (separable) field extensions of K, or subfields of K^{sep}. Of course, Galois conjugate subfields are isomorphic, so there may be fewer isomorphism classes than subfields of K^{sep}. More precisely:

Lemma 14.1. *Let L be a separable field extension of K of degree n. Then,*

$$\#\{K \subseteq L' \subseteq K^{\mathrm{sep}} \mid L' \cong L \text{ as } K\text{-algebras}\} = \frac{n}{\#\operatorname{Aut}(L)}.$$

Proof. There are n embeddings $L \hookrightarrow K^{\mathrm{sep}}$. Two embeddings ρ_1, ρ_2 have the same image if and only if $\rho_1 = \rho_2 \circ \sigma$ for some automorphism σ of L. □

For the rest of this section, let K be a nonarchimedean local field with residue field $\mathbb{F}_q$.

Theorem 14.2 (Serre's mass formula, [Ser78])**.** *Consider the totally ramified separable degree n field extensions L of K, up to isomorphism. We have*

$$\sum_L \frac{|\operatorname{disc}(L|K)|_K}{\#\operatorname{Aut}(L)} = \frac{1}{q^{n-1}}.$$

Remark 14.3. *Any inseparable extension L of K has* $\operatorname{disc}(L|K) = 0$*, so including them wouldn't change the sum.*

Remark 14.4. *There are infinitely many (separable) totally ramified degree n field extensions L of K if and only if the characteristic of K divides n.*

Proof. By Lemma 14.1, we can write the left-hand side as the following sum over totally ramified degree n field extensions $L \subseteq K^{\mathrm{sep}}$ of K:

$$\frac{1}{n} \cdot \sum_L |\operatorname{disc}(L|K)|.$$

For any L as above, let $U_L \subseteq L$ be the set of uniformizers in L. Let P be the set of separable monic degree n Eisenstein polynomials $f \in \mathcal{O}_K[X]$. The characteristic polynomial of any $a \in U_L$ lies in P since L is totally ramified. Conversely, the n roots of any $f \in P$ in K^{sep} each generate a totally ramified degree n extension of K. We thus have an n-to-1 map

$$\psi : \bigsqcup_{\substack{L \subseteq K^{\text{sep}} \\ \text{totally ramified} \\ \text{degree } n}} U_L \to P$$

sending $a \in U_L$ to its characteristic polynomial. We again identify monic degree n polynomials with their coefficient tuple, so $P \subseteq \mathcal{O}_K^n$.

The theorem will follow from the change of variables formula applied to this map.

We first compute the volume of P directly. The set of Eisenstein polynomials $X^n + c_{n-1}X^{n-1} + \cdots + c_0$ (with $c_0 \in \pi_K \mathcal{O}_K^\times$ and $c_1, \ldots, c_{n-1} \in \pi_K \mathcal{O}_K$) has volume $q^{-n}(1-q^{-1})$. The set of inseparable monic degree n polynomials f in $\mathcal{O}_K[X]$ has volume 0 because all inseparable polynomials f have discriminant zero. (The discriminant is a nonzero polynomial in the coefficients of f. The set of roots of any nonzero polynomial has volume 0.) Hence,

$$\operatorname{vol}(P) = q^{-n}(1 - q^{-1}).$$

Fix a field L as above, and any uniformizer π_L of L. (As L is totally ramified, we have $v_K(\pi_L) = \frac{1}{n} v_K(\pi_K)$.) Our goal is to compute the volume of the image of U_L. Note that $(1, \pi_L, \ldots, \pi_L^{n-1})$ is an integral basis of L. The map $d : K^n \to L$, $(b_0, \ldots, b_{n-1}) \mapsto b_0 + b_1\pi_L + \cdots + b_{n-1}\pi_L^{n-1}$ therefore sends $\mathcal{O}_K^n$ to $\mathcal{O}_L$. Our Haar measure on K^n corresponds to our Haar measure on L under this map. The uniformizers of L are exactly the linear combinations $b_0 + b_1\pi_L + \cdots + b_{n-1}\pi_L^{n-1}$ with $b_0 \in \pi_K \mathcal{O}_K$ and $b_1 \in \mathcal{O}_K^\times$ and $b_2, \ldots, b_{n-1} \in \mathcal{O}_K$. Hence,

$$\operatorname{vol}(U_L) = q^{-1}(1 - q^{-1}).$$

Consider the n homomorphisms $\rho_1, \ldots, \rho_n : L \to K^{\text{sep}}$, and combine them to a map $\rho : L \to (K^{\text{sep}})^n$. The linear map $\rho \circ d : K^n \to (K^{\text{sep}})^n$ is described by the matrix $(\rho_i(\pi_L^j))_{i,j}$. Since $(1, \pi_L, \ldots, \pi_L^{n-1})$ is an integral basis of L, its determinant is $|\operatorname{disc}(L|K)|^{1/2}$.

As in section 9, we consider the map

$$\chi : (K^{\text{sep}})^n \to \{f \in K^{\text{sep}}[X] \text{ monic, degree } n\} \cong K^n$$

that sends $a = (a_1, \ldots, a_n)$ to $(X - a_1) \cdots (X - a_n)$. Its Jacobian determinant has norm $\prod_{i<j} |a_i - a_j|$. (See Lemma 9.4.) If $a = \rho(\pi'_L)$ for a uniformizer π'_L of L, then this product is $|\operatorname{disc}(\pi'_L)|^{1/2} = |\operatorname{disc}(L|K)|^{1/2}$, again because $(1, \pi'_L, \ldots, \pi'^{n-1}_L)$ is an integral basis.

The composition $\chi \circ \rho \circ d : K^n \to (K^{\text{sep}})^n$ sends $(b_0, \ldots, b_{n-1})$ to (the coefficient tuple of) the characteristic polynomial of $b_0 + b_1\pi_L + \cdots + b_{n-1}\pi_L^{n-1}$. Combining the above computations, we see that the norm of the Jacobian determinant of this map is $|\operatorname{disc}(L|K)|$.

Hence, by Theorem 13.3, if we interpret the image $\psi(U_L)$ as a multiset, then

$$\operatorname{vol}(\psi(U_L)) = |\operatorname{disc}(L|K)| \cdot \operatorname{vol}(U_L) = |\operatorname{disc}(L|K)| \cdot q^{-1}(1 - q^{-1}).$$

As ψ is n-to-1, we have

$$\sum_{\substack{L \subseteq K^{\text{sep}} \\ \text{totally ramified} \\ \text{degree } n}} \operatorname{vol}(\psi(U_L)) = n \cdot \operatorname{vol}(P),$$

so

$$\sum_L |\operatorname{disc}(L|K)| \cdot q^{-1}(1-q^{-1}) = n \cdot q^{-n}(1-q^{-1}),$$

so indeed

$$\frac{1}{n} \cdot \sum_L |\operatorname{disc}(L|K)| = q^{-(n-1)}. \qquad \square$$

Corollary 14.5. *Consider the separable field extensions L of K with ramification index e and inertia degree f, up to isomorphism. We have*

$$\sum_L \frac{|\operatorname{disc}(L|K)|}{\#\operatorname{Aut}(L)} = \frac{1}{f \cdot q^{(e-1)f}}.$$

Proof. To avoid confusion, we will write $|\cdot|_K$ and $|\cdot|_L$ for the normalized norm on K and L, respectively, and similarly q_K and q_L for the residue field size of K and L, respectively.

Using, Lemma 14.1, the left-hand side can again be rewritten as a sum over field extensions $L \subseteq K^{\mathrm{sep}}$ of K with ramification index e and inertia degree f:

$$\frac{1}{ef} \cdot \sum_{L \subseteq K^{\mathrm{sep}}} \frac{|\operatorname{disc}(L|K)|_K}{\#\operatorname{Aut}(L)}.$$

Each such field extension $L|K$ decomposes uniquely as $L|F|K$ with $F|K$ unramified of degree f and $L|F$ totally ramified of degree e. (Here, F is the splitting field of the polynomial $X^{q^f} - X$.) By the relative discriminant formula,

$$|\operatorname{disc}(L|K)|_K = |\operatorname{Nm}_{F|K}(\operatorname{disc}(L|F)) \cdot \operatorname{disc}(F|K)|_K = |\operatorname{Nm}_{F|K}(\operatorname{disc}(L|F))|_K = |\operatorname{disc}(L|F)|_L.$$

Since there is exactly one unramified extension $F \subseteq K^{\mathrm{sep}}$ of degree f, the theorem implies:

$$\frac{1}{ef} \cdot \sum_{L \subseteq K^{\mathrm{sep}}} |\operatorname{disc}(L|K)|_K = \frac{1}{f} \cdot \frac{1}{q_L^{e-1}} = \frac{1}{f \cdot q_K^{(e-1)f}}. \qquad \square$$

We can now prove the following mass formula regarding all étale extensions of K.

Theorem 14.6 ([Bha07, Theorem 1.1] and [Ked07, Theorem 1.1])**.** *Consider the étale K-algebras L of degree n, up to isomorphism. We have*

$$\sum_L \frac{|\operatorname{disc}(L|K)|}{\#\operatorname{Aut}(L)} = \sum_{r=0}^{n} \frac{P(n,r)}{q^{n-r}},$$

where $P(n,r)$ is the number of partitions of the integer n into r positive summands.

Example 14.7. *If $2 \nmid q$, then the degree 2 extensions are $K \times K$, $K(\sqrt{a})$, $K(\sqrt{\pi_K})$, $K(\sqrt{a\pi})$, where $a \in \mathcal{O}_K^\times$ is a quadratic nonresidue. They all have two automorphisms, and their discriminant norms are $1, 1, q^{-1}, q^{-1}$, respectively. Hence, $\sum_L \frac{|\operatorname{disc}(L|K)|}{\#\operatorname{Aut}(L)} = 1 + q^{-1}$.*

Proof. Any L can be written as $L = L_1 \times \cdots \times L_r$, with $\operatorname{disc}(L|K) = \operatorname{disc}(L_1|K) \cdots \operatorname{disc}(L_r|K)$, $n = [L_1 : K] + \cdots + [L_r : K]$. Consider the obvious action of S_r on the set of tuples $(L_1, \dots, L_r)$ of isomorphism classes of field extensions of K. We have

$$\#\operatorname{Aut}(L) = \#\operatorname{Aut}(L_1) \cdots \#\operatorname{Aut}(L_r) \cdot \#\operatorname{Stab}_{S_r}((L_1, \dots, L_r)).$$

(Any automorphism consists of a permutation of isomorphic factors of L together with isomorphisms of the individual factors.)

