JEAN-PIERRE SERRE

Adeles and Tamagawa numbers

Cours de Jean-Pierre Serre, tome 1 (1981)
<http://www.numdam.org/item?id=CJPS_1981__1_>

Adeles and Tamagawa Numbers

J-P. Serre — Harvard 1981

	pages
§0 — History	1
Siegel formula	3
Tamagawa	8
— §I — Integration on p-adic manifolds	9
Notation	9
Measure att. to a form ω	10
Rational summation	15
Igusa	16
Vector bundles	17
Smooth schemes	18
Number of points of classical and except. groups	20
Decomposition of a measure	24
Connexion with densities	28
Dig. Liftable solutions	31
Smooth case	32
Real case	37
Use of resol. of singularities	40
Oesterlé : hypersurfaces	41
Lojasiewicz inequality	48
Oesterlé : general case	49
— §II — Adeles	55
History	55
Definition	55
A_K/K compact	58
Haar measure on A_K	61
Characters and Duality	64
Haar measure for dual groups	66

pages

Compatible measures w.r. to duality 67

Adelic integration and heuristic formulas (Goldbach, ...) 69

Adelic points on algebraic varieties 75

Properties of the functor $V \mapsto V(A_K)$ 78

Restriction of scalars 84

Algebraic groups and adelic points 88

Abelian varieties (S. Bloch) 88

Weak approximation 90

Strong approximation 91

Adeles, classes and genera 99

Tensors 102

Vector bundles 104

Adelic measures 106

Convergent case 108

Algebraic Groups 111

Tori 114

Convergence 117

Tamagawa number (semi-simple case) 122

Th. of Ono - Weil conjecture 123

Tamagawa number (reductive case) 126

$\tau(\mathbb{G}_m) = 1$ 131

Tori (Ono) 133

$\tau(PGL_n) = n\,\tau(SL_n)$ 135

pages

Tamagawa $\Leftrightarrow$ Siegel (mass formula) 136

Tamagawa $\Leftrightarrow$ Siegel (the two-groups game) 145

Correction to Ono's theory 146

Positive definite quadratic forms over $\mathbb{Q}$ 147

Proof that $\tau(SO_n) = 2$ for $n = 2, 3, 4$ 152

Proof of Siegel's formula 156

Proof $(m \geqslant 5)$ 163

" $(m = 4)$ 165

" $(m = 2)$ 166

" $(m = 3)$ 169

Remarks on Siegel's proof 172

Application to modular forms 176

§ III – SL_n 180

The Minkowski-Hlawka Theorem 180

Proof 184

Serre-
7/22/81
-1-

Adeles and Tamagawa Numbers

§0. History:

Gauss (D.A.) 1801 : $n \geq 4$ square-free considers
$r_3(n) = \#$ of rep's of n as a sum of 3 squares

shows

$$r_3(n) = \begin{cases} 12\, h(n) & n \not\equiv 3 \bmod 8 \\ 24\, h(n) & n \equiv 3 \bmod 8 \end{cases}$$

$h(4) = \frac{1}{2}$ per convention
$h(3) = \frac{1}{3}$ "

(for $n \not\equiv 7 \bmod 8$), where $h(n) = $ class # of $\mathbb{Q}(\sqrt{-n})$.

Jacobi 1829 (Fund. Nova): In his theory of elliptic functions via "theta function identities": $r_4(n)$, $r_6(n)$, $r_8(n)$. e.g.

$$r_4(n) = 8 \sum_{\substack{d \mid n \\ 4 \nmid d}} d \iff (1 + 2q + 2q^4 + 2q^9 + \dots)^4 = 1 + 8\left\{ \frac{q}{1-q} + \frac{2q^2}{1+q^2} + \frac{3q^3}{1-q^3} + \dots \right\}$$

$$1 + 8\left\{ \frac{q}{1-q} + \frac{2q^2}{1+q^2} + \frac{3q^3}{1-q^3} + \dots \right\}$$

($\Rightarrow r_4(n) > 0$ for $n \geq 1$!)

Similarly:

$$r_8(n) = 16 \sum_{d \mid n} (-1)^{n+d} d^3 \quad (n \text{ square-free})$$

also equiv. to a θ-function identity:

$$\theta^8 = 1 + 16\left\{ \frac{q}{1+q} + \frac{8q^2}{1-q^2} + \frac{27q^3}{1+q^3} + \dots \right\}$$

Dirichlet 1838 Sur l'usage des séries infinies dans la théorie des nombres (Crelle): introduces analysis.
Computes $h(n)$ using "Dirichlet series".

example : $\left| \begin{array}{l} n \equiv 1 \quad (8) \\ n \text{ sqf} \\ n > 1 \end{array} \right.$: $r_5(n) = -80 \sum\limits_{1 \leq x \leq \frac{n}{2}} \underset{\chi_n(x)}{\underset{\parallel}{\left(\frac{x}{n}\right)}} x$

$L_\chi(s) = \sum \chi(n) n^{-s}$.

(1) Assume first $\mathbb{Q}(\sqrt{-D})$, $D > 0$ $[\chi(-1) = -1]$. Then

$-D$ = discriminant

$$\frac{2\pi}{\sqrt{|D|}} \frac{h}{w_D} = L(1) = \sum_{n\uparrow} \frac{\chi(n)}{n}, \quad \text{By computing } L(1), \text{ one gets:}$$

d'où $(D > 4)$

pour $\begin{cases} D = 3 \to \frac{1}{3} \\ D = 4 \to \frac{1}{2} \end{cases}$

$$h = -\frac{1}{D} \sum_{1 \le x \le D-1} \chi(x) x = +\frac{1}{2 - \chi(2)} \sum_{1 \le x < D/2} \chi(x)$$

exercise: $D = 4$: $L(1) = \frac{\pi}{4}$ Show $\frac{\pi}{4} = L(1) = \prod_{p\uparrow} \frac{1}{1 - \chi(p) p^{-1}}$

~~(uses Dirichlet's Thm on arithmetic progressions with a reasonable error term).~~

Consequence: $p \equiv -1 \bmod 4$ $\mathbb{Q}(\sqrt{-p}) \Rightarrow h = \begin{cases} R - N & p \equiv 7 \ (8) \\ \frac{1}{3}(R - N) & p \equiv 3 \ (8) \end{cases}$

R = # of quad. residues mod p between $1, p/2$
N = # of non-res.

e.g. $p = 7$ $1, 2$ $R = 2$, $N = 1$

Eisenstein 1847 (1) Introduces "Mass", "Weight" of a "genus" of quadratic forms
← (2) formulae for $r_5(n), r_7(n)$ (stated without proof)

X = set of quad. forms, Weight of $X = \sum_{x \in X} \frac{1}{\mathrm{Aut}(X)}$

$|X| = 1$.

Defⁿ of genus: $Q = \sum a_{ij} x_i x_j$ $a_{ij} \in \mathbb{Z}$, $a_{ij} = a_{ji}$
$Q' = \sum a'_{ij} x_i x_j$

When are they "equivalent": e.g. $A \in GL_n(\mathbb{Z})$ $Q' = A^t Q A$

... $\mathbb{R}$-equivalent

Then Q, Q' are in the same <u>genus</u> if they are $\mathbb{R}, \mathbb{Z}_p$ equivalent (local equivalence).

Every genus contains finitely many classes under $\mathbb{Z}$-equivalence.

e.g. $x_1^2 + x_2^2 + \dots + x_n^2$ for $n \leq 8$: only one class in genus
for $n \geq 9$ > 1 class in genus.

In quadratic forms : $x^2 + 23y^2$ has another class in its genus.

$$\text{weight} = w(\underset{\sim}{g}) = \sum \frac{1}{|\text{Aut}(\ )|}.$$
genus

<u>H. Smith</u> 1867 : Gave proofs of Eisenstein's statements

<u>Académie des Sciences de Paris</u> 1881 : Topic : a proof of Eisenstein statements on $r_5(n)$

1883 : Smith ! } split the prize
Minkowski (undergraduate : 17 years old)

English infuriated : Smith's work → split prize
French " : 10 yrs after war with Germany !

<u>Hardy</u> "circle method" to give asymptotic formulae $r_s(n) \sim \dots$ $(n \to \infty)$
1920's $r_s(n) =$ Main Term + (error) and error $= 0$ if $s \leq 8$.

<u>C.L. Siegel</u> 1935-37 (Annals of Math : in german) Fundamental papers

I. positive definite / $\mathbb{Q}$

II. indefinite / $\mathbb{Q}$

III pos. definite / totally real field and statements for the general case.

Siegel's formula: includes Minkowski/Eisenstein etc. as special cases.

Λ' = lattice with pos. def. quadratic form, rank $\leq$ rank Λ

count: embeddings $\Lambda' \hookrightarrow \Lambda$

[e.g. $\Lambda' = \mathbb{Z}$, x^2
$\downarrow$
Λ is looking for
x with $x \cdot x = n$ i.e.
# of solutions of $Q(x) = n$].

In terms of quadratic forms: $Q: m$, $Q': n$, $m \geq n$

"representing Q' by Q" $\Leftrightarrow$ ${}^tX\,Q\,X = Q'$ so: $Q[X] = Q'$ notation

$X = m \times n$ matrix

Def^{n}: $N(Q,Q')$ = # of X's with $Q[X] = Q'$.

Computes instead something else: $Q_1, \dots, Q_h$ repr's of the genus of Q.

$w_i = |\mathrm{Aut}(Q_i)|$

W = weight of genus $= \sum \frac{1}{w_i}$

Siegel computes the "mean value":

$$A(Q,Q') = \left\{ \sum_{i=1}^{h} \frac{N(Q_i,Q')}{w_i} \right\} \Big/ \sum \frac{1}{w_i}$$

so if $h=1$, this is in fact $N(Q,Q')$.

Siegel computes: (check the formula!) $\lambda = 2$ $m = n-1$; $= \frac{1}{2}$ $m = n+1$; $= 1$ otherwise

$$A(Q,Q') = \lambda\, S_\infty \prod_{p} S_p$$

in fact absolute convergence except if $m = \cancel{n} = 2$ and $m = n+2$

Here the δ's are local factors:

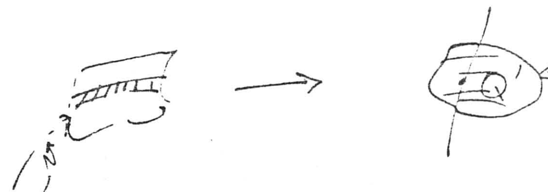
δ_∞: $\quad X \overset{Q}{\longmapsto} Q[X] \subset$ Symmetric matrices of rank n

$\quad\quad X$ is mn dimensional

so a map

$$\mathbb{R}^{mn} \xrightarrow{Q} \mathbb{R}^{\frac{n(n+1)}{2}} \ni Q'$$

i.e. map



$\leftarrow$ neighborhood U'

U = inverse image

can prove $\lim_{U' \to 0} \frac{\mathrm{vol}(U)}{\mathrm{vol}(U')}$ exists and $= \begin{cases} \delta_\infty & m > n \\ 2\delta_\infty & m = n \end{cases}$

δ_p: $\quad \mathbb{Q}_p^{mn} \xrightarrow{Q} \mathbb{Q}_p^{\frac{n(n+1)}{2}}$ get $\lim_{U' \to 0} \frac{\mathrm{vol}(U)}{\mathrm{vol}(U')} = \begin{cases} \delta_p & m > n \\ 2\delta_p & m = n. \end{cases}$

examining what a "neighborhood of Q'" is gives the alternative formulation:

U' = all symm. matrices $\equiv Q' \bmod p^M$ $\quad (M \to \infty)$
U = all X's with $Q[X] \equiv Q' \bmod p^M$

p-adic volume of a class mod p^M $= \frac{1}{p^{Mmn}}$

$$\Rightarrow \quad val_p(U) = \frac{\#\text{ of solutions mod } p^M \text{ of } Q[X] = Q' \text{ mod } p^M}{p^{Mmn}}$$

$$val_p(U') = \frac{1}{p^{M\,n(n+1)/2}}$$

$$\Rightarrow \quad \delta_p \text{ defined by } \lim_{M\to\infty} \underbrace{\frac{\#\text{ solutions of } Q[X] \equiv Q' \text{ mod } p^M}{p^{M\left(mn - \frac{n(n+1)}{2}\right)}}}$$

in fact constant for M large.
so limit is innocuous

Product converges since alg. variety of dim r has $\sim p^r$ pts mod p. More generally: $\delta_p = 1 + O(\frac{1}{p^2})$ abs conv.
or $1 - \frac{\chi(p)}{p} + O(\frac{1}{p^2})$ cond. conv.

In Siegel II: δ_p same, since $\mathbb{Z}_p$ compact; δ_∞ trouble: over $\mathbb{R}$ loc. compact $\to$ measure of inverse image of U' is ∞.

corrected δ_∞, $A(Q,Q')$ ["Q are "units" "] gives formula

Siegel III: number fields

Consequence of III: k totally real, pos. definite quadr. forms.

<u>Warm-up</u>: Siegel I for $m=n$, $Q'=Q$ (mass formula)

Assume $Q = Q_1$ (genus classes $Q_1, \ldots, Q_h$)

$$\Rightarrow \quad N(Q,Q) = |\mathrm{Aut}\, Q| = w_1$$
$$N(Q_i, Q) = 0 \quad i \geq 2$$

Then $\quad A(Q,Q) = \dfrac{1}{\sum \frac{1}{w_i}}$ ← mass of genus

so Siegel's formula gives

$$\frac{1}{\text{Mass of genus}} = \delta_\infty \prod_{p} \delta_p \Leftarrow Q, Q' = Q$$ relative to — formula for mass

Back to k = tot. real:

e.g. $X_1^2 + \dots + X_n^2$

LHS. $\in \mathbb{Q}$ $\quad \delta_\infty$ = vol. of some orthog. gp. $= \pi^{\text{some power}} \cdot (\text{rat'l} *)$

Find: $\quad \prod \delta_p = \dfrac{\text{rat'l} *}{\zeta_k(2)\zeta_k(4)\dots\zeta_k(\;)}$ (?)

For successive values of n, gives

$(n=3)$ $\quad \zeta_k(2) = \pi^{2[k:\mathbb{Q}]} \times d_k^{\text{some power}} \times (\text{rat'l} *)$ $\quad d_k^{1/2}$

functional'l equation $\Rightarrow$ $\zeta_k(-1) \in \mathbb{Q}$

etc:

Corollary: (Siegel) $\zeta_k(1-n) \in \mathbb{Q}$ when n is even, $n \geq 2$, k totally real. (n odd, numbers are all 0).

Result was stated by Hecke, who published no proof.

~1960 (Kuga, M. Kneser), Tamagawa on $G_{\mathbb{A}}$ G = Special Orthogonal Gp SO some quad. form

define a measure ("Tamagawa measure") s.t.

$$\underset{\text{Tamagawa number } \tau}{\underset{\parallel}{\mathrm{vol}(G_{\mathbb{A}}/G_K)}} = 2.$$

More or less unpublished, sent manuscript to Weil: lectures at Institute: Adeles and Algebraic Groups IAS ~1961.

$\mathrm{Tam}(SL_n) = 1$ (simply connected : $\mathrm{Tam}(SO) = 2$ "⟺" $|\pi_1 SO| = 2$)

Conjecture (Weil): G simply connected $\Rightarrow \mathrm{Tam}(G) = 1$.
[Langlands: sketch (pf. by K. Lai : qusi-split) and for the classical groups]
C Math 1980

Ono (~1966) computes Tam(tori) and $\dfrac{\mathrm{Tam}(G)}{\mathrm{Tam}(G')} = \deg \phi$
not abs. convergence

G' s. conn. $G' = G/\phi$.
ϕ finite.

Weil (Acta Arithm.) Serre professes not to understand material here
Weil Representations

— o —

Topics in Course:
I. Integration (of real functions) on p-adic manifolds with applications to counting points mod p^N.
II. Adele spaces / Tamagawa numbers
III. Case: SL_n : applications to { Minkowski-Hlawka theorem; Vector bundles over curves (Harder)
IV SO

§I. Integration on p-adic manifolds

K = local field (complete w.r.t. discrete valuation on $v: K^* \twoheadrightarrow \mathbb{Z}$ with finite residue field k)
(locally compact field, not discrete, $\neq \mathbb{R}, \mathbb{C}$).

Let $q = \# |k|$, π = a uniformizer in K.

$\mathcal{O}_K$ = ring of integers in K.

Denote by $\| \ \|$ the normalized absolute value; $\|x\| = q^{-v(x)}$, $x \in K$ (with $v(0) = +\infty$). Reason for normalized absolute value also comes from the Haar measure: μ on K, normalized by $\mu(\mathcal{O}_K) = 1$. ($\mathcal{O}_K$ = open, compact in K). $\mathcal{O}_K$ is compact since $\mathcal{O}_K = \varprojlim \mathcal{O}_K/\pi^n\mathcal{O}_K$ and Haar measure defined by taking obvious measure on $\mathcal{O}_K/\pi^n\mathcal{O}_K$ (every element of mass $\frac{1}{q^n}$). So if U = congruence class in $\mathcal{O}_K$ mod $\pi^n\mathcal{O}_K$ $\Rightarrow \mu(U) = \frac{1}{q^n}$.

Then if $\Omega \subset \mathcal{O}_K$ is open, compact, this is equivalent to U being the (finite) union of classes mod π^m for some m. Then $\mu(U) = \frac{\#\text{classes}}{q^m}$ (independent of m, of course). $\in \mathbb{Z}[\frac{1}{p}]$ if $q = p^e$.

μ is invariant by translations (sometimes $\mu = dx = \|dx\|$) but not by multiplication:

$$\|d(ax)\| = \|a\| \, \|dx\|. \qquad \text{for fixed } a \in K^*.$$

The proof reduces to: $a \in \mathcal{O}_K$, $\mu(a\mathcal{O}_K) = \|a\|^{+}$, $a\mathcal{O}_K$ = open subgp. of $\mathcal{O}_K$,
so need to show: $|\mathcal{O}_K / a\mathcal{O}_K| = \|a\|^{-1}$

V = K-manifold, analytic manifold over K of dim n defined as usual (analytic = locally expandable as a Taylor series (convergent of course)).

---

example: X an algebraic variety $/K$, smooth (every pt. non-sing.) of dim n. Then take

$$X(K) = K \text{ points of } X$$

(reduce to case of affine variety, embedded in K^n).

e.g. $F(t_0,\dots,t_n) \in K[t_0,\dots,t_n]$, assume hypersurface $F(\ ) = 0$ is smooth, i.e. no point with $F=0$, $\frac{\partial F}{\partial t_i} = 0 \ \forall i$.

(smooth affine variety of dim n $/K$).

Let ω be a differential form on V of degree n (maximal), i.e. locally, if $x_1,\dots,x_n$ local coordinates

$$\omega = f(x_1,\dots,x_n)\, dx_1 \wedge \dots \wedge dx_n$$

[real def^n: dual tangent bundle, ext. prod line bundle

Associate to ω a measure:

$$\mu_\omega = \|\omega\| = \|f(x)\|\, dx_1 \dots dx_n = \|f(x)\|\, \|dx_1 \dots dx_n\|$$

Claim: μ_ω does not depend on the choice of coordinates

Pf: new coord's $y_1, \ldots, y_n$ power series giving y's in terms of x's etc
Need to prove the "change of variables formula":

$$J = \text{Jacobian} = \det \frac{\partial y_i}{\partial x_j}$$ (K valued analytic function)

need to prove:

real

$$dy = \| J \| \, dx$$

Have $K^n \quad K^n$
$U \xrightarrow{\phi} U'$ neigh's of origin
(read "y" above)

$y = \phi(x) \quad \| J_\phi \|$
want $dy = \| J_\phi \| \, dx$

Want: $\int \theta(y) \, dy = \int \| J\phi(x) \| \, \theta(\phi x) \, dx$
some function

Weil: reduction to 1 variable.
Serre: typical cases:

(1) ϕ linear map: by homothety (know action of scalars)
may change basis so that:

$$\phi : \begin{array}{ccc} e_1 & \longrightarrow & \pi^{m_1} e_1 \\ \vdots & & \vdots \\ e_n & \longrightarrow & \pi^{m_n} e_n \end{array}$$
(basis for $\mathcal{O}_K^n$)

breaks into product of scalar mult's ✓ by previous

(2) $\left.\begin{array}{l} y_1 = x_1 + \text{higher terms} \\ \vdots \\ y_n = x_n + \text{higher terms} \end{array}\right\} \Rightarrow$ Jacobian $= 1$ at origin

$\Rightarrow \quad \|J\| = 1$ in a neighborhood of origin

so we have to prove that such a change of variables fixes Haar measure (in a neighborhood of origin).
Explicate the "neighborhood": change variables

$$y_1 = \pi^N Y_1, \ldots, y_n = \pi^N Y_n$$
$$x_1 = \pi^N X_1, \ldots, x_n = \pi^N X_n.$$

on power series, this has the effect: $y_1 = x_1 + f_2' + f_3' + \ldots$
$\Rightarrow \quad Y_1 = X_1 + \pi^N f_2'(X_1, \ldots, X_n)$ etc.

so that if N is large, all coeff's of the new higher terms are in $\mathcal{O}_K$, and even tend to 0 as index tends to $+\infty$.
("Restricted Power Series" with integral coefficients)
These power series are now invertible (even as formal power series).

Further, such a map maps classes mod π^m into another such class so it permutes the classes mod p^m $\Rightarrow$ preserves the Haar measure.
(Surjectivity by invertibility)

Since any transf. is of the type (1), (2) under composition, we are done.

We consider the special type of ω which are nowhere 0 (Weil: "gauge forms"), i.e. $\omega = f(x)\, dx_1 \wedge \ldots \wedge dx_n$ locally at P, $f(P) \neq 0$ ($\forall P$).

μ = measure on V is called "regular" if given locally by a nowhere 0 ω.

so then $\mu = c\, dx_1 \ldots dx_n$ locally $\quad c \in q^{\mathbb{Z}}$ i.e. $c = q^m$ for some m

[since $\|f(x)\|$ is locally constant, $\omega = f(x)\, dx_1 \ldots dx_n$].

$\Rightarrow$ If Ω is an open compact set in V, then $\mu(\Omega) \in \mathbb{Z}[\frac{1}{q}]$

Also, if f is a real-valued function on V, locally constant, compact support, with values in $\Lambda \subset \mathbb{R}$ (subgp), then

$$\int f(x)\mu(x) \in \mathbb{Z}[\tfrac{1}{q}]\Lambda = \Lambda$$

(so integration is very "algebraic").

More generally, let Λ = an abelian gp. s.t. $\lambda \mapsto q\lambda$ is invertible (e.g. any field with characteristic $\neq p$). Suppose $f: V \to \Lambda$ is locally constant with compact support, then for regular μ,

$$\int f(x)\mu(x) \quad \text{can be defined}$$

[f loc. const. / comp. support $\Rightarrow$ $\exists\, U_i$ open compact subsets of V
U_i disjoint
$f = 0$ outside $\bigcup U_i$
$f(U_i) = \{\lambda_i\}$ constant, $\lambda_i \in \Lambda$

$$\Rightarrow \quad \int f(x)\mu(x) \overset{\text{def}^n}{=} \sum_i \underbrace{\mu(U_i)}_{\in\, \mathbb{Z}[\frac{1}{q}]} \lambda_i$$

$\mathbb{Z}[\frac{1}{q}]$, Λ a module over $\mathbb{Z}[\frac{1}{q}]$]

(indep. of cover), i.e.

$$\underbrace{\mathcal{C}_V(\Lambda)}_{\substack{\text{loc. const.} \\ \text{of compt support}}} = \mathcal{C}_V(\mathbb{Z}) \otimes \Lambda \qquad \text{(exercise)}$$

—

What about non-regular ω?

ω = some diff. form of degree n. (e.g. $x^3 dx$ on the line)

$\mu_\omega = \|\omega\|$.

First question: $\mathcal{U}$ open, compact, what is $\mu_\omega(\mathcal{U})$? [$\notin \mathbb{Z}[\frac{1}{q}]$

exercise, compute $\int_{\mathcal{O}_K} \|x\|^3 dx$].

Lebesgue type: $\int_{\mathcal{O}_K} \|x\|^3 dx = \sum$ value of $\|x\|^3 \cdot \mu$ (set where this value is taken)

(Riemann: partition values of x, Lebesgue: partition values of range of f)

$$= \sum_{m=0}^{\infty} \frac{1}{q^m} \underbrace{\left(1-\frac{1}{q}\right)}_{\text{remove } 0} q^{-3m} = \frac{q^3}{\underbrace{q^3+q^2+q+1}_{\text{not a power of } q}}$$

<u>Conjecture</u>: $\mu_\omega(\mathcal{U}) \in \mathbb{Q}$

"essentially" proved: if $\mathrm{ch} K = 0$ then "<u>Thm</u>" $\mu_\omega(\mathcal{U}) \in \mathbb{Q}$ (pf. uses a technique of Igusa — pf. for polynomial f: $\int \|f\| dx_1 \cdots dx_n \in \mathbb{Q}$ using resolution of singularities, then get "Thm".

f power series, restricted, integ. coeff's, $\mathcal{O}_K^n$; $x_1, \dots, x_n$

m integer ≥ 0 :

$$U_{m,f} = \{x \mid v(f(x)) = m\} \quad \text{open, compact}$$

$$\Rightarrow \quad I = \int \|f(x)\| dx = \sum_{m=0}^{\infty} \mu(U_{m,f}) q^{-m}$$

$$\left(\|f\| = \frac{1}{q^m} \text{ on } U_{m,f} \right)$$

why rational?

A series $u_0 + u_1 + \dots + u_n + \dots$ is "rationally convergent" if

$u_0 + u_1 T + \dots + u_m T^m + \dots = f(T)$ is a rat'l funct. of T with no pole at $T = 1$

$$f(1) \overset{\text{def}^n}{=} \sum u_i \quad , \quad u_i \in \mathbb{Q} \Rightarrow \sum_{i=0}^{\infty} u_i \in \mathbb{Q}$$

Igusa:

Using resolution of singularities, proof shows $u_n = \mu(U_{n,f})$, then $\sum u_n$ is rationally summable

(so gives a stronger statement than the "Thm" above).

1-29 Further remarks on Igusa's Theorem: X = p-adic manifold ($= \mathcal{O}_K^n$ in Igusa), f analytic (= polynomial in Igusa), coeff's in $\mathcal{O}_K$).

For any m, let $U_m = \{x \mid v(f(x)) = m\}$ i.e. $\|f(x)\| = q^{-m}$

μ_m = measure of U_m

Theorem (Igusa): $\sum \mu_m T^m$ is a rational function of T

(Pf: reduce to normal crossings by blowing up and then compute).

Alternatively, let $V_m = \{x \mid f(x) \equiv 0 \bmod \pi^m\}$

$v_m = \text{meas}(V_m)$ (so $v_m - v_{m+1} = u_m$)

$= (\#\text{ of sol}^n\text{s} \bmod \pi^m \text{ of } f(x) \equiv 0 \bmod \pi^m)/q^{mn}$

($n = \dim X$).

then:

Thm: Hypersurface $f = 0$, $w_m = \#$pts of $(f=0) \bmod \pi^m$

$\Rightarrow \sum w_m T^m$ is a rational function of T

Remark: this was posed by Borevich/Shafarevich (but may have been raised earlier).

i.e. $w_m = \# |S(\mathcal{O}_K/\pi^m\mathcal{O}_K)|$ above

Remark: The Thm. above is true for any scheme (finite type) over $\mathcal{O}_K$ (reduces to Igusa) by Diane Meuser, M. Ann. 1981
Also J. Oesterlé reduces this to a 1 polynomial case (so Igusa's result gives this theorem directly).

$ch(K) = 0$ because resolution of singularities is needed.

exercise: X compact ($\neq \emptyset$), K-manifold of dimension n, ω a differential form of degree n on X, everywhere nonzero (nowhere zero).

$$\int_X \omega \in \mathbb{Z}[\tfrac{1}{q}] \longrightarrow \mathbb{Z}/(q-1)\mathbb{Z} \quad \text{(natural map)}$$

$$(\tfrac{1}{q} \mapsto 1)$$

Show: (1) this residue class depends only on X (not on ω)
(2) two X, X' are isomorphic $\Leftrightarrow$ invariants are the same.
In fact, taking coset representative $0 \lneq \alpha \leq q-1$,
X is isomorphic to the disjoint union of α "unit balls" $\mathcal{O}_K^n$.

Yoga: manifolds are very simple,

In terms of vector bundles:

X/K manifold, take $\Lambda^n T_X^* = \Omega_X^n$ T_X = tangent bundle
T_X^* = cotangent bundle

Ω_X^n = a line bundle, st. group K^* (sections are differential forms)

We have a map
$$K^* \to \mathbb{R}_+^*$$
$$x \mapsto \|x\|$$

so by change of group we get a line bundle over $\mathbb{R}$ ("density bundle") $\mathcal{D}_X$, sections are measures.

Fibers: $x \in X$, $\mathcal{D}_X(x)$ = the translation invariant measures on $T_X(x)$

So to define a regular measure is to give a collection of tr. inv. measures

Rmk: classically, need an orientation to get measures, so $\mathcal{D}_X \stackrel{\text{def}^n}{=} \Omega^n \otimes \mathcal{O}r(X)$
orientation bundle

Then $\mathbb{R}^* \to \mathbb{R}_+^*$ is used as above.
$x \mapsto |x| = x \cdot \operatorname{sgn}(x)$

In the complex case, take $\mathbb{C}^* \to \mathbb{R}_+^*$ (so take the
$x \mapsto |x|^2 = x\bar{x}$

measure $\omega \wedge \bar{\omega}$).

The Special Case of Manifolds arising geometrically:

$$\begin{array}{c} S \\ \downarrow \\ \mathrm{Spec}(\mathcal{O}_K) \end{array}$$

scheme (of finite type and separated (= Hausdorff)) smooth over $\mathcal{O}_K$, everywhere of dimension n.

Then in this case, have not only a K-manifold, but even a canonical measure:

X = "integral points" of $S = S(\mathcal{O}_K)$ has structure of K analytic manifold of dimension n.

(i.e. the set of sections P $\begin{array}{c} S \\ \downarrow \uparrow P \\ \mathrm{Spec}(\mathcal{O}_K) \end{array}$)

There is a canonical measure; in terms of sections on line bundles:

$P \in X$ integral point of S $T_P(X) \supset T_P(S) \simeq \mathcal{O}_K^n$. lattice

tangent space to S

Digression: "Riemann structure" on a K-manifold
= choice of an $\mathcal{O}_K$-lattice Λ_P in $T_P(X)$ for each $P \in X$ with $P \to \Lambda_P$ being locally constant [$\Lambda_P \otimes_{\mathcal{O}_P} K = T_P(X)$, Λ_P an $\mathcal{O}_K$-mod. free of rank n]

Associated to this is a canonical measure: gives measure 1 to Λ_P.

in $\mathbb{R}^n$, give ds^2
Know volume of cube.

So above, we have a canonical measure on X. More concretely;

$$X = \mathcal{S}(\mathcal{O}_K) \quad \left(\overset{\text{"i.e." solutions}}{f_\alpha(x) = 0}, x \in \hat{\mathcal{O}}_K = \varprojlim \mathcal{O}_K/\pi^n \mathcal{O}_K \right)$$

$$= \varprojlim \mathcal{S}(\mathcal{O}_K/\pi^m \mathcal{O}_K) = X_m$$

$X_1 = \mathcal{S}(k) =$ pts of the "reduction mod π" of $\mathcal{S}'$ ["pts of the "closed" fibre"]
$X_2 = \mathcal{S}(\mathcal{O}_K/\pi^2\mathcal{O}_K)$
$\vdots$

Then the canonical measure is characterized by;

"the pts of X whose reduction mod π^m is a given point of X_m ($m \geq 1$) form a compact open set of volume $\frac{1}{q^{mn}}$, $n = \dim \mathcal{S}$".

From differential forms point of view, μ is obtained from a differential form which is "integral" whose "reduction mod π is nowhere 0".
[$\mathcal{S}/\mathcal{O}_K \Rightarrow \omega$ has integral life, $\omega \mapsto \tilde{\omega}$ diff. form on $\tilde{\mathcal{S}} = \mathcal{S} \otimes_{\mathcal{O}_K} k$
ω may not exist on all of $\mathcal{S}$, but locally exists]

What is $\mu(X)$?

$$\mu(X) = \frac{\#\text{ pts of } \mathcal{S}' \text{ mod } \pi^m}{q^{mn}} \quad \text{for any } m \geq 1$$

in particular ($m=1$): $$= \frac{|\mathcal{S}(k)|}{q^n} \quad n = \dim X$$

[the indepence of $\mu(X)$ on m can be seen directly: $X_{m+1} \to X_m$ fibres all have q^n elements]

Proofs of all these statements : take morphism $S \to$ Affine which is étale at a given point of interest. Have local isomorphisms of all items of interest, so can compute.

Remark: Lang-Weil $\Rightarrow$ $\tilde{S}$ abs. irreducible of dimension n affine or projective in $\mathbb{P}_N$ of degree d.

$$|\tilde{S}(k)| = q^n\left(1+\frac{\varepsilon}{q^{1/2}}\right) \quad \text{where } |\varepsilon| \leq C(N,d)$$
$$k = \mathbb{F}_q$$
$$\Rightarrow \mu(X) - 1 + \frac{\varepsilon}{q^{1/2}}$$

so $\mu(X) \sim 1$ for large q (d fixed).

examples of canonical measures (on group schemes):

Lie Groups	GL_n	$\mu = \left(1-\frac{1}{q}\right)\left(1-\frac{1}{q^2}\right)\ldots\left(1-\frac{1}{q^r}\right)$
"A"	SL_r	$\mu = \left(1-\frac{1}{q^2}\right)\ldots\left(1-\frac{1}{q^r}\right)$
"C"	Sp_{2r}	$\mu = \left(1-\frac{1}{q^2}\right)\left(1-\frac{1}{q^4}\right)\ldots\left(1-\frac{1}{q^{2r}}\right)$
"B"	SO_{2r+1}	$\mu = \mu(Sp_{2r})$
"D"	SO_{2r}	$\mu = \left(1-\frac{1}{q^2}\right)\left(1-\frac{1}{q^4}\right)\ldots\left(1-\frac{1}{q^{2r-2}}\right)\left(1-\frac{\varepsilon}{q^r}\right)$

where $\varepsilon = 1$ if discriminant $\Delta(-1)^r$ is a square ($ch \neq 2$)

$= -1$ not a square

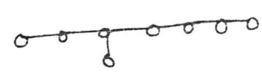
(in charact. 2, need to replace by "Arf invariant" (?))

$$E_8 \qquad \mu = \left(1-\frac{1}{q^2}\right)\left(1-\frac{1}{q^8}\right)\left(1-\frac{1}{q^{12}}\right)\left(1-\frac{1}{q^{14}}\right)\left(1-\frac{1}{q^{18}}\right)\left(1-\frac{1}{q^{20}}\right)\times$$
$$\times\left(1-\frac{1}{q^{24}}\right)\left(1-\frac{1}{q^{30}}\right).$$

The numbers, e.g. for E_8 2, 8, 12, 14, 18, 20, 24, 30 [usually "m_i"] are the "exponents". Rule: $m_i - 1$ the numbers less than 30 prime to 30.

Procedure: semi-simple groups for $\mathbb{F}_q = k$

Assume absolutely simple. $\leftrightarrow$ Dynkin diagram with an action of Frobenius

A_4 ($\leftrightarrow SL_5$)  E_8 

(generally, few automorphisms)

(a) Automorphism trivial $\leftrightarrow$ so-called "split form". Then the Dynkin diagram corresponds to a root system (not precisely 1-1) $\rightarrow$ Weyl group W
l=rank

W is group of aut. of an l-lattice
polynomials invariant by W are generated by l independent ones
$m_1, \ldots, m_l$ = degree of these polynomials

e.g. GL_n ; $W = S_n$, acting on polynomials in n variables, invariants are symmetric poly's., $m_i = 1, 2, \ldots, n$

SL_n rank $= n-1$, $W = S_n$, $m_i = 2, 3, \ldots, n$

Then # pts $/k$ is $q^{\dim G} \prod_{i=1}^{l}\left(1-\frac{1}{q^{m_i}}\right)$ (for the "split case").

(b) In the non-split case, take instead the space of invariant polynomials of degree n / decomposable ones $= V_m$

Frobenius acts on V_m
$\underset{F_m}{\wedge}$

Then

$$\# \text{ points} = q^{\dim G} \prod_m \det\left(1 - \frac{1}{q^m} F_m\right)$$

—

example: non-split form of A; SU_n (unitary w.r.t. $\begin{matrix} k_2 & \mathbb{F}_{q^2} \\ | & \\ k & \mathbb{F}_q \end{matrix}$)

Then

$$|SU_n| = q^{\dim SU_n} \prod_{i=2}^{n} \left(1 - \frac{(\pm 1)^i}{q^i}\right)$$

Rmk only time the terms aren't $1 \pm \frac{1}{q^i}$ ~~are~~ is for D_4  Frobenius acting ("triality"), then get 3rd rts. of 1 in formulas, get

$m_i = 2, 4, 6, 4$

$$\# |D_4^{\text{triality}}| = q^{\dim} \left(1 - \frac{1}{q^2}\right)\left(1 - \frac{1}{q^6}\right)\underbrace{\left(1 - \frac{\varepsilon}{q^4}\right)\left(1 - \frac{\bar{\varepsilon}}{q^4}\right)}_{\left(1 + \frac{1}{q^4} + \frac{1}{q^8}\right)}$$

$(\varepsilon^3 = 1, \varepsilon \neq 1)$

—

W is generated by "fundamental reflections" $s_1, \dots, s_\ell$

form $c = s_1 \dots s_\ell$ ("Coxeter element") h = order of c.

Then

$N = \dim$

$\ell = \text{rank}$ Then $h = \frac{2r}{\ell}$

$2r = \#$ of roots

$(N = \ell + 2r)$

e.g. $N = 248$, $\ell = 8$, $240 = 2r$
(E_8) $h = 30$

Take the eigenvalues of c, write them as $e^{\frac{2\pi i}{h}(m_i - 1)}$ $0 < m_i - 1 < h$ (same m_i's!) Hence knowledge of Coxeter is enough.

Known: $m_i - 1 = 1$ is there

$\Rightarrow$ all numbers ν, $1 \leq \nu \leq h$ $(\nu, h) = 1$
c preserves lattice
are $m_i - 1$

(conjugate by Galois group: roots of unity).

This gives all the values for E_8.

Also know $\prod m_i = |W|$ (so need only all but one of the m_i to get them all).

Remark: connections with topology: each G has a "compact form" G_C (e.g. $SL_n \to$ compact form $SU_n(\mathbb{C})$)

Then compute cohomology and

Poincaré polynomial of $G_C = \prod_{i=1}^{l} (1 + t^{2m_i - 1})$

Also, using classifying series

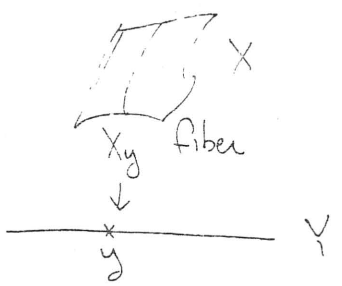
$$B_{G_c} \text{ P. series } = \prod \frac{1}{1 - t^{2m_i}}$$

exercise (in étale cohomology): compute # of pts in k using Lefschetz trace on cohom. with compact support, eigenvalues of Frobenius etc. in topological data.

10-1 cf. Notes on "Number of Points of reductive (connected) algebraic gps / $\mathbb{F}_q$".

Decomposition of a Measure

Manifolds:



Want to define measures so that $\int$ on X can be done on base and on fibers:

$$X, Y \qquad K\text{-manifolds}, \quad \dim X = N_X, \quad \dim Y = N_Y$$

<u>Def^n</u>: $f: X \to Y$ is a "submersion" if for all $x \in X$, $T_x(X) \to T_y(Y)$, ($y = f(x)$) is <u>surjective</u>.

<u>locally</u>: choose coordinates on X, Y $\quad f: \quad \begin{matrix} x_1, \dots, x_{N_X} \\ \downarrow \\ y_1, \dots, y_{N_Y} \end{matrix}$

Given such a situation, let ω_X = differential form of $d^\circ N_X$, nowhere 0
ω_Y = " " " $d^\circ N_Y$, "

For every $y \in Y$, define a differential form $\Theta_y = $ "$(\omega_X/\omega_Y)_y$" defined by:

At a point x, two differential forms ω_X, $f^*\omega_Y$ (pull back). Then $\exists$ on a neighborhood of x an $(N_X - N_Y)$-form α s.t.

$$\omega_X = \alpha \wedge f^* \omega_Y$$

and ~~such that~~ the restriction of α to X_y is unique.

Check via local coord's : eg. x_1, x_2, y coord at x

$$\begin{array}{c} x_1, x_2, y \\ \downarrow \\ y \end{array}$$

$$\omega_X = \varphi_X \, dx_1 \wedge dx_2 \wedge dy$$
$$\omega_Y = \varphi_Y \, dy$$

so take for α : $\frac{\varphi_X}{\varphi_Y} dx_1 \wedge dx_2$ (hence regularity of ω_Y is important). Then α is determined up to $\alpha + \psi\, dx_1 \wedge dy + \psi' dx_2 \wedge dy$ (so the restriction is well-defined, since the other two terms are 0 where y = constant, i.e. on the fiber).

---

equivalently: ("topologist's pt. of view")

exact sequence $0 \to T_x(X_y) \to T_x(X) \to T_y(Y) \to 0$
by taking exterior powers (V dim n, denote $\Lambda^n V = \det V$), taking duals, get a canonical isomorphism :

$$\underset{\omega_X}{\det T_x^*(X)} = \underset{\substack{\omega_Y \\ \neq \\ 0}}{\det T_x^*(Y)} \otimes \det T_x^*(X_y)$$

so can "divide" to get θ_y

In terms of bundles : $\Omega^{N_X} X | X_y \simeq \Omega^{N_X - N_Y} X_y \otimes f^* Y$.

Explicitly in terms of coordinates :

X open in K^n, $Y = K$ $\quad X \xrightarrow{f} K = Y$

$$\omega_X = dx_1 \wedge \ldots \wedge dx_n$$
$$\omega_Y = dy$$

Then f = submersion means $\frac{\partial f}{\partial x_i}$ are not simultaneously 0 at any point of X so given $x \in X$, $\exists\, i$ with $\frac{\partial f}{\partial x_i} \neq 0$, so on $X_y = f^{-1}(y)$, [which is a reasonable manifold by the submersion hypothesis], supposing $\frac{\partial f}{\partial x_n} \neq 0$, find

$$\theta_y = \frac{dx_1 \wedge \ldots \wedge dx_{n-1}}{(\partial f / \partial x_n)} \quad \text{on } X_y .$$

$\vec{\text{Check}}$: different coord's: e.g. $X = K^2$, $f(x_1, x_2) = y$ level set

then

$$\theta_y = \frac{dx_1}{\partial f / \partial x_2} = -\frac{dx_2}{\partial f / \partial x_1}$$

since $\frac{\partial f}{\partial x_1} dx_1 + \frac{\partial f}{\partial x_2} dx_2 = 0$ on $\underline{X_y}$.

=

Another way of writing this is $\theta_y = \operatorname{Res}_{X_y} \frac{dx_1 \wedge \ldots \wedge dx_n}{f(x) - y}$

(Serre: not "enthusiastic" about this point of view).

=

<u>Measures</u> in this context:

$X \xrightarrow{f} Y$ $\quad$ μ_X <u>regular</u> on X, μ_Y <u>regular</u> on Y $\Big\} \Rightarrow$ by essentially the same process get $\theta_y = $ "$(\mu_X / \mu_Y)_y$"

(terminology θ_y à la Weil).

<u>locally</u>: $\begin{aligned} \mu_X &= \|\omega_X\| \\ \mu_Y &= \|\omega_Y\| \end{aligned}$ then take $(\omega_X/\omega_Y)_y$ and take the associated measure.

Then

$$\theta_y \text{ is a } \underline{\text{regular}} \text{ measure on } X_y.$$

In terms of the local coordinates:

$$\theta_y = \frac{dx_1 \ldots dx_{n-1}}{\| \partial f / \partial x_n \|} \qquad \text{as a measure on } X_y.$$

<u>Remark</u>: This was done locally for only $K^n \to K$, but of course $f: K^n \to K^p$ can be done entirely similarly using the suitable Jacobian matrices.

(*) Suppose now we have $\begin{array}{c} X \\ \downarrow f \\ Y \end{array}$ $\begin{array}{c} \mu_X \\ \\ \mu_Y \end{array}$ $\theta_y \ (y \in Y)$ and $\Phi(x)$ is a continuous function on X with compact support. Then

$$\underset{(y \in Y)}{F(y)} = \int_{X_y} \Phi(x)\, \theta_y \qquad \text{is continuous with compact support}$$

and

$$\int_Y F(y)\, \mu_Y = \int_X \Phi(x)\, \mu_X .$$

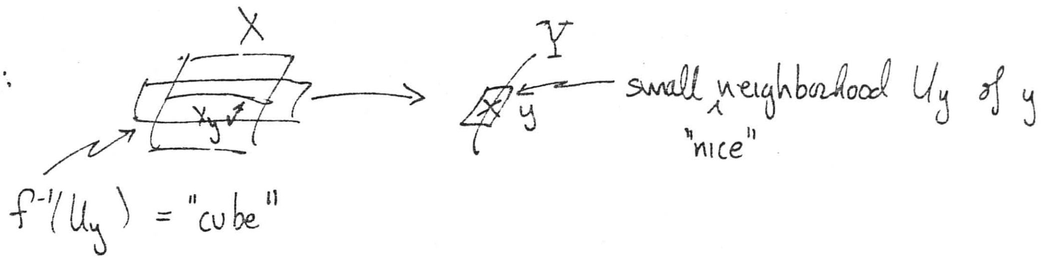
Pf: by partition of unity ("cheap" in p-adic case), may assume support on fibres, then the statement is just a simple version of Fubini's theorem. //

Remark: If Φ is locally constant (and compactly supported), then F is also locally constant and compactly supported.

Assume now that X is compact (no real loss as Φ has compact support), and that $\Phi = 1$. Then

$$\int_{X_y} \Theta_y = F(y).$$

Intuitively:



in the p-adic case, we have the

Fact: If U_y is small enough, then

$$\frac{\text{measure of the cube } f^{-1}(U_y)}{\text{measure of } U_y} = F(y) = \int_{X_y} \Theta_y .$$

Proof: Point: F is locally constant, so we take U_y to be a neighborhood on which F is constant. Define then Φ on X by (assume U_y = open, compact)

$$\Phi(x) = \begin{cases} 1 & \text{on } f^{-1}(U_y) \\ 0 & \text{elsewhere.} \end{cases}$$

Then the "double integration" formula gives

$$z \in Y: \quad \int_X \Phi(x)\,\mu_X(x) = \int_Y \left(\int_{X_z} \Phi(x)\,\theta_z(x) \right) \mu_Y(z)$$

$$\underset{\substack{\text{by definition}\\ \text{of } \Phi\,!}}{=} \int_{U_y} F(z)\,\mu_Y(z)$$

$$\underset{\substack{\text{since } F \text{ is}\\ \text{constant on } U_y\\ \text{by assumption}}}{=} F(y)\cdot \text{measure of } U_y.$$

Remark: this is the "density" that Siegel uses – we explain this a little more:

Let f = polynomials in $X_1, \dots, X_n$, coefficients in $\mathcal{O}_K$

$$f: X = \mathcal{O}_K^n \to \mathcal{O}_K^r = Y$$

and assume F is a submersion (i.e. F has no "critical values" in Igusa's terminology)

for $y \in \mathcal{O}_K = Y$, choose $U_y = \{z \mid z \equiv y \mod \pi^m\}$. The measure of U_y is then $\frac{1}{q^{rm}}$ and

$$f^{-1}(U_y) = \text{the set of points } x \in \mathcal{O}_K^n \text{ with } f(x) \equiv y \mod (\pi^m)$$

so $\quad \text{measure } f^{-1}(U_y) = \frac{1}{q^{nm}} \times \#\text{ of solutions mod } \pi^m \text{ of } f(x) \equiv y$

Then:

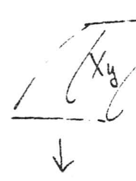
(a) $\dfrac{\#\text{ solutions mod } \pi^m \text{ of } f(x) \equiv y}{q^{(n-r)m}}$ is independent of m for m large;

dimension of the fibre!

(b) the value of the quotient in (a) for large m is

$$F(y) = \int_{X_y} \theta_y$$

Siegel: $A_{m \times n} \xmapsto{f} {}^tASA$ (one removes the critical pts of this map)
That this density (Siegel) can be defined as the integral of a measure (and the existence of a canonical measure in the adele situation may have been the starting point for Tamagawa.

As before:  If φ = a function on Y, then

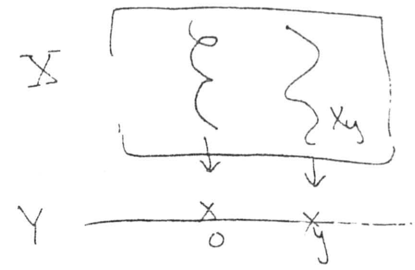
$$\int_Y \varphi(y) F(y)\, \mu_Y(y) = \int_X \varphi(f(x))\, \mu_X(x)$$

(Pf: use the "double integration formula (p. 27, $*$) to $\varphi(f(x))$ ✓).

Igusa: Back to $X = \mathbb{Q}_K^n \xrightarrow[\text{analytic}]{f} \mathbb{Q}_K = Y$ where 0 is (at most) the only critical value of f, i.e.
$f \mid f^{-1}(Y - \{0\}) \to Y - \{0\}$ is a submersion.

Then on $Y - \{0\}$, X_y, Θ_y $(y \in Y - \{0\})$ are well-defined and

$$F(y) = \int_{X_y} \Theta_y$$



satisfies:

(a) $\qquad F \in L^1$, $\displaystyle\int_Y F(y)\,\mu_Y(y) < +\infty$

$$\overset{\shortparallel}{\int_X \omega_X(x)} \quad \text{(by taking limits of } X - (\text{neighborhoods of } f^{-1}(0)))$$

(assumption: f is nowhere locally 0)
$\Uparrow$
needed to insure measure on neighborhoods of 0 go to 0. /

If ψ is an additive character ; $\psi : \mathcal{O}_K \to \mathbb{C}^*$, define

$$F^*(\psi) = \int_Y F(y)\psi(y) \quad \mu_Y(y)$$

$$= \int_X \psi(F(x))\mu_X(x) = g(\psi)$$

(a "Gauss sum" !)

Analyze $g(\psi)$ by resolving the singularities ... //

Liftable Solutions

Consider the solutions to $f(x) \equiv 0 \mod \pi^m$, $[x = (x_1, \dots, x_n)$, $x_i \in \mathcal{O}_K/\pi^m\mathcal{O}_K]$

Call x "liftable" if x can be lifted to a solution to $f(x) = 0$, $x \in \mathcal{O}_K^n$

How can one count such liftable x ? :

$$X = \mathcal{O}_K^n, \quad Y \subset X \text{ a subset of } X.$$

Call $X_m = X/\pi^m X$ ("reduction")

Y_m = the image of Y in X_m.

Then $(\bar{x}_1, \dots, \bar{x}_n)$, $\bar{x}_i \in \mathcal{O}_K/\pi^m\mathcal{O}_K$ is in $Y_m \Leftrightarrow$ there are points $(x_1, \dots, x_n) \in \mathcal{O}_K$ s.t. $\underset{\in Y}{(x_1, \dots, x_n)} \mapsto (\bar{x}_1, \dots, \bar{x}_n)$.

Let $|Y_m|$ = # of elements of Y_m $(\le |X_m| = q^{nm})$

<u>Theorem</u> Assume Y is a (smooth) closed submanifold of X, everywhere of dim d (i.e. not the union of "pieces" , , etc). Then

$$|Y_m| = \lambda \cdot q^{dm} \quad \text{for all } m \text{ sufficiently large,}$$

where $\lambda \geq 0$, which can be given as an integral over Y:

$$\lambda = \int_Y \mu_Y$$

for a canonical measure μ_Y on Y, (defined below).

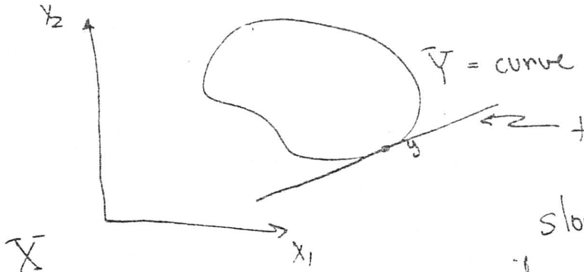
X has a natural Riem metric, so $Y \subset X$ has an induced metric, and such a metric gives a canonical measure μ_Y. ✓

Concretely;

$$y \in Y, \text{ consider tangent space } T_y(Y) \subset T_y(X) \underset{\text{canonically}}{=} K^n$$

Since $\mathcal{O}_K^n \subset K^n$, can induce a lattice $\Lambda_y = \mathcal{O}_K^n \cap T_y(Y)$ in $T_y(Y)$, and μ_Y is the measure giving this lattice the volume 1, $\mu_Y(\Lambda_y) = 1$.

For $n=2, (r=1)$, make this more explicit



slope of tangent $= \frac{dx_2}{dx_1} \in K$
consider $\| \frac{dx_2}{dx_1} \|$.

Two cases: I. $\| \frac{dx_2}{dx_1} \| \leq 1$, then μ_Y at this point is dx_1
(Yoga: " x_1 is a decent coordinate for Y at this point ")

II: $\| \frac{dx_1}{dx_2} \| \leq 1$, then μ_Y is dx_2

(overlap: OK!; defined everywhere by smoothness, so measure defined everywhere!)

equivalently: $\mu_Y = \operatorname{Sup}(\|dx_1\|, \|dx_2\|)$!!

In the general case, $\mu_Y = \operatorname{Sup}(\mu_I)$ for all $I = i_1 < \dots < i_r$
where $\mu_I = \| dx_{i_1} \wedge \dots \wedge dx_{i_r} \|$.

10-6 Proof: First show the formula is true in special cases, then reduce the general case to these.

Case I: 

Y is given by equations

$$x_{r+1} = f_{r+1}(x_1, \dots, x_r)$$
$$\vdots$$
$$x_n = f_n(x_1, \dots, x_r)$$

where each f_i is a power series in $x_1, \dots, x_r$ with coefficients

[Then $f_i(\vec{x})$ converges for any $(x_1,\dots,x_r) \in \mathcal{O}_k^r$].

Then compute:

$$\mu_Y = dx_1 \dots dx_r$$

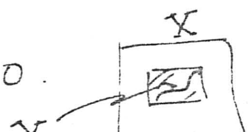
(this is the sup, since if some dx_{r+1}, say, occurs, then using the coefficients $\in \mathcal{O}_k$ in (*) shows one has an integral (hence smaller) μ)

$$\int_Y \mu_Y = 1 = \lambda .$$

$$|Y_m| = q^{rm} \quad (m \geq 0) \qquad \checkmark \text{ formula o.k.}$$

<u>Case II</u>: Deduced from Case I by permutation of $\{1,\dots,n\}$. ✓

<u>Case III</u>$_\nu$, $\nu \geq 0$.



Deduced from case II by $x \mapsto \pi^\nu x + x_0$, $x_0 \in X$

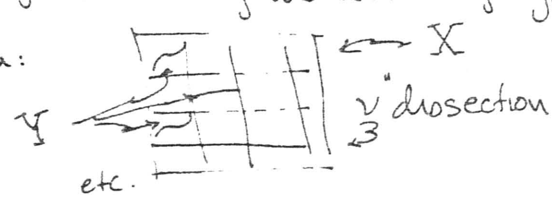
Then the homothety has the effect:

$$\lambda = q^{-\nu r} \qquad |Y_m| = \begin{cases} 1 & \text{if } m \leq \nu \\ q^{r(m-\nu)} & \text{if } m \geq \nu \end{cases}$$

Again the formula is o.k.

<u>Reduction of the general case</u>

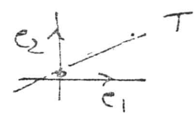
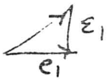
<u>Lemma</u> Any Y of the Theorem is the disjoint union of manifolds of type III$_\nu$ above for ν large enough. Diagram:



We need the additional

Sub Lemma: Let $T \subset K^n$ (basis $e_1, \dots, e_n$: canonical basis of K^n) be a K-vector subspace of dimension r. Then there exists a subset I of $\{1, \dots, n\}$ consisting of r elements and a basis ε_i $(i \in I)$ of T such that

$$\varepsilon_i = e_i + \sum_{j \notin I} \alpha_{ij} e_j \quad \text{with } \alpha_{ij} \in \mathcal{O}_K.$$

(e.g., $n = 2$, $r = 1$: $T \subset K^2$ line in the plane K^2  ; if slope of T is ≤ 1, take $I = \{1\}$  , then by slope, have the formula $\varepsilon_1 = e_1 + (\text{integer})\, e_2$. If slope of T is ≥ 1, take $\varepsilon_1 = e_2 + -$ $(I = \{2\})$.)

Proof: Take the Plücker coordinates of T.
Alternatively, the Sub-Lemma is OK. for a field (with no condition on the α_{ij}), e.g. by $\bigwedge^n T \to \bigwedge^n K^n$. Reduce to this case;
$\Lambda = \mathcal{O}_K^n$, $\Lambda_T = \Lambda \cap T$, an $\mathcal{O}_K$-module free of rank r.
Then

$$\Lambda_T / \pi \Lambda_T \hookrightarrow \Lambda / \pi \Lambda = k^r$$

gives a set I s.t. there is a basis $\{\tilde{\varepsilon}_i\}$ of $\Lambda_T / \pi \Lambda_T$ s.t.
$\tilde{\varepsilon}_i = \tilde{e}_i + \sum \tilde{\alpha}_{ij} \tilde{e}_j$. Now $\Lambda_T \to \prod_{i \in I} \mathcal{O}_K$, $(x_i)_{i \in I}$. This projection is an isomorphism (by Sub Lemma for the field) + Nakayama

Then have the basis e_i on the right, this gives the ε_i's.

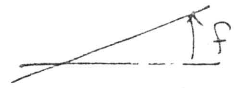
Proof of Lemma: Take tangent space [want: in a neighborhood of $O \in Y$, of type III,]

$T_0(Y) \subset K^n$

get I as in the Sub-Lemma and assume by permutation of coordinates that $I = [1,\dots,r]$.