Let

$$a_n := \sum_{\substack{L \\ \text{separable field ext.} \\ \text{of degree } n}} \frac{|\operatorname{disc}(L|K)|}{\#\operatorname{Aut}(L)}.$$

It follows from the above discussion that

$$b_n := \sum_{\substack{L \\ \text{étale } K\text{-algebra} \\ \text{of degree } n}} \frac{|\operatorname{disc}(L|K)|}{\#\operatorname{Aut}(L)} = \sum_{r\geqslant 0} \sum_{\substack{S_r\text{-orbit of } (L_1,\dots,L_r) \\ \text{with } n=\sum_i [L_i:K]}} \prod_i \frac{|\operatorname{disc}(L_i|K)|}{\#\operatorname{Aut}(L_i)} \cdot \frac{1}{\#\operatorname{Stab}_{S_r}((L_1,\dots,L_r))}.$$

By the orbit-stabilizer theorem, this is

$$\sum_{r\geqslant 0} \frac{1}{r!} \sum_{\substack{(L_1,\dots,L_r) \\ \text{with } n=\sum_i [L_i:K]}} \prod_i \frac{|\operatorname{disc}(L_i|K)|}{\#\operatorname{Aut}(L_i)}.$$

This implies that the generating functions $\sum_n a_n X^n$ and $\sum_n b_n X^n$ are related by the power series identity

$$\sum_{n\geqslant 0} b_n X^n = \exp\left(\sum_{n\geqslant 0} a_n X^n\right).$$

According to the previous corollary, we have

$$a_n = \sum_{\substack{e,f\geqslant 1: \\ ef=1}} \frac{1}{f\cdot q^{(e-1)f}},$$

so

$$\sum_{n\geqslant 0} a_n X^n = \sum_{e,f\geqslant 1} \frac{X^{ef}}{f\cdot q^{(e-1)f}} = -\sum_{e\geqslant 1} \log\left(1-\frac{X^e}{q^{e-1}}\right).$$

Hence,

$$\sum_{n\geqslant 0} b_n X^n = \prod_{e\geqslant 1} \frac{1}{1-\frac{X^e}{q^{e-1}}} = \prod_{e\geqslant 1}\sum_{t\geqslant 0}\left(\frac{X^e}{q^{e-1}}\right)^t = \sum_{t_1,t_2,\dots\geqslant 0} \frac{X^{\sum_{e\geqslant 1} et_e}}{q^{\sum_{e\geqslant 1}(e-1)t_e}} = \sum_{n\geqslant 0} \frac{P(n,r)}{q^{n-r}} X^n.$$

(Any choice of $t_1, t_2, \dots$ with $n = \sum_{e\geqslant 1} et_e$ corresponds to a partition of n into $\sum_{e\geqslant 1} t_e$ summands, where e occurs t_e times.) □

References

[Bha07] Manjul Bhargava. "Mass formulae for extensions of local fields, and conjectures on the density of number field discriminants". In: *Int. Math. Res. Not. IMRN* 17 (2007), Art. ID rnm052, 20. ISSN: 1073-7928. DOI: 10.1093/imrn/rnm052.

[Igu00] Jun-ichi Igusa. *An introduction to the theory of local zeta functions*. Vol. 14. AMS/IP Studies in Advanced Mathematics. American Mathematical Society, Providence, RI; International Press, Cambridge, MA, 2000, pp. xii+232. ISBN: 0-8218-2015-X.

[Ked07] Kiran S. Kedlaya. “Mass formulas for local Galois representations”. In: *Int. Math. Res. Not. IMRN* 17 (2007). With an appendix by Daniel Gulotta, Art. ID rnm021, 26. ISSN: 1073-7928. DOI: `10.1093/imrn/rnm021`.

[Pop] Mihnea Popa. *Modern aspects of the cohomological study of varieties (Lecture notes)*. `https://people.math.harvard.edu/~mpopa/571/`.

[Ser78] Jean-Pierre Serre. “Une “formule de masse” pour les extensions totalement ramifiées de degré donné d’un corps local”. In: *C. R. Acad. Sci. Paris Sér. A-B* 286.22 (1978), A1031–A1036. ISSN: 0151-0509.

15. Cubic extensions

15.1 Binary cubic forms

Let R be an int. dom. with field of fractions K.

$V(R) :=$ set of binary cubic forms

$$f(X,Y) = aX^3 + bX^2Y + cXY^2 + dY^3 \quad (a,b,c,d \in R)$$

Let $GL_2(R)$ act on $V(R)$ by

$$(Mf)(v) = \det(M)^{-1} \cdot f(M^T v) \text{ for } M \in GL_2(R),\ f \in V(R),\ v \in R^2.$$

Lemma 15.1.1

The discriminant

$$\begin{aligned} \mathrm{disc}(f) &= b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^2 + 18abcd \\ &= \mathrm{disc}(f(X,1)) \quad \text{if } a \neq 0 \\ &= \mathrm{disc}(f(1,X)) \quad \text{if } d \neq 0. \end{aligned}$$

Rmk $\begin{pmatrix} \lambda & \\ & \lambda \end{pmatrix} f = \lambda \cdot f$

Lemma 15.1.2

a) $\mathrm{disc}(Mf) = \det(M)^2 \cdot \mathrm{disc}(f)$

b) The linear map $\varphi_M : V(K) \to V(K)$, $f \mapsto Mf$ has determinant $\det(\varphi_M) = \det(M)^2$.

c) Let $\eta_f : GL_2(K) \to V(K)$, $M \mapsto Mf$. $\rightsquigarrow$ $\mathrm{Jac}(\eta_f)(M) : T_M GL_2(K) \to V(K)$

$$T_M GL_2(K) = M_{2\times 2}(K) = K^4, \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \leftrightarrow (a,b,c,d); \qquad V(K) = K^4 \ (a,\dots$$

$$|\mathrm{Jac}(\eta_f)(M)| = |\mathrm{disc}(f)|.$$

15.2. Cubic extensions

Let R be a principal ideal domain.

Def A degree n ext. of R is an R-algebra S which is isomorphic to R^n as an R-module.

Ex $S = \underbrace{R \times \dots \times R}_{n}$

Ex $R = \mathbb{Z}$, $S =$ ring of integers of number field of degree n.

Lemma 15.2.1 For any degree n ext. of R, ~~has an R-basis of the form $(1, \omega_1, \dots, \omega_{n-1})$~~ we have $S/R \cong R^{n-1}$ as R-modules.

Pf

$$\begin{tikzcd} R \arrow[r, hook] \arrow[d, hook] & S \arrow[d, hook] \\ K \arrow[r, hook] & S \otimes_R K \end{tikzcd}$$

S is an integral extension of R.

R is a UFD, hence integrally closed in K.

$\Rightarrow S \cap K = R$

$\Rightarrow$ The R-module S/R is torsion-free.

$\Rightarrow S/R \cong R^{n-1}$

~~$\Rightarrow$ There is a basis of the form $(1, \omega_1, \dots, \omega_{n-1})$~~ $\square$

We now consider the case $n=3$ (cubic extensions).

Lemma 15.2.2

Let (θ_1, θ_2) be a basis of S/R.

There is a unique basis $(1, \omega_1, \omega_2)$ of S

with $\omega_i \equiv \theta_i \bmod R$ for $i=1,2$.

and $\omega_1 \omega_2 \in R$.

Pf Take any $\omega_i' \equiv \theta_i \bmod R$. $\Rightarrow (1, \omega_1', \omega_2')$ is an R-basis of S.

$\omega_i' \in S$ with

Write $\omega_1' \omega_2' = r \cdot 1 + p \cdot \omega_1' + q \cdot \omega_2'$ with $r, p, q \in R$.

Write $\omega_i := \omega_i' + \delta_i$ with $\delta_1, \delta_2 \in R$.

Then, $\omega_1 \omega_2 = (r + \delta_1 \delta_2) \cdot 1 + (p + \delta_2) \cdot \omega_1' + (q + \delta_1) \cdot \omega_2'$

lies in R if and only if $p + \delta_2 = 0$ and $q + \delta_1 = 0$. $\square$

Lemma 15.2.3

Define a commutative R-bilinear mult. operation on a free R-module $S := \langle 1, \omega_1, \omega_2 \rangle_R$ as follows, with $a, b, c, d, n, m, l \in R$:

$$\omega_1\omega_2 = n$$
$$\omega_1^2 = m - b\omega_1 + a\omega_2$$
$$\omega_2^2 = l - d\omega_1 + c\omega_2$$
$$(1 \cdot 1 = 1, \quad 1\cdot\omega_1 = \omega_1, \quad 1\cdot\omega_2 = \omega_2)$$

This mult. op. is associative if and only if

$$n = -ad, \quad m = -ac, \quad l = -bd.$$

Pf associative

$$\Leftrightarrow \underbrace{\omega_1\cdot(\omega_2^2)}_{\parallel} = \underbrace{(\omega_1\omega_2)}_{=\, n\omega_2}\cdot\omega_2 \quad \text{and} \quad (\omega_1^2)\cdot\omega_2 = \omega_1\cdot(\omega_1\omega_2)$$

$$l\omega_1 - d(m - b\omega_1 + a\omega_2) + cn$$

$$\Updownarrow$$

$$-dm + cn = 0 \text{ and } l = -bd \text{ and } n = -ad$$

$\Updownarrow$

$\square$

Consider the set of pairs $(S, (\theta_1, \theta_2))$ as above, with equivalence rel.

$(S,(\theta_1,\theta_2)) \sim (S',(\theta_1',\theta_2'))$ if there is an R-alg. isom. $S \to S'$ sending θ_i to θ_i'.

Cor 15.2.4

We have a bijection

$$\{(S,(\theta_1,\theta_2))\}/\sim \;\longleftrightarrow\; V(R)$$

$$(S,(\theta_1,\theta_2)) \longmapsto aX^3+bX^2Y+cXY^2+dY^3 = f(X,Y)$$

with $a,b,c,d \in R$ as in Lemma 15.2.3, $\omega_i \equiv \theta_i \bmod R$.

Lemma 15.2.5

Let $(S,(\theta_1,\theta_2))$, f as above.

We have a map

$$S/R \longrightarrow \Lambda^2(S/R)$$

$$[\alpha] \longmapsto \underbrace{[\alpha]\wedge[\alpha^2]}$$

indep. of repr. α mod R:

$[\alpha+r]\wedge[(\alpha+r)^2]$

$=[\alpha]\wedge[\alpha^2+2\alpha r+r^2]$

$=[\alpha]\wedge[\alpha^2+2\alpha r]$

$=[\alpha]\wedge[\alpha^2]$

and an isomorphism $\Lambda^2(S/R) \xrightarrow{\cong\, \Lambda^2 R^2} R$.

$$\theta_1\wedge\theta_2 \longmapsto 1$$

Let $\varphi: S/R \to R$ be the composition.

Then, $f(X,Y) = \varphi([X\theta_1+Y\theta_2])$.

Pf $\alpha := X\omega_1 + Y\omega_2$

$\alpha^2 \equiv -(bX^2+dY^2)\omega_1 + (aX^2+cY^2)\omega_2 \mod R$ by the formula in Lemma 15.2.3.

$\Rightarrow [\alpha] \wedge [\alpha^2] = f(X,Y)\cdot(\theta_1 \wedge \theta_2)$. $\square$

Cor 15.2.6

The bijection is $GL_2(R)$-equivariant.

Pf $(Mf)(v) = \dfrac{f(M^T v)}{\det(M)}$ ← "from the map $S/R \to \Lambda^2(S/R)$" ← "from the map $\Lambda^2(S/R) \to R$" $\square$

Thm 15.2.7

a) We have a bijection

$$\{\text{cubic ext.}^s \text{ of } R\}/\cong \;\longleftrightarrow\; GL_2(R)\backslash V(R)$$

b) If S corr. to f, then

$$\operatorname{Aut}(S) \cong \operatorname{Stab}_{GL_2(R)}(f).$$

c) $\operatorname{disc}(S) = \operatorname{disc}(f)$

Pf This follows because $GL_2(R)$ acts transitively on the set of bases (θ_1, θ_2) of S/R.

c) is a computation. $\square$

Lemma 15.2.8

Let $f \in \mathcal{V}(R)$. If $a \in R^\times$, then the corr. $(S, (\theta_1, \theta_2))$ is
$\quad\overset{\shortparallel}{ax^3+\dots}$

given by $\quad S = R[X]/(f(X,1))$

$$\omega_1 = aX$$
$$\omega_2 = aX^2 + bX + c$$
$$(\theta_i \equiv \omega_i \bmod R).$$

Pf computation $\square$

Another example:

$-X^2Y + XY^2$ corr. to $\quad S = R \times R \times R$

$\omega_1 = (1, 0, 0)$

$\omega_2 = (0, 1, 0)$

Rmk 15.2.9

For any $f \in \mathcal{V}(R)$, the corr. S is the ring of global sections of the scheme $\mathcal{V}_{\mathbb{P}^1_R}(f)$ (= the vanishing locus of the hom. pol. f on $\mathbb{P}^1_R$).

Lemma 15.2.10

S is an integral domain if and only if $f \in K[X,Y]$ is irreducible.

Pf S int. dom.

$\iff L := S \otimes_R K$ int. dom.

~~Hence, we can assume $R \equiv K$~~

If $a \neq 0$, then $L \cong K[X]/(f(X,1))$ int. dom.

$\iff f(X,1) \in K[X]$ irred.

$\iff f(X,Y) \in K[X,Y]$ irred.

If $a = 0$, then $\omega_1 \omega_2 = 0$, so L is not an int. dom.

and $f(X,Y) = (bX^2 + cXY + dY^2) \cdot Y$ is not irred.

$\square$

15.3. Three points in $\mathbb{P}^1$

We have a bijection

$$\overline{K}^\times \backslash \{ f \in V(\overline{K}) \mid \operatorname{disc}(f) \neq 0 \} \longleftrightarrow \{ A \subseteq \mathbb{P}^1(\overline{K}) \mid \# A = 3 \}$$

$$[f] \longmapsto \text{roots of } f \text{ in } \mathbb{P}^1(\overline{K})$$

$$\left[\prod_{i=1}^{3} (b_i X - a_i Y) \right] \longleftarrow \{ [a_1 : b_1], \ldots, [a_3, b_3] \}$$

Let $GL_2(K)$ act on $\mathbb{P}^1(K)$ by $M[x:y] = [x':y']$ where $\begin{pmatrix} x' \\ y' \end{pmatrix} = (M^T)^{-1}\begin{pmatrix} x \\ y \end{pmatrix}$.

This actually factors through an action of $PGL_2(K) = GL_2(K)/K^\times$.

Lemma 15.3.1

$PGL_2(K)$ acts simply and transitively on the set of (ordered!) triples (P_1, P_2, P_3) of distinct points in $\mathbb{P}^1(K)$.

Pf Let $P_i = [x_i : y_i]$, $v_i := (x_i, y_i) \in K^2$

$$\left.\begin{matrix} M[1:0] = P_1 \\ M[0:1] = P_2 \end{matrix}\right\} \Leftrightarrow (M^T)^{-1} = \begin{bmatrix} \lambda x_1 & \mu x_2 \\ \lambda y_1 & \mu y_2 \end{bmatrix} \text{ for some } \lambda, \mu \in K^\times.$$

Then, $M[1:1] = P_3 \Longleftrightarrow \lambda v_1 + \mu v_2 = \tau v_3$ for some $\tau \in K^\times$.

Since any two of the vectors v_1, v_2, v_3 are linearly independent, there is a unique such triple (λ, μ, τ) up to mult. by $K^\times$.

$\square$

~~Cor 15.3.2 If [f] corr. to the set $A \subseteq \mathbb{P}^1(\bar{K})$ of size 3, then~~

~~$\mathrm{Stab}_{PGL_2(\bar{K})}([f]) = \mathrm{Stab}$~~

~~$\bar{K}^\times \backslash \{f \in \ldots \mid \mathrm{disc}(f) \neq 0\}$~~

Cor 15.3.2

$PGL_2(\overline{K})$ acts transitively on $\{A \subseteq \mathbb{P}^1(K) \mid \# A = 3\}$

with $\mathrm{Stab}_{PGL_2(K)}(A) \cong S_3$.

Pf The three points in A can be permuted. $\square$

Cor 15.3.3

$PGL_2(\overline{K})$ acts transitively on $K^\times \backslash \{f \in V(\overline{K}) \mid \mathrm{disc}(f) \neq 0\}$

with $\mathrm{Stab}_{PGL_2(\overline{K})}([f]) \cong S_3$.

Same for K^{sep} instead of $\overline{K}$.

Cor 15.3.4

$GL_2(\overline{K})$ acts transitively on $\{f \in V(\overline{K}) \mid \mathrm{disc}(f) \neq 0\}$

with $\mathrm{Stab}_{GL_2(\overline{K})}(f) \cong S_3$.

Pf This follows from the prev. cor together with

$\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} f = \lambda \cdot f$. $\square$

Rmk 15.3.5

If the three distinct roots of $f \in V(K)$ lie in $\mathbb{P}^1(K)$, then

$\mathrm{Stab}_{GL_2(K)}(f) = \mathrm{Stab}_{GL_2(\overline{K})}(f) \cong S_3$.

15.4. Nonabelian group cohomology

Def Let G be a finite group. A <u>G-group</u> is a group A (not necessarily abelian!) with a left action of G (such that $g(a_1 a_2) = (ga_1)(ga_2)$).

We get the subgroup

$$H^0(G,A) = A^G = \{a \in A \mid ga = a \ \forall g \in G\}.$$

Let $Z^1(G,A)$ be the set of 1-cocycles: ~~maps~~ $\varphi : G \to A$ (not necessarily group hom.)

such that $\varphi(gh) = \varphi(g) \cdot g\varphi(h) \quad \forall g, h \in G$

Define an action of A on $Z^1(G,A)$ by

$(a\varphi)(g) = a \cdot \varphi(g) \cdot (ga^{-1})$ for $a \in A$, $\varphi \in Z^1(G,A)$, $g \in G$.

(check that $a\varphi \in Z^1(G,A)$!)

~~Let $B^1(G,A)$ be the~~

The <u>1-st cohomology set</u> is the set of orbits:

$$H^1(G,A) = A \backslash Z^1(G,A).$$

There is a special A-orbit $B^1(G,A) \subseteq Z^1(G,A)$, consisting of the <u>1-coboundaries</u>: maps of the form $(g \mapsto a \cdot (g^{-1}a))$ for some $a \in A$.

$\rightsquigarrow$ $H^1(G,A)$ is a pointed set with base point $B^1(G,A)$.

Rmk ~~[scribble]~~ Defining $H^2, H^3, \dots$ is problematic!

~~[scribble]~~

Lemma 15.4.1

If G acts trivially on A, then

$$H^0(G,A) = A, \qquad Z^1(G,A) = \mathrm{Hom}_{\text{group}}(G,A),$$

and A acts on $Z^1(G,A)$ by conjugation: $(a\varphi)(g) = a\varphi(g)a^{-1}$.

Hence, $H^1(G,A) = A \backslash_{\text{conj.}} \mathrm{Hom}_{\text{group}}(G,A)$

Rmk The pointed sets $H^1(G,A)$ satisfy functoriality, you get a truncated long exact sequence, ...

Reference 1) Milne: Algebraic groups, Lie groups, and their arithmetic subgroups, chapter VI.

2) Gille-Szamuely: Central simple algebras and Galois cohomology, section 2.3 (Galois descent)

Nonabelian ~~Galois~~ cohomology:

<u>Def</u> Let $L|K$ be a Galois ext. with Galois group G and let A be a G-group such that

~~every element of A is fixed~~

for every $a \in A$,

$$[G : \mathrm{Stab}_G(a)] < \infty .$$

("a is defined over a finite subext $F \subseteq L$ of K")

<u>Ex</u> $A = L$, $A = L^\times$, $A = GL_n(L)$, $A =$ any group with trivial G-action

<u>Def</u> (cont.)

$$H^0(L|K, A) := H^0(G, A) = A^G$$

If $L|K$ is a finite ext.,

$$H^1(L|K, A) := H^1(G, A).$$

For arbitrary $L|K$, let

$$H^1(L|K, A) := \varinjlim_{\substack{H \leq G \text{ normal} \\ \text{subgr. with} \\ [G:H] < \infty}} H^1(G/H, A^H),$$

or define cocycles requiring that $\varphi : \underset{\text{Krull}}{G} \to \underset{\text{discrete top.}}{A}$ is continuous.

Phenomenon 15.4.2

For any object P defined over K, let P_L be the corresponding object over L. ("base change to L")

Then, we often have a bijection

$$H^1(L|K, \mathrm{Aut}(P_L)) \longleftrightarrow \{\text{objects } Q \text{ defined over } K \text{ with } P_L \cong_L Q_L\}/_{\cong}$$

$$\begin{array}{ccc} (\sigma \mapsto f\circ(\sigma f^{-1})) & \longleftarrow\!\!| & Q \text{ with } Q_L \xrightarrow[\sim]{f} P_L \\ \cap & & \\ \mathrm{Gal}(L|K) \quad B^1(L|K, \mathrm{Aut}(P_L)) & \longmapsto & P \end{array}$$

Here, $\mathrm{Gal}(L|K)$ acts on isom. $Q_L \to P_L$ (and on automorphisms of P_L) by acting on the coefficients of the map. In other words, $\sigma f = \sigma\circ f\circ\sigma^{-1}$.

$$\varphi \longmapsto Q = \{x \in P_L \mid \sigma(x) = \varphi(\sigma)x \ \forall \sigma \in G\}$$

$\boxed{\text{The crux is whether this actually gives back } Q \text{ with } P_L \cong Q_L.}$

Moreover, if the 1-cocycle φ corr. to the object Q, then

$$\mathrm{Stab}_{\mathrm{Aut}(P_L)}(\varphi) \cong \mathrm{Aut}(P).$$

An example:

Thm 15.4.3 Consider n-dimensional vector spaces V over K.