Then Y in a neighborhood of 0 is given by analytic equations

$$x_{r+1} = f_{r+1}(x_1,\dots,x_r)$$
$$\vdots$$
$$x_n = f_n(x_1,\dots,x_r)$$



f_i analytic in a neighborhood of 0.

But expanding;

$$x_{r+1} = f_{r+1}^{(1)}(x) + f_{r+1}^{(2)}(x) + \dots$$
$$\vdots$$
$$x_n = \dots$$

$f_i^{(j)}$ homog. poly. of degree j.

where the linear parts $f_i^{(1)}$ have coefficients in $\mathcal{O}_K$.

Then change coordinates $x_i = \pi^m X_i$;

$i \geq r$; $\quad \pi^m X_i = \pi^m f_i^{(1)}(X) + \pi^{2m} f_i^{(2)}(X) + \dots$

i.e.

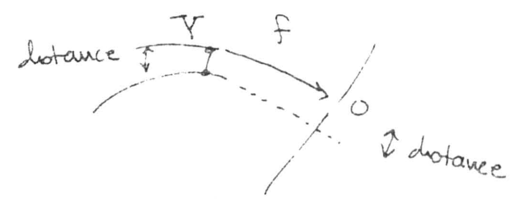
$$X_i = f_i^{(1)}(X) + \pi^m f_i^{(2)}(X) + \dots + \pi^{(j-1)m} f_i^{(j)}(X) + \dots$$

Choosing m sufficiently large, make the RHS. a restricted power series with coefficients in $\mathcal{O}_K$, so of type III_m. ✓

<u>exercise</u> (alternate method of proof): Prove there exists an analytic map

$$f: U \to K^{n-r}$$

U = a neighborhood of $\tilde{Y}$ s.t.



(a) $f^{-1}(0) = Y$

(b) f is a submersion

(c) $x \in \mathcal{U}$, $\|f(x)\| = \text{distance}(x, Y)$

then use the "double integral formula" of p. 27 to give the Theorem.

(Here

$$d(x_1, x_2) = \|x_1 - x_2\| = q^{-m} \quad \text{if } m \text{ is the largest integer s.t. } x_1 \equiv x_2 \bmod \pi$$

(Sup norm).)

Letting

$$Y(m) = \{x \in X \mid d(x, Y) \leq q^{-m}\} = \text{union of the mod } \pi^m \text{ congruence classes of } Y_m$$

then

$$\text{measure } Y(m) = |Y_m| \, q^{-nm}$$

If Y is smooth, $= \lambda q^{-(n-r)m}$ for m large.

<u>Remark</u>: analogous to real ($\mathbb{R}$) situation: $\underset{\text{compact}}{Y \subset \mathbb{R}^n}$, $\varepsilon > 0$

can define $Y_\varepsilon = \{x \in \mathbb{R}^n \mid d(x, Y) \leq \varepsilon\}$ ("ε-neighborhood")

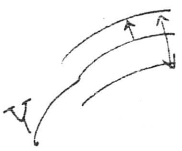
can ask how meas (Y_ε) varies as a function of ε.

<u>Theorem</u> (H. Weyl); $Y \subset \mathbb{R}^n$ smooth, compact, (everywhere of dim. r)

Then meas (Y_ε) is a polynomial in ε for ε sufficiently small. [coeff's are expressend in terms of the curvature of the manifold].

In our case, have only a monomial, so terms corresponding to "curvature" are missing. Yoga: "padic manifolds are flat".

example of Weyl's Thm : $n=3, r=2$; surface in $\mathbb{R}^3$
then meas $(Y_\varepsilon) = 2A_1\varepsilon + \frac{2}{3}A_3\varepsilon^3$ where



A_1 = "area" of surface = $\int_Y d\sigma$

principal curvatures

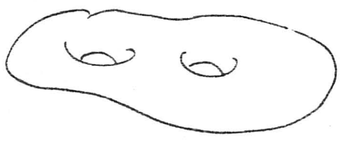
Euler-Poincaré characteristic

A_2 = total curvature = $\int_Y \frac{d\sigma}{R_1 R_2} \underset{\text{Gauss-Bonnet}}{=} 2\pi\, EP(Y)$

Also, meas$(Y_\varepsilon^+) = A_1\varepsilon + \frac{1}{2}A_2\varepsilon^2 + \frac{1}{3}A_3\varepsilon^3$ where A_2 = "mean curvature" $= \int_Y d\sigma\left(\frac{1}{R_1}+\frac{1}{R_2}\right)$

part "outside" Y at distance $\le \varepsilon$.

Application to finding* holes on a connected surface by painting three times :



Assume now that char $K = 0$, $X = \mathcal{O}_K^n$, Y a compact analytic of dimension $\le r$, [(i.e. Y is locally given by analytic equations $f_\alpha(x) = 0$)], where dimension is computed as follows: take a point $O \in Y$, R_O = ring of germs of analytic functions on X near O. Let $I_{Y,O}$ = the ideal of R_O consisting of those $f \in R_O$ vanishing in a neighborhood of O on Y. Then $R_O / I_{Y,O} = R_{Y,O}$ = ring of germs of analytic functions on Y (restrictions of analytic functions on X). Then define $\dim R_{Y,O} = \dim_O Y$.

Fact: $r = \dim_O Y \Rightarrow \dim_P Y \le r$ for every P in a neighborhood of O
(note $R_{Y,O}$ is reduced, having no nilpotent elements since it's a ring of functions)

Hence, Y has no smooth points of dimension $> r$ (in a neighborhood of 0), but Y does in fact have smooth points of dimension r (in any neighborhood of 0).

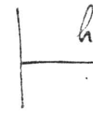
Define

$$Y^{reg} = Y^{\text{"regular"}} = \text{the subset of smooth points of dimension } r$$

Y^{reg} is clearly open.

<u>Fact</u>: if $Y^{sing} = Y - Y^{reg}$, then $Y^{sing} \subset$ an analytic subset (closed) of dimension at most $r-1$.

2 Over $\mathbb{C}$, Y^{sing} is itself analytic. Not true over $\mathbb{R}$, say


half-line

e.g. $\mathbb{R}^3$, $x(x^2 + zy^2) = 0$

singular locus: line $\begin{cases} x = 0 \\ y = 0 \end{cases}$

Same equation works p-adically (when z is a square "cuts an angle" at the origin).

Can prove the fact above by taking locally $\varphi_1, \ldots, \varphi_m$ generators of $I_{Y,0}$ and $J^A_B = \det_{\substack{a \in A \\ b \in B}} \left(\frac{\partial \varphi_a}{\partial x_b}\right)$.

A, B subsets of $[1,m]$, $[1,n]$ respectively, of orders $n-r$

Take now $I'_{Y,0}$ = the ideal generated by $\varphi_1, \ldots, \varphi_m$, J^A_B for all A, B.

Y' the corresponding germ, $Y \supset Y'$, $\dim Y' \leq r-1$ at 0, Y is smooth outside Y', so Y' contains Y^{sing} [Y' = the singular locus of the algebraic closure $\cap Y$]. If $\mathrm{ch}(K) \neq 0$, may not be true that

Theorem (depends on resolution of singularities): Y analytic, $\dim \leq r$, then

$$|Y_m| = O(q^{mr}) \qquad \text{for } m \to \infty$$

(i.e. $\leq C q^{mr}$)

Remark J. Oesterlé may be able to do this without resolution of singularities (maybe even with some idea on C - elementary)

Def^n: Y has an "r-parametrization" if Y can be covered by a finite number of r-dimensional balls ($\mathcal{O}_K^n$) by analytic maps

(i.e. $\varphi_i : \mathcal{O}_K^r \to X$, $Y = \bigcup_i \mathrm{Image}(\varphi_i)$).

By resolution of singularities,

$\Rightarrow$ any compact analytic Y of $\dim \leq r$ is r-parametrizable.

(resolution gives a space $\tilde{Y}$, non-singular, compact, dim r

$$\tilde{Y} \downarrow Y$$

covers the regular points (image contains $Y - Y'$)

Now Y' is $\subseteq$ analytic of $\dim \leq r-1$.
Then Y' can be covered by balls ✓

Now, Y r-parametrized $\Rightarrow$ $|Y_m| = O(q^{rm})$. Pf: suffice to take one φ:

Since Analytic $\Rightarrow$ Lipschitz, i.e. $\exists$ a constant $m_0 \geq 0$ s.t. $\phi : \mathcal{O}_K^r \to X$
$\| \phi(x) - \phi(y) \| \leq q^{m_0} \| x-y \|$, $x, y \in \mathcal{O}_K^r$.

Then

$$x \equiv y \bmod (\pi^{m+m_0}) \Rightarrow \phi(x) \equiv \phi(y) \bmod \pi^m .$$

Hence there is a diagram

$$\begin{tikzcd}
\mathcal{O}_K^n \arrow[rr, dashed, "\phi"] \arrow[d] & & X \arrow[d] \\
\left(\mathcal{O}_K / \pi^{m+m_0} \mathcal{O}_K \right)^r \arrow[rr, dashed, "\phi_m"] & & X_m = X / \pi^m X
\end{tikzcd}$$

and Y_m = image of ϕ_m. Then $|Y_m| \leq q^{(m+m_0)r} \leq C q^{mr}$
by: # pts in image $\leq$ # pts in domain !!

10-8 For a hypersurface, one can use an alternate approach, due to J. Oesterlé, cf. Ph. Robba, "Lemmas de Schwarz et lemmes d'appr. p-adiques en plusient variables", Inv. Math. 48 (1978), 245-277.

$$f \in \mathcal{O}_K[x_1, \ldots, x_N], \quad f \neq 0, \quad \deg f = d, \quad Y = Y_f = \{\text{zeros of } f\}$$

Y_m = set of zeros of $f \bmod \pi^n$ which are liftable to $\mathcal{O}_K$-zeroes.

Theorem: $|Y_n| \leq d q^{(N-1)n}$ for all $n \geq 0$ (does not depend on resolution of singularities)

(e.g. $N = 1$, $|Y| \leq d \Rightarrow |Y_n| \leq d$ ✓)

Suppose now that $f = \sum a_\alpha X^\alpha \neq 0$ (where $\alpha = (\alpha_1, \ldots, \alpha_N)$, $\alpha_i \geq 0$) with $a_\alpha \in K$ which is a restricted power series: $a_\alpha \to 0$ when $|\alpha| = \sum \alpha_i \to \infty$.

Define a "degree" for f as follows;

$$\|f\| = \sup_{\alpha} \|a_\alpha\| = q^{\nu} \quad \text{(since } f \text{ restricted)}$$

so letting

$$f_0 = \pi^{\nu} f \;, \quad \|f_0\| = 1, \text{ and the "new" } a_\alpha^{\circ} = \pi^{\nu} a_\alpha \text{ are}$$

all integers, with one of them (at least) a unit.

Hence f_0 can be reduced mod π, giving

$$\tilde{f_0} = \sum_{\alpha} \tilde{a}_\alpha X^\alpha \in k[X]$$

, a non-zero polynomial (f_0 restricted $\Rightarrow$ almost all coefficients divisible by π). Then define

$$D(f) = \deg \tilde{f_0}$$

(Alternatively, $D(f) = \sup_m \{ \text{there exists an } \alpha, |\alpha| = m \text{ with } \|a_\alpha\| = \|f\| \}$)

Theorem same theorem as above with d replaced by $D(f)$.

Proof: Note first that $D(f)$ is invariant under change of origin in $(\mathcal{O}_K)^n = X$, since

$$f_c(X) = f(X+c) \Rightarrow \|f_c\| = \|f\| \,, \quad D(f_c) = D(f) \quad ✓$$

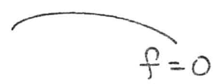
Let B be a ball of radius q^{-m} (i.e. a congruence class mod $\pi^m \mathcal{O}_K$). - so there is 1 ball of radius 1 : X

q^N balls of radius $\frac{1}{q}$; etc.

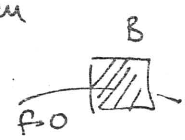
Then let (note that by the comment above, this def^{n} depends only on the ball B):

$$D_B(f) = D(f(\pi^m Y)) \qquad \begin{matrix} c \in B \\ c = 0 \end{matrix} \;\Big|\; \begin{matrix} X_i = \pi^m Y_i \\ Y_i \in \mathcal{O}_K. \end{matrix}$$

<u>Remark</u>: the $\mathbb{C}$ analog is :



define measure by $\log|f|$, view as distribution, take Laplacian $\Delta \log|f|$, now concentrated on variety $f=0$, is a measure $\Theta_f = \Delta \log|f|$ on $f=0$. Then



can take $\int_B \Theta_f = D_B(f)$.

<u>Properties of $D_B(f)$</u>:

(1) $B' \subset B \Rightarrow D_{B'}(f) \leq D_B(f)$.

(Suffices to check for $B = X$, $B' = \pi X$, $\|f\| = 1$ (by a homothety if necessary), so $f = \sum a_\alpha X^\alpha$, $a_\alpha \in \mathcal{O}_K$, one of them a unit, so $\exists \alpha$ s.t. $|\alpha| = D(f)$, a_α unit and $|\beta| > |\alpha| \Rightarrow a_\beta \in \pi\mathcal{O}_K$.
Then to compute $D_{B'}(f)$, consider $\sum a_\alpha \pi^{|\alpha|} X^\alpha = f_1$ (i.e. X replaced by πX) and we need D of this function. But
$$|\beta| > |\alpha| = D_B(f) \Rightarrow \|a_\beta \pi^{|\beta|}\| \lneq \|a_\alpha \pi^{|\alpha|}\|,$$ so the maximum of $\|a_\alpha \pi^{|\alpha|}\|$ cannot be attained by such a β ✓)

(2) If f has a zero in a ball B, then $D_B(f) \geq 1$

(take the zero as origin, then f has no constant term, so $\tilde{f}$ is non-zero with no zero constant term, so $\deg \tilde{f} \geq 1$ ✓)

Proposition: Let B be a ball of radius $\frac{1}{q^m}$; $B_1, \dots, B_h$ distinct balls of radius $\frac{1}{q^{m+1}}$ contained in B (i.e. cosets mod $\pi^{m+1}\mathcal{O}_K$). Then

$$\sum_i D_{B_i}(f) \leq q^{N-1} D_B(f)$$

Assuming this (proof momentarily), the Theorem follows; by induction, the Proposition $\Rightarrow$ the analogous fact for balls of radius $\frac{1}{q^{m+n}}$:

$$\sum_{\substack{B_i \text{ disjoint} \\ \text{balls of radius } \frac{1}{q^{m+n}}}} D_{B_i}(f) \leq q^{(N-1)n} D_B(f).$$

Apply this now for $B = X = \mathcal{O}_K^n$ and B_i = the different classes mod π^n:

$$\underset{\substack{\text{\rotatebox{90}{$\leq$}} \\ |Y_n|}}{\sum D_{B_i}(f)} \leq q^{(N-1)n} D_B(f)$$

$|Y_n|$ by Property 2. ✓

Hence it suffices to prove the Proposition above. We need a Lemma:

Ω = a field, $\phi \in \Omega[X_1, \dots, X_N]$, $\phi \neq 0$

$x = (x_1, \dots, x_N) \in \Omega^N$,

$O_x(\phi)$ = the order of ϕ at x

= lower bound of integers $m \geq 0$ s.t. $\phi \in (m_x)^m$

(i.e. expand ϕ: $\phi = \sum a_\alpha (X-x)^\alpha$, $O_x(\phi) = \operatorname*{Inf}_{a_\alpha \neq 0} |\alpha|$).

Let $\Omega_1, \dots, \Omega_N$ be subsets of Ω with the same cardinality, $|\Omega_i| = q$ (q an integer ≥ 1).

Lemma Notations as above, then

$$\sum_{x \in \Omega_1 \times \dots \times \Omega_N} o_x(\varphi) \leq q^{N-1} \deg(\varphi)$$

Proof: By induction on N. $N=1$, essentially obvious $- \sum_{x \in \Omega_1} o_x(\varphi) \leq \deg(\varphi)$

(i.e. a polynomial has at most $\deg \varphi$ zeroes, counted with multiplicities) ✓

For $N > 1$; $\varphi(x_1, \dots, x_N) = \prod_{\omega \in \Omega_N} (X_N - \omega)^{m_\omega} \cdot \psi(x_1, \dots, x_N)$

where ψ does not vanish identically on any hyperplane $X_N = \omega$, $(\omega \in \Omega_N)$

(want to use induction, counting zeroes of φ when $X_N =$ some fixed $\omega \in \Omega_N$ (of "type" $N-1$), then add; must worry about φ vanishing identically on $X_N = \omega$, since then the induction assumption doesn't apply - hence the reason for introducing ψ).

$$\psi_{\omega_N}(x_1, \dots, x_{N-1}) = \psi(x_1, \dots, x_{N-1}, \omega_N)$$
$$\omega = (\omega_1, \dots, \omega_N) \in \Omega = \prod \Omega_i$$
$$(\, o_x(\varphi) = m_{\omega_N} + o_\omega(\psi) \,)$$

so

$$o_\omega(\psi) \leq o_{\omega_1, \dots, \omega_{N-1}}(\psi_{\omega_N}) \quad \text{gives}$$

$$o_x(\varphi) \leq m_{\omega_N} + o_{\omega_1, \dots, \omega_{N-1}}(\psi_{\omega_N}) \quad \text{and therefore}$$

$$\Rightarrow \sum_{\omega_1,\dots,\omega_{N-1}} o_\omega(\psi_{\omega_N}) \underset{\text{by induction}}{\leq} q^{N-2} \deg \psi_{\omega_N} \leq q^{N-2} \deg \psi \qquad \left(\text{for a fixed } \omega_N\right)$$

Hence

$$\sum_{\substack{\omega \text{ with} \\ \text{fixed } \omega_N}} o_\omega(\varphi) \leq q^{N-1} m_{\omega_N} + q^{N-2} \deg \psi$$

$$\Rightarrow \sum_{\substack{\text{all} \\ \omega}} o_\omega(\varphi) \leq q^{N-1} \sum m_{\omega_N} + q^{N-1} \deg \psi = q^{N-1} (\deg \varphi) \quad ✓$$

<u>Proof of the Proposition</u>: Assume $B = O_K^n$, B_i the classes mod πB, and assume $\|f\| = 1$, so $\tilde{f} = \varphi \in k[X_1,\dots,X_N]$. The B_i correspond to points in k^N. For $x \in k^N$, let B_x be the corresponding ball (i.e. the points reducing to x mod π).

<u>Claim</u>: $D_{B_x}(f) \leq o_x(\varphi)$

(this will prove the Proposition by applying the Lemma above to $\Omega = \Omega_i = k$, $|k| = q$) ✓

<u>Proof of Claim</u>: by changing coordinates, may assume $x = 0$. Then $f = \sum a_\alpha X^\alpha$, $\varphi = \sum_\alpha \tilde{a}_\alpha X^\alpha$ $\tilde{a}_\alpha$ not all 0, $m = o_x(\varphi)$, so $\varphi = \sum_{|\alpha| \geq m} \tilde{a}_\alpha X^\alpha$ ($\tilde{a}_\alpha$ not all zero for $|\alpha| = m$). Consider

$$f_1 = \sum a_\alpha \pi^{|\alpha|} X^\alpha \quad \text{to compute } D_{B_x}(f).$$

(note $D_{B_x} = \pi B$ here as $x = 0$). Choose α with $|\alpha| = m$ so $\tilde{a}_\alpha \neq 0$, i.e. a_α is a unit. Then

$$\|a_\alpha \pi^{|\alpha|}\| = q^{-|\alpha|}.$$

If now $|\beta| > |\alpha|$, then $\quad \| a_\beta \pi^{|\beta|} \| \leq q^{-|\beta|} < \| a_\alpha \pi^{|\alpha|} \|$

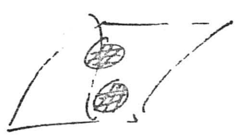
i.e.

$|\beta| > m \Rightarrow$ have strictly smaller absolute values of coefficients

$$\Rightarrow \quad D_{B_x}(f) \leq m = o_x(\mathcal{A}) \quad \checkmark \qquad //.$$

Remark: this result has a "uniformity" not given by the method of resolution of singularities; namely, if B is a ball of radius q^{-m} in X, $n \geq 0$ and we want to count the number of balls of radius q^{-m-n} contained in B intersecting Y (i.e. $|Y_{m+n} \cap B_{m+n}|$), then the result above gives

$$|Y_{m+n} \cap B_{m+n}| \leq D(f) q^{(N-1)n}$$

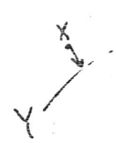
(even with $D(f)$ replaced by $D_B(f)$). So # pts in small balls  is bounded uniformly w.r.t. the balls.

Remark: the bound $|Y_n| \leq \deg(f) q^{(N-1)n}$ is best possible for all polynomials, but in "mean value" it is bad, for example:

<u>exercise</u>: consider the space of polynomials in $\mathcal{O}_K/\pi^m\mathcal{O}_K$ (in N variables) of degree $\leq d$. For each such polynomial, call C_f = # of solutions in $\mathcal{O}_K/\pi^m\mathcal{O}_K$. Show that the <u>mean value</u> of C_f is $q^{(N-1)m}$ (e.g. a "random" polynomial of degree d)

in one variable has roughly   solutions).

<u>Remark</u> (on the Łojasiewicz inequality): Hörmander (polynomial case), Ł... (general case) ~ 1958-60? proved Schwarz' problem on invertibility of distributions. Łojasiewicz used an inequality:



$f=0$ $\mathbb{R}^N$ $d(x,Y)$ $\overset{\shortparallel}{d_Y(x)}$ also $|f(x)|$ is a measure of distance from x to Y

f real analytic

Then $|f(x)| = O(d_Y(x))$ and

Łojasiewicz inequality: $|d_Y(x)| = O(|f(x)|^\alpha)$ for some α.

Can prove this by res. of sing's, so get an analogous result p-adically. Concretely:

inequality $\Leftrightarrow$ f coeff's $\in \mathcal{O}_K$, $\tilde{Y}_n$ = solutions mod π^n of $f \equiv 0 \pmod{\pi^n}$

Y_n = the "liftable part" of $\tilde{Y}_n$.

then

$$\begin{array}{lll} \vdots & & \\ \downarrow & & \\ \tilde{Y}_3 & \text{projective system} & \downarrow \text{etc} \\ \downarrow & & \supset Y_2 \text{ onto} \\ \tilde{Y}_2 & & \downarrow \\ \downarrow & & \supset Y_1 = \bigcap_{n\geq 1} \text{Image of } \tilde{Y}_n \\ \tilde{Y}_1 & & \end{array}$$

liftable part $\parallel$

How high must one go to provide "liftability"?

Łojasiewicz: there is a <u>linear</u> function $n \mapsto an+b$ $a,b>0$, s.t.

$$Y_n = \text{image of } \tilde{Y}_{an+b} \text{ in } \tilde{Y}_n$$

(i.e. a solution given by one in π^{an+b} is a <u>liftable</u> solution).

2-20 Complements:

$Y \subset \mathcal{O}_K^n = X$ dimension $\leq d$, interested in Y_m = the image of Y in $X/\pi^m X$.
analytic

By resolution of singularities (ch $K=0$), $|Y_m| \leq$ constant $\cdot\, q^{dm}$.

Oesterlé: some information on the constants (a generalization of the "degree" as in the case of a hypersurface).

Assume Y is given by $\phi_\alpha = 0$, ϕ_α a restricted power series (coeff $\to 0$) (w.l.o.g. since this is true locally).

Let

$$R = K\{X_1, \ldots, X_n\} \quad ; \quad f = \sum a_\alpha X^\alpha, \quad a_\alpha \to 0.$$

Then the ϕ_α generate an ideal $\mathfrak{a}$ of R.
Assume $R/\mathfrak{a}$ is "equidimensional" of dim. d [Spec $R/\mathfrak{a}$ has components of dim d]. Then say Y is "equidimensional" of dimension d.

Let

$$R_0 = \mathcal{O}_K\{X_1, \ldots, X_n\} \quad ; \quad f = \sum a_\alpha X^\alpha, \quad \begin{matrix} a_\alpha \in \mathcal{O}_K \\ a_\alpha \to 0 \end{matrix}$$

and set

$$\mathfrak{a}_0 = \mathfrak{a} \cap R_0.$$

Reduce R_0 mod π: $\tilde{R} = R_0/\pi R_0 \simeq k[X_1, \ldots, X_n]$ (the coeff's $a_\alpha \to 0$ shows $\tilde{f}$ above is a polynomial).

$$\tilde{\mathfrak{a}} = \text{the image of } \mathfrak{a}_0 \text{ in } \tilde{R}$$

so

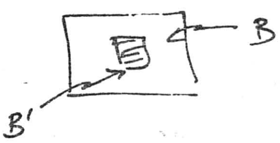
$$\tilde{\mathfrak{a}} \subset k[X].$$

Then the variety $\tilde{Y}$ attached to $\tilde{\mathfrak{a}}$ is again equidimensional of dim d. Hence the degree of $\tilde{Y} = \mathrm{Spec}\,(\tilde{R}/\tilde{\mathfrak{a}})$ is defined. [in Weil's terminology, $\tilde{\mathfrak{a}}$ defines a cycle of dim d, $\sum n_i W_i$ W_i irreducible varieties of dimension d, $n_i \geq 0$, the $\deg(\tilde{Y}) = \sum n_i \deg(W_i)$]. Let $\delta(Y) = \deg \tilde{Y}$.

Then $\delta(Y)$ for a hypersurface Y is the same as our previous def^{n} for the degree of Y. ✓

<u>Theorem</u> (Oesterlé) $|Y_m| \leq \delta(Y) q^{dm}$ for all $m \geq 0$.

<u>Pf</u>: Recall as above that $\delta(Y) = \delta_B(Y)$, $B = \mathcal{O}_K^n$ (depends only on the ball.)

If B' is a class mod π^ν 

$= \pi^\nu B$, say, then

$X_i' = X_i/\pi^\nu$ are the new coord's, $R' = K\{X_1', \dots, X_n'\}$

$$\begin{array}{c} R' \\ | \\ R \end{array}$$

$\mathfrak{a}$ generates $\mathfrak{a}' = \mathfrak{a}R'$, can get then a degree $\delta_{B'}(Y)$.

<u>Claim</u>: (Properties of the $\delta_{B'}(Y)$)

(1) $\delta_{B'}(Y) \leq \delta_B(Y)$

(2) $\delta_{B'}(Y) \geq 1$ if $Y \cap B' \neq \emptyset$

(3) If $B_1', \dots, B_r'$ are distinct classes mod π in B, then

$$\sum_i \delta_{B_i'}(Y) \leq q^d \delta(Y).$$

The theorem follows immediately from the Claim: If $B_1, \dots, B_s$ are the distinct classes mod π^ν, get (inductively) from (3)

$$\sum \delta_{B_i}(Y) \leq q^{d\nu}\delta(Y)$$

and by Property 2,

$$|Y_0| \leq \sum \delta_{B_i}(Y) \quad \text{so the Theorem follows.}$$

<u>Proof of the Claim</u>: relate δ to the multiplicity $m_P(V)$ of the point P on a variety V as follows;

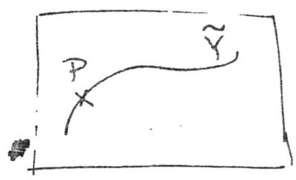
$$B \supset B'$$

ball mod π

i.e. have chosen $(x_1, \dots, x_n)$, x_i mod π for center.

Hence

B' is attached to a point P in k^n.



mod π

B

So it makes sense to consider

$$m_P(\tilde{Y}).$$

Then (3) reduces to 2 statements:

$$(3_1): \quad \delta_{B'}(Y) \leq m_P(\tilde{Y})$$

$$(3_2): \quad \sum_{P \in \mathbb{F}_q^n} m_P(\tilde{Y}) \leq q^d \cdot \deg \text{ of } \tilde{Y} = q^d \cdot \delta(\tilde{Y}).$$

(this is true for any variety)

<u>Remark</u>: compare to hypersurface proof.

Accept (3_1) (cf. Oesterlé)

For (3_2), see this geometrically:

k arbitrary field, V a variety of (equi-) dimension d. $\subset$ affine n-space $/k$

have subsets

$$\Omega_1, \ldots, \Omega_n \subset k \quad \text{with equal cardinality}, \ |\Omega_i| = q$$

Then

$$\sum_{\substack{P \in \Omega \\ \Omega = \Omega_1 \times \ldots \times \Omega_n}} m_P(V) \leq q^d \deg(V)$$

(cf. proof for hypersurface - exercise). //

<u>Theorem</u> (Oesterlé): Y analytic of dim $\leq d$ in X. Then

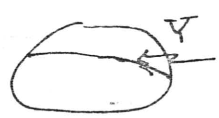
$$\lim_{m \to \infty} \frac{|Y_m|}{q^{md}} = \int_{Y^{\text{regular}}} \mu_Y$$

μ_Y = the canonical measure on Y (so the $\int \mu_Y$ is the "area" of Y)

<u>Proof</u>: Suffice to prove

$$\liminf \geq \int \mu_Y \geq \limsup.$$

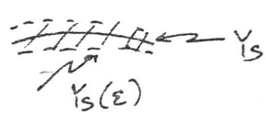
But Y^{reg} is smooth (by def^{n}!)



Y^s analytic subset of dim $\leq d-1$ containing singularities

then

$$Y_\varepsilon = Y - Y^s(\varepsilon) \quad \text{is non-singular, compact}$$



so

$$|Y_{\varepsilon, n}| / q^{nd} \to \int_{Y_\varepsilon} \mu_Y$$

(proved previously) (p.