~~Let $V = K^n$ (previously called D_2)~~

For any V, $\quad V_L := V \underset{K}{\otimes} L$.

Take $V = K^n$.

$\rightsquigarrow$ $\mathrm{Aut}(V_L) = GL_n(L)$, with the obvious action of $G = \mathrm{Gal}(L|K)$.

We have a bijection

$$H^1(L|K,\ GL_n(L)) \longleftrightarrow \{n\text{-dim. vector spaces } W \text{ over } K \text{ with } V_L \cong W_L\}/\cong$$

$$(\sigma \mapsto M(\sigma M^{-1})) \longleftarrow W, \text{ with an isom. } W_L \xrightarrow{\sim} V_L$$

given by a matrix $M \in GL_n(L)$ w.r.t. choices of K-basis of V and W.

$\mathrm{Stab}_{GL_n(L)}(\varphi) \cong GL_n(K) \cong \mathrm{Aut}(K^n)$.

Cor 15.4.4 $\quad H^1(L|K, GL_n(L)) = \{*\}$ since there is only one n-dim. vector space over K (up to $\cong$).

(For $n=1$, this fact $H^1(L|K, L^\times)$ is called Hilbert 90.)

Pf See the references 2 or 1. $\square$

Another example

Thm 15.4.5

Consider the étale degree n ext. V of K.

$$V_L := V \otimes_K L$$

Take $V = \underbrace{K \times \ldots \times K}_{n}$.

$\mathrm{Aut}(V_L) = S_n$ with the trivial action of G.

We have a bijection

$$\begin{array}{ccc} H^1(L|K, S_n) & \longleftrightarrow & \{\text{étale deg. } n \text{ ext. } W \text{ of } K \text{ with } V_L \cong W_L\}/\cong \\ \| & & \\ S_n \backslash \mathrm{Hom}(G, S_n) & & \end{array}$$

$$\mathrm{Stab}_{S_n}(f) \cong \mathrm{Aut}(W).$$

Ex If $L = K^{sep}$, then $RHS = \{\text{étale deg. } n \text{ ext. of } K\}/\cong$.

(That's Thm 12.2!)

Thm 15.4.6

Let $\mathcal{G}$ be an algebraic group defined over K (e.g. $\mathcal{G} = GL_n, SL_n, \ldots$).

Let $\mathcal{V}$ be a variety defined over K (e.g. $\mathcal{V} = \mathbb{A}^n, \ldots$).

Consider an algebraic action of $\mathcal{G}$ on $\mathcal{V}$ defined over K.

Consider the $\mathcal{G}(K)$-orbits in $\mathcal{V}(K)$. Fix one such orbit $\mathcal{G}(K)v_0$.

Assuming that $H^1(L|K, \mathcal{G}(L)) = \{*\}$, we have a bijection

$$H^1(L|K, \mathrm{Stab}_{\mathcal{G}(L)}(v_0)) \longleftrightarrow \left\{ \begin{array}{l} \mathcal{G}(K)\text{-orbits in } \mathcal{V}(K) \\ \text{contained in the } \mathcal{G}(L)\text{-orbit} \\ \mathcal{G}(L)v_0 \end{array} \right\}$$

$$\| $$

$$\mathcal{G}(K) \backslash (\mathcal{G}(L)v_0 \cap \mathcal{V}(K))$$

$$(\sigma \mapsto g^{-1}\sigma(g)) \longleftarrow\!\!\shortmid \quad \mathcal{G}(K)gv_0 \text{ with } g \in \mathcal{G}(L)$$

If the 1-cocycle φ corresponds to the orbit $\mathcal{G}(K)v$, then $\mathrm{Stab}_{\mathrm{Stab}_{\mathcal{G}(L)}(v_0)}(\varphi) \cong \mathrm{Stab}_{\mathcal{G}(K)}(v)$.

Pf. 1) Every 1-cocycle φ $\scriptstyle{\mathrm{Gal}(L|K) \to \mathrm{Stab}_{\mathcal{G}(L)}(v_0)}$ is of the form $(\sigma \mapsto g^{-1}\sigma(g))$ for $g \in \mathcal{G}(L)$

because it is a 1-cocycle $\varphi : \mathrm{Gal}(L|K) \to \mathcal{G}(L)$ and $H^1(L|K, \mathcal{G}(L)) = \{*\}$.

2) If $gv_0 \in \mathcal{V}(K)$, then $\underset{\substack{\| \\ \sigma(g)v_0}}{\sigma(gv_0)} = gv_0 \;\; \forall \sigma \in G$, so $g^{-1}\sigma(g) \in \mathrm{Stab}(v_0)$ $\forall \sigma \in G$.

~~3) If $h g_1 v_0 = g_2 v_0$ with $h \in \mathcal{G}(K)$, $g_1, g_2 \in \mathcal{G}(L)$, then~~

Let $S = \mathrm{Stab}_{\mathcal{G}(L)}(v_0)$. (10)

3) $\mathcal{G}(K) g_1 v_0 = \mathcal{G}(K) g_2 v_0$

$\Leftrightarrow \mathcal{G}(K) g_1 S = \mathcal{G}(K) g_2 S$

$\Leftrightarrow \exists h \in \mathcal{G}(K), s \in S: \; g_2 = h g_1 s$

$\Leftrightarrow \exists s \in S: \quad g_2 s^{-1} g_1^{-1} \in \mathcal{G}(K)$

$\Leftrightarrow \exists s \in S: \forall \sigma \in G: \quad g_2 s^{-1} g_1^{-1} = \sigma(g_2 s^{-1} g_1^{-1})$

$$\Updownarrow$$

$$s^{-1} g_1^{-1} \sigma(g_1) \sigma(s) = g_2^{-1} \sigma(g_2)$$

$\Leftrightarrow$ The 1-cocycles $(\sigma \mapsto g_1^{-1}\sigma(g_1))$ and $(\sigma \mapsto g_2^{-1}\sigma(g_2))$ lie in the same S-orbit.

4) ...

$\square$

<u>Exe</u> $\mathcal{G} = GL_2$, V = binary cubic forms,

$v_0 = -X^2Y + XY^2$ cubic form with roots $[0:1], [1:0], [1:1] \in \mathbb{P}^1(K)$

By Rmk 15.3.5, $\mathrm{Stab}_{GL_2(K)}(v_0) = \mathrm{Stab}_{GL_2(\overline{K})}(v_0) \cong S_3$.

$\Rightarrow$ trivial action of $\mathrm{Gal}(K^{sep}|K)$

By Cor 15.3.3, the $GL_2(K^{sep})$-orbit is $\{f \in V(K^{sep}) \mid \mathrm{disc}(f) \neq 0\}$.

$\Rightarrow$ The Thm gives a bijection

$$S_3 \backslash \mathrm{Hom}(\Gamma_K, S_3) \longleftrightarrow GL_2(K) \backslash \{f \in V(K) \mid \mathrm{disc}(f) \neq 0\}.$$

Thm 12.2 $\Updownarrow$ $\quad\quad$ $\swarrow\!\!\nearrow$ Thm 15.2.7

$\{$étale deg. 3 ext. of $K\}/\cong$

Ex (Kummer theory)

Let K be a field with $\mathrm{char}(K) \nmid n$ and which contains the n-th roots of unity.

$$\mathcal{G} = GL_1 = \mathbb{G}_m \rightsquigarrow \mathcal{G}(L) = L^\times$$

$$V = \mathbb{A}^1$$

Define the action of $\mathcal{G}$ on V by $x \cdot y = x^n y$

$v_0 = 1$

$$\mathrm{Stab}_{\mathcal{G}(K^{sep})}(v_0) \underset{\uparrow}{=} \mathrm{Stab}_{\mathcal{G}(K)}(v_0) = \langle \zeta_n \rangle \cong C_n$$ (cyclic group of order n)

$\Rightarrow$ triv action

$$\mathcal{G}(K^{sep})\, v_0 = (K^{sep})^{\times n} = (K^{sep})^\times$$

$\Rightarrow$ The Thm gives a bijection

$$\underset{\uparrow}{\cancel{C_n}\backslash} \mathrm{Hom}(\Gamma_K, C_n) \longleftrightarrow K^\times \underset{\uparrow}{\backslash} K^\times = K^{\times n} \underset{\uparrow}{\backslash} K^\times .$$

conjugation is trivial because C_n is abelian

the $x.y = x^n y$-action

usual action

15.5. Counting cubic number fields

~~Goal: Thm 15.5.1 $N(T) = \sum$~~

~~Overview:~~

~~1. construct fund. dom. for $GL_2(\mathbb{Z}) \circlearrowright V$~~

[The goal of this section:]

<u>Thm 15.5.1</u> For $T \to \infty$,

$$N(T) := \sum_{\substack{L \text{ cubic n.f. up to } \cong \\ |\mathrm{disc}(L)| \le T}} \frac{1}{\# \mathrm{Aut}(L)} \sim \frac{1}{3\zeta(3)} \cdot T.$$

<u>Rmk 15.5.2</u>

~~$\# \mathrm{Aut}(L) = 1$ for 100% of L (ordered~~

a) $\mathrm{Aut}(L) = \begin{cases} C_3 & \text{if } L \text{ is a Galois ext. (with grp } C_3\text{) of } \mathbb{Q} \\ 1 & \text{otherwise} \end{cases}$

b) $$\sum_{\substack{L \text{ cubic n.f.} \\ |\mathrm{disc}(L)| \le T \\ \mathrm{Aut}(L) = C_3}} 1 \sim C \cdot T^{1/2}.$$

<u>Rmk 15.5.3</u> $$\sum_{\substack{L \text{ quadr. n.f.} \\ |\mathrm{disc}(L)| \le T}} \frac{1}{\# \mathrm{Aut}(L)} \sim \frac{1}{2\zeta(2)} \cdot T, \text{ so } \sum_{\substack{L \text{ étale} \\ \mathbb{Q}\text{-alg.} \\ \text{of degree } 3 \\ |\mathrm{disc}(L)| \le T}} \frac{1}{\# \mathrm{Aut}(L)} \sim \left(\frac{1}{3\zeta(3)} + \frac{1}{2\zeta(2)} \right)$$

Recall the bijection from Thm 15.2.7:

$$\{\text{cubic ext. } S \text{ of } \mathbb{Z}\}/\cong \;\longleftrightarrow\; GL_2(\mathbb{Z}) \backslash V(\mathbb{Z})$$

$$\mathrm{Aut}_{\mathbb{Z}}(S) \cong \mathrm{Stab}_{GL_2(\mathbb{Z})}(f)$$

$$\mathrm{disc}(S) = \mathrm{disc}(f)$$

Def $V^m(\mathbb{Z}) := \{ f \in V(\mathbb{Z})$ corr. to a cubic ext. S of $\mathbb{Z}$ which is ($\cong$ to) the ring of integers $\mathcal{O}_L$ of an étale $\mathbb{Q}$-alg. L of degree 3$\}$

$$V^i(\mathbb{Z}) := \{ f \in V(\mathbb{Z}) \text{ corr. to an integral domain } S \}$$

$$\underset{\substack{\uparrow \\ \text{Lemma 15.2.10}}}{=} \{ f \in V(\mathbb{Z}) \text{ irreducible over } \mathbb{Q} \}$$

$$V^{mi}(\mathbb{Z}) = V^m(\mathbb{Z}) \cap V^i(\mathbb{Z})$$

$= \{ f \in V(\mathbb{Z})$ corr. to a cubic ext. of S which is ($\cong$ to) the ring of integers $\mathcal{O}_L$ of a cubic number field$\}$.

Rmk 15.5.3 We have a bijection

$$\{\text{cubic number field } L\}/\cong \;\longleftrightarrow\; GL_2(\mathbb{Z}) \backslash V^{mi}(\mathbb{Z})$$

$$\mathrm{Aut}_{\mathbb{Q}}(L) \qquad \cong \qquad \mathrm{Stab}_{GL_2(\mathbb{Z})}(f)$$

$$\mathrm{disc}(L) \qquad = \qquad \mathrm{disc}(f)$$

Overview of the proof of ~~[illegible]~~ the Thm:

<u>Step 1</u>: Construct a (nice) fund. dom. α_T for

$$GL_2(\mathbb{Z}) \circlearrowright \{ f \in V(\mathbb{R}) \mid 0 < |\mathrm{disc}(f)| \leq T \}.$$

<u>Rmk 15.5.4</u>

$$N(T) = \sum_{f \in V^{mi}(\mathbb{Z})} \alpha_T(f)$$

<u>Pf</u> Cor of Lemma 5.1. $\square$

<u>Step 2</u>: Compute the "volume" $V \cdot T = \underbrace{\int_{V(\mathbb{R})} \alpha_T(f)\,df}$.

[proportional to T because $V(\mathbb{R}) = \mathbb{R}^4$ and $\mathrm{disc}(f)$ is a hom. deg. 4 pol. in a, b, c, d]

<u>Def</u> $V^{a \neq 0}(\mathbb{Z}) := \{ f = ax^3 + \ldots \in V(\mathbb{Z}) \mid a \neq 0 \}$

<u>Rmk 15.5.5</u> $V^i(\mathbb{Z}) \subseteq V^{a \neq 0}(\mathbb{Z})$.

<u>Step 3</u>: Show that for any full lattice $\Lambda \subseteq V(\mathbb{Z})$,

$$\sum_{f \in V^{a \neq 0}(\mathbb{Z}) \cap \Lambda} \alpha_T(f) \underset{\Lambda}{\sim} \frac{V}{\mathrm{covol}(\Lambda)} \cdot T \text{ for } T \to \infty.$$

<u>Step 4</u>: Show that

$$\sum_{\substack{f \in V^{a \neq 0}(\mathbb{Z}) \\ f \notin V^i(\mathbb{Z})}} \alpha_T(f) = o(T) \text{ for } T \to \infty.$$

Def $\mathcal{V}^m(\mathbb{Z}_p) := \{f \in \mathcal{V}(\mathbb{Z}_p)$ corr. to a cubic ext. S of $\mathbb{Z}_p$ which is ($\cong$ to) the ring of integers of an étale $\mathbb{Q}_p$-algebra of degree 3$\}$.

Rmk 15.5.6

$\mathcal{V}^m(\mathbb{Z}) = \{f \in \mathcal{V}(\mathbb{Z}) \mid f \in \mathcal{V}(\mathbb{Z}_p) \ \forall p\}$

Step 5: Show that $\mathcal{V}^m(\mathbb{Z}_p) \subseteq \mathcal{V}(\mathbb{Z}_p)$ is given by finitely many congruence conditions (mod powers of p) and compute $W_p := vol(\mathcal{V}^m(\mathbb{Z}_p))$.

Step 6: Show that

$$\sum_{f \in \mathcal{V}^{a\neq 0}(\mathbb{Z}) \cap \mathcal{V}^m(\mathbb{Z})} \alpha_T(f) \sim \underbrace{\prod_p W_p}_{\frac{1}{3\zeta(3)}} \cdot V \cdot T \text{ for } T \to \infty$$

Pf (of Rmk 15.5.6)

Say $f \in \mathcal{V}(\mathbb{Z})$ corr. to the ext. S of $\mathbb{Z}$ and L of $\mathbb{Q}$ and S_p of $\mathbb{Z}_p$ and L_p of $\mathbb{Q}_p$. Note that $\underset{f \in \mathcal{V}(\mathbb{Z}) \text{ or } f \in \mathcal{V}^m(\mathbb{Z}_2)}{\underset{\Uparrow}{disc(f) \neq 0}}$ implies that L is an étale $\mathbb{Q}$-algebra of degree 3.

Any $\mathbb{Z}$-basis of S is also a $\mathbb{Z}_p$-basis of S_p.

Any $\mathbb{Z}$-basis of $\mathcal{O}_L$ is also a $\mathbb{Z}_p$-basis of L_p.

Let M be the linear map sending a $\mathbb{Z}$-basis of $\mathcal{O}_L$ to a $\mathbb{Z}$-basis of S.

The ring S is an integral ext. of $\mathbb{Z}$ because it is a finitely generated $\mathbb{Z}$-module. $\Rightarrow S \subseteq \mathcal{O}_L \Rightarrow M \in M_{3\times 3}(\mathbb{Z})$

Now, $S = \mathcal{O}_L \Leftrightarrow M \in GL_3(\mathbb{Z}) \Leftrightarrow \det(M) \in \mathbb{Z}^\times$

$S_p = \mathcal{O}_{L_p} \Leftrightarrow M \in GL_3(\mathbb{Z}_p) \Leftrightarrow \det(M) \in \mathbb{Z}_p^\times$.

Hence, $\underset{\overset{\Downarrow}{f \in \mathcal{V}^m(\mathbb{Z})}}{S = \mathcal{O}_L} \Leftrightarrow S_p = \mathcal{O}_{L_p} \ \forall p \Leftrightarrow f \in \mathcal{V}^m(\mathbb{Z}_p) \ \forall p$. $\square$

<u>Step 1</u>: construct a fund. dom. α_T for $GL_2(\mathbb{Z}) \circlearrowright \underbrace{\{f \in V(\mathbb{R}) \mid 0 < |\mathrm{disc}(f)| \in T\}}_{V_T(\mathbb{R})}$

Idea: $GL_2(\mathbb{Z}) \circlearrowright GL_2^{\pm 1}(\mathbb{R}) \circlearrowright V_T(\mathbb{R})$

$$GL_2^{\pm 1}(\mathbb{R}) = \{g \in GL_2(\mathbb{R}) \mid \det(g) = \pm 1\}$$

Let σ be a fund. dom. for the action of $GL_2(\mathbb{Z})$ on $GL_2^{\pm 1}(\mathbb{R})$ by left mult.

Let β_T be a fund. dom. for $GL_2^{\pm}(\mathbb{R}) \circlearrowright V_T(\mathbb{R})$.

Let
$$\alpha_T(f) := \sum_{\substack{g \in GL_2^{\pm 1}(\mathbb{R}),\\ f' \in V_T(\mathbb{R}):\\ f = gf'}} \sigma(g)\, \beta_T(f').$$

<u>Rmk 15.5.7</u>
α_T is a fund. dom. for $GL_2(\mathbb{Z}) \circlearrowright V_T(\mathbb{R})$.

<u>Pf</u>
$$\sum_{h \in GL_2(\mathbb{Z})} \alpha_T(hf) = \sum_{h \in GL_2(\mathbb{Z})} \sum_{\substack{g \in GL_2^{\pm 1}(\mathbb{R}),\\ f' \in V_T(\mathbb{R}):\\ hf = gf'}} \sigma(g)\, \beta_T(f')$$

$$= \sum_{\substack{g \in GL_2^{\pm 1}(\mathbb{R}),\\ f' \in V_T(\mathbb{R}):\\ f = gf'}} \underbrace{\sum_{h \in GL_2(\mathbb{Z})} \sigma(hg)}_{1}\, \beta_T(f')$$

$$= \sum_{g \in GL_2^{\pm 1}(\mathbb{R})} \beta_T(g^{-1}f) = 1 \qquad \square$$

To construct β_T:

$$GL_2(\mathbb{R})\backslash\{f\in V(\mathbb{R}) \mid \mathrm{disc}\neq 0\} \longleftrightarrow \{\text{étale cubic ext.}^{\text{s}} \text{ of } \mathbb{R}\}/\cong$$

$$\{\mathbb{R}\times\mathbb{R}\times\mathbb{R},\ \mathbb{R}\times\mathbb{C}\}$$

$$\begin{pmatrix}\lambda & \\ & \lambda\end{pmatrix} f = \lambda\cdot f \ \longrightarrow\ \updownarrow$$

$$GL_2^{\pm 1}(\mathbb{R})\backslash\{f\in V(\mathbb{R}) \mid |\mathrm{disc}| = 1\}$$

$$\mathrm{Stab}_{GL_2^{\pm1}(\mathbb{R})}(f) = \mathrm{Stab}_{GL_2(\mathbb{R})}(f) \cong \mathrm{Aut}_{\mathbb{R}}(L)$$

$$\mathrm{disc}(gf) = \det(g)^2\,\mathrm{disc}(f)$$

~~Easy to construct~~

$\mathbb{R}\times\mathbb{R}\times\mathbb{R}$ corr. to $f_1 = -X^2Y + XY^2$ with $\#\mathrm{Stab} = \#\mathrm{Aut} = 6 =: r_1$

$\mathbb{R}\times\mathbb{C}$ corr. to $f_2 = \frac{1}{\sqrt{2}} X(X^2+Y^2)$ with $\#\mathrm{Stab} = \#\mathrm{Aut} = 2 =:$

$$\Rightarrow \beta_T(f) = \begin{cases} 1/6, & f = \lambda\cdot f_1 \text{ for some } 0<\lambda\le T^{1/4} \\ 1/2, & f = \lambda\cdot f_2 \text{ for some } 0<\lambda\le T^{1/4} \\ 0, & \text{otherwise} \end{cases}$$

is a fund. dom. for $GL_2^{\pm1}(\mathbb{R}) \circlearrowright V_T(\mathbb{R})$.