Hence easily

$$\liminf \frac{|Y_n|}{q^{nd}} \geq \int_{Y_\varepsilon} \mu_Y \qquad \text{for any } \varepsilon > 0$$

$$\geq \int_{Y - Y_s} \mu_Y$$

$$= \int_{Y^{reg}} \mu_Y \qquad \left[\begin{array}{l} \text{difference between} \\ Y - Y_s \,,\, Y^{reg} \text{ is of} \\ \text{measure } 0 \end{array} \right].$$

Now, for the lim sup: take $\varepsilon = q^{-\nu}$, $\nu \geq 0$ and consider

$$Y_\varepsilon = Y - (Y^s(\varepsilon) \cap Y)$$

Then $$|Y_m| \leq |Y_{\varepsilon,m}| + |(Y \cap Y^s(\varepsilon))_m|$$

$$\Rightarrow \quad q^{-md} |Y_m| \leq q^{-md} |Y_{\varepsilon,m}| + q^{-md} |(Y \cap Y^s(\varepsilon))_m|$$

$$\Rightarrow \quad \limsup (\quad) \leq \limsup (\quad) + \limsup (\quad)$$

(ε fixed, $m \to \infty$). It suffices to prove

$$\lim_{m \to \infty} q^{-md} |(Y \cap Y^s(\varepsilon))_m| \to 0 \quad \text{when } \varepsilon \to 0.$$

So we need to estimate the # of pts. in an ε-neighborhood of a singularity: $Y^s(\varepsilon)$ is the π^ν neighborhood of Y^s, certainly contained in some n_ε balls of radius $q^{-\nu}$ [$n_\varepsilon = |Y^s_\nu|$, which by the first result is $\leq C \cdot q^{\nu(d-1)}$]

Call $B_1, \ldots, B_{n_\varepsilon}$ these balls of radius $q^{-\nu}$, so

$$Y^S(\varepsilon) \subset \bigcup_i B_i .$$

Then

$$q_0^{-md} \left| (Y \cap Y^S(\varepsilon))_m \right| \leq q_0^{-md} \sum_{i=1}^{n_\varepsilon} |(Y \cap B_i)_m|$$

(may assume $m \geqslant \nu$ of course since interest is in the limit)

By the uniformity of Oesterlé's first result:

$$|(Y \cap B_i)_m| \leq \delta(Y) q_0^{d(m-\nu)}$$

Hence

$$q_0^{-md} \left| (Y \cap Y^S(\varepsilon))_m \right| \leq q_0^{-md} \cdot n_\varepsilon \cdot q_0^{d(m-\nu)} \cdot \delta(Y)$$

$(m \geqslant \nu)$

$$\leq q_0^{-md} \, C \, q_0^{\nu(d-1)} \, q_0^{d(m-\nu)} \, \delta(Y)$$

$$= C \, \delta(Y) \, q_0^{-\nu} = C \varepsilon \, \delta(Y) \to 0 \text{ as } \varepsilon \to 0$$

and so the result follows //

— o —

§II: Adeles

References: A. Weil — Basic Number Theory
S. Lang — Alg. No. Th.
A. Weil — Adeles and Algebraic Groups (IAS notes)
Tate's thesis

History: Ideles; Chevalley CR note 1936 - infinite Galois gps. (introduced to study)
(Krull gps. introduced ~ 1928) ← following Herbrand
Weil CR note 1936 gave ideles their current topology (Chevalley introduced a non-Hausdorff topology to kill the connected component). Weil observed that the characters on his ideles are Hecke's "Grössencharakters".
Adeles; letter of Weil to Hasse on Riemann-Roch on curves (1938) (cf. collected works)

Artin - Whaples (1945) Bull. AMS. (adeles = valuation vectors)
(first systematic treatment)

Ideles: 1950 Tate's thesis ← (number fields)
K. Iwasawa
A. Weil
} all noticed the analysis on adeles and ideles

— o —

K is a "global field" (Weil: "A-field"), i.e. either a number field (finite extension of $\mathbb{Q}$) or a function field (of one variable) over a finite field (i.e. a finite extension of some $\mathbb{F}_q(t)$)

Define

$$\Sigma = \Sigma_K = \text{the set of "places"}$$

(embeddings $K \hookrightarrow \mathbb{R}$ or $\mathbb{C}$: Archimedean places
(conjugate pairs of embeddings))
" Σ^∞ "

equivalently,

an Archimedean place is a topology on K s.t. the completion is $\simeq \mathbb{R}$ or $\mathbb{C}$ etc.

(these exist only for number fields)

Non-Archimedean places $\Leftrightarrow$ discrete valuations (i.e. value group $\simeq \mathbb{Z}$))
($\Leftrightarrow$ prime ideals $\neq 0$ of $\mathcal{O}_K$ in number field case).

Define then

$\mathbb{A}_K$ = the adele ring = the subring of $\prod_{v \in \Sigma} K_v$

consisting of elements $x = (x_v)_{v \in \Sigma}$ where almost all x_v are in $\mathcal{O}_v$ (= the ring of integers in K_v)

The topology on $\mathbb{A}_K$ is defined as follows: S = a finite set of places, containing Σ^∞, let

$\mathbb{A}_K(S) = \prod_{v \in S} K_v \times \prod_{v \notin S} \mathcal{O}_v$ with the product topology
(so locally compact since $\prod_{v \notin S} \mathcal{O}_v$ is compact).

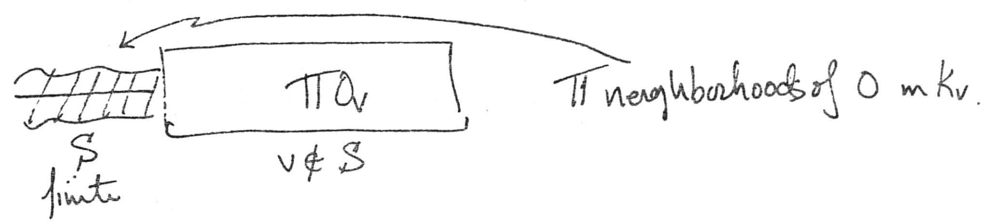
Clearly $\quad A_K(S) \subset A_K(S')$ both open and closed (where $S \subset S'$)

Then give

$$A_K \left(= \bigcup_S A_K(S) \right) \text{ the "direct limit topology"}$$

i.e. a basis of neighborhoods of $x \in A_K$ is given by the basis in $A_K(S)$ for (any) S s.t. $x \in A_K(S)$.

Open sets:



Then the adeles are a locally compact ring.

$$I_K = \text{ideles} = A_K^{\times}, \text{ the multiplicative gp.}$$

$$= \left\{ x = (x_v) \;\middle|\; \begin{array}{l} x_v \neq 0 \text{ for all } v \text{ and} \\ x_v \in O_v^{\times} \text{ for almost all } v \end{array} \right\}.$$

Generally $R =$ top. ring, $I = R^{\times}$ has a natural topology, by viewing $I \subset R \times R$ with the induced topology [it is closed in $R \times R$], not the induced topology (I not closed in R).

$x \mapsto (x, x^{-1})$

So convergence of sequence $\Leftrightarrow$ sequence converges and the sequence of inverses also converges

10-22 Properties of the adeles:

(1) $\mathbb{A}_K/K$ is compact, K is discrete in $\mathbb{A}_K$ (so closed!)

follows from: K' = finite extension of K,

then

$$\mathbb{A}_{K'} = K' \otimes_K \mathbb{A}_K \quad \text{(identification)}$$

via

$$\mathbb{A}_K = \prod_{v \in \Sigma} K_v \quad , \quad K' \otimes \mathbb{A}_K = \prod_{v \in \Sigma} (K' \otimes K_v)$$

(restricted direct product w.r.t. $\mathcal{O}_v$)

and $K' \otimes K_v \simeq \prod_{w|v} K'_w$ ✓

(keeping "track of" $\mathcal{O}_v$ shows $K' \otimes \mathbb{A}_K = \mathbb{A}_{K'}$).

Using this to prove (1); suffice to show $\mathbb{A}_K/K$ compact for

$$\begin{cases} K = \mathbb{Q} \\ K = \mathbb{F}_q(T), \text{ the function field of } \mathbb{P}^1/\mathbb{F}_q \end{cases}$$

then get a system of representatives for $\mathbb{A}_K/K$:

(1) $\mathbb{A}_{\mathbb{Q}} = \mathbb{R} \times \prod \mathbb{Q}_p$ take $I = [0,1]$, $I \times \prod_p \mathbb{Z}_p \subset \mathbb{A}_{\mathbb{Q}}$

gives a system of rep's for $\mathbb{A}_{\mathbb{Q}}/\mathbb{Q}$ - even almost a fund. domain: $(0,\nu) \sim (1, \nu+1)$ [because of $\mathbb{R}/\mathbb{Z}$!] is the only identification necessary to give a fund. domain. Hence $\mathbb{A}_{\mathbb{Q}}/\mathbb{Q}$ is indeed compact. ✓

(a system of rep's as follows:

$$\mathbb{Q}/\mathbb{Z} = \coprod_p \mathbb{Q}_p/\mathbb{Z}_p = \prod \mathbb{Q}_p \Big/ \prod \mathbb{Z}_p .$$

so

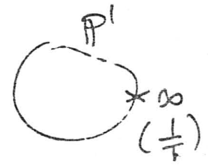
$a \in \mathbb{A}_{\mathbb{Q}}$ say $a = (a_\infty, (a_p))$, then $(a_p) = \lambda + \nu$, $\lambda \in \mathbb{Q}$, $\nu \in \prod \mathbb{Z}_p$

$$\Rightarrow (a_\infty, (a_p)) \equiv (a_\infty, \nu), \quad 0 \le a_\infty \le 1 \quad \text{mod } I \times \prod_p \mathbb{Z}_p$$

Of course, the same argument works for $K/\mathbb{Q}$ finite; take instead $e_1, \dots, e_n$ = $\mathbb{Z}$-basis of $\mathcal{O}_K$, $I_n = \{ \sum_{i=1}^{n} t_i e_i \mid 0 \le t_i \le 1 \}$, then

$I_n \times \prod_v \mathcal{O}_v$ is a compact (essentially fundamental domain) system of rep's. ✓

(2) $\mathbb{A}_{\mathbb{F}_q(T)}$, $\quad H = \prod_{v \ne \infty} \mathcal{O}_v \times \mathfrak{p}_\infty$, compact



$\mathfrak{p}_\infty$ = the maximal ideal at ∞ in $\mathcal{O}_\infty$

Then here in fact $\mathbb{A}_{\mathbb{F}_q(T)} = K \oplus H$, as follows:

$K \cap H = \{0\}$ as $a \in K \cap H \Rightarrow a = a(T)$ is a rat'l function with no poles, with a zero at ∞ (hence reason for the $\mathfrak{p}_\infty$ above) ✓

Now, if $(a_v)_v \in \mathbb{A}_{\mathbb{F}_q(T)}$, consider the various a_v:

$v \ne \infty$ $\quad K_v/\mathcal{O}_v \ni \alpha_v \Rightarrow \alpha_v = \sum_{n \ge 1} \frac{\beta_n}{P_v^n}$ $\quad \deg \beta_n < \deg P_v$ (finite sum)

since $v \Leftrightarrow$ an irreducible polynomial in $\mathbb{F}_q[T]$, say P_v

so defining

$$f = \sum_{\substack{n,v \\ v \neq \infty}} \frac{\beta_n}{P_v^n}$$

has precisely the correct "polar" parts at all $v \neq \infty$. Hence replacing a by $a - f$, may assume $a_v \in \mathcal{O}_v$ for all $v \neq \infty$. At $v = \infty$,

$K_\infty / \mathfrak{g}_\infty$ represented by polynomials in T, so again get a representative in K.

[equivalently, $K \xrightarrow{\sim} A_K/H$ = polynomials + $\sum$ polar terms ; "partial fraction decomposition"!
$$\overset{\rule{0pt}{0pt}}{\underset{K_\infty/\mathfrak{g}_\infty}{\parallel}} \qquad \underset{\prod K_v/\mathcal{O}_v}{\parallel}$$
].

(2) for ideles $\mathbb{I}_K$, have a related result. First, if $a = (a_v) \in \mathbb{I}_K$, have the norm $N(a) = \|a\| = |a|_{\mathbb{A}} = \prod_v \|a\|_v \leftarrow$ normalized abs. values. Then the "product formula" says $|a|_{\mathbb{A}} = 1$ for $a \in K^\times$, so have induced

$$\mathbb{I}_K / K^\times \xrightarrow{|\,|_{\mathbb{A}}} \mathbb{R}_+^\times \quad \text{with image} = \begin{cases} \mathbb{R}_+^\times & \text{number field case} \\ q^{\mathbb{Z}} & \text{function field case} \end{cases}$$

(q = card constant

Then letting $\mathbb{I}_K^\circ = \{a \mid Na = 1\}$,

$\mathbb{I}_K^\circ / K^\times$ is compact. (i.e. the kernel above is compact).

Will prove this later for division algebras (or, cf. Weil's Basic No. Th.).

Remark again, $K^\times$ is discrete in $\mathbb{I}_K$.

(3) (<u>Haar measure</u>) There is a "natural" Haar measure on $\mathbb{A}_K$:

$$\mathbb{A}_K = \bigcup_S \mathbb{A}_K(S)$$ where S is a finite subset of Σ containing Σ_∞.

where
$$\mathbb{A}_K(S) = \prod_{v \in S} K_v \times \prod_{v \notin S} \mathcal{O}_v$$

and there is a natural Haar measure on each of these factors [meas $(\mathcal{O}_v) =$ for v non-Archimedean], i.e. put on $\prod_{v \notin S} \mathcal{O}_v$ (= compact) the measure giving it volume 1.

This gives the Haar measure on $\mathbb{A}_K$. [formally, "$da = \otimes da_v$"]. (recall, over $\mathbb{R}$, dx over $\mathbb{C}$, $2\,dx\,dy =$ "$|dz d\bar{z}|$").

Then $\mathbb{A}_K/K$ has an induced measure, and

$$\mathrm{vol}(\mathbb{A}_K/K) = \begin{cases} \sqrt{|d_K|} & d_K = \text{the discriminant of } K/\mathbb{Q} \\ q^{g-1} & g = \text{genus of } K \text{ in the function field case} \end{cases}$$

This follows from the explicit description in (1) of the fundamental set (e.g. $K = \mathbb{Q}$, $[0,1] \times \prod \mathbb{Z}_p$, volume $= 1$ ✓). In the case $[K:\mathbb{Q}] > 1$, the identification necessary for a fundamental domain is as follows:

$e_1, \ldots, e_n$ $\mathbb{Z}$-basis for $\mathcal{O}_K$ $\quad n = [K:\mathbb{Q}]$

$$I_n \hookrightarrow K_\infty = \prod_{v \in \Sigma_\infty} K_v \quad (\simeq \mathbb{R}^{r_1} \times \mathbb{C}^{r_2})$$

Then compute the volume (notice the choice of $2dxdy$ on $\mathbb{C}$ removes the factor 2^{r_2} in this volume) ✓

The computation for $\mathbb{A}_K/K$ for K a function field can be done by techniques to be investigated later (giving $G_{\mathbb{A}}/G_K$ for other groups G). Or, can proceed similarly to the number field case:

$$X = \mathbb{A}_K/K \qquad K = \text{function field}$$

$$H = \prod_{v \in \Sigma} \mathcal{O}_v \qquad \text{vol}(H) = 1 \qquad H \cap K = \mathbb{F}_q$$

Then H acts on X, and each orbit has volume $\frac{1}{q}$ (since $\simeq H/\mathbb{F}_q$) (generally, G = gp, dx Γ = discrete subgp of G, G/Γ has again dx), so need to know the # of orbits, i.e. X/H or $\mathbb{A}_K/(H+K)$. (in non-abelian situations, better to write $H \backslash \mathbb{A}_K/K$).

$$\mathbb{A}_K/H = \coprod_v K_v/\mathcal{O}_v = \text{the set of "principal parts"}$$
("polar parts" above)

dividing then by K, are interested in those principal parts arising from elements of K, i.e. principal parts / principal parts from $f \in K$. This follows from Riemann-Roch:

ω = diff. form of the 1st kind on a curve C

$a_v \in K_v/\mathcal{O}_v$

$\Rightarrow \text{Res}_v(a_v\omega) \in$ residue field at v = a finite extension of $\mathbb{F}_q$

$$\Rightarrow \text{Tr}_{\mathbb{F}_q} \text{Res}_v(a_v\omega) \in \mathbb{F}_q.$$

"<u>Duality Thm</u>" (a_v) comes from an element of K

$\Updownarrow$

for all ω of the 1st kind $\sum \text{Tr}_{\mathbb{F}} \text{Res}(a_v\omega) = 0$.

Then, if $\omega_1, \dots, \omega_g$ is a basis for the diff. forms of 1st kind, each gives a map

$$\mathbb{A}_K/(K+H) \to \mathbb{F}_q$$

and $\cap$ kernels $= \{0\}$. But these maps are independent (there is an adele giving distinct values - easy). Hence $\mathbb{A}_K/K+H \xrightarrow{\sim} \mathbb{F}_q^{\,g}$

$$\Rightarrow \quad \mathrm{vol}(\mathbb{A}_K/K) \simeq q^g \cdot \frac{1}{q} = q^{g-1} \quad ✓.$$

exercise computing $\mathrm{vol}(\mathbb{A}_K/K)$ using another H, different divisor, can get Riemann-Roch.

Remark: in cohomological terms: C curve, sheaf $\mathcal{O}$ of local rings (then $\mathcal{O}_v$ = local ring with completion the $\mathcal{O}_v$ above), K = constant sheaf, so an exact sequence

skyscraper sheaf

$$0 \to \mathcal{O} \to K \to K/\mathcal{O} \to 0$$

$\Rightarrow$ cohomology

principal parts of the skyscraper sheaf

$$0 \to \mathbb{F}_q \to K \to \mathbb{A}_K/H \to \underset{\dim\, g}{\underset{\shortparallel}{H^1(C,\mathcal{O})}} \to 0.$$

(so $\mathbb{A}_K/K+H = H^1(C,\mathcal{O})$ and the isomorphism $\mathbb{A}_K/K+H \simeq \mathbb{F}_q^{\,g}$ above is just the statement $H^1(C,\mathcal{O}) \underset{\text{dual}}{=} H^0(C,\Omega^1)$).

(4) Characters and Duality

G commutative, locally compact

$\hat{G}$ = dual of G = $\mathrm{Hom}_{\mathrm{cont}}(G, \mathbb{C}^1)$ with compact-open topology

$\mathbb{C}^1 = \{z \in \mathbb{C} \mid |z| = 1\}$

(a) Locally: $K_v \simeq (\hat{K_v})^*$ as follows:

ψ_v = any non-trivial character of K_v

$\Rightarrow$ any character of K_v is $x \mapsto \psi_v(ax)$ for some $a \in K_v$.

which gives the duality

(this simply says $\hat{K_v}$ is K_v-free of rank 1).

Remark the identification depends on a choice of ψ_v.

(b) Globally: $\mathbb{A}_K \simeq \hat{\mathbb{A}}_K$

More precisely, $\exists$ a non-trivial character ψ of $\mathbb{A}_K$, trivial on K. With ψ fixed, then

(i) any character of $\mathbb{A}_K$ is $x \mapsto \psi(ax)$ for some $a \in \mathbb{A}_K$

(ii) such a character is trivial on $\mathbb{A}_K$ if and only if $a \in K$.

In other words, $\hat{\mathbb{A}}_K \simeq \mathbb{A}_K$ (via choice of ψ)

then

$$K^\perp = K.$$

(the orthogonal to K w.r.t. the pairing of $\mathbb{A}_K$ with $\hat{\mathbb{A}}_K$)

Slick Proof (Tate's thesis): $K^\perp$ = the dual of $\underbrace{\mathbb{A}_K/K}_{\text{compact}}$, so $K^\perp$ is discrete.

certainly $K^\perp \supseteq K$, $K^\perp$ is a K-vector space. Then

$$\underset{\text{discrete}}{K} \subseteq \underset{\text{discrete}}{K^\perp} \subseteq \mathbb{A}_K \Rightarrow \underset{\text{compact}}{\mathbb{A}_K/K} \supset \underbrace{K^\perp/K}$$

$\Rightarrow$ compact, discrete
$\Rightarrow$ finite

$\Rightarrow$ since $K^\perp$ is a K-vector space, $K^\perp = K$ ✓.

— o —

<u>Explicit description of ψ:</u>

(i) $\mathbb{Q}$: $\psi = \otimes \psi_v$

$$\psi_\infty : \mathbb{R} \to \mathbb{C}^1, \quad x \mapsto e^{-2\pi i x}$$

$$\psi_p : \mathbb{Q}_p \to \mathbb{C}^1$$

via

$$\mathbb{Q}_p \downarrow \mathbb{Q}_p/\mathbb{Z}_p \subset \mathbb{Q}/\mathbb{Z} \to \mathbb{C}^1, \quad x \mapsto e^{2\pi i x}$$

keep signs opposite so two choices for ψ

check: $\alpha \in \mathbb{Q} \Rightarrow \psi_\infty(\alpha)\prod_p \psi_p(\alpha) = 1$ ✓.

$[K:\mathbb{Q}]$ finite:

$$\mathbb{A}_K = K \otimes_{\mathbb{Q}} \mathbb{A}_{\mathbb{Q}}$$
$$\downarrow \text{Trace} \otimes 1$$
$$\mathbb{Q} \otimes_{\mathbb{Q}} \mathbb{A}_{\mathbb{Q}} = \mathbb{A}_{\mathbb{Q}}$$

gives $\psi_K = \psi_{\mathbb{Q}} \circ (\text{Trace} \otimes 1)$ ✓ [any $\mathbb{Q}$-linear map from $K \to \mathbb{Q}$ will suffice].

(ii) function field case: take any character $\tilde{\psi} : \mathbb{F}_q \to \mathbb{C}^1$, $\tilde{\psi} \neq 1$.

and take ω any non-zero differential form, $\omega \in K\,dK$.
Locally at v,

$$\psi_v(a_v) = \tilde{\psi}\left(\mathrm{Tr}_{/\mathbb{F}_q}\left(\mathrm{Res}_v(a_v\omega)\right)\right)$$
$a_v \in K_v$

$$\psi = \otimes \psi_v.$$

Observe that for $a = (a_v) \in K \Rightarrow \mathrm{Res}(a_v\omega)$ (global diff.) and $\mathrm{Tr}_{/\mathbb{F}_q}(\mathrm{Res}_v(a_v\omega))$ gives the sum of all the residues, so $0 \Rightarrow \Psi(a) = 1$ ✓

(5) Haar Measure for Dual Groups

G with given Haar measure μ
$\updownarrow$ duality
$\hat{G}$ with a Haar measure $\hat{\mu}$ so that the Plancherel formula is valid:

$$f \text{ on } G, \quad \hat{f}(y) = \int_G f(x)\langle x,y\rangle \mu(x) \qquad \hat{f} \text{ on } \hat{G}$$

dual pairing

then

$$\|f\|_{2,\mu} = \|\hat{f}\|_{2,\hat{\mu}}$$

: call $\mu, \hat{\mu}$ "compatible" if this holds

[so $c\mu \overset{}{\underset{\text{duality}}{\Leftrightarrow}} c^{-1}\hat{\mu}$ for any Haar measure $c\mu$ on G].

Compatible measures w.r.t. duality:

"Recipe": (1) G compact, $\hat{G}$ discrete

μ_G Haar with total volume 1

$$\hat{\mu}_{\hat{G}} = \sum_{y \in \hat{G}} \delta_y \leftarrow \text{Dirac } \delta \text{ at } y.$$

(2) $G \supset \Gamma$, Γ discrete, G/Γ compact

$\hat{G} \supset \Gamma^\perp$, $\Gamma^\perp = \widehat{(G/\Gamma)}$, $\hat{G}/\Gamma^\perp$ compact

so on compact G/Γ take measure with total volume 1
on compact $\hat{G}/\Gamma^\perp$ take measure with total volume 1

Then these two measures are compatible (i.e. $\mu, \hat{\mu}$ given, then $\mu, \hat{\mu}$ are compatible $\Leftrightarrow$ $\mu(G/\Gamma)\hat{\mu}(\hat{G}/\Gamma^\perp) = 1$)

(3) $G \supset H$, H open, compact

$\hat{G} \supset H^\perp$, $H^\perp$ open, compact

Then μ on G/H, $\hat{\mu}$ on $\hat{G}/H^\perp$ are compatible $\Leftrightarrow$ $\mu(H)\hat{\mu}(H^\perp) = 1$.

10-27 There are of course situations in which $\hat{G}$ can be identified with G, e.g. K_v, A_K, $(\widehat{A_K/K}) \simeq K$ (by choice of ψ). Then there is a unique choice of measure μ_G $(= \mu_{G,\psi})$ s.t. "$\mu_G = \hat{\mu}_G$".

Thus ~~even~~ (~~$\exists$ such~~ a measure on $(\mathbb{A}_K/K)$ with $\mu(\mathbb{A}_K/K)=1$, indep. of ψ)

example : $\begin{array}{c} K \\ \mid Tr \\ \mathbb{Q} \end{array}$ number field

canonical ψ on $\mathbb{Q}$

$\begin{array}{c} K_v \\ \mid \\ \mathbb{Q}_p \end{array}$, $\mathcal{O}_v$ open, compact in K_v

Then the inverse different is $= \{ z \in K_v \mid Tr(z\mathcal{O}_v) \subset \mathbb{Z}_p \} = \pi_v^{-\delta_v} \mathcal{O}_v$

δ_v = the exponent of the different.

Then $\mu_{\psi,v}(\mathcal{O}_v) = \lambda_v$, so want

$$\mu_{\psi,v}(\mathcal{O}_v) \cdot \mu_{\psi,v}(\pi_v^{-\delta}\mathcal{O}_v) = 1$$

$$\lambda_v (N_v)^{\delta_v} \lambda_v = 1$$

$$\Rightarrow \quad \lambda_v = N_v^{-\frac{\delta_v}{2}}.$$

Hence,

$$\mu_{\psi,v} = (N_v)^{-\frac{\delta_v}{2}} \cdot \mu_v \Leftarrow \text{the natural Haar.}$$

For Archimedean primes, $\mu_{\psi,v} = \mu_v$ (by choice : explains the 2 in $2dx\,dy$)

Then set

$$\mu_\psi = \otimes \mu_{\psi,v}$$

$$= \prod_{\substack{v \text{ non} \\ \text{Archimedean}}} (N_v)^{-\frac{\delta_v}{2}} \mu$$

$$= |d_K|^{-1/2} \mu.$$

Therefore $\mu(\mathbb{A}_K/K) = |d_K|^{1/2}$.

Adelic Integrations : Heuristic !

Heuristic Goldbach : $k = p + p'$ $x \le k$

$$\# \, p\text{'s with } k = p+p' \sim \int_2^k \frac{dx}{\log x \, \log(k-x)} \sim \frac{dx}{(\log x)^2}$$

"probability of choosing a prime" · "probability of remainder also being prime".

Similarly, can do the following [after Deligne, letter to Serre 1971]:

F polynomial, coeff's in $\mathbb{Z}$, $F(n_1, \ldots, n_r ; p_1, \ldots, p_s)$

Take $U \subset \mathbb{R}^{r+s}$ open and some $k \in \mathbb{Z}$. Want to count

$N = N_{U,F,k}$ = the number of $(n_i, p_j) \in U$ s.t. $n_i \in \mathbb{Z}$, p_j prime such that $F(n_i, p_j) = k$.

[e.g. for Goldbach, $r=0$, $s=2$, $F = p_1 + p_2$, $U = [2,k] \times [2,k]$].

Have $\mathbb{A}_{\mathbb{Q}} \supset \mathbb{R} \times \prod_p \mathbb{Z}_p = \mathbb{R} \times \hat{\mathbb{Z}}$, so a space of interest $X = (\mathbb{R} \times \hat{\mathbb{Z}})^{r+s}$.

Define measures:

$$da = \text{the standard measure} = \underset{\text{on } \mathbb{R}}{dx} \otimes (\text{Haar on } \hat{\mathbb{Z}} \text{ total measure } 1)$$

Measure with support on $[2, \infty] \times \prod \mathbb{Z}_p^*$

$$d^P a = \frac{dx}{\log x} \otimes (\text{Haar of } \textstyle\prod_p \hat{\mathbb{Z}}_p^*)$$

Then on X:

$$da_1 \otimes \dots \otimes da_r \otimes d^{p}b_1 \otimes \dots \otimes d^{p}b_s = dx$$

for $x \in X$, $x = (a_1, \dots, a_r, b_1, \dots, b_s)$.

Remark: for $\mathbb{Z} \subset \mathbb{R}$ and $\varphi(x)$ which does not vary "much", then one might compare $\sum_{n \in \mathbb{Z}} \varphi(n)$ and $\int_{-\infty}^{\infty} \varphi(x)dx$ [corresponding to ignoring all terms but $n = 0$ on the left in $\sum \hat{\varphi}(n) = \sum \varphi(n)$ in Poisson].

Viewing $\mathbb{Z} \subset \mathbb{R} \otimes \hat{\mathbb{Z}}$, P = primes "almost" contained in $\mathbb{R} \times \hat{\mathbb{Z}}$. Then might compare $\sum_{P} \varphi(n)$ and $\int \varphi(x) \frac{dx}{\log x}$ since $\frac{dx}{\log x}$ "measures" the primes.