Step 2: Compute $V \cdot T := \int_{\mathcal{V}(\mathbb{R})} \alpha_T(f)\, df$.

For $i=1,2$, consider the map

$$\psi_i : \mathbb{R}_{>0} \times GL_2^{\pm 1}(\mathbb{R}) \longrightarrow \mathcal{V}(\mathbb{R})$$
$$(\lambda, g) \longmapsto \lambda \cdot g f_i$$

We have $\alpha_T(f) = \sum_{i=1}^{2} \sum_{\substack{(\lambda, g): \\ \psi_i(\lambda,g)=f}} \frac{1}{r_i} \cdot \mathbb{1}_{(0,T^{1/4}]}(\lambda) \cdot \sigma(g)$.

$$\Longrightarrow \int_{\mathcal{V}(\mathbb{R})} \alpha_T(f) = \sum_{i=1}^{2} \frac{1}{r_i} \cdot \int_{\mathbb{R}_{>0}} \mathbb{1}_{(0,T^{1/4}]}(\lambda) \cdot 2\lambda^4 d^\times\lambda \cdot \int_{GL_2^{\pm 1}(\mathbb{R})} \sigma(g)\, d^\times g$$

change of variables (using Lemma 15.1.2 c and section 7.1) & ~~Note: Both sides~~ are 4-dimensional

$$= \left(\sum_{\substack{L \text{ étale} \\ \mathbb{R}\text{-alg.} \\ \text{of deg. } 3}} \frac{1}{\#\mathrm{Aut}(L)} \right) \cdot \frac{1}{2} T \cdot \underbrace{\mathrm{vol}(GL_2(\mathbb{Z}) \backslash GL_2^{\pm 1}(\mathbb{R}))}_{= \mathrm{vol}(SL_2(\mathbb{Z}) \backslash SL_2(\mathbb{R}))}$$

$$\Longrightarrow \boxed{\begin{aligned} V &= \left(\sum_{L/\mathbb{R}} \frac{1}{\#\mathrm{Aut}(L)} \right) \cdot \frac{1}{2} \cdot \mathrm{vol}(SL_2(\mathbb{Z}) \backslash SL_2(\mathbb{R})) \\ &= \frac{1}{3} \cdot \mathrm{vol}(SL_2(\mathbb{Z}) \backslash SL_2(\mathbb{R})) \end{aligned}}$$

__Step 3__ Show $\displaystyle\sum_{f\in V^{a\neq 0}(\mathbb{Z})\cap\Lambda} \alpha_T(f) \underset{\Lambda}{\sim} \frac{V}{\mathrm{covol}(\Lambda)}\cdot T$ for $T\to\infty$.

Let σ_0 be Siegel's fund. dom. for $GL_2(\mathbb{Z}) \curvearrowright GL_2^{\pm 1}(\mathbb{R})$:

$\mathrm{supp}(\sigma_0) \subseteq N' A' O_n(\mathbb{R})$, where $N' = \left\{\begin{pmatrix} 1 & 0 \\ n_{21} & 1\end{pmatrix} \,\middle|\, |n_{21}| \leq \frac{1}{2}\right\}$

and $A' = \left\{\begin{pmatrix} a_1 & 0 \\ 0 & a_2\end{pmatrix} \,\middle|\, \begin{matrix} a_1, a_2 > 0 \\ a_2 \geq \frac{\sqrt{3}}{2} a_1\end{matrix}\right\}$

Let $\eta : GL_2^{\pm 1}(\mathbb{R}) \to \mathbb{R}_{\geq 0}$ be smooth and compactly supported, ~~smooth $\int \eta(g)\,dg = 1$~~ or the indicator fct. of a cpt. semialg. set, with $\int \eta(g)\,dg = 1$.

Then, $\sigma := \sigma_0 * \eta$ is a fund. dom. for $GL_2(\mathbb{Z}) \curvearrowright GL_2^{\pm 1}(\mathbb{R})$ by Lemma 5.4.

Let $\displaystyle \gamma_T(f) := \sum_{\substack{g\in GL_2^{\pm 1}(\mathbb{R}),\\ f'\in V_T(\mathbb{R}):\\ f = gf'}} \eta(g)\beta_T(f')$.

Then, $\displaystyle \alpha_T(f) = \int_{GL_2^{\pm 1}(\mathbb{R})} \sigma_0(g)\,\gamma_T(g^{-1}f)$ by the def. of $\sigma = \sigma_0 * \eta$.

$$\Rightarrow \sum_{f\in V^{a\neq 0}(\mathbb{Z})\cap\Lambda} \alpha_T(f) = \int_{GL_2^{\pm 1}(\mathbb{R})} \sigma_0(g) \underbrace{\sum_{f\in V^{a\neq 0}(\mathbb{Z})\cap\Lambda} \gamma_T(g^{-1}f)}_{g\gamma_T(f)}\, dg \qquad (\mathrm{I})$$

Let $g = \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix}\begin{pmatrix} a_1 & 0 \\ 0 & a_2 \end{pmatrix} k \in N' A' O_n(\mathbb{R}) \cap GL_2^{\pm 1}(\mathbb{R})$.

~~We have $\mathrm{supp}(g\gamma_T) \subseteq \{ f = ax^3 + \dots \mid a \ll$~~

If $f \in \underbrace{\mathrm{supp}(\gamma_T)}_{\substack{\text{compact,} \\ \text{contained in} \\ \text{box of size} \asymp T^{1/4}}}$, then $gf(1,0) = f(\underbrace{g^T\begin{pmatrix}1\\0\end{pmatrix}}_{\|\cdot\| \ll a_1}) \ll a_1^3 T^{1/4}$.

$\Rightarrow \mathrm{supp}(g\gamma_T) \subseteq \{ f = ax^3 + \dots \mid a \ll a_1^3 T^{1/4} \}$.

$\Rightarrow$ If $a_1^3 T^{1/4} \ll 1$, then $\sum_{f \in V^{a \neq 0}(\mathbb{Z})} g\gamma_T(f) = 0$. (II)

Otherwise, apply Poisson summation or Davenport's lemma to ~~...~~ ~~...~~ justify $\sum g\gamma_T(f) = \frac{1}{\ldots}\int g\gamma_T(f)\,df + O(\dots)$

$$\| \quad \int \gamma_T(f)\,df \qquad \text{(III)}$$

The claim follows by ~~integrating ... ...~~ plugging (II)/(III) into (I).

Step 4 Show $\displaystyle\sum_{\substack{f \in V^{a\neq 0}(\mathbb{Z}) \\ f \notin V^{i}(\mathbb{Z})}} \alpha_T(f) = o(T)$

If $f \bmod p \in V(\mathbb{F}_p)$ is irreducible for some p, then f is irreducible over $\mathbb{Q}$.

The claim follows from Step 3 using a sieve as in the proof of Thm 3.2.1.

Step 5 a) Show that $V^m(\mathbb{Z}_p) \subset V(\mathbb{Z}_p)$ is given by fin. many cong. cond. and b) compute $w_p := \mathrm{vol}(V^m(\mathbb{Z}_p))$.

$$GL_2(\mathbb{Z}_p) \backslash V^m(\mathbb{Z}_p) \longleftrightarrow \{(\text{rings of int. of}) \text{ étale cubic ext.}^{L} \text{ of } \mathbb{Q}_p\}/\cong$$

$$\mathrm{Stab}_{GL_2(\mathbb{Z}_p)}(f) \qquad \cong \qquad \mathrm{Aut}(L)$$

$$|\mathrm{disc}(f)|_p \qquad = \qquad |\mathrm{disc}(L)|_p$$

For each L, pick a corresponding $f_L \in V^m(\mathbb{Z}_p)$.

$$\Rightarrow V^m(\mathbb{Z}_p) = \bigsqcup_L GL_2(\mathbb{Z}_p) f_L \qquad (\mathrm{I})$$

Let $\eta_L : GL_2(\mathbb{Z}_p) \to V^m(\mathbb{Z}_p)$, $g \mapsto g f_L$. Each element of $GL_2(\mathbb{Z}_p) f$ has exactly $\# \mathrm{Aut}(L)$ preimages.

By Lemma 15.1.2, $|\mathrm{Jac}(\eta_L)(g)|_p = |\mathrm{disc}(f_L)|_p = |\mathrm{disc}(L)|_p$.

$\Rightarrow$ By change of variables (Thm 13.3),

$$\mathrm{vol}(GL_2(\mathbb{Z}_p)f_L) = \frac{|\mathrm{disc}(L)|_p}{\#\mathrm{Aut}(L)} \cdot \mathrm{vol}(GL_2(\mathbb{Z}_p)).$$

$$\underset{(I)}{\Rightarrow} w_p = \mathrm{vol}(V^m(\mathbb{Z}_p)) = \sum_L \frac{|\mathrm{disc}(L)|_p}{\#\mathrm{Aut}(L)} \cdot \mathrm{vol}(GL_2(\mathbb{Z}_p))$$

$$\sum_L \frac{|\mathrm{disc}|}{\#\mathrm{Aut}} \underset{\substack{\text{Mass formula}\\ \text{(Thm 14.6)}}}{=} 1 + \frac{1}{p} + \frac{1}{p^2}$$

$$\mathrm{vol}(GL_2(\mathbb{Z}_p)) \underset{\substack{\text{Thm 7.5.2,}\\ \text{Thm 7.5.3}}}{=} \left(1 - \frac{1}{p}\right) \cdot \mathrm{vol}(SL_2(\mathbb{Z}_p))$$

$$\Rightarrow w_p = \left(1 + \frac{1}{p} + \frac{1}{p^2}\right)\left(1 - \frac{1}{p}\right) \cdot \mathrm{vol}(SL_2(\mathbb{Z}_p))$$

$$= \left(1 - \frac{1}{p^3}\right) \cdot \mathrm{vol}(SL_2(\mathbb{Z}_p)).$$

$$\xRightarrow{\text{Cor 15.5.8}} \prod_p w_p \cdot V = \prod_p \left(1 - \frac{1}{p^3}\right) \mathrm{vol}(SL_2(\mathbb{Z}_p)) \cdot \frac{1}{3} \mathrm{vol}(SL_2(\mathbb{Z}) \backslash SL_2(\mathbb{R}))$$

$$\underset{\text{Cor 7.5.4}}{=} \frac{1}{3} \prod_p \left(1 - \frac{1}{p^3}\right) = \frac{1}{3\zeta(3)} \text{ as claimed}$$

For a), note that the image of the compact set $GL_2(\mathbb{Z}_p)$ ($GL_2(\mathbb{Z}_p)f_L$) is compact. $\underset{\#\{L\} < \infty}{\Longrightarrow}$ $V^m(\mathbb{Z}_p)$ is compact.

Moreover, the image of $GL_2(\mathbb{Z}_p)$ is open

by Hensel's lemma because the Jacobian det. $|\mathrm{disc}(L)|_p$

of η_L is $\neq 0$.

$\Rightarrow V^m(\mathbb{Z}_p)$ is a compact and open subset of $V(\mathbb{Z}_p)$.

$\Rightarrow V^m(\mathbb{Z}_p)$ is defined by finitely many congruence

conditions.

<u>Step 6</u> Show $\displaystyle\sum_{f\in V^{a\neq 0}(\mathbb{Z})\cap V^m(\mathbb{Z})} \alpha_T(f) \sim \prod_p w_p \cdot V \cdot T$.

Recall that $V^m(\mathbb{Z}) = \{ f \in V(\mathbb{Z}) \mid f \in V^m(\mathbb{Z}_p)\ \forall p \}$.

$\rightsquigarrow$ We use a sieve (with step 3). This immediately shows "$\leq$".
For "$\geq$", the only difficulty is showing the following uniformity estimate:

<u>Thm 15.5.9</u> For any T, p,

$$\sum_{\substack{f\in V(\mathbb{Z})\\ f\notin V^m(\mathbb{Z}_p)}} \alpha_T(f) \ll \frac{T}{p^2}$$ where the constant is independent of T and p.

<u>Note</u> If $f \in V(\mathbb{Z}_p)$, $f \notin V^m(\mathbb{Z}_p)$, then $p^2 \mid \mathrm{disc}(f)$.

<u>Lemma 15.5.10</u> Let L be an étale cubic $\mathbb{Q}_p$-algebra and $S \subseteq \mathcal{O}_L$ a cubic ext. of $\mathbb{Z}_p$.

If $S \neq \mathcal{O}_L$, then S is a subext. of some cubic ext.

$S \subsetneq S' \subseteq \mathcal{O}_L$

of <u>type I</u>: if (θ_1', θ_2') is a $\mathbb{Z}_p$-basis of $S'/\mathbb{Z}_p$ then $(p\theta_1', p\theta_2')$ is a $\mathbb{Z}_p$-basis of $S/\mathbb{Z}_p$. $(\Rightarrow [S':S] =$

or of <u>type II</u>: there is a $\mathbb{Z}_p$-basis (θ_1', θ_2') of $S'/\mathbb{Z}_p$ such that $(p\theta_1', \theta_2')$ is a $\mathbb{Z}_p$-basis of $S/\mathbb{Z}_p$ and the cubic form $f' \in V(\mathbb{Z}_p)$ corr. to $(S', (p\theta_1', \theta_2'))$ is not divisible by p. $(\Rightarrow [S':S] = p$

Lemma 15.5.10

$= \{ f \in V(\mathbb{Q}_p) \text{ irred. over } \mathbb{Q}_p \}$

Consider an orbit $GL_2(\mathbb{Z}_p) f$ in $V^i(\mathbb{Z}_p)$ with $f \notin V^m(\mathbb{Z}_p)$.
One of the following holds:

a) $p \mid f$

b) $p \nmid f$, but $GL_2(\mathbb{Z}_p) f = GL_2(\mathbb{Z}_p) \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} f'$

for some $f' \in V^i(\mathbb{Z}_p)$. [f, f' corr. to ext. S, S' of $\mathbb{Z}_p$ with $S \subsetneqq S'$ (index p^2 in case a), index p in case b))

Pf Let f corr. to the ext. S of $\mathbb{Z}_p$ and the ext. L of $\mathbb{Q}_p$.

$\Rightarrow S \subsetneqq \mathcal{O}_L$.

Let $\mathcal{O}_L$ corr. to the cubic form $f'' \in V^i(\mathbb{Z})$.

Since $S \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = L = \mathcal{O}_L \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$, we have $f = M f''$

for some $M \in GL_2(\mathbb{Q}_p)$ (a base change matrix from $\mathcal{O}_L/\mathbb{Z}_p$ to $S/\mathbb{Z}_p$).

Since $S \subseteq \mathcal{O}_L$, we have $M \in M_{2\times 2}(\mathbb{Z}_p)$. (I)

Since $S \neq \mathcal{O}_L$, we have $M \notin GL_2(\mathbb{Z}_p)$, so $\det(M) \notin \mathbb{Z}_p^\times$. (II)

Only the $GL_2(\mathbb{Z}_p)$-orbits of f and f'' matter, so we can (w.l.o.g.) multiply M by elements of $GL_2(\mathbb{Z}_p)$ on the left and on the right (independently) to put M into <u>Smith normal form</u>: $M = \begin{pmatrix} p^r & 0 \\ 0 & p^s \end{pmatrix}$ with $r \geq s$.

(I) $\Rightarrow$ $s \geq 0$.

(II) $\Rightarrow$ $r + s \neq 0$.

Assume $p \nmid f$.

$\Rightarrow$ We can't have $r = s \geq 1$ because then $\mathcal{V}(\mathbb{Z}_p) \ni f'' = M^{-1} f = p^{-r} \cdot f$.

Hence, $r \geq s+1$.

Write $f = aX^3 + bX^2Y + cXY^2 + dY^3$.

$$\Rightarrow \mathcal{V}(\mathbb{Z}_p) \ni f'' = M^{-1} f = p^{-2r+s} aX^3 + p^{-r} bX^2Y + p^{-s} cXY^2 + p^{r-2s} dY^3$$

$$\Rightarrow p^{-2}a,\ p^{-1}b \in \mathbb{Z}_p.$$

$$\Rightarrow \underbrace{\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}^{-1} f}_{=:f'} \in \mathcal{V}(\mathbb{Z}_p).$$

$\square$

Cor 15.5.11

If moreover $f \in \mathcal{V}^i(\mathbb{Z})$, then

a) $p \mid f$ or

b) $p \nmid f$, but $GL_2(\mathbb{Z}) f = GL_2(\mathbb{Z}) \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} f'$ for some $f' \in \mathcal{V}(\mathbb{Z})$.

Pf a) clear

b) We know

$$\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}^{-1} Mf \in \mathcal{V}(\mathbb{Z}_p) \text{ for some } M \in GL_2(\mathbb{Z}_p).$$

We can multiply M on the left by an element of the form $\begin{pmatrix} 1 & 0 \\ 0 & \epsilon \end{pmatrix} \in GL_2(\mathbb{Z}_p)$ (which commutes with $\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$!) to make $\det(M) = 1$. There is some $M' \in SL_2(\mathbb{Z})$ such that $M' \equiv M \bmod p^2$. Then, $Mf \equiv M'f \bmod p^2$ implies that we also have $\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}^{-1} M'f \in \mathcal{V}(\mathbb{Z})$.

$\square$

Pf of Thm 15.5.9

For case a),

$$\sum_{\substack{f\in V^i(\mathbb{Z})\\ p\mid f}} \alpha_T(f) \underset{f=pf'}{\uparrow}{=} \sum_{f'\in V^i(\mathbb{Z})} \underbrace{\alpha_T(pf')}_{\alpha_{T/p^4}(f')} \ll \frac{T}{p^4} \text{ by step 3.}$$

For case b):

Claim For each $GL_2(\mathbb{Z})$-orbit $GL_2(\mathbb{Z})f'$ in $V(\mathbb{Z})$ with $p\nmid f'$ for $f'\in B$, there are at most 3 $GL_2(\mathbb{Z})$-orbits A such that

$$A = GL_2(\mathbb{Z})\begin{pmatrix} p & 0\\ 0 & 1\end{pmatrix} f' \text{ for some } f''\in GL_2(\mathbb{Z})f'.$$

If $p\mid f$, there are at most $p+1$ such orbits.

This then implies:

$$\sum_{\substack{f\in V^i(\mathbb{Z})\\ p\nmid f\\ \text{but } GL_2(\mathbb{Z})f = GL_2(\mathbb{Z})\begin{pmatrix} p & 0\\ 0 & 1\end{pmatrix}f'\\ \text{for some } f'\in V(\mathbb{Z})}} \alpha_T(f) \le 3\sum_{f'\in V^i(\mathbb{Z})} \alpha_{T/p^2}(f') \ll \frac{T}{p^2}.$$

$$+ (p+1)\sum_{\substack{f'\in V^i(\mathbb{Z})\\ p\mid f'}} \alpha_{T/p^2}(f')$$

Pf of claim

We have $\begin{pmatrix} p & 0\\ 0 & 1\end{pmatrix} f'' \in V(\mathbb{Z})$ if and only if $f''([0:1]) \equiv 0 \bmod p$.

~~Consider the map $GL_2(\mathbb{Z}) \to \mathbb{P}^1(\mathbb{F}_p)$~~

~~$M \mapsto M^T[0:1] \bmod p$~~

We have $\begin{pmatrix} p & 0\\ 0 & 1\end{pmatrix} M^T f' \in V(\mathbb{Z})$ if and only if $M^T[0:1]$ is a root of $f' \bmod p$. If $M^T[0:1] \equiv M'^T[0:1] \bmod p$, then $GL_2(\mathbb{Z})\begin{pmatrix} p & 0\\ 0 & 1\end{pmatrix} M f' = GL_2(\mathbb{Z})\begin{pmatrix} p & 0\\ 0 & 1\end{pmatrix} M' f'$ because $M'M^{-1} \equiv \begin{pmatrix} * & *\\ 0 & *\end{pmatrix} \bmod p$ and therefore $\begin{pmatrix} p & 0\\ 0 & 1\end{pmatrix} M'M^{-1}\begin{pmatrix} p & 0\\ 0 & 1\end{pmatrix}^{-1} \in GL_2(\mathbb{Z})$.

Hence, the number of orbits A is the nr. of roots of f' in $\mathbb{P}^1_{\mathbb{F}_p}$, which is ≤ 3 if $p \nmid f$ and $p+1$ if $p \mid f$.

claim $\to \square$

Thm 15.5.9 $\to \square$

Thm 15.5.1 $\to \square$

15.6. Outlook on higher degrees

Rmk Every degree n form $f \in K[X,Y]$ with $\mathrm{disc}(f) \neq 0$ gives rise to an étale deg. n ext. of K (namely the ring of global sections of the vanishing locus of f on $\mathbb{P}^1_K$).

Every étale deg. n ext. arises from some f.

But for $n \geq 4$ there are "way more" $GL_2(K)$-orbits of forms than étale extensions: say K is algebraically closed.

$\dim(GL_2(K)) = 4$

$\dim(\{\text{deg. } n \text{ forms}\}) = n+1$

$\Rightarrow$ There are ∞ many orbits.

But there is only 1 étale ext.