Similarly $\mathbb{Q} \subset \mathbb{A}_{\mathbb{Q}}$, might compare $\sum_{x \in \mathbb{Q}} \varphi(x)$ and $\int_{\mathbb{A}_{\mathbb{Q}}} \varphi(x)dx$.

Let

$$I = \int_{\substack{U \times \hat{\mathbb{Z}}^{r+s} \\ F(a,b) = k}} \frac{dx}{dF} \quad \text{- the so-called "singular series".}$$

(where $\frac{dx}{dF} = \otimes \left(\frac{dx_v}{dF_v}\right)$ where $\frac{dx_v}{dF_v}$ are defined locally, see below).

One might compare then I and the number N defined above. Examples follow:

Examples

(1) Goldbach: $r=0, s=2$; x,y variables of the 2nd type (i.e., primes)

so measure is

$$\frac{dx}{\log x}\ \frac{dy}{\log y} \qquad , \qquad \mathcal{U} = [2,k] \times [2,k]$$

$$F(x,y) = x+y \,, \qquad N = \# \text{ of rep's of } k \text{ as a sum of two primes.}$$

Then

$$I = I_\infty \times \prod I_p \,, \quad \text{where}$$

$$I_\infty = \int_{\substack{2 \le x \le k \\ 2 \le y \le k \\ x+y=k}} \frac{dx\,dy}{\log x \log y \; d(x+y)}$$

Remark $F(x,y) = x + \varphi(y)$, then $\frac{dx\,dy}{dF} = dy$ since $dF = 1 + \varphi'(y)dy$ so $dF \wedge dy = dx \wedge dy$; this is just the measure restricted to the fiber, defined previously.

$$\Rightarrow \quad I_\infty = \int_2^k \frac{dy}{\log(k-y)\log y} \sim \frac{k}{(\log k)^2}$$

asymptotically, as $\log(k-y)$, $\log y$ are roughly constant $\sim \log k$.

For I_p, note that the measure on $\mathbb{Z}_p^\times$ is $\frac{p}{p-1}dx$, dx the standard additive measure on $\mathbb{Z}_p$, so

$$I_p = \left(\frac{p}{p-1}\right)^2 \int_{\substack{x+y=k \\ x \in \mathbb{Z}_p^\times \\ y \in \mathbb{Z}_p^\times}} dy \,,$$

where

$$\int dy = \frac{1}{p}\left(\#\underset{\text{mod } p}{\text{solutions}} \text{ of } x+y \equiv k \text{ mod } p,\ x,y \text{ not } 0\right).$$

Hence

$$I_p = \begin{cases} \left(\frac{p}{p-1}\right)^2 \frac{1}{p}(p-1) = \frac{p}{p-1} & \text{if } p \mid k \\ \left(\frac{p}{p-1}\right)^2 \frac{1}{p}(p-2) = \frac{p(p-2)}{(p-1)^2} = 1 - \frac{1}{(p-1)^2} & \text{if } p \nmid k \end{cases}$$

(two classes mod p must be avoided for y if $p \nmid k$). Then

$$I \sim C_k \cdot \frac{k}{(\log k)^2} \qquad C_k = \prod_{p \mid k} \frac{p}{p-1} \prod_{p \nmid k} \left(1 - \frac{1}{(p-1)^2}\right).$$

<u>Remark</u> if k is <u>odd</u>, then $2 \nmid k$, so $1 - \frac{1}{(2-1)^2} = 0$ occurs in C_k, so get $I \sim 0$! (as one should!)

<u>Remark</u>: By sieves, one can show N is asympt. $\leq 4I(1+o(1))$

(2) <u>Twin Primes</u> $F = (x \cdot y)$, k fixed, say $x - y = 2$. Then the size of U goes to ∞, $U \underset{\text{say}}{=} [2,N] \times [2,N]$. Then as in (1), one computes to find

$$I \sim C_2 \frac{N}{(\log N)^2}$$

Here also, sieves show that
$N \leq 4I(1+o(1))$.

(3) $p = 1+n^2$? [Remark: best known; $\exists$ ∞'ly many $1+n^2$ the product of only 2 primes - Iwaniewicz.]

Here let $F = x - y^2 - 1$ (x the "prime variable")

$$\mathcal{U} = \underset{\text{for } x}{[2, N]} \times \underset{\text{for } y}{[2, \infty]}$$

$\Rightarrow N = \#$ primes $\leq M$ of the form $1+n^2$.

Then

$$I_\infty = \int_{x=y^2+1} \frac{dx\,dy}{\log x\; dF} = \int_2^{\sqrt{M+1}} \frac{dy}{\log(y^2+1)} \sim \frac{1}{2}\int_2^{\sqrt{M}} \frac{dy}{\log y}$$

$$\sim \frac{1}{2}\frac{\sqrt{M}}{\log\sqrt{M}} \sim \underline{\frac{M^{1/2}}{\log M}} \ldots$$

$$I_p = \frac{p}{p-1}\cdot\frac{1}{p}\{\#\text{ of solutions mod } p \text{ of } x = y^2+1,\ x \neq 0\}$$

$\leftarrow$ p solutions for y − # of sol'n's of $y^2 = -1$

$$= \begin{cases} 1 & p = 2 \\ \frac{p-2}{p-1} & p \equiv 1 \bmod 4 \\ \frac{p}{p-1} & p \equiv 3 \bmod 4 \end{cases}$$

$$\left(= \frac{p}{p-1}\cdot\frac{1}{p}\cdot\left[p - 1 - \left(\frac{-1}{p}\right)\right] \right)$$

$$= 1 - \frac{\left(\frac{-1}{p}\right)}{p-1}.$$

Hence

$$I \sim C\,\frac{M^{1/2}}{\log M}$$

where

$$C = \prod_p \left(1 - \frac{\left(\frac{-1}{p}\right)}{p-1}\right) \quad \text{(conditionally convergent)}.$$

Remark: Sieves show N is at most twice this conjectured value asymptotically.

Remark: Similarly, $p = g(n)$, then g irreducible $\Leftrightarrow$ product above is convergent cf. Halberstam-Richert "Sieves".

(4) Waring all ordinary variables ; $k = x_1^m + \dots + x_r^m$; $x_i \geq 0, \in \mathbb{Z}$.

Here let

$$I = I_\infty \times \prod I_p \quad \text{as before}$$

(with

$$\mathcal{U}: \; x_i \geq 0, \quad \mathcal{U} = [0, \infty]^r \;)$$

$$I_\infty = \int_{\substack{x_i \geq 0 \\ \sum x_i^m = k}} \frac{dx_1 \dots dx_r}{d(x_1^m + \dots + x_r^m)} = c \cdot k^{\frac{r}{m}-1}$$

by homogeneity

where in fact

$$C = \Gamma\left(1+\tfrac{1}{m}\right)^r \Gamma\left(\tfrac{r}{m}\right)$$

$$I_p = (\text{smooth hypersurface}), \text{ so } \frac{1}{p^{r-1}}\{\#\text{ of sol}^{\text{n}}\text{'s mod } p \text{ of } \textstyle\sum x_i^m = k\}$$

$$\begin{matrix} p \nmid m \\ p \nmid k \end{matrix} \quad = 1 + \varepsilon(p)$$

If $r > 4$, $\prod_p I_p$ converges and so

$$I = C \cdot k^{\frac{r}{m}-1}.$$

(See J.G.M. Mars, Sur l'approximation..., Ann. ENS 6 (1973), 357-388, for an adelic version of the "circle method".)

-29-81 Adelic Points of Algebraic Varieties

(cf. Weil: Adeles and Algebraic Groups)

Let K be a global field, $\mathbb{A}_K$ the adele ring of K, K_v the completion of K at the prime v, $v \in \Sigma$, with ring of integers $\mathcal{O}_v$, for v non-Archimedean

Suppose V is an algebraic variety over K. Since $K \subset \mathbb{A}_K$ makes $\mathbb{A}_K$ a K-algebra, it makes sense to consider the set of points of V in the algebra $= V(\mathbb{A}_K)$. In the language of schemes, $V(\mathbb{A}_K)$ is $\mathrm{Mor}_K(\mathrm{Spec}\, \mathbb{A}_K, V)$.

If V is an affine variety, say $V \subset A^n$ (affine n space) defined by the vanishing of $\Phi_i(x_1, \ldots, x_n)$, polynomials in x_i with coefficients in K, then for any K algebra Λ,

$$V(\Lambda) = \{(x_1, \ldots, x_n),\ x_i \in \Lambda \text{ with } \Phi_i(x) = 0\}.$$

Coordinate-free defn: a point of V in Λ is a homomorphism $k[V]$ to Λ ($k[V]$ the coordinate ring of V).

examples: A^1 = line, $A^1(\mathbb{A}_K) = \mathbb{A}_K$

Similarly: $A^n(\mathbb{A}_K) = \mathbb{A}_K \times \ldots \times \mathbb{A}_K$ (n times)

$\mathbb{G}_m$ = multiplicative group, $\mathbb{G}_m \subset A^2$ (e.g. by $xy = 1$)

Then $\mathbb{G}_m(\mathbb{A}_K) = \{(x,y),\ x,y \in \mathbb{A}_K \text{ with } xy = 1\}$

$= \mathbb{A}_K^\times$ = the idele group

In the general case, V an algebraic variety, cover by affine open subspaces $V = \bigcup_{i \in I} U_i$.

2 Warning: $V(\mathbb{A}_K) \neq \bigcup_{i \in I} U_i(\mathbb{A}_K)$ in general

Rather, proceed as follows: Choose $U_i \overset{\varphi_i}{\subset} A^N$, as a closed subvariety. Then $U_i(K_v)$ is defined and $V(K_v) = \bigcup_i U_i(K_v)$. In $U_i(K_v)$ are the "integral points" $U_i(\mathcal{O}_v)$, which depends on φ_i, so write $U_i(\varphi_i, \mathcal{O}_v)$. Define then $V(\mathcal{O}_v) = \bigcup_i U_i(\mathcal{O}_v)$, which depends on the cover and on the φ_i, say $V_\varphi(\mathcal{O}_v)$, where $\varphi = (U_i, \varphi_i)$. Then

$$V(K_v) \supset V_\varphi(\mathcal{O}_v)$$

locally compact $\qquad$ open and compact.

Then if φ'_j, U'_j are another cover, then one shows

$$V_\varphi(\mathcal{O}_v) = V_{\varphi'}(\mathcal{O}_v)$$ for all but a finite number, i.e. for almost all v.

Definition (Weil): The adelic points of V are the points $x = (x_v)_{v \in \Sigma}$ with $x_v \in V(K_v)$ for all v and $x_v \in V_\varphi(\mathcal{O}_v)$ for almost all v (this is now independent of φ).

Notation:

$$V_{\text{Weil}}(\mathbb{A}_K) = \text{the set of adelic points.}$$

This can be topologized:

Let S be a finite set of places including the Archimedean primes, and define

$$V_\varphi(\mathbb{A}_K, S) = \underbrace{\prod_{v\in S} V(k_v)}_{\text{locally compact}} \times \underbrace{\prod_{v\notin S} V_\varphi(\mathcal{O}_v)}_{\text{compact}}$$

Then for $S \subset S'$, $V_\varphi(\mathbb{A}_K, S) \subset V_\varphi(\mathbb{A}_K, S')$ as a closed and open subset. Hence

$$V_{Weil}(\mathbb{A}_K) = \bigcup_{S} V_\varphi(\mathbb{A}_K, S)$$

carries the corresponding (direct limit) topology.

Remark: if $V_1 \to V_2$, then $V_1(\mathbb{A}_K) \to V_2(\mathbb{A}_K)$, so $V(\mathbb{A}_K)$ contains the adelic points of all the affine opens in V, but may contain more.

Remark: write $\Sigma = \Sigma_1 \cup \ldots \cup \Sigma_h$ disjoint subsets. Then
$\mathbb{A}_K = \coprod k_v = \prod_{i=1}^{h} \coprod_{v\in\Sigma_i} k_v$. Let $\mathbb{A}_{K,i} = \coprod_{v\in\Sigma_i} k_v$, so

$\mathbb{A}_K = \prod \mathbb{A}_{K,i}$. Write $V = \bigcup_{i=1}^{h} U_i$, U_i open on V. Then

$x_i \in U_i(\mathbb{A}_{K,i})$, $x = (x_1, \ldots, x_h) \in V(\prod \mathbb{A}_{K,i}) = V(\mathbb{A}_K)$

The converse is true:

exercise: Prove that any open covering of $\mathrm{Spec}(\mathbb{A}_K)$ has a refinement of type $\mathbb{A}_K = \prod \mathbb{A}_{K,i}$ above for suitable $\Sigma_1, \ldots, \Sigma_h$ (recall that decomposing $\mathrm{Spec}\, R =$ disjoint is equivalent to decomposing R by idempotents)

Remark the Weil definition is in fact equivalent to the Grothendieck definition.

Properties of the functor $V \mapsto V(\mathbb{A}_k)$

(1) $V \subset V'$, V closed in V', then $V(\mathbb{A}_k)$ is closed in $V'(\mathbb{A}_k)$

(2) $V \subset V'$, V open in V', then $V(\mathbb{A}_k)$ is not open in $V'(\mathbb{A}_k)$ (e.g. mult-gp in add gp but ideles not open in adeles)

(3) $V = V_1 \times V_2$, then $V(\mathbb{A}_k) = V_1(\mathbb{A}_k) \times V_2(\mathbb{A}_k)$.

Regarding (2): write $V = V' - F$ for closed F. What are the adelic points of V?

$$x = (x_v), \quad x_v \in V'(k_v), \quad x_v \notin F(k_v) \text{ for all } v$$
$$x_v \in (V' - F)(\mathcal{O}_v) \text{ for almost all } v.$$

This can be described by; $x_v \in V'(\mathcal{O}_v) \mapsto \tilde{x}_v \in V'(\kappa_v)$ [by reduction, here $\kappa_v = \mathcal{O}_v/\pi_v\mathcal{O}_v$, π_v a uniformizing element in $\mathcal{O}_v$]. Then

$$(V' - F)(\mathcal{O}_v) = \{\text{points } x \in V'(\mathcal{O}_v) \text{ s.t. } \tilde{x} \notin F(\kappa_v)\}.$$

So then an adelic point of $V' - F$ is a point (x_v) with $x_v \in V'(K_v)$ and

$$\begin{cases} x_v \notin F(k_v) & \text{all } v \\ \tilde{x}_v \notin F(\kappa_v) & \text{for almost all } v \end{cases}$$

example: $V' = \mathbb{G}_a = \mathbb{A}^1$ the affine line, $(V = \mathbb{G}_m)$
$F = \{0\}$.

example 1: $V \underset{\substack{\text{locally}\\ \text{closed}}}{\subset} \mathbb{A}^n$, i.e. defined by $\Phi_i(x) = 0$ for all i (defines closure), $\Psi_j(x) \neq 0$ for some j (quasi-affine).

What are the adelic points? They are the pts $x = (x_v)$ with

$$x_v \in K_v$$
$$\Phi_i(x_v) = 0 \quad \text{for all } i$$
$$\Psi_{j_v}(x_v) \in \mathcal{O}_v^\times \quad \text{for almost all } v.$$
for some j_v

example 2: $V = \mathbb{P}_r^*$. Then $V(\mathcal{O}_v) = V(K_v) = \mathbb{P}_r(K_v)$ (the same is true for any projective variety, also for any complete variety). Hence

$$V(\mathbb{A}_K) = \prod_{v \in \Sigma} V(K_v), \quad \text{compact}.$$

example 3: quasi-projective: V defined in $\mathbb{P}_r$ by homogeneous equations $\phi_i(x_0, \dots, x_r) = 0$ for all i, and by homogeneous "in"-equations $\Psi_j(x_0, \dots, x_r) \neq 0$ for some j.

The adelic points of V are given then by $x = (x_v) = (x_{0,v}, \dots, x_{r,v})$ [with coordinates chosen s.t. all $x_{i,v}$ are integral (v non-Archimedean) and with one coordinate a unit],

(1) $\phi_i(x) = 0$

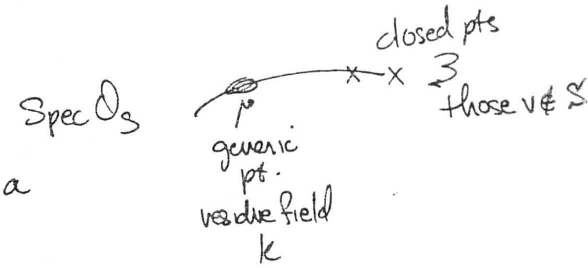
(2) for almost all v, one of the $\Psi_j(x_v)$ should be a unit in $\mathcal{O}_v$.

Remark:

Scheme theoretic interpretation of integral points:

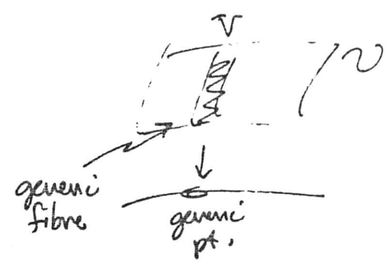
$$\begin{array}{c} V \\ \downarrow \\ K \end{array} \qquad \text{Define this "over the integers"?:}$$

Let $S \supset \Sigma^\infty$ be a finite set of places, $\mathcal{O}_S$ = the ring of S-integers of K (so with quotient field K).



Then an "$\mathcal{O}_S$-form of V" is defined as follows: a scheme $\mathcal{V}$ over $\mathcal{O}_S$ of finite type

$$\mathcal{V} \otimes_{\mathcal{O}_S} K = V.$$



an "$\mathcal{O}_S$-model" for V.

With $\mathcal{V}$ chosen, $\mathcal{O}_S \to \mathcal{O}_v$, $v \notin S$, then

$$\mathcal{V}(\mathcal{O}_v) = \underbrace{V_\varphi}_{\text{Weil notation}}(\mathcal{O}_v)$$

Can speak of the fibre $\mathcal{V}(k_v)$ = the fibre of $\mathcal{V}$ at v.

(4) Let $f: V \to V'$ be a proper map of algebraic varieties over K.
Then $f_{A_K} : V(A_K) \to V'(A_K)$ is proper (topologically).

(Recall : $\phi: X \to Y$ is proper if ϕ^{-1}(compact) is compact.
(yoga: " if $x \to \infty$, then $\phi(x) \to \infty$").
If V is embedded in some projective variety P, then $x \in V$ "goes to infinity" if x tends to something in $P - V$. How to say $\phi(x)$ has this property?

$$V \underset{\substack{\text{closed}\\\text{immersion}}}{\hookrightarrow} V \times V' \subset P \times V' \to V'$$

$$x \mapsto \underset{\text{graph}}{(x, f(x))}$$

$$\underset{\text{graph}}{\Gamma_f} \subset V \times V' \subset P \times V'$$

Then f is proper $\Leftrightarrow$ Γ_f is closed in $P \times V'$ ⇜ this is indep. of the projective embedding (there are a number of characterizations of this property))

By construction, a proper map is a composition of a closed immersion and a "projective projection" $P \times X \to X$, P = projective space.
Hence, suffices to prove (4) for these two types of f. First is done (this is (1)).
But $P(A_K) \times X(A_K) \to X(A_K)$ is proper since $P(A_K)$ is compact

(5) Let $f: V \to V'$ be a morphism with local cross sections, i.e. V' can be covered by open V_i' which can be lifted to V.
Then :

$$f : V(A_K) \to V'(A_K) \text{ is surjective}$$

Proof: $x' \in V'(\mathbb{A}_K)$ can be viewed as $x' = (x'_1, \dots, x'_h)$ where $x'_i \in V'_i(\mathbb{A}_{K,i})$ $(\mathbb{A}_K = \prod_i \mathbb{A}_{K,i})$. Then lifting of V'_i gives a lifting for each x'_i: $x'_i \mapsto x_i \in V(\mathbb{A}_{K,i})$ and the x_i define a point in $V(\mathbb{A}_K)$ ✓.

example: g a subgroup of G, $G \to G/g$, but will need local cross-sections.
Theorem: $g \simeq \mathbb{G}_a, \mathbb{G}_m, SL_n, GL_n, Sp_{2n}$ then there is always a local cross section.

Remark proper $\Rightarrow$ closed, so (4) gives a criterion for being closed. For open maps:

(6) $f: V \to V'$ V, V' smooth and f smooth, surjective (submersion: surjective on tangent spaces)

with fibers absolutely irreducible, i.e. connected even after extension of ground field k.

Then

$$f_{\mathbb{A}}: V(\mathbb{A}_K) \to V'(\mathbb{A}_K) \text{ is an open map.}$$

Over each K_v, $V(K_v)$ is a smooth manifold and $f: V(k_v) \to V'(K_v)$
$V'(k_v)$ is a smooth manifold

is a submersion, so open. Trouble arises from the infinite product:
lemma (topology): Given X_i, X'_i, almost all of which are compact spaces
and $f_i: X_i \to X'_i$ with f_i open for all i
and onto for almost all i.

Then

$$f: \prod X_i \to \prod X'_i \text{ is also open.}$$

Hence, need to show $V(\mathcal{O}_v) \longrightarrow V'(\mathcal{O}_v)$ is surjective for almost all v. By smoothness, this is tantamount (equivalent) to proving $V(\mathfrak{K}_v) \to V'(\mathfrak{K}_v)$ is surjective for almost all v. This means:

$$\begin{array}{ccc} V & & V_{\mathfrak{K}_v} \supset F_x \\ \downarrow & & \downarrow \quad\quad \downarrow \\ V' & & V'_{\mathfrak{K}_v} \ni x \end{array}$$

given $x \in V'(\mathfrak{K}_v)$, there is an associated fibre $F_x \subset V$~~$(\mathfrak{K}_v)$~~, and one must show there is a rational point over $\mathfrak{K}_v$ on this fibre (for almost all v).

Now F_x is smooth and absolutely irreducible; and the F_x is in a "limited family". By Lang-Weil, there is an estimate for the number of pts. in a limited family:

" F_λ absolutely irreducible over $\mathbb{F}_q$ of dim d
F_λ a "limited family", then

$$|F_\lambda(\mathbb{F}_q)| = q^d + O(q^{d-\frac{1}{2}})$$

and the constant in O is indep. of λ, i.e. $\exists$ a constant A independent of λ s.t.

$$\left| |F_\lambda(\mathbb{F}_q)| - q^d \right| \leq A q^{d-\frac{1}{2}} \text{ "}$$

In particular, this is non-zero for all but finitely many q. This gives the result above.

3-81 Restriction of Scalars

Let K be a finite extension of k, K/k separable. Then Weil has defined a functor : $\{K\text{-varieties}\} \rightsquigarrow \{k\text{-varieties}\}$ ("restriction of scalars").

e.g. if V = a K-vector space, then $R_{K/k}V$ is just V viewed as a k-vector space. Note that then $\dim_k R_{K/k} V = [K:k] \dim_K V$.

More generally : $R_{K/k}$: K-variety $\mapsto$ k-variety
$$V \mapsto R_{K/k} V.$$

Since it suffices to know the k-Morphisms into $R_{K/k}V$, define $R_{K/k}$ as follows: Suppose V is quasi-projective :

Definition : let S be a scheme over k, and define $R_{K/k}V$ by

$$\mathrm{Mor}_k(S, R_{K/k}V) = \mathrm{Mor}_K(S/_K, V)$$

(where $S/_K = K \otimes_k S$). More precisely, $R_{K/k}$ represents the functor $\mathrm{Mor}_K(S_{K/k}, V)$ (representable by the assumption V quasi-projective).

example(1) : $S = \mathrm{Spec}(k)$ $\quad \mathrm{Mor}_K(S/_K, V) = V(K)$, the K points of V
$S/_K = \mathrm{Spec}(K)$ $\quad \mathrm{Mor}_k(S, R_{K/k}V) = R_{K/k}(V)(k)$, the k points of $R_{K/k}(V)$.

so $W = R_{K/k}V$ satisfies $W(k) \simeq V(K)$.

Hence, can determine W as follows: suppose V affine, $\phi_\alpha(x) = 0$ (with coefficients in K) the defining equations. Take a basis $\{e_i\}$ for K/k. Then W is defined by the equations $\Phi_{\alpha,i}(\xi) = 0$ where $\phi_\alpha(x) = \phi_\alpha(\sum \xi e) = \sum \Phi_{\alpha,i}(\xi) e_i$ $(x^j = \sum \xi_i^j e_i)$.

— o —

<u>An Alternate Definition</u>

The variety W is given with an isomorphism $i : W/_K \xrightarrow{\sim} V$.
$(\mathrm{id} \in \mathrm{Hom}_k(R_{K/k} V, R_{K/k} V) = \mathrm{Hom}_K((R_{K/k} V)_K, V))$

Take k_s = a separable closure of k, and Σ the embeddings
$$\sigma_j : K \hookrightarrow k_s \qquad j = 1, \dots, d = [K:k]$$
So V^σ is defined over k_s $(\sigma \in \Sigma)$

Then i defines a map $i^\sigma : W/_{k_s} \to V/_{k_s}$.

Then:

$$(i^\sigma) : W/_{k_s} \xrightarrow{\sim} \prod_{\sigma \in \Sigma} V^\sigma/_{k_s}$$

This now defines W (over k_s), and by taking Galois fixed pts (note there is a natural Galois action on the right), one recovers W/k. ✓

— o —

Take now K/k global fields. Then

$$W(\mathbb{A}_k) \simeq V(\mathbb{A}_K).$$

In practice, the use of this is in considering varieties which arise naturally as the restriction of scalars of something simpler. For example, let k be a field, G over k a semi-simple (connected, smooth), which is either adjoint or simply connected (i.e. over an algebraic closure where the root theory applies, T = a max. torus $\simeq \mathbb{G}_m^n$, X the character group $\simeq \mathbb{Z}^n$, then $\underset{\text{roots}}{R} \subset X \subset \underset{\text{weights}}{P}$ then

G is adjoint if $X = R$ (i.e. center is $\{1\}$ as a subscheme), G is simply connected if $X = P$ (i.e. no non-trivial "coverings", again as a scheme).

Then we have the definitions:

(a) G is simple if $G \neq \{1\}$ and G has no normal subgroups over k other than $\{1\}$ and G, e.g. PGL_2

(b) G is absolutely simple if G is simple over k_s, a separable closure of k e.g. PGL_2.

(c) G is "almost (resp. absolutely) simple" if $G \neq \{1\}$ and if every normal subgroup $(\neq G)/k$ is finite, e.g. SL_2 (respectively, over k_s).

The adjoint group of an absolutely almost simple is absolutely simple. (and conversely).

Also equivalent: an absolutely almost simple group is one with an irreducible root system (so $\simeq A_\ell, B_\ell, \ldots, E_8$ etc).

Claim: If as above, G is either adjoint or simply connected, then G can be decomposed ($G = \prod G_\alpha$) where $G_\alpha = R_{K_\alpha/k} S_\alpha$ where S_α is absolutely almost simple over K_α and S_α is (adjoint (resp. simply connected) if G is.

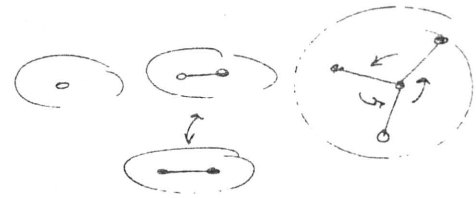
Remark: hence the computation of Tamagawa numbers is reduced to the study of absolutely almost simple groups.

Proof: over k_s, the root system = sum of irreducible systems (in a unique way), (say Ω = the set of irred. components of the graph of the roots; these are the irred. systems).

$\mathfrak{g}$.
$\|$

Then $Gal(k_s/k)$ acts on the graph, hence on Ω.
Write

$$\Omega = \bigcup_\alpha \Omega_\alpha ,$$



Ω_α = the orbits under $\mathfrak{g}$;
$\Omega_\alpha = \mathfrak{g}/\mathfrak{g}_\alpha$, $\mathfrak{g}_\alpha$ the isotropy gp. of a point in Ω_α, say ω_α

Define then K_α = the fixed field of $\mathfrak{g}_\alpha$
$\cancel{S}G_\alpha$ = the factor of G relative to ω_α,
so defined over K_α.
This then gives the claim.

Remark: in general, the root system does not define the group: The roots define two lattices, $\underset{\text{roots}}{\overset{\|}{R}}$, $\underset{\text{weights}}{\overset{\|}{P}}$, and intermediate lattices defines isogenous groups. Here we have $R = \bigoplus_{\omega\in\Omega} R_\omega$
$P = \bigoplus_{\omega\in\Omega} P_\omega$

Hence, if X is either R or P (adjoint or simply connected), then we get a corresponding decomposition for G ✓
e.g. SO_4 is not of this type (corresponds to a lattice strictly between R and P. [however, $SO_4/\{\pm 1\} = SO_3 \times SO_3$ if (discr. a square)
or $= R_{K/k}\, SO_3$
(with K a quadratic extension of k, $K = k\sqrt{\text{discr}}$ if discr. not a square]
(exercise).
This reduces quadratic forms in 4 variables to 3 variables.

Algebraic Groups and Adelic Points

Let G be an algebraic group over the global field K (G smooth is assumed).
Then we have the adelic points of G;

$$G_{\mathbb{A}} = G(\mathbb{A}) \supset G(K). \qquad \mathbb{A} = \mathbb{A}_K$$

Then $G_{\mathbb{A}}$ is locally compact, and $G(K)$ is discrete in $G(\mathbb{A})$ if G is a linear group. [More generally if V is affine or quasi-affine then $V(K)$ is discrete in $V(\mathbb{A})$].