Rmk $GL_2(\mathbb{Q}) \backslash \{\text{quartic forms with disc} \neq 0\} \Longleftrightarrow$ 2-Selmer elements of ell. curves

locally soluble

Prop (Wright–Yukie)

étale deg. 4 ext. $\longleftrightarrow (GL_2 \times GL_3)(K) \backslash \{(A,B)$ pair of ternary quadr. forms (with coeff. in K) $\mid \dots \neq 0\}$

Prop (W–Y)

étale deg. 5 ext. $\Leftrightarrow (GL_4 \times GL_5)(K) \backslash \{(A_1, \dots, A_4)$ tuple of skew-symm. 5×5-matrices $\mid \dots \neq 0\}$

Bhargava counted deg. 4,5 ext. of $\mathbb{Q}$ by discriminant by studying the relationship between rings of integers and integral orbits.

16. Abelian extensions

Let G be a finite abelian group.

Rmk 16.1

If $L|K$ is a Galois ext. with group G, we have a surjection

$$\begin{array}{ccccc} \Gamma_K & \twoheadrightarrow & \mathrm{Gal}(L|K) & \xrightarrow{\sim} & G. \\ \sigma & \longmapsto & \sigma|_L & & \end{array}$$

Conversely, any continuous surj. $f: \Gamma_K \twoheadrightarrow G$ arises from a Galois ext. with group G (the subfield of K^{sep} fixed by $\ker(f)$).

We'll count arbitrary cont. grp. hom. $\Gamma_K \twoheadrightarrow G$ (corr. to étale ext. vs. just field ext.)

~~If G is abelian, any hom.~~

Let K^{ab} be the maximal abelian ext. of K
(= compositum of all abelian ext.)
(= subext. of K^{sep} fixed by commutator subgr. of Γ_K)

For abelian G, any cont. hom. $\Gamma_K \to G$ factors through $\Gamma_K^{ab} = \mathrm{Gal}(K^{ab}|K)$.
Let K be a number field from now on.
For any p, let $I_p \subseteq \Gamma_K^{ab}$ be the inertia subgroup for p
(It's generally defined only up to conjugation!)

Def $f: \Gamma_K^{ab} \to G$ is <u>unramified at p</u> if $f(I_p) = \{id\}$.

Rmk 16.2 a) $L|K$ unram. at $p \Leftrightarrow$ corr. $f: \Gamma_K^{ab} \to G$ unram. at p.

b) Any (cont.) f has only finitely many ramified primes p.

Let $\operatorname{ram}(f) := \prod_{\substack{p: \\ f \text{ ramified at } p}} p$ [prod. of ramified primes].

<u>Question</u> Let $K = \mathbb{Q}$.

$N(T) :=$ $\#\{f : \Gamma_K^{ab} \to G \mid \operatorname{ram}(f) \leq T\} \sim ?$ as $T \to \infty$

Approach #1: Use Kummer theory over an extension $\mathbb{Q}(\zeta_n)$ of $\mathbb{Q}$ with $nG = \{id\}$.

Think about which hom. $\Gamma_{\mathbb{Q}(\zeta_n)} \to G$ extend to hom. $\Gamma_{\mathbb{Q}} \to G$, and in how many ways.

<u>Approach #2</u>: Class field theory

<u>Thm 16.3</u> (Kronecker-Weber)

a) $\mathbb{Q}^{ab} = \bigcup_{n \geq 1} \mathbb{Q}(\zeta_n) = \bigcup_{p} \bigcup_{k \geq 1} \mathbb{Q}(\zeta_{p^k})$

b) $\Gamma_{\mathbb{Q}}^{ab} \cong \lim_{n \geq 1} (\mathbb{Z}/n\mathbb{Z})^\times \cong \prod_p \lim_{k \geq 1} (\mathbb{Z}/p^k\mathbb{Z})^\times = \prod_p \mathbb{Z}_p^\times$

c) $I_p = \mathbb{Z}_p^\times \subseteq \prod_{p'} \mathbb{Z}_{p'}^\times$

Lemma 16.4 Assume $p \nmid \#G$. Let $\mathcal{C}$ be the set of nontrivial cyclic subgroups of G.

Then, $$\#\{f : \mathbb{Z}_p^\times \to G \text{ (cont.)}\} = \sum_{\substack{U \in \mathcal{C}: \\ p \equiv 1 \bmod \#U}} \varphi(\#U)$$ ← Euler's totient function

Pf f must factor through $(\mathbb{Z}/p^k\mathbb{Z})^\times$ for some $k \geq 1$.

We have $x^{p^{k-1}} \equiv 1 \bmod p^k$ for any $x \equiv 1 \bmod p$.

$\Rightarrow f(x^{p^{k-1}}) = id$ for all $x \equiv 1 \bmod p$.

$\quad \| \quad f(x)^{p^{k-1}}$

$\Rightarrow f(x) = id$ — " —

$\uparrow$ $p \nmid \#G$

$\Rightarrow f$ factors through $(\mathbb{Z}/p\mathbb{Z})^\times \cong C_{p-1}$.

$\uparrow$ [cyclic grp. of order $p-1$]

Let $U = \mathrm{im}(f)$.

$\Rightarrow p \equiv 1 \bmod \#U$.

In this case, there is exactly one factor group of C_{p-1} isom. to U, with $\varphi(\#U)$ isomorphisms. $\square$

Let $D_p(s) := \sum_{f:\mathbb{Z}_p^\times \to G} \underbrace{\mathrm{ram}_p(f)^{-s}}_{\substack{1 \text{ if } f \text{ is trivial map} \\ p^{-s} \text{ otherwise}}} = 1 + C_p \cdot p^{-s}$

~~We've shown~~

Remarks

a) This is a finite sum.

b) We've shown $C_p = \sum_{U \in \mathcal{E}\,:\, p \equiv 1 \bmod \#U}^{(HW!)} \varphi(\#U)$ if $p \nmid \#G$.

Since $\Gamma_{\mathbb{Q}}^{ab} = \prod \mathbb{Z}_p^\times$, we have

$$D(s) := \sum_{f:\Gamma_{\mathbb{Q}}^{ab} \to G} \mathrm{ram}(f)^{-s} = \prod_p D_p(s). \qquad \text{(formally)}$$

Write $D(s) = \sum_{n \geq 1} a_n n^{-s}$ (formally).

~~By Wiener Ikehara~~

~~Using Ikehara Theorem~~

By the Wiener-Ikehara Theorem / Ikato's Thm / Perron's formula / Tauberian Thm, the asymptotics of $\sum_{n \in T} a_n = \#\{f:\Gamma_{\mathbb{Q}}^{ab} \to G \mid \mathrm{ram}(f) \leq T\}$ are determined by the rightmost pole of $D(S)$.

~~Write $D_1(s) \sim D_2(s)$ if $\frac{D_1(s)}{D_2(s)}$ can be holomorphically continued to~~

Thm 16.5

$D(s)$ can be meromorphically continued to $\{\operatorname{Re}(s) \geq 1\}$, holomorphic except for a pole of order $\#\mathcal{C}$ at $s=1$.

Pf Write $D_1(s) \sim D_2(s)$ if $\frac{D_1(s)}{D_2(s)}$ can be holomorphically continued to $\{\operatorname{Re}(s) \geq 1\}$. Write $A(s) \approx B(s)$ if $\frac{A(s)}{B(s)} = 1 + O(p^{-2s})$ and $\frac{B(s)}{A(s)} = 1 + O(p^{-2s})$.

For any $p \nmid \#G$, we have

$$D_p(s) = 1 + \sum_{\substack{U \in \mathcal{C}: \\ p \equiv 1 \bmod \#U}} \varphi(\#U) p^{-s} \approx \prod_{\substack{U \in \mathcal{C} \\ p \equiv 1 \bmod \#U}} \left(1 + \varphi(\#U) p^{-s}\right)$$

$$= \prod_{U \in \mathcal{C}} \Big(1 + \sum_{\substack{\chi: (\mathbb{Z}/|U|\mathbb{Z})^\times \to \mathbb{C}^\times \\ \text{group hom.}}} \chi(p) \cdot p^{-s}\Big)$$

$$\approx \prod_{U \in \mathcal{C}} \prod_{\chi} \left(1 + \chi(p) \cdot p^{-s}\right)$$

$$\approx \prod_{U \in \mathcal{C}} \prod_{\chi} \left(1 + \chi(p) \cdot p^{-s} + \chi(p^2) \cdot p^{-2s} + \dots\right).$$

$$\Rightarrow D(s) = \prod_p D_p(s) \sim \prod_{U \in \mathcal{C}} \prod_{\chi} L(s, \chi).$$

~~The RHS is hol. on $\{\mathrm{Re}(s)\geq 1\}$ except~~

The Dirichlet L-series $L(s,\chi)$ is hol. on $\{\mathrm{Re}(s)\geq 1\}$ except for a simple pole at $s=1$ in case χ is the trivial hom. $(\mathbb{Z}/|U|\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times$. $\square$

Using some form of Wiener-Ikehara, it follows that:

<u>Thm 16.6</u> There is a constant $C>0$ such that
$$N(T) \sim C\cdot T(\log T)^{|\mathcal{C}|-1} \quad \text{for } T\to\infty.$$

Instead of combining all ramified primes in the same invariant, one can for each $U\in\mathcal{C}$ define

$$\mathrm{inv}_U(f) := \prod_{\substack{p\nmid \#G:\\ f(\underbrace{I(p)}_{\mathbb{Z}_p^\times})=U}} p \qquad \text{for } f:\underbrace{\Gamma_{\mathbb{Q}}^{ab}}_{\prod_p \mathbb{Z}_p^\times}\longrightarrow G.$$

<u>Rmk</u> $$\prod_U \mathrm{inv}_U(f) = \prod_{\substack{p\nmid\#G\\ p\mid \mathrm{ram}(f)}} p.$$

Using similar techniques as above (e.g. Wiener-Ikehara for Dirichlet series in $|\mathcal{C}|$ variables), one can show:

<u>Prop 16.7</u> $\#\{f \mid \mathrm{inv}_U(f)\leq T_U\ \forall U\in\mathcal{C}\} \sim C'\cdot\prod_U T_U$ for all $T_U\to\infty$.

Rmk 16.8 b) Thm 16.6 can be recovered from ~~[illegible]~~ a).

~~[illegible]~~

a) The same still holds (with a different constant) if we fix the restriction of f to $\mathbb{Z}_p^\times$ for finitely many p or if we fix some of the invariants $\mathrm{inv}_v(f) = i_v$ instead of $\mathrm{inv}_v(f) \le T_v$ with $T_v \to \infty$.

c) You can use this to count e.g. Galois extensions $L/\mathbb{Q}$ with group G by $\mathrm{ram}(L)$ or $\mathrm{disc}(L)$ or...

Previously done ~~by~~ by Wright: Distribution of discriminants of abelian ext.