? This is not true for an abelian variety G with $G(K)$ infinite. (since this is projective).

—— o ——

Abelian varieties

cf. S. Bloch (Inv. M. 1980)

Let B be an abelian variety over K.

Recall that $\mathrm{Ext}^1(B, \mathbb{G}_m) \simeq B^\wedge(K)$, $B^\wedge$ the dual variety of B
(classifies $0 \to \mathbb{G}_m \to * \to B \to 0$) $= \mathrm{Pic}^0(B)$
and $B^\wedge(K)$ is finitely generated.
So consider an extension:

$$1 \to \mathbb{G}_m^h \to G \to B \to 1$$

Then G is determined by $(\alpha_1, \dots, \alpha_h)$, $\alpha_i \in B^\wedge(K)$, i.e. this extension is associated to a map

$$\alpha : \mathbb{Z}^h \to B^\wedge(K).$$

Theorem (Bloch): (1) $G(K)$ is discrete in $G(\mathbb{A}_K) \Leftrightarrow$ Coker α is finite

(2) If $G(K)$ is discrete in $G(\mathbb{A}_K)$, then

$$G(\mathbb{A}_K)/G(K) \text{ is compact} \Leftrightarrow \operatorname{Ker} \alpha = 0.$$

example: $h = \operatorname{rank}(B^\wedge) = \operatorname{rank}(B)$, $\alpha_1, \ldots, \alpha_h$ indep. in $B^\wedge(K)$. Then the corresponding G must have $G(K)$ discrete in $G(\mathbb{A}_K)$ with compact quotient.

The exact sequence on groups is exact on points: (since $\mathbb{G}_m$!)

$$\begin{array}{ccccccccc} 1 \to & (K^*)^h & \to & G(K) & \to & B(K) & \to 1 \\ & & & \cap \text{ discrete here;} & & \vdots \text{ dense in here} & \\ 1 \to & (I_K)^h & \to & G(\mathbb{A}_K) & \to & B(\mathbb{A}_K) & \to 1 \end{array}$$

Remark: the proof of the Theorem reduces to showing that the theorem is essentially equivalent to the non-degeneracy of the Néron-Tate bilinear form on $B^\wedge(K)$.

— o —

We shall always assume G is a linear group (i.e. affine), which is smooth (frequently connected as well).

The embedding $G(K) \hookrightarrow G(\mathbb{A}_K)$ raises several density questions:

(1) Weak density property : Let S be a finite set of places.
(= Weak approx. property)

Then the weak density property is the statement
"the image of $G(K)$ in $\prod_{v \in S} G(K_v)$ is dense".

This property does not hold for all groups (even for tori!). There are several cases where this property does hold, e.g.:

(a) G is a "rational variety over K", i.e. is birationally equivalent to some projective space $\mathbb{P}_N$, i.e. there is an open subvariety of G which is isomorphic to a non-empty open subvariety of $\mathbb{P}_N$. (G connected here).

examples : (i) $\mathbb{G}_a$ (v) SO_n
(ii) $\mathbb{G}_m$ (vi) Sp_{2n}
(iii) SL_n
(iv) GL_n

(e.g. SL_n : n^2 coord's a_{ij}, $\det(a_{ij}) = 1$, which can be written a_{11} = a rat'l function of the others, so SL_n is birationally $\simeq$ to A^{n^2-1} via the a_{ij}, $a_{ij} \neq a_{11}$).

(e.g. SO_n : Cayley transformation. $SO_n \leftrightarrow$ any non-degenerate quadratic form ($ch.(K) \neq 2$); $U^*U = 1$
U^* = the adjoint of U w.r.t. the bilinear form, with $\det U = 1$ defines SO_n.

Then if U has no eigenvalue equal to -1, then U can be written uniquely as $U = \frac{1+V}{1-V}$ $\left(V = \frac{U-1}{U+1}\right)$, $V^* = -V$.
Then SO_n is birationnally equivalent to the vector space of V with $V^* = -V$.
(= Cayley "parametrization")
This is the Cayley transformation (applicable only on an open subspace). This is clearly linear now ✓)

Remark: Showing a group G does not have weak approximation then shows G is not rational!

Proof of Weak Approx. for G rational: Since G is smooth, if U is (Zariski) open in G, then $U(K_v)$ is dense in $G(K_v)$.
Then

$$\begin{array}{ccc} G(K) & \to & \prod_S G(K_v) \\ \cup & & \cup \\ U(K) & \to & \prod_S U(K_v) \end{array}$$

so it is enough to show $U(K)$ is dense in $\prod U(K_v)$. But then we may (by rationality) take $U \simeq$ an open subset in affine space, and the result is well-known in this case.

(b) If $S = \{$Archimedean places$\}$, then W_S holds

(c) If G is semisimple and simply connected, then W_S holds.

(2) Strong Approximation: Let S be a finite set. Then
(or Strong Density) $\mathbb{A}_K = \prod_{v\in S} K_v \times \mathbb{A}_{K,S}$, $\mathbb{A}_{K,S} = \prod_{v\notin S}' K_v$.

Then the Strong approximation property (Str_S) is the property: "$G(K)$ is dense in $G(\mathbb{A}_{K,S})$".
Equivalently,
"$G(K)\prod_{v\notin S} G(K_v)$ is dense in $G(\mathbb{A}_K)$".

so that $S\cup\Sigma$ is a set containing the Arch. places

(concretely, given any $(g_v)\in G(\mathbb{A}_K)$, Σ a finite set of places disjoint from S and U_v a neighborhood of g_v ($v\in\Sigma$), then there is a $\gamma \in G(K)$, $\gamma \in U_v$ for all $v \in \Sigma$ and $\gamma \in G(\mathcal{O}_v)$ for all $v \notin S \cup \Sigma$

Examples (and counterexamples!):

(a) $G = \mathbb{G}_a$, the additive group. Then Str_S is true for all S ($\neq \emptyset$).

Proof (by duality): Assume $G(K)\prod_{v\in S} G(k_v)$ not dense in $G(\mathbb{A}_K)$. Then

$$\Big(\prod_{v\in S} k_v\Big) + K \quad \text{is not dense on } \mathbb{A}_K$$

$\underset{\text{Pontryagin duality}}{\Rightarrow}$ $\exists$ a character ψ of $\mathbb{A}_K$, $\psi \neq 1$, with $\psi = 1$ on $(\prod_{v\in S} k_v) + K$.

But the characters trivial on K are known;

$\Rightarrow \quad \psi(a) = \psi_0(\lambda a)$ for some $\lambda \in K^*$.

and since $\psi_{0,v} \neq 1$, this character cannot be trivial on $\prod_{v\in S} K_v$ ✓.

(b) false for $\mathbb{G}_m$, false for GL_n

(c) true for SL_n, Sp_{2n}

(d) false for SO_n $(n \geq 2)$

-5-81

In (b) above, Str_S is false (for any S): Assume S contains the Archimedean primes. Were $G(K)$ dense, then the projection $\pi_S : G^{(K)} \to \prod_{v\notin S} G(k_v)$ satisfies

$$\pi_S(G(K)) \cap \underset{\uparrow\,(\text{open, compact})}{\prod_{v\notin S} G(\mathcal{O}_v)} \quad \text{is dense in } \prod_{v\notin S} G(\mathcal{O}_v).$$

For $G = \mathbb{G}_m$, $\pi_S(\mathbb{G}_m(K)) \cap \prod_{v\notin S} \mathbb{G}_m(\mathcal{O}_v) = \Gamma_S$ = the S-units of K

so the question becomes: are the S-units dense in $\prod_{v \notin S} \mathcal{O}_v^*$?
No, since the S units are finitely generated, whereas $\prod_{v \notin S} \mathcal{O}_v^*$ is not even topologically finitely generated [e.g. if $ch(K) \neq 2$, then $\prod_{v \notin S} \mathcal{O}_v^* \to \prod_{v \notin S} k_v^* \xrightarrow{\text{Legendre}} \{\pm 1\}^{\aleph_0}$]
residue fields

exercise: Consider $\prod_{p \notin S} \mathbb{Z}_p^\times \simeq \left(\prod_{p \notin S} \mathbb{Z}_p\right) \times T$
S finite

where

$$T = \prod_{m=1}^{\infty} \mathbb{Z}/m\mathbb{Z} = \prod_{p, n \geq 1} (\mathbb{Z}/p^n\mathbb{Z})^{\aleph_0} .$$

and prove an analogous result for any global field.

Remark (exercise): Use multiplicative characters to prove the failure of strong approximation for $\mathbb{G}_m$: $S \supset \Sigma^\infty$, want to show $\left(\prod_{v \in S} K_v^\times\right) \cdot K^\times$ is not dense in I_K (the ideles). Want a continuous character $\chi : I_K \to$ finite group (say) $\chi = 1$ on $\left(\prod_{v \in S} K_v^\times\right) \cdot K^\times$, $\chi \neq 1$. By class field theory, any reasonable cyclic extension E/K of degree ≥ 2 will produce such a character:

(a) always $\chi(K^\times) = 1$
(b) need only insure that every prime in S splits completely in E.

Such an E can always be constructed, e.g. ($ch K \neq 2$), take $E = K(\sqrt{\alpha})$, $\alpha \notin K^{\times 2}$, α a square in each $K_v^\times$, $v \in S$ (by weak approximation!), and similar arguments apply if $ch(K) = 2$.

In (c) above, Str_S is true for SL_n, Sp_{2n}, as follows:
Let

$$\Omega = \prod_{v \in S} G(K_v) \cdot G(K)$$

$$\bar{\Omega} = \text{the closure of } \Omega \text{ in } G(\mathbb{A}_K)$$

(want to show $\bar{\Omega} = G(\mathbb{A}_K)$): Show that for any $G(K_v)$, $v \in \Sigma$ we have $G(K_v) \subset \bar{\Omega}$. (view $G(K_v) \subset G(\mathbb{A}_K)$ by $g_v \mapsto (1, 1, \dots 1, \underset{\text{at } v}{g_v}, 1, \dots)$.)

Since Ω is a subgroup [$= \pi_S^{-1}(\pi_S G(K))$ in previous notation], this suffices to show $\bar{\Omega} = G(\mathbb{A}_K)$.

If $G(K_v)$ is generated by elements $(g_v^{(i)})$, it suffices to prove $g_v^{(i)} \in \bar{\Omega}$.

For SL_n, generators are $e_{ij}(\alpha)$ ($= I + \alpha$ in ij^{th} position), $i \neq j$, $\alpha \in k$
So consider $e_{ij}(\alpha)$, $i \neq j$, $\alpha \in K_v$ and show $e_{ij}(\alpha) \in \bar{\Omega}$; have
$G_a \hookrightarrow SL_n$ ("root subgroup" attached to i, j). By strong approximation
$\alpha \longmapsto e_{ij}(\alpha)$
for G_a, this shows $e_{ij}(\alpha) \in \bar{\Omega}$ ✓.

Remark: The same argument therefore works for any (simply connected, semisimple) "split" (or "Chevalley") group, i.e. has a maximal torus $\simeq (G_m)^l$, $l =$ rank. [semi-simplicity is used to insure that locally the group is generated by it's root systems].

Theorem (Kneser-Platonov): ($K =$ number field) Suppose G is almost simple. Then a necessary and sufficient criteria for Str_S to hold for G is
(a) G is simply connected (recall all G are assumed semisimple and connected)
(b) there exists a $v \in S$ such that $G(K_v)$ is not compact
($\Leftrightarrow \prod_{v \in S} G(K_v)$ is not compact)

Remark: Prasad (Annals 1977) has proved that $\mathrm{Str}_S \Leftarrow$ simply connected in the function field case.

cf. Borel, Symp. AMS, 1966 (Kneser)
Platonov, Isv., 1969
Prasad, Annals, 1977.

Idea of proof: $\underbrace{\underbrace{G(K)}_{\text{discrete}}\underbrace{\prod_{v\in S} G(K_v)}_{\text{compact}}}_{\Downarrow \text{ closed}}$ dense in $G(A_K)$

$$\Rightarrow \quad G(K)\prod_{v\in S} G(K_v) = G(A_K).$$

Hence: $\underset{\text{denumerable!}}{G(K)}$ maps onto $\underset{\text{not denumerable!}}{\prod_{v\notin S} G(K_v)}$ $\Rightarrow$ condition (b) is necessary.

For simple connectedness;

$$1 \to \Phi \to \tilde{G} \to G \to 1 \qquad \tilde{G} = \text{simply connected covering of } G$$

(where Φ is a non-trivial finite subgroup of $\tilde{G}$, contained in the center of G). Assume Φ is étale. Then

$$\tilde{G}(A_K) \to G(A_K)$$

gives
$$\begin{array}{ccccc} \tilde{G}(\mathbb{A}_K) & \to & G(\mathbb{A}_K) & \to & \prod H^1(K_v, \Phi) \\ \uparrow & & & & \uparrow \\ \tilde{G}(K) & \to & G(K) & \longrightarrow & H^1(K, \Phi) \end{array}$$

(the product is restricted w.r.t. the subgps $H^1_{\text{unramified}}(\mathcal{O}_v, \Phi)$).

The group $\prod H^1(K_v, \Phi)$ is locally compact, with $\prod_v H^1_{\text{unram.}}(\mathcal{O}_v, \Phi)$ open and compact.

The image of $H^1(K, \Phi)$ is a discrete subgroup in $\prod H^1(K_v, \Phi)$.

The cokernel of $G(\mathbb{A}_K)$ is finite.

Were the Strong Density property true for G, then an induced density property would hold for $H^1(K, \Phi)$. This reduces the problem ~~of~~ to showing that $\phi \neq 1 \Rightarrow \prod_{v \notin S} H^1_{\text{unramified}}(K_v, \Phi)$ is infinite (which is done by using v's for which Frobenius acts trivially on the Galois module) //

This gives the result for (d) above

—o—

Special Cases of Strs:

Let M be a central simple algebra over K. Then the multiplicative group of M, $\mathbb{G}_{m,M}$ gives a K-algebraic group, namely, for any commutative K-algebra K',
$$\mathbb{G}_{m,M}(K') = K' \otimes_K M$$

(in particular, $\mathbb{G}_{m,M}(K) = M^*$).

<u>example</u>: If $M = M_n$, then $G_{m,M} = GL_n$
($n \times n$ matrices).

This allows a generalization of SL_n: take the reduced norm map for M; $G_{m,M} \to G_m$ (basically, after extension of scalars to split M, the reduced norm is the determinant; one checks it is in fact defined over k). Define then;

$$G^{(1)}_{m,M} \text{ (or } SL_M) = \text{the kernel of the reduced norm map.}$$

(Note that after an extension of scalars it becomes isomorphic to SL_n).
Then $G^{(1)}_{m,M}$ is almost simple ($n \geq 2$) and is simply connected. (since this is the case after extension of scalars).

It follows that the strong approximation property holds for $G^{(1)}_{m,M}$ if there exists a v, $v \in S$ such that $G^{(1)}_{m,M}(K_v)$ is not compact (ie. there exists a v, $v \in S$ with $K_v \otimes_K M$ <u>not</u> a division algebra). This is a Theorem of Eichler.

— o —

For $Spin_n$: ($n \neq 1,2,4 \Rightarrow$ almost simple), simply connected, and non-compact at $v \Leftrightarrow$ the quadratic form represents 0 at v, eg. if $S = \Sigma^\infty$, then the quadratic form should be "indefinite" at at least one Archimedean place.

— o —

Non-semisimple groups (over a number field):

Recall that for connected linear algebraic groups G there is a normal unipotent subgroup U ($\sim \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$, i.e. $\simeq$ successive extensions of $\mathbb{G}_a$) such that G/U is a "reductive" group (i.e. has no non-trivial unipotent normal subgroups).

In characteristic 0, reductive is equivalent to having only semisimple representations.

Generally, if C is the center of G, $C^0 = T$ its connected component, then T is a "torus" (i.e. isomorphic over $\bar{k}$ to copies of $\mathbb{G}_m$: $\mathbb{G}_m \times \ldots \times \mathbb{G}_m$), and then G is reductive $\Leftrightarrow$ G/T is semisimple. For arbitrary G, there is an exact sequence $1 \to U \to G \to G/U \to 1$ with unipotent U and reductive G/U, which splits due to the presence of the "Levi subgroup" of G, so G is always the semi-direct product (unipotent).(reductive), and a reductive group is always isogenous to (torus) $\times$ (semisimple); in fact, G reductive $\Leftrightarrow$ $G = T.S$, T torus, S semisimple, with $S \cap T$ finite (and then $S \times T \to G$ gives the isogeny), so there is an exact sequence $1 \to$ torus $\to$ reductive $\to$ semisimple (a quotient of S here) $\to 1$.

(example: $G = GL_2$, $T = \mathbb{G}_m$, $S = SL_2$: $G = T.S$ and $T \cap S = \{\pm 1\}$

the exact sequence $1 \to$ torus $\to$ reductive $\to$ semisimple $\to 1$ in this case is then $1 \to \mathbb{G}_m \to GL_2 \to PGL_2 \; (= SL_2/\{\pm 1\}) \to 1$).

Hence, since unipotent groups offer no obstruction to strong approximation (by example (a)), it follows for arbitrary G that

"Str_S is valid for G $\Leftrightarrow$ G/U is semisimple, simply connected and for each α, $\prod_{v \in S} G_\alpha(K_v)$ is not compact

(where $G/U \simeq \prod G_\alpha$, G_α simple)."

§ Adeles, Classes, and Genera

Let K be a global field and let V be a finite dimensional vector space over K. Let GL_V be the linear group of V (the "multiplicative group of End V" in the notation above). Suppose i is a homomorphism $i: G \to GL_V$ which has a finite kernel.

Let S be a finite set of places, $S \supset \Sigma^\infty$, $S \neq \emptyset$, and set $\mathcal{O}_S$ = the ring of S-integers in K. Then $\mathcal{O}_S$ is a Dedekind ring with quotient field K.

A "lattice" in V is an $\mathcal{O}_S$-module M in V, finitely generated over $\mathcal{O}_S$, such that $K \otimes_{\mathcal{O}_S} M \cong V$. (i.e. M generates V as a vector space).

Since $\mathcal{O}_S$ is Dedekind, M is projective of rank n ($n = \dim V$).

Definition: Two $\mathcal{O}_S$-lattices M, N in V are said to be in the same "genus" (w.r.t. G) if for every $v \notin S$, there exists a $g_v \in G(K_v)$ with $g_v(M_v) = N_v$, where $M_v = \mathcal{O}_v \otimes M$, $N_v = \mathcal{O}_v \otimes N$, i.e. M and N are G-equivalent locally everywhere outside S. (which is the same as saying $M_v \cong N_v$ over $\mathcal{O}_v$ for all $v \notin S$

— o —

11-10-81 Remark on Strong Approximation: $St_S \Rightarrow$ no étale central isogeny ($\neq 1$) above G, i.e. no finite étale $W \neq 1$ with $1 \to W \to \tilde{G} \to G \to 1$ ($W \subset$ center of G, connected). In ch. 0, this implies semisimple (a torus gives such a W, since $1 \to W \to \tilde{G} \to G \to$ $\tilde{G}$ simply connected, $W = \pi_1(G)$, always étale in ch. 0). In characteristic 2, however, $SL_2 \to PGL_2$ gives a non-trivial isogeny, Kernel $= \mu_2$, which has

only one point in ch. 2 (with nilpotence), so Galois cohomology of itself
will not give the result $Str_S \Rightarrow G$ simply connected. Problem: prove this implication for general K (perhaps using more sensitive cohomology).

exercise on Strong Approximation: $G/\mathbb{Q}$ reductive, connected. Then $G(\mathbb{F}_p)$ is well-defined for almost all p. ($p \notin S$, say). Then $\prod_{p\notin S'} G(\mathbb{F}_p) = X$ is a profinite group. Show

(1) If G is simply connected (semisimple), then X is topologically finitely generated

(2) If G is not simply connected, then X has a quotient group isomorphic to $\mathbb{Z}/l\mathbb{Z} \times \dots \times \mathbb{Z}/l\mathbb{Z} \times \dots$ ($\aleph_0$ copies) for some prime number l; hence X is not (topologically) finitely generated.

— o —

Definition two $\mathcal{O}_S$ lattices M and N are "Gisomorphic" (or "in the same class) if there exists $\gamma \in G(K)$ with $\gamma M = N$.

Hence each genus consists of classes of equivalent (i.e. G-isomorphic) lattices.

Lemma: The Classes in the genus of M are isomorphic to

$$G(K) \backslash G(\mathbb{A}_K) / \prod_{v\in S} G(K_v) \times \prod_{v \notin S} G_M(\mathcal{O}_S)$$

(where $G_M(\mathcal{O}_v)$ is the stabilizer of M_v in $G(K_v)$, i.e. the elements of $G(K_v)$ which have coefficients in $\mathcal{O}_v$ with respect to a basis of M_v (and have determinant in the units $\mathcal{O}_v^\times$)).

Proof: Suppose N is in the genus of M. For each $v \notin S$, choose $g_v \in G(K_v)$ with $g_v M_v = N_v$. Then the association of the Lemma is given by

$$N \to g \in G(\mathbb{A}), \quad g = (\underbrace{1,\dots,1}_{S}, \underset{v \notin S}{(g_v)})$$

Then for almost all v, $M_v = N_v$, so for almost all v, $g_v \in G_M(\mathcal{O}_v)$, so g_v is "integral", hence g is in fact in $G(\mathbb{A})$.

Any g_v is defined only up to multiplication by h_v, $h_v \in G_M(\mathcal{O}_v)$, so there is a well-defined map

$$\text{set of } N \mapsto G(\mathbb{A}) \Big/ \prod_{v \in S} G(K_v) \times \prod_{v \notin S} G_M(\mathcal{O}_v)$$

This map is in fact bijective. Injectivity is clear since the lattice N is uniquely defined by knowledge of all the N_v ($x \in V$, $x \in N \iff$ for all $v \notin S$, $x \in N_v$). For the surjectivity given $g = (g_v)$, $g \in G(\mathbb{A})$, define $N_v = g_v M_v$ for all $v \notin S$. Then N_v is an $\mathcal{O}_v$-lattice and $M_v = N_v$ for almost all v. But this then defines a global lattice N with $(N)_v = N_v$ (i.e. $\mathcal{O}_v \otimes N = N_v$ for all $v \notin S$).

When are two such $\mathcal{O}_S$-lattices N G-equivalent? By definition precisely when the corresponding elements in $G(\mathbb{A}) / \prod_{v \in S} G(K_v) \times \prod_{v \notin S} G_M(\mathcal{O}_v)$ are (left) equivalent by an element in $G(K)$. This proves the Lemma.

<u>Definition</u>: For convenience, let $\Omega = \prod_{v \in S} G(K_v) \times \prod_{v \notin S} G_M(\mathcal{O}_v)$

<u>Remark</u>: Borel (I.H.E.S. ~ 1963) showed that $G(K) \backslash G(\mathbb{A}) / \Omega$ is <u>finite</u> if K is a number field.

— o —

Tensors

K and V as above. Let $(x_\alpha) \in \otimes^{r_\alpha} V \otimes^{s_\alpha} V^*$ be a collection of tensors, denoted $x \in TV$. Let G be the subgroup of GL_V which fixes x, so the initial data given is: (V, x), and G.

examples: (a) $G = GL_V$ $(x = 0)$

(b) $G = SL_V$ (x - non-degenerate alternating form in n variables)

(c) $G = O_V$ (x = quadratic form)

(d) $G = SO_V$ (x = quadratic form and a non-zero element in $\Lambda^n V$)

(e) $G = S_p$

Remark: in fact any reductive group can be defined as the invariance group of some set of tensors.

Then we shall be interested in pairs (M, x_M) where M is a projective $\mathcal{O}_S$-module of rank n and $x_M \in T(K \otimes_{\mathcal{O}_S} M)$, such that after extension from $\mathcal{O}_S$ to K, $(M, x_M) \simeq (V, x)$, and their associated classes and genera.

examples: (a) above: $\mathcal{O}_S$ - projective modules of rank n

(b) SL_V alternatian form

(c) O_V quad. form with rational coeff's which is a given one over K.

etc.

Then the classes of such pairs are defined by:

$$(M, x_M) \overset{\text{class}}{\sim} (N, x_N)$$

if there is an isomorphism $(M, x_M) \xrightarrow{\gamma} (N, x_N)$, i.e. γ is an $\mathcal{O}_S$ isomorphism $M \to N$ and $\gamma x_M = x_N$.

The genera are defined by local isomorphisms, i.e. (M, x_M) and (N, x_N) are in the same genus if for all $v \notin S$, there is an $\mathcal{O}_v$ isomorphism $\gamma_v : (M_v, x_M) \xrightarrow{\sim} (N_v, x_N)$ (i.e. $\gamma_v : M_v \simeq N_v$ and $\gamma_v x_M = x_N$).

— o —

These two points of view of classes and genera are in fact equivalent:

Let (M, x_M) be a pair of the type considered above (so $(M, x_M) \xrightarrow{\sim} (V, x)$ after extension of $\mathcal{O}_S$ to K). Choose an isomorphism $K \otimes M \xrightarrow{\sim} V$. Then M becomes an $\mathcal{O}_S$-lattice in V and x_M becomes x.

Then similarly (N, x_N) are viewed as: $N \subset V$ (as an $\mathcal{O}_S$-lattice) with $x_N = x$.

The elements (M, x_M), (N, x_N) are in the same class if $\exists\, \gamma \in GL_V(K)$ with $\gamma M = N$, $\gamma x = x$, so $\gamma \in G(K)$, so this definition agrees with the previous notion.

The elements (M, x_M), (N, x_N) are in the same genus if for all $v \notin S$, there is a $\gamma_v : M_v \xrightarrow{\sim} N_v$, $\gamma_v x_M = x_N$. Then

$\gamma_v = g_v \in GL(V_v)$, $g_v M_v = N_v$, $g_v x = x$ and so $g_v \in G(K_v)$ and again the notions of genus agree.

— o —

example: M = an $\mathcal{O}_S$ projective module of rank n, with F a quadratic form on $K \otimes M$ (the interesting case is when F is "integral": Cassels's clarification: "integral" means $F(m) \in \mathcal{O}_S$ for all $m \in M$, "classically integral" means the associated bilinear form is integral, i.e. $\frac{1}{2}\{F(m+m') - F(m) - F(m')\} \in \mathcal{O}_S$ for all $m, m' \in M$ (assuming ch $\neq 2$). e.g. $x^2 + xy + 6y^2$ is "integral" but not "classically integral" (which correspond to symmetric matrices with integer entries - as in Gauss).

The condition required on M and $x = F$ is that over K, M becomes isomorphic to a given (V, F).

Then (N, Q_N), (M, Q_M) are in the same genus means

(a) N and M are K-isomorphic (to V)

(b) N_v and M_v are isomorphic over $\mathcal{O}_v$ (for all $v \notin S$).

By Hasse-Minkowski, locally equivalent quadratic forms (at all places) are globally equivalent.

Let (a_S) be the statement $K_v \otimes M \cong K_v \otimes N$ for all $v \in S$. Then by Hasse-Minkowski, (a) + (b) above is equivalent to $(a_S) + (b)$

Remark for $S = \emptyset$ (so K = function field), $\mathcal{O}_S = \mathbb{F}_q$, so the definition of classes and genera are modified slightly, using vector bundles. Let n be an integer, $n \geq 1$. Then

$$\begin{array}{c}\text{classes of dimension } n \\ \text{vector bundles over } C \\ (C_{/\mathbb{F}_q} \text{ the curve} \leftrightarrow K/\mathbb{F}_q)\end{array} = GL_n(K) \backslash GL_n(\mathbb{A}) / \prod_v GL_n(\mathcal{O}_v)$$

as follows:

Let $V = K^n$, $\mathcal{M} = \{M_v\}_v$ where M_v is an $\mathcal{O}_v$-lattice in $K_v \otimes V = K_v^n$ and such that $M_v = \mathcal{O}_v^n$ for almost all v.

Then define $\underset{\text{same class}}{\mathcal{M} \sim \mathcal{N}}$ if there is a $\gamma \in GL(V)$ with $\gamma M_v - N_v$ for all v.

Then there is a bijection $G(K)\backslash G(\mathbb{A})/\prod G(\mathcal{O}_v)$ $(G = GL_n)$ $\leftrightarrow$ classes of $\mathcal{M}$, via: for every vector space, can choose a $g_v \in GL_n(K_v)$ such that $g_v \mathcal{O}_v^n = M_v$, this gives the adele, and the set of $\mathcal{M}$'s is then $GL_n(\mathbb{A})/\prod_v GL_n(\mathcal{O}_v)$, and classes correspond as before to equivalence under $G(K)$ on the left.

Let now E be a vector bundle of rank n over the curve C (i.e. a locally free sheaf of rank n over the sheaf of rings $\mathcal{O}_C$). Let $\mathcal{O}_v^{alg}$ be the algebraic local ring at v in K (i.e. $\{f \in K \mid v(f) \geq 0\}$, i.e. the rational functions holomorphic at v). Then E_v^{alg} are $\mathcal{O}_v^{alg}$- free modules of rank n. $E(K)$, the stalk at the generic point K = the rational sections of E, $\dim E(K) = n$.

Choose a basis of $E(K)$, $E(K) \simeq K^n$.

Then $E_v^{alg} \subset E(K)$ as an $\mathcal{O}_v^{alg}$ submodule of rank n

Let then M_v = the completion $\mathcal{O}_v \otimes_{\mathcal{O}_v^{alg}} E_v^{alg}$

and

$$\mathcal{M}_E = \{M_v\}$$

Then $\mathcal{M}_E$ is an "$\mathcal{M}$" of the type considered above., and further, it is a fact that any $\mathcal{M}$ comes from a suitable vector bundle E: given M_v, $\mathcal{O}_v$, define $E_v^{alg} = K^n \cap M_v$; this gives a sheaf and vector bundle cf. Weil, 1936, (C.P. vol I) Généralité des fonctions abéliennes : considers an analogue of Jacobian for n-dimensional manifolds, gives a bijection between classes of vector bundles and "matrix divisors" (our $G(K)\backslash G(A)/\prod G(k_v)\times\prod G_\mu(O_v)$) etc.

Remark : classes of n-dim'l vector bundles with trivial Chern class $\overset{\longleftrightarrow}{\text{more or less}}$ $SL_n(K)\backslash SL_n(A)/\prod SL_n(O_v)$

⇒ not usually finite
since over any curve ∃ ∞ly many vector bundles of given degree
$(S=\emptyset)$

— o —

Remark : If G has Str_S, then there is only one class per genus, i.e. $G(K)\backslash G(A)/\Omega = 1$, i.e.

$$G(A) = G(K)\prod_{v\in S} G(k_v)\times\prod_{v\notin S} G_\mu(O_v)$$

since $Str_S \Rightarrow G(K)\prod_{v\in S}G(k_v)$ is dense

and $\prod_{v\in S} G(k_v)\times\prod_{v\notin S} G_\mu(O_v)$ is open

} R.H.S. is both dense and open, hence equal:

(Lemma : if A, B are subgroup, A dense, B open, then $A.B$ = whole group. Indeed, if $g\in G$, then $g.B\cap A\neq\emptyset$.)

— o —

2-81 Adelic Measures

Let V be an algebraic variety defined over K. Then the "adelic measures" on V are the measures on $V(A_K)$.

Assume that V is <u>smooth</u> over K, everywhere of dimension n. Let ω be a differential form on V of degree n, which is nowhere 0. Then on each $V(K_v)$, we have a measure $|\omega|_v$: recall the def^n of ω depends on the chosen Haar measure on K_v: $(\mathbb{R}, dx)$, $(\mathbb{C}, 2dxdy)$, (K_v p-adic, $\int_{O_v} |dx|_v = 1$). Locally, $\omega = f\, dx_1 \wedge \ldots \wedge dx_n$ and the measure is defined by $|\omega|_v = |f|\,|dx_1|_v \ldots |dx_n|_v$.

Then on any <u>finite</u> product $\prod_{v \in S} V(K_v)$, the measure $\bigotimes_{v \in S} |\omega|_v$ is well-defined.

Choose a model $\tilde{V}$ for V over O_S (for some S), and then for $v \notin S$, $\mathcal{V}(O_v) = V(O_v)$ (by abuse, since $V(O_v)$ is not uniquely defined independent of the choice of a basis), open and compact in $V(K_v)$.

If ω has "good reduction" w.r.t. $\mathcal{V}$, then

$$\int_{V(O_v)} |\omega|_v = \frac{1}{q_v^n} \left(\#\text{elements in } \mathcal{V}(\kappa_v)\right)$$

where κ_v is the residue field of K_v, $q_v = N_v = |\kappa_v|$.

(Recall that ω has "good reduction" if:

(a) ω is "integral over O_v"; section of the sheaf of differential forms of $\mathcal{V}$ ($\mathcal{V}$ smooth)

(b) reduction mod π_v is nowhere 0 on $\mathcal{V} \otimes \kappa_v$.)

Generally, if X_i are compact spaces, $X = \prod X_i$ and each X_i has (positive) measure μ_i, how to construct a measure on X? If all the μ_i have mass 1, $\otimes \mu_i = \mu$ can be defined: $\int f\mu = \int_{\prod X_i} f(\otimes \mu_i)$ if f depends only on a finite number of variables $x_j \in J$. (f cont.). This is the model to follow;

"<u>Convergent Case</u>":

Let $c_i = \int_{X_i} \mu_i = \mu_i(X_i)$ (all μ_i are $\neq 0$)

Suppose $\prod_{i \in I} c_i$ is <u>convergent</u> ($\overset{\text{limit}}{\neq 0, +\infty}$) (i.e. the series $\sum \log c_i$ is absolutely convergent). Then in this case, $\otimes \mu_i$ is defined: $\prod c_i \otimes \left(\frac{\mu_i}{c_i}\right) = \otimes \mu_i$ as above; if f is continuous and depends only on a finite number of variables x_j, ($j \in J$, finite), define

$$\int_X f \otimes \mu_i = \prod_{i \notin J} c_i \cdot \int_{\prod_{j \in J} X_j} f(\otimes_{j \in J} \mu_j).$$

The same definition then applies when the X_i are locally compact and almost all of the X_i are compact.

(slightly more generally, o.k. if $\prod c_i$ converges conditionally by the same definition).

— o —

In our case, each $V(k_v)$ has a given measure $|\omega|_v$. Let S be a finite set of places (as above). Then

$$V(\mathbb{A}_{K,S}) = \underbrace{\prod_{v \in S} V(K_v)}_{\text{locally compact}} \times \underbrace{\prod_{v \notin S} V(O_v)}_{\text{compact}}$$

and we must check the convergence condition:

$$c_v = \int_{V(O_v)} |\omega|_v = \frac{1}{(N_v)^n}(\# \mathcal{V}(\mathcal{R}_v)) \quad \text{for } v \notin S$$

Convergence means $\prod c_v$ converges. For this, we use the results of Grothendieck and Deligne on the number of points on varieties over finite fields:

"Thm: $$|\mathcal{V}(\mathcal{R}_v)| = \sum_{i=0}^{2n} (-1)^i \operatorname{Tr}(\text{Frob}, H^i_c(\overline{\mathcal{V}}_{\mathcal{R}_v}, \mathbb{Q}_\ell)) \quad \left(\begin{matrix}\text{trace}\\ \text{formula}\end{matrix}\right)$$

$$(\ell \neq ch(\mathcal{R}_v))$$

$$= \sum_{i=0}^{2n} (-1)^i \left(\sum_{j \in J_i} \alpha_j\right)$$ where the α_j are the eigenvalues of Frobenius on H^i_c.

Further: the α_j are algebraic integers, with

$$|\alpha_j| = q_v^{m(j)/2} \qquad \text{for } j \in J_i$$

where $m(j)$ is an integer with $0 \leq m(j) \leq i$. "

(Remark: when V is projective, $m(j) = i$)

<u>Remark</u>: the total number of eigenvalues α_i is bounded independent of v.

<u>Remark</u>: Since the variety $\mathcal{X}_v$ is smooth (by assumption on S), Poincaré duality applies and so H^i_c is dual to H^{2n-i}.

Hence,

(1) H^{2n}_c is dual to H^0 $\Rightarrow$ if $\mathcal{V}$ is absolutely irreducible, H^{2n}_c gives <u>one</u> eigenvalue, which is q_v^n.

(2) H^{2n-1}_c dual to H^1 $\Rightarrow$ $m(2n-1) \leq 2n-1$

(3) H^{2n-2}_c dual to H^2 $\Rightarrow$ $m(2n-2) \leq 2n-2$.

Then

$$c_v = \frac{1}{q_v^n}\left(\sum_{i,j}(-1)^i\alpha_j\right)$$

$$= \frac{1}{q_v^n}\left(q_v^n - \sum_{i=2n-1}\alpha_j + \sum_{i=2n-2}\alpha_j - \cdots\right)$$

$$= 1 - \frac{\sum \alpha_j}{q_v^n} + \frac{\sum \alpha_j}{q_v^n} - \cdots$$

The contributions are as follows:

$$H^1 \;(H_c^{2n-1}) \quad : \quad \leq \frac{1}{q_v^{1/2}}$$

$$(H_c^{2n-2}) \quad : \quad \leq \frac{1}{q_v}$$

$$\text{Others} \quad : \quad \leq \frac{1}{q_v^{3/2}}$$

This gives the

<u>Theorem</u>: If $H^1 = H^2 = 0$ (i.e. $H_c^{2n-1} = H_c^{2n} = 0$), then

$$\prod c_v \quad \text{is (absolutely) convergent.}$$

<u>Remark</u>: $H^1 = 0$ means topologically that $\pi_1(V)^{ab}$ is <u>finite</u>. (suffice to check this over $\mathbb{C}$, then it will be true for almost all v).

<u>examples</u>: $\mathbb{P}_1$. Then $\dfrac{\#\mathbb{P}_1(k_v)}{P_v} = \dfrac{P_v+1}{P_v}$; no convergence

SL_2; get the factor $\frac{1}{p^3}(p(p^2-1)) = 1 - \frac{1}{p^2}$; convergence

elliptic curve; $\frac{1}{p}(p - (\pi + \bar{\pi}) + 1) = 1 - \underbrace{\frac{\pi+\bar{\pi}}{p}}_{\sim\sqrt{p}} + \frac{1}{p}$

not absolutely convergent (the variance of $\frac{\mathrm{Tr}(\pi)}{p}$ with p remains open), in general.

— o —

<u>The Case of Algebraic Groups</u>

I. <u>Linear Groups</u> (Connected)

<u>Remark</u>: the restriction to <u>connected</u> groups is due to the convergence condition; non-connected groups require correction factors = the number of components e.g. the orthogonal group (2 components) gives

2 elements in highest cohomology (so contribution of $\frac{2q_v^n}{q_v^n} = 2$ in c_v).

Here ω exists, can be chosen left invariant (and then it is unique up to multiplication by a non-zero constant). For convergence,

$$\frac{1}{q_v^n}(\#\text{ points in } \mathcal{R}_v) = c_v \quad (= c_v(G)).$$

Since in the Number field case, $1 \to \underset{(\text{unipotent})}{U} \longrightarrow G \to \underset{(\text{reductive})}{G/U = R} \to 1$

we have $c_v(G) = c_v(U)\,c_v(R) = c_v(R)$, the question reduces to reductive groups.

Then

"absolute convergence for a reductive group

$\Leftrightarrow$ the group is semisimple" (true also over function fields)

Proof: consider the root system of the reductive group and the primitive invariant polynomials of degree m on the root system. These carry an action of $\mathrm{gal}(\bar{k}/k)$, giving a linear representation ρ_m. Then

$$c_v = \prod_{m \geq 1} \det(1 - \underbrace{\rho_m(\mathrm{Frob}_v)}_{\text{eigenvalues are roots of unity.}} q_v^{-m})$$

Hence, absolute convergence $\Leftrightarrow \rho_1 = 0 \Leftrightarrow R$ is semisimple.

examples: $\underline{SL_2}$: 

invariant polynomials; polynomials in x^2, and the only invariant polynomial representation ρ_m not zero occurs with $m=2$; then $c_v = 1 - \frac{1}{q_v^2}$ $\left(= q_v^{-3} \cdot q_v \cdot (q_v^2 - 1) \right)$.

$\underline{GL_n}$: $W = S_n$; invariant polynomials are the symmetric polynomials $\sigma_1, \dots, \sigma_n$ of degrees $1, \dots, n$ (respectively). $Gal(\bar{F}/k)$ acts trivially, and

$$c_v = \left(1 - \frac{1}{q_v}\right)\left(1 - \frac{1}{q_v^2}\right)\dots\left(1 - \frac{1}{q_v^n}\right)$$

and the product does not converge (due to the first term).

$\underline{SL_n}$: on the subvariety where $\sigma_1 = 0$, and then

$$c_v = \prod_{2 \le m \le n} \left(1 - \frac{1}{q_v^m}\right)$$

and so here this product $\prod_v c_v$ converges absolutely.

Unitary group: E/k a quadratic extension with a quadr. form. Then $U_n \underset{/E}{\sim} GL_n$ (H is a twist of GL_n over k).

Then $Gal(E/k)$ acts on the root space by ± 1, and the action on the representations is:

$$\sigma_1 \mapsto \pm \sigma_1$$
$$\sigma_2 \mapsto \sigma_2$$
$$\sigma_3 \mapsto \pm \sigma_3 \dots$$

Here then the $\rho_1, \dots, \rho_n$ are 1-dimensional Galois representions $Gal(E/k) \to \{\pm 1\}$ and

$$\begin{cases} \rho_i = 1 & \text{for } i \text{ even} \\ \rho_i \neq 1 & \text{for } i \text{ odd} \end{cases}$$

Hence

$$c_v = \prod_{i=1}^{n} (1 - \rho_i(\mathrm{Frob}_v) q_v^{-i}) \quad \text{with}$$

$$\rho_i(\mathrm{Frob}_v) = \begin{cases} 1 & i \text{ even} \\ 1 & i \text{ odd}, \ v \text{ splits in } E/k \\ -1 & i \text{ odd}, \ v \text{ stays prime in } E/k \end{cases}$$

e.g. U_2, $E/k = \mathbb{Q}(i)/\mathbb{Q}$: $\quad c_p = \left(1 - \frac{\left(\frac{-1}{p}\right)}{p}\right)\left(1 - \frac{1}{p^2}\right)$

$\left(\frac{-1}{p}\right)$ the quadratic residue symbol.

(so conditional convergence).

Tori

If T is a torus, let $X(T) = \mathrm{Hom}_{\bar{k}}(T, \mathbb{G}_m)$ (the character group)
and

$Y(T) = \mathrm{Hom}_{\bar{k}}(\mathbb{G}_m, T)$ (the co-character group).

Then X and Y are $\mathbb{Z}$-dual, and are $\mathbb{Z}$-free of rank $n = \dim T$. Then $\mathrm{gal}(\bar{k}/k)$ acts on $X(T)$, $Y(T)$ and knowledge of this action determines T.

If the ground field is finite, say $\mathbb{F}_q$, then Frobenius acts on $X(T)$, $Y(T)$ and the following formula is elementary:

$$\# T(\mathbb{F}_q) = \det_{\substack{X(T) \\ (\text{or } Y(T))}} (q - \text{Frob}) = \prod_{i=1}^{n} (q - \varepsilon_i)$$

since repr's are the same : characters conjugate by dual) characters equal by over $\mathbb{Z}$

(ε_i the eigenvalues).

$$\Rightarrow \qquad \frac{1}{q^n} \# T(\mathbb{F}_q) = \prod_{i=1}^{n} \left(1 - \frac{\varepsilon_i}{q}\right).$$

Hence, for a torus,

$$c_v = \det\left(1 - \frac{1}{q} \text{Frob}_v\right) = \frac{1}{L_v(\rho, 1)}$$

so

$$\prod c_v \text{ "=" } \frac{1}{L(\rho, 1)}. \qquad \text{(not in fact convergent)}$$

(Where $L(\rho,1)$ is the Artin L-series at 1 for the Galois representation ρ of G in $X(T)$; $L_v(\rho,s)$ is the v-factor of $L(\rho,s)$).

It is known that if $n = \dim T \geq 1$, then this product does not converge absolutely. For conditional convergence, it is necessary and sufficient that $L(\rho,s)$ have no pole at $s=1$, i.e. ρ does not contain the trivial representation, i.e. X does not contain $\mathbb{G}_m$ (or have a quotient $\simeq \mathbb{G}_m$), and when conditional convergence is given, then $\prod_{v \notin S} c_v = L_S(\rho,1)^{-1}$ $\left(L_S = \prod_{v \notin S} L_v(\rho,s)\right)$ where S consists of the primes of bad reduction.

— o —

For a general semisimple group,

$$\prod_{v \notin S} c_v = \prod_m L_S(\rho_m, m)^{-1}$$

<u>examples</u>: SL_n : $\prod_{v \notin S} c_v = \zeta_S(2)^{-1} \zeta_S(3)^{-1} \cdots \zeta_S(n)^{-1}$

SU_n : $\prod_{v \notin S} c_v = \zeta_S(2)^{-1} L_S(3)^{-1} \cdots$

— o —

<u>Summary</u>:

G reductive : convergence $\Leftrightarrow$ G is semisimple

conditional convergence (K = number field) $\Leftrightarrow$ there is no non-trivial homomorphism from G to $\mathbb{G}_m$ (over K)

G connected (linear): reduces to G reductive (apply the above criteria to G/U, U unipotent in G, G/U reductive).

In the convergent case, there is a measure $\bigotimes_v |\omega|_v$ on each $G(\mathbb{A}_{K,S})$, hence on $G(\mathbb{A}_K)$, denoted $|\omega|_{\mathbb{A}}$.

<u>Remark</u> (Tamagawa): $|\omega|_{\mathbb{A}}$ is <u>independent</u> of ω, since another ω gives $|\lambda\omega|_v = |\lambda|_v |\omega|_v$ and $\prod_v |\lambda_v| = 1$ by the product formula.

— o —

1-17-81 Let V be a non-singular, absolutely irreducible variety over the number field K, say quasiprojective.

Then by Hironaka, $V = \bar{V} - D$, where $\bar{V}$ is projective, non-singular, and D is a closed subvariety.

For almost all v, reduction mod v is defined, so the fibre $\mathcal{V}(\mathfrak{X}_v) = \tilde{V}_v$ is defined (the set of pts. of reduction mod v).

Then

$$|\tilde{\bar{V}}_v| = q_v^n - q_v^{n-1}\,Tr_1(Frob_v) + Tr^{2n-2}(Frob_v) + O(q_v^{n-\frac{3}{2}})$$

$(n = \dim V)$

$$= q^{n-2}\,Tr_2(Frob_v)$$

(the notation is "topological" in origin, e.g. Tr_1 = Trace of $Frob_v$ acting on H_1, Tr^{2n-2} = Trace of Frobenius on H^{2n-2} etc).

(Then $\bar{V}$ has an Albanese variety $A(\bar{V})$ (roughly: the largest abelian variety that $\bar{V}$ "generates"); this gives the groups on which Frob acts).

Since $Tr_1 = \sum \alpha_i$, $|\alpha_i| = q_v^{1/2}$, $Tr_2 = \sum \beta_j$, $|\beta_j| = q_v$, this gives

$$c_v(\bar{V}) = \bar{c}_v = \frac{1}{q_v^n}|\tilde{\bar{V}}_v| = 1 - \frac{1}{q_v}Tr_1 + \frac{1}{q_v^2}Tr_2 + O\left(\frac{1}{q_v^{3/2}}\right)$$

For D, we have $D = \underset{\text{over } \bar{K}}{\bigcup}\underbrace{W_\alpha}_{\text{irreducible divisor}} \cup \{\text{subvariety of dimension} \le n-2\}$.

Over K, $Gal(\bar{K}/K)$ acts on the W_α, defining a permutation; let Tr_D denote the corresponding trace of the repr. ρ_D.

Then

$$c_v = \bar{c}_v - \frac{1}{q_v} \mathrm{Tr}_D(\mathrm{Frob}_v) + O\left(\frac{1}{q_v^{3/2}}\right).$$

(one easily sees by dimensions that the error (i.e. action on $D - \cup W_\alpha$ is $O\left(\frac{1}{q_v^{3/2}}\right)$))

So

$$c_v = 1 - \frac{1}{q_v} \mathrm{Tr}_1(\mathrm{Frob}_v) + \frac{1}{q_v^2} \mathrm{Tr}_2(\mathrm{Frob}_v) - \frac{1}{q_v} \mathrm{Tr}_D(\mathrm{Frob}_v)$$
$$+ O\left(\frac{1}{q_v^{3/2}}\right).$$

Hence, a sufficient condition for absolute convergence is : $H_1 = 0$ (so $\mathrm{Tr}_1 = 0$) and

$$\frac{1}{q_v} \mathrm{Tr}_2 = \mathrm{Tr}_D$$

(e.g. $\mathrm{Tr}_2 = \mathrm{Tr}_D = 0$), i.e. if the 1st Betti number is 0 ($\Leftrightarrow$ there is no non-constant map of V into an abelian variety over $\bar{K}$), and $\frac{1}{q_v}\mathrm{Tr}_2 = \mathrm{Tr}_D$. (implied by Tate's conjecture).

Assume then that (for $\bar{V}$)

(a) $H_1 = 0$ $\quad (B_1 = 0)$

(b) Cohomology in dimension 2 is "algebraic"

(i.e. $h^{2,0} = 0$: $B_2 = h^{2,0} + h^{1,1} + h^{0,2}$

$\Rightarrow$ by Lefschetz all cycles are of algebraic type)

(i.e. there are no non-zero differential forms of the 1st kind of deg 1 and 2 on $\bar{V}$).

example: any rational variety is of this type

— o —

There is an action of $gal(\bar{k}/k)$ on $\mathbb{Q} \otimes NS(\bar{V})$
Néron-Severi (divisors mod alg. equiv.)
and so an associated trace, Tr_{NS}. Then

$$Tr_2(Frob_v) - q_v \overline{Tr_{NS}(Frob_v)}.$$

(Tate twist to go from NS to cohomology). This gives

$$c_v = 1 + \frac{1}{q_v}\left(Tr_{NS}(F_v) - Tr_D(F_v)\right) + O\left(\frac{1}{q_v^{3/2}}\right).$$

Theorem: Under assumptions (a) and (b) above, $\prod_v c_v$ is absolutely convergent $\Leftrightarrow$ $Tr_{NS} = Tr_D$.

Proof: ($\Leftarrow$) is trivial by the formula for c_v above
($\Rightarrow$) Suppose now that the representations on D and NS are not isomorphic (both representations are over $\mathbb{Z}$, observe). Hence $Tr_{NS} \neq Tr_D$ at v

$$\Rightarrow \quad |c_v - 1| \geqslant \frac{1}{q_v} + O\left(\frac{1}{q_v^{3/2}}\right)$$

(an integer $\neq 0$ must be at least $\geqslant 1$ in absolute value!).

Lemma: If $Tr_{NS} \neq Tr_D$ at $v \Rightarrow Tr_{NS}(F_v) \neq Tr_D(F_v)$ in fact for a set of v of positive density.

Pf. of Lemma: Tchebotarov

Hence, the product is not absolutely convergent. ✓

Theorem: Assume only condition (b) holds. Then if $\prod c_v$ converges absolutely, then $H_1 = 0$.

Proof: $c_v = 1 - \frac{1}{q_v}\mathrm{Tr}_1 + \frac{1}{q_v}(\mathrm{Tr}_{NS} - \mathrm{Tr}_D) + O\left(\frac{1}{q_v^{3/2}}\right)$

$$= 1 - \frac{1}{q_v}\underbrace{\left(\mathrm{Tr}_1 + \mathrm{Tr}_D - \mathrm{Tr}_{NS}\right)}_{\cap\ \mathbb{Z}} + O\left(\frac{1}{q_v^{3/2}}\right)$$

If $\mathrm{Tr}_1 \neq 0$, then $\mathrm{Tr}_1 + \mathrm{Tr}_D \neq \mathrm{Tr}_{NS}$ (the absolute values of Frobenius are not matched). Then this relation must hold for a positive density of v's (first going to an associated l-adic repr. and applying Tcheb.) and the proof is as before.

As a consequence:

Theorem: If V is a non-singular curve, the $\prod c_v$ is abs. convergent if and only if V is isomorphic to $\mathbb{P}^1 - \{\infty\}$.

Proof: (a) $\Rightarrow$ genus of $\overline{V} = 0$
(b) $\underset{\overset{\shortparallel}{\mathbb{Z}}}{\mathrm{Tr}_{NS}} = \mathrm{Tr}_D \Rightarrow$ only one point was removed. //

Question: conditional convergence? Example: $y^2 = x^3 - x$ over $\mathbb{Q}$, good reduction for $p \neq 2$. Then $c_p = \frac{N_p}{p}$, N_p is well-known in this special case:
$$N_p = \begin{cases} p+1 & p \equiv 3 \bmod 4 \\ p+1+2a & p \equiv 1 \bmod 4 \end{cases}$$
where a is defined by $p = a^2 + 4b^2$, $N_p \equiv 0 \bmod 8$. Then consider $\prod \frac{N_p}{p}$ for increasing p. Convergence is open. (standard conjectures would say the limit should differ from $\int_0^1 \frac{dx}{\sqrt{x^3-x}}$ by a known rational number). (cf. Remark on p. 126)

Remark: $\prod_{p \leq x} \frac{N_p}{p} \sim c (\log x)^{\rho}$ (ρ = rank of rational points) may be true.

— o —

Recall: Let V be a non-singular (smooth) variety over K, and ω an invariant differential form of maximal degree, which is nowhere zero. Absolute convergence is assumed. Then $\prod_{v \in S} V(k_v) \times \prod_{v \notin S} V(O_v) = V(A_{K,S})$,

carries the measure $\bigotimes_v |\omega|_v$, and since these measures are compatible, they define
$$|\omega|_A = \bigotimes_v |\omega|_v \quad \text{on} \quad V(A_K).$$

For linear groups:

Let first K be a number field, G a linear connected group. Then

$1 \to U \to G \to G/U \to 1$, U unipotent, G/U reductive. Then $\prod c_v$ converges absolutely $\Leftrightarrow$ G/U is semisimple $\Leftrightarrow$ $\mathrm{Hom}_{\bar{K}}(G, \mathbb{G}_m) = \{1\}$ $\Leftrightarrow$ $\mathrm{Hom}(G,T) = \{1\}$ for any torus T over K.

Then ω invariant (left or right $\Rightarrow$ both, by triviality of $\mathrm{Hom}(G,T)$) $\Rightarrow$ G is unimodular, gives a measure $|\omega|_A$.

Assume G is semi-simple:

<u>Definition</u>: The <u>Tamagawa</u> number $\tau(G)$ of G is defined by

$$\tau(G) = \delta_K^{-n} \int_{G(A)/G(K)} |\omega|_A$$

where $n = \dim G$ and

$$\delta_K = \begin{cases} |d_K|^{1/2} & (d_K = \text{discriminant}), \text{ number fields} \\ q^{g-1} & \text{finite field.} \end{cases}$$

<u>Remark</u>: the factor δ_K gives $\tau(\mathbb{G}_a) = 1$, even $\tau(G) = 1$ for <u>any</u> unipotent group G, in fact $\tau(G) = \tau(G/U)$ for any G.

<u>Remark</u>: Borel (number fields), Harder (function fields) showed $G(A)/G(K)$ has finite volume.

The crucial case to consider is the case when G is <u>semisimple</u>.

<u>Conjecture</u> (Weil): G semisimple and simply connected $\Rightarrow$ $\tau(G) = 1$.

<u>Theorem</u> (Ono): Let G be simply connected, and set $G' = G/F$ where F is a finite subgroup contained in the center of G. ($F = \pi_1(G')$). Then

$$\tau(G') = \tau(G) \cdot \frac{h^0(F^\wedge)}{h^1(F^\wedge)} ,$$

where $F^\wedge$ is the Cartier dual of F ($= \mathrm{Hom}_{\bar{K}}(F, G_m)$) for the $gal(\bar{K}/k)$-module F, and

$$h^0(\hat{F}) = |H^0(k, \hat{F})| = |\mathrm{Hom}_k(F, G_m)|$$

$$h^1(\hat{F}) = |\mathrm{Ker}(H^1(k, \hat{F}) \to \prod_v H^1(k_v, \hat{F}))| .$$

<u>example</u>: $F \simeq \mu_n$, the n^{th} roots of unity ($\mathrm{ch}\, K \nmid n$). Then $\hat{F} = \mathbb{Z}/n\mathbb{Z}$ with trivial Galois action. Hence

$$h^0(\hat{F}) = |\mathbb{Z}/n\mathbb{Z}| = n$$

$$h^1(\hat{F}) = |\mathrm{Ker}(H^1(k, \hat{F}) \to \prod_v H^1(k_v, \hat{F}))|$$

$$= |\mathrm{Ker}(\mathrm{Hom}(gal(\bar{K}/k), \mathbb{Z}/n\mathbb{Z}) \to \text{product of the local groups}|$$

$$= |\{\varphi : gal(\bar{K}/k) \to \mathbb{Z}/n\mathbb{Z},\ \varphi = 0 \text{ locally}\}|$$

$$= \underline{1}$$

since the extension of K corresponding to φ would be decomposed totally at every prime, so must be K itself.

Hence

$$\tau(G/\mu_n) = n\,\tau(G).$$

(Under the Weil conjecture, then $\tau(G/\mu_n) = n$.)

<u>examples</u>(a) $SL_n/\mu_n = PGL_n \;(\simeq PSL_n)$

$$\Rightarrow \tau(PGL_n) = n\cdot\tau(SL_n) = n$$

(b) $G = Spin_n$, $G/\mu_2 \simeq SO_n$ $(n \neq 2)$. Then G is semisimple and simply connected (even simple if $n=3$ or $n \geq 5$), hence

$$\tau(SO_n) = 2\,\tau(Spin_n) = 2. \quad //$$

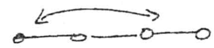
Assuming the Weil conjecture, i.e. $\tau(\text{simply connected } G) = 1$, then $\tau(G')$ depends only on the Galois-module $F = \pi_1(G')$, $G' = G/F$.

In particular, under an "inner twist" of G (see below), then τ remains invariant.

(an "inner-twist" is defined by taking a 1 cocycle c of $gal(\bar{k}/k)$ in $Aut(X)$ to define a "twisted" X, denoted by X_c, (e.g. principal homogeneous spaces), in the special case where the cocycle is taken from $Ad(G)$: $Aut(G) \supset Inn(G) = Ad(G)$, G semisimple. This is equivalent to saying
$\qquad\qquad\qquad\qquad\qquad\quad \overset{\|}{G/\text{center}}$
the galois action on the Dynkin diagram is the same.)

<u>example</u>: an inner twist of SL_n is SL of a central simple algebra.

<u>non-example</u>: a non-inner twist



K'/K quadratic $\Rightarrow$ SU_n for that K'/K
(an inner twist is given by keeping K' <u>fixed</u>).

<u>Remark</u>: observe that F is invariant under an inner twisting, so (under Weil) the Tamagawa number is invariant under inner twisting. Conversely, if τ is invariant under all inner twistings, then Weil's conjecture is true. (a deep result of Langlands, Lai).

<u>Idea</u>: (number fields): G semisimple, simply connected and "quasi-split" (i.e. there is a Borel subgroup of G defined over k), then Langlands and Lai have shown $\tau(G) = 1$.

Now, <u>any</u> semisimple group is an inner twist of a quasi-split group (which is essentially unique), which gives the converse.

The conjecture of Weil is known for the following groups:

(i) G quasi-split (as in the Remark above)

(ii) the classical groups (cf. Adeles and Algebraic groups)
(the "triality" D_4 is not considered classical)

(iii) some exceptional groups: G_2, F_4, E_6 (inner forms), 19-81 Remark: For $y^2 = x^3 - x$, Goldfeld can show that $\prod_{p \le X} \frac{N_p}{p}$ converges as $X \to +\infty$ implies the Riemann Hypothesis for the L function attached to the curve. (indicating why the convergence of $\prod \frac{N_p}{p}$ is non-trivial).

—o—

<u>The Tamagawa number for reductive groups</u>:

Let G be a connected, reductive group, defined over k, and let G' be it's derived group (semi-simple); then $G/G' = T$ is a torus over k.

Let $X = \mathrm{Hom}_{\bar{k}}(T, G_m)$, which is a module over $gal(\bar{k}/k)$, unramified at almost all v. Let this repr. be denoted ρ_X.

Then

$$|\det_X(1 - q_v \mathrm{Frob}_v)| = \text{the number of points of reduction mod } v \text{ of } T.$$

hence

$$\frac{1}{q_v^{\dim T}} (\#\text{pts on } T \bmod v) = \det_X (1 - q_v^{-1} \mathrm{Frob}_v) = L_v(1, \rho_X)^{-1}$$

$$= \prod (1 - \varepsilon_\alpha q_v^{-1}) \quad \text{where the } \varepsilon_\alpha \text{ are roots of unity.}$$

Define as usual $c_v = c_v(T) = L_v(1, \rho_X)^{-1}$, so

$$c_v(G) = c_v(G') . c_v(T) = c_v(T) \left(1 + O\left(\frac{1}{q_v^2}\right)\right)$$

(and the $c_v(T)$ are the obstruction to convergence). Define then the "correcting factors" as follows:

Choose a finite set S of places, $S \supset \Sigma^\infty$ and set

$$L_S(s,\rho_X) = \prod_{v\notin S} L_v(s,\rho_X) \quad ; \quad \lambda_v = L_v(1,\rho_X).$$

Then define a measure on $\prod_{v\in S} G(K_v) \times \prod_{v\notin S} G(O_v)$ by the formula:
(ω a differential form)

$$\bigotimes_{v\in S} |\omega|_v \bigotimes_{v\notin S} \lambda_v |\omega|_v \quad ; \quad \text{which is convergent.}$$

This depends on the choice of S, so a slight variant is made:
Since $\underset{(as\ s\to 1)}{L_S(s,\rho_X) \sim l_S(s-1)^{-r}}$, where r = the number of times the trivial representation 1 occurs in ρ_X = rank $\mathrm{Hom}_{\bar K}(G, G_m)$. Then our measure is defined to be:

$$l_S^{-1} \bigotimes_{v\in S} |\omega|_v \bigotimes_{v\notin S} \lambda_v |\omega|_v .$$

It is then easy to see that this measure is independent of S. Finally, define

$$|\omega|_A = \delta_K^{-n}\, l_S^{-1} \bigotimes_{v\in S} |\omega|_v \bigotimes_{v\notin S} \lambda_v |\omega|_v \qquad (n = \dim G).$$

for the adele measure on $G(A)$. (Recall: $\delta_K = \begin{cases} |d_K^{1/2}| & K \text{ number field} \\ g^{g-1} & K \text{ function field} \end{cases}$).

<u>Theorem</u> (Borel for number fields, Harder for function fields):

$$\mathrm{vol}\left(G(A)/G(K) \right) \text{ is finite} \iff r = 0$$

(i.e. there are no non-trivial homomorphisms over K from G to $\mathbb{G}_m$).

In fact, if $\varphi: G \to \mathbb{G}_m$, then

$$\varphi: G(\mathbb{A}) \to I_K = \mathbb{G}_m(\mathbb{A})$$
$$G(K) \to K^\times \subset I_K^1 \quad \text{(ideles of volume 1)}$$

so define

$$G^1(\mathbb{A}) = \{ g \in G(\mathbb{A}) \mid \varphi(g) \in I_K^1 \text{ for all } \varphi: G \to \mathbb{G}_m \}.$$

Then,

<u>Theorem</u>: $G^1(\mathbb{A})/G(K)$ has finite volume.

(which contains as a consequence the previous Theorem.)

If $r = \operatorname{rank} \operatorname{Hom}_K(G, \mathbb{G}_m)$, choose a basis $\varphi_1, \dots, \varphi_r$ for $\operatorname{Hom}_K(G, \mathbb{G}_m) \simeq \mathbb{Z}^r$. Then each φ_i gives a homomorphism:

$$G(\mathbb{A}) \xrightarrow{\varphi_i} I_K \xrightarrow{\text{Norm}} \mathbb{R}_+^\times \quad \left\{ = \begin{array}{ll} \mathbb{R}_+^\times & \text{for number fields} \\ q^{\mathbb{Z}} & \text{for function fields} \end{array} \right.$$

and so we have a sequence

$$1 \to G^1(\mathbb{A}) \to G(\mathbb{A}) \xrightarrow{m} \left\{ \begin{array}{ll} (\mathbb{R}_+^\times)^r & \text{for number fields} \\ (q^{\mathbb{Z}})^r & \text{for function fields} \end{array} \right.$$

(exact by definition of $G^1(\mathbb{A})$, of course).

Define a Haar measure on each factor: given measure ν on $G(\mathbb{A})$,

ν on $\mathbb{R}_+^\times$ choose measure $\frac{dt}{t}$

$q^{\mathbb{Z}}$ choose measure giving every point mass $\log q$.

(motivation: $\displaystyle\int_1^x \nu = \begin{cases} \log x & \text{on } \mathbb{R}_+^\times \\ (\log q)\underbrace{\{1+\dots+1\}}_{m \text{ times}} & \text{where } m \text{ is the largest integer with } q^m \le x, \text{ i.e. } m \sim \frac{\log x}{\log q} \end{cases}$

wrong! (in funct. fields)

so the measure on $q^{\mathbb{Z}}$ also gives (asymptotically), $\int_1^x \nu \sim \log x$).

Then the measure on $G'(\mathbb{A})$ is the Haar measure compatible with the exact sequence and the measures on the quotient above, denoted $\frac{|\omega|_{\mathbb{A}}}{\nu} = \mu$

<u>Definition</u>: the Tamagawa number of G is defined by

$$\tau(G) = \mathrm{vol}_\mu\left(G'(\mathbb{A})/G(K) \right).$$

— o —

<u>Special Case</u>: $r = 0$, i.e. $\mathrm{Hom}_K(G, \mathbb{G}_m) = 0$

Then $\displaystyle\tau(G) = \int_{G(\mathbb{A})/G(K)} |\omega|_{\mathbb{A}}$.

Suppose that K is a number field. Then the "correcting factors" above can be "ommitted"; following Siegel, a measure can be defined by using <u>conditional</u> convergence: define $|\omega|_{\mathbb{A}} = \delta_K^{-n} \bigotimes_{v\uparrow} |\omega|_v$.

These two approaches are the same, by the following

<u>Lemma</u>: Suppose $\begin{matrix} E \\ | \\ K \end{matrix} \mathfrak{g}$ is a Galois extension of number fields, ρ a linear representation of $\mathfrak{g}$ not containing the unit representation. Then $L(s,\rho)$ is holomorphic and non-zero at $s=1$ and

$$L(1,\rho) = \prod_{v \nearrow} L_v(1,\rho) \quad \text{(a conditionally convergent product).}$$

<u>Proof</u> (exercise): use the prime number theorem with error term:

$$\sum_{Nv \leq x} \chi(v) = O\left(\frac{x}{(\log x)^2}\right) \quad \text{for characters } \chi.$$

— o —

If G is semisimple, the "new" $\tau(G)$ is the same as the previous definition. For $G = \mathbb{G}_m$,

$$\tau(\mathbb{G}_m) = 1. \quad \text{(see below)}$$

If $G = G_1 \times G_1$, $\tau(G) = \tau(G_1)\tau(G_2)$.

For an extension of fields (separable in the function field case) $\begin{matrix} K' \\ | \\ K \end{matrix}$ and G' over K', there is a restriction of scalars $\mathrm{Res}_{K'/K}(G') = G_{/K}$ and

$$\tau_{K'}(G') = \tau_K(G)$$

(basically by the functorial properties of the Artin L-series under induction).

<u>example</u> $\tau(\mathbb{G}_m) = 1$ for function fields:
(cf. Igusa for number fields). Must compute the volume of $I_K^1/K^\times$ w.r.t. the measure $(S=\emptyset)$, $|\omega|_A = \delta_K^{-n} \ell_S^{-1} \bigotimes_{v\in S} |\omega|_v \bigotimes_{v\notin S} \lambda_v |\omega|_v$:

$$\lambda_v = \left(1-\frac{1}{q_v}\right)^{-1} \quad (=\zeta_v(1))$$

$$\ell_S = \text{Residue}_{s=1}\, \zeta(s)$$

Let $U = \prod_v O_v^\times$ be the product of the units, an open compact subgroup of I_K^1. Then count orbits:

$$U \cap K^\times = \mathbb{F}_q^\times$$

and $U/\mathbb{F}_q^\times$ acts faithfully on $I_K^1/K^\times$, and so if h is the number of cosets, then

$$\tau(\mathbb{G}_m) = h \cdot \mu(U)/q-1.$$

so it is necessary to compute $\mu(U)$.
The measure on I_K^1 (open in I_K) is $\frac{1}{\log q}|\omega|_A$, so

$$\tau(\mathbb{G}_m) = \frac{h}{(\log q)(q-1)} \int_U |\omega|_A$$

and

$$\int_U |\omega|_A = q^{1-g} \cdot (\text{Residue}_{s=1}\,\zeta(s))^{-1} \cdot 1$$

by the definition of $|\omega|_A$. Hence

$$\tau(\mathbb{G}_m) = \frac{h \cdot q^{1-g}}{(q-1)(\text{Residue}_{s=1}\,\zeta(s))\log q}.$$

What is h? Since $I_K/U \simeq$ divisor group, $I_K/U\cdot K^\times \simeq$ divisor classes, so finally $I_K'/K^\times U \simeq$ divisor classes of degree 0, so $h = |\mathrm{Jac}(\mathbb{F}_q)|$.

Now,

$$\zeta(s) = Z(q^{-s})$$

where

$$Z(T) = \frac{\prod_{i=1}^{2g}(1-\pi_i T)}{(1-T)(1-qT)}$$

(where g = genus, π_i are the eigenvalues of Frobenius on J: $\pi_1\bar{\pi}_1 = q$).

Since $h = \prod_{i=1}^{2g}(\pi_i - 1)$, we have

$$\text{Residue}_{s=1}\,\zeta(s) = \frac{-q}{\log q}\,\text{Residue}_{T=\frac{1}{q}}\,Z(T)$$

$\left(T = q^{-s};\ dT = \frac{-\log q}{q}\,ds\right)$

$$= \frac{-q}{\log q}\left[-\frac{1}{q}\,\frac{\prod_{i=1}^{2g}\left(1-\frac{1}{\pi_i}\right)}{1-\frac{1}{q}}\right]$$

$$\Rightarrow \quad \tau(\mathbb{G}_m) = 1 \quad !$$

Remark in the number field case, taking $U = K_\infty^1 \times \prod_{v \text{ non-Arch.}} O_v^\times$

(where $K_\infty^1 = \left(\prod_{v\in\Sigma_\infty} K_v^\times\right)$ of norm 1), which is open in I_K', having image in $I_K'/K^\times$ of index = the class number. Again, knowledge of the residue at $s=1$ of $\zeta_K(s)$ $\left(= h\cdot 2^{r_1}(2\pi)^{r_2}R/w d_K^{1/2}\right)$ gives the result $\tau(\mathbb{G}_m)=1$ similarly as above.
(exercise!)

— o —

Tori (Ono)

Let G be a torus T, which has associated character group $X = \mathrm{Hom}_{\bar{K}}(T, \mathbb{G}_m)$.
Then

<u>Theorem</u> (Ono): $\tau(T) = \dfrac{|H^1(K,X)|}{|Ш(T)|}$

where $Ш(T) = \mathrm{Ker}\left(H^1(K,G) \to \prod_v H^1(K_v,G)\right)$.

The <u>idea</u> of the proof:

Put $d(T) = \dfrac{\tau(T)\cdot|Ш(T)|}{|H^1(K,X)|}$ and consider exact sequences of tori.

Properties of $d(T)$:

(1) $d(\mathbb{G}_m) = 1$ (by the computation above and easy computations showing $Ш(\mathbb{G}_m) = H^1(K, X_{\mathbb{G}_m}) = 1$.)

(2) $d(R_{K'/K}T') = d(T')$ (need only $d(R_{K'/K}\mathbb{G}_m) = 1$).

(3) $1 \to T' \to T \to T'' \to 1 \Rightarrow d(T) = d(T')d(T'')$.

(idea of proof: $1 \to T'_A/T'_K \to T_A/T_K \to T''_A/T''_K \overset{?}{\to} 1$
were the map surjective, the formula would follow: obstruction measured by cohomology; Ono shows the factors just cancel ✓)

There is a Lemma on linear representations of <u>finite</u> groups:

Let g be a finite group and $\mathcal{C}$ the category of $\mathbb{Z}[g]$-modules which are free of rank n. (over $\mathbb{Z}$).

Let R be a torsion-free abelian group, and

$$\varphi : \mathcal{C} \to R$$
$$X \in \mathcal{C} \mapsto \varphi(X) \in R$$

s.t.

(a) $0 \to X' \to X \to X'' \to 0 \Rightarrow \varphi(X) = \varphi(X') + \varphi(X'')$

(b) $\varphi(X) = 0$ if X has a g-stable basis (a "permutation module")

Then:

$$\varphi = 0.$$

Given this, Ono's Theorem follows (take the log of the φ defined for tori ✓).

Proof of the Lemma: Grothendieck group $K(\mathcal{C})$; $\varphi : K(\mathcal{C}) \to R$ (by (a)) (b) says, that if $K'(\mathcal{C})$ is the subgroup generated by permutation representations then φ is 0 on $K'(\mathcal{C})$.

Remains to see whether $\mathbb{Q} \otimes K(\mathcal{C}) = \mathbb{Q} \otimes K'(\mathcal{C})$. By Swan, $\mathbb{Q} \otimes K(\mathcal{C}) = \mathbb{Q} \otimes K(\mathbb{Q}\text{-representations of } g)$. But now, every character of a $\mathbb{Q}$-representation of g is a $\mathbb{Q}$-linear combination of the characters of permutation representations, and the result follows.

Using this, Ono (and then Sansuc) proved (for number fields) the following result:

" Let G be a reductive group, G' its derived (semisimple) subgroup, and let $\tilde{G}'$ be the universal covering for G'. Assume $\tilde{G}'$ has no factor isomorphic to E_8. Then

$$\tau(G) = \tau(\tilde{G}') \frac{|\operatorname{Pic} G|}{|Ш G|}$$

where $\operatorname{Pic}(G)$ is the Picard group of the scheme G." (In the semisimple case, proved by Ono; Sansuc extended: Crelle 1981).

Remark conjecturally: should not need restriction on E_8 factors, and $\tau(\tilde{G}') = 1$, so $\tau(G) = \frac{|\operatorname{Pic} G|}{|Ш G|}$ for arbitrary reductive G.

example (and indication of the proof): SL_n and PGL_n.
Show $\tau(PGL_n) = n\, \tau(SL_n)$ $(= n)$.
Use two exact sequences:

$$1 \to \mathbb{G}_m \to GL_n \to PGL_n \to 1$$

$$1 \to SL_n \to GL_n \to \mathbb{G}_m \to 1$$

These behave well w.r.t. adelic points.
For points of norm 1:

$$1 \to \mathbb{G}_m^1(\mathbb{A}) \to GL_n(\mathbb{A})' \to PGL_n(\mathbb{A}) \to 1$$

Checking compatibilities of the measures chosen gives

measure on $Gl_n(\mathbb{A})$ - determinant
on $\mathbb{G}_m$: ident
restricts to nth power

$$\tau(Gl_n) = \tau(PGL_n) \cdot \tfrac{1}{n}\, \tau(\mathbb{G}_m)$$

$$\tau(Gl_n) = \tau(Sl_n) \cdot \tau(\mathbb{G}_m) \quad \checkmark.$$

example: proving $1 \to \mu_N \to \underset{\substack{\text{simply connected}\\ \text{semisimple}}}{\tilde{G}} \to G \to 1 \Rightarrow \tau(G) = n\,\tau(\tilde{G})$.

Define a group analogous to Gl_n above:

$$H = (\tilde{G} \times \mathbb{G}_m)/\mu_n \text{ (diagonally embedded)}$$

then have

$$1 \to \mathbb{G}_m \to H \to G \to 1$$
$$1 \to \tilde{G} \to H \to \mathbb{G}_m \to 1$$

and then, first removing factors of E_8 and using Ш$\tilde{G} = 1$ (which implies $\tilde{G}_{\mathbb{A}}/G_K \to H_{\mathbb{A}}/H_K \to \mathbb{G}_m(\mathbb{A})/\mathbb{G}_m(K) \to 1$ exact), gives the result as above.

example: replacing μ_n by a finite group F: similar, but embed F into a torus (not $\mathbb{G}_m$ in general, which complicates matters).

— o —

11-24-81

Tamagawa numbers interpreted as Siegel's formulas:

Let G be a locally compact group, Γ a discrete subgroup. There is given on G a Haar measure dg, w.r.t. which $\mathrm{vol}(G/\Gamma) = \int_{G/\Gamma} dg < \infty$ (this implies that G is "unimodular", i.e. dg is bi-invariant).

Suppose that Ω is an open subgroup of G. Then $\Omega \subset G$ acts on G/Γ with orbits which are open. For $x \in G$, $\bar{x} \in G/\Gamma$ let $\Omega\bar{x}$ be the corresponding orbit and set $\Gamma_x = \{ g \in \Omega \mid gx \equiv x \bmod \Gamma \}$.

Then $gx = x\gamma$, $\gamma \in \Gamma \iff g \in x\Gamma x^{-1}$, so

$$\Gamma_x = \Omega \cap x\Gamma x^{-1} \simeq x^{-1}\Omega x \cap \Gamma.$$

Hence

$$\mathrm{vol}\,(\text{orbit of } \bar{x}) = \text{volume of } \Omega/\Gamma_x .$$

Choose a set I of representatives of the Ω-orbits in G/Γ, i.e. representatives of the double coset space $\Omega\backslash G/\Gamma$. Then clearly

$$\mathrm{vol}\,(G/\Gamma) = \sum_{x \in I} \mathrm{vol}\,(\Omega/\Gamma_x).$$

<u>Special Case</u>: Ω open and <u>compact</u>. Then Γ_x is discrete in Ω, hence is finite, and $\mathrm{vol}(\Omega/\Gamma_x) = \frac{1}{|\Gamma_x|}\mathrm{vol}\,(\Omega)$. Then the formula becomes

$$\frac{\mathrm{vol}\,(G/\Gamma)}{\mathrm{Vol}\,(\Omega)} = \sum_{x \in \Omega\backslash G/\Gamma} \frac{1}{|\Gamma_x|}$$

(resembles a mass formula, as will be clear later).

We shall apply this to $G = G(\mathbb{A})$, $\Gamma = G(K)$ (or $G^1(\mathbb{A})$ if $\mathrm{Hom}_K(G, G_m) \neq 0$ as before). Then by definition,

$\mathrm{vol}(G/\Gamma) = \tau(G)$, the Tamagawa number of G.

Choose a finite set S of places, $\Sigma^\infty \subset S$ and put

$$\Omega = \prod_{v \in S} G(K_v) \prod_{v \notin S} G_v^\circ$$

where

G_v° is open and compact, equal to the "integral points" for almost all v.

Then Ω is open in $G(A)$.

Let $G_S = \prod_{v \in S} G(K_v)$ and $\Omega_f = \prod_{v \notin S} G_v^\circ$ (so $\Omega = G_S . \Omega_f$).
(assume $S \neq \emptyset$). Then Γ_x embeds in G_S, and the formula becomes (using

$$\mathrm{vol}(\Omega/\Gamma_x) = \mathrm{vol}(G_S/\Gamma_x) \cdot \prod_{v \notin S} \mathrm{vol}(G_v^\circ) \quad)$$

$$\tau(G) = \prod_{v \notin S} \mathrm{vol}(G_v^\circ) \cdot \sum_x \mathrm{vol}(G_S/\Gamma_x).$$

— o —

The set of x may be small: if Str_S holds for G, then $G = \Omega . \Gamma$, and so $x = 1$ is the only representative.

Examples: (1) $G = SL_n$ over $\mathbb{Q}$, $S = \Sigma^\infty$, $G_v^\circ = G_p^\circ = SL_n(\mathbb{Z}_p)$

then

$$\mathrm{vol}(G_p^\circ) = \prod_{i=2}^{n} \left(1 - \frac{1}{p^i}\right)$$

(the Haar measure is given by viewing SL_n as a smooth $\mathbb{Z}$-scheme, so there is a "$\mathbb{Z}$-life" measure).

$$\Gamma = SL_n(\mathbb{Q}), \quad \Gamma_\chi = SL_n(\mathbb{Z}) \quad (= \Gamma \cap \Omega)$$
$$G_\infty = SL_n(\mathbb{R})$$

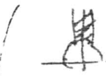
Then

$$\tau(SL_n) = \frac{1}{\zeta(2)\dots\zeta(n)} \cdot \mathrm{vol}\left(SL_n(\mathbb{R}) / SL_n(\mathbb{Z}) \right)$$

(where $SL_n(\mathbb{R})$ has the natural Haar measure : on GL_n, natural Haar measure is $\prod d(a_{ij}) / |\det(a_{ij})|$). We shall see later that $\tau(SL_n) = 1$, giving

$$\mathrm{vol}\left(SL_n(\mathbb{R})/SL_n(\mathbb{Z})\right) = \prod_{i=2}^{n} \zeta(i).$$

(this formula was known classically; probably Minkowski was aware of it, certainly Siegel proved it).

<u>exercise</u> : $n=2$, using the fundamental domain for $\mathfrak{h}/SL_2(\mathbb{Z})$ ( as usual compute the area $\frac{dx\,dy}{y^2}$, relate the measures and show
$$\mathrm{vol}\left(SL_2(\mathbb{R})/SL_2(\mathbb{Z})\right) = \frac{\pi^2}{6}.$$

(2) The same method applies to the split groups, giving, for example

$$\tau(Sp_{2n}) = \frac{1}{\zeta(2)\ldots\zeta(2n)} \operatorname{vol}\left(Sp_{2n}(\mathbb{R})/Sp_{2n}(\mathbb{Z})\right).$$

(and again, the volume on the right was computed classically).

Remark (cf. Harder, Ann ENS, '72) Connections with Gauss-Bonnet, gives as a consequence of the formula above,

$$EP\left(Sp_{2n}(\mathbb{Z})\right) = \zeta(-1)\zeta(-3)\ldots\zeta(1-2n).$$

(Euler Poincaré)

(observe that this can be used to show the rationality of the values of zeta).

(3) Assume $G_S = \prod_{v\in S} G(K_v)$ is compact (so Strg is "far" from true)

(e.g. $S=\emptyset$, $K=$ function field or $S=\Sigma^\infty$, G the orthogonal group of a definite quadratic form).

Then,

$$\frac{\operatorname{vol}(G/\Gamma)}{\operatorname{vol}(\Omega)} = \sum \frac{1}{|\Gamma_x|}$$

and $\operatorname{vol}(\Omega) = \operatorname{vol}(G_S)\prod_v \operatorname{vol}(G_v^\circ)$, so the formula becomes

$$\sum_{x\in I} \frac{1}{|\Gamma_x|} = \frac{\tau(G)}{\operatorname{vol}(G_S)\prod_{v\notin S}\operatorname{vol}(G_v^\circ)}.$$

Example: $G \subset GL_V$, V a vector space over K. Let M be a lattice in V. Assume for simplicity that $K=\mathbb{Q}$, $S=\Sigma^\infty$. Take

$$G_v^\circ = G_p^\circ = \text{the stabilizer of } M_v = O_v \otimes M \text{ in } G(K_v) = G_M(O_v).$$

Then Ω is as defined in the notion of "genus" (p.101). The classes in the genus are then bijective with $G(K)\backslash G(A)/\Omega = \Gamma\backslash G/\Omega$.

For the representatives of $\Omega\backslash G/\Gamma$, $x=(x_v)$ with $(x^{-1}M)_v = x_v^{-1}M_v$ and every lattice in the genus of M is isomorphic to a unique $x^{-1}M$.

Then $\Gamma_x = \Omega \cap x\Gamma x^{-1} \cong \Gamma \cap x^{-1}\Omega x$ is the subgroup of $\Gamma = G(K)$ which stabilize the lattice $x^{-1}M$. Since $(x^{-1}wx)x^{-1}M_v = x^{-1}wM_v = x^{-1}M_v$, we see that $\Gamma_x \simeq \underline{\mathrm{Aut}}(x^{-1}M)$.

Hence our formula becomes:

$$\sum_{x\in I} \frac{1}{|\Gamma_x|} = \frac{\tau(G)}{\mathrm{vol}(G_S)\prod_{v\notin S}\mathrm{vol}(G_v^\circ)}$$

I = the number of classes in the genus of M

and $|\Gamma_x|$ is the number of automorphisms of a representative of the class corresponding to $x\in I$.

e.g. the Orthogonal Group O_n $(n\geq 1)$, w.r.t. a non-degenerate quadratic form (or SO_n, the special orthogonal group): $(O_n : SO_n) = 2$.

For $n\neq 2$; SO_n is semisimple. For $n=2$, SO_2 is a one-dimensional torus (not isomorphic to $\mathbb{G}_m$ over K, however, so conditional convergence procedures are necessary).

To compute the Tamagawa number of O_n:

Suppose G is an algebraic group, G° its connected component. Assume every coset modulo G° contains a point of K (e.g. this is true for O_n).

If μ_v is the local measure on G_v° $(= G^\circ(K_v))$, then define the local measures on $G(K_v)$ by $\frac{1}{(G:G^\circ)} \mu_v$ (then convergence is all right).

For example, if G is a finite group (G° = a single point!), say F, then $F(\mathbb{A}) = \prod_v F(K_v) = \prod_v F$. Then μ_v of F gives measure 1 to each component $F(K_v) = F$, and the total measure is 1, so $\tau(F) = \frac{1}{|F|}$.

Now, for our non-connected group G,

$$1 \to G^\circ \to G \to \underset{\overset{\parallel}{F}}{G/G^\circ} \to 1$$

and so

$$\tau(G) = \tau(G^\circ)\,\tau(F) = \frac{1}{(G:G^\circ)}\,\tau(G^\circ).$$

Take as given that $\tau(SO_n) = 2$ for $n \geqslant 2$, so $\tau(O_n) = 1$ for $n \geqslant 2$. and $\tau(O_1) = \frac{1}{2}$.

Hence, the formula for the mass becomes

$$\text{Mass of a genus} \quad \left(= \sum \frac{1}{|\Gamma_x|}\right) \quad = \quad \frac{\tau(G)}{\mathrm{vol}(G_S)\prod_v \mathrm{vol}(G_\mu(\mathcal{O}_v))}.$$

We shall contort this formula into Siegel's mass formula $\left(\text{mass} = \frac{\tau(G)}{\delta_\infty \prod \delta_p}\right)$ i.e. we shall show

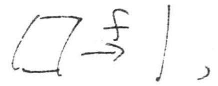
$$\delta_\infty = \mathrm{vol}(O_n(\mathbb{R}))$$
(defined by Siegel)

$$\delta_p = \mathrm{vol}(G_\mu(\mathcal{O}_v))$$

i.e. find a suitable differential ω so that

$$\delta_\infty = \int_{O_n(\mathbb{R})} |\omega|_\infty$$

$$\delta_p = \int_{G_\mu(\mathcal{O}_v)} |\omega|_p .$$

Given differential forms on a variety  and a map , there are, as described before (cf. p. 25ff), induced differentials on the <u>fibers</u>, i.e. on the set of points where $f(x)$ = something given.

Let Q be a quadratic form on a vector space V, $u \in \mathrm{Aut}(V)$. Then $Q(ux) = Q(x)$ can be picked out as follows:

$$f : \mathrm{End}(V) \longrightarrow \mathrm{Quad}(V) \ (= \mathrm{Sym}^2 V^*)$$
$$u \longmapsto Q \circ u$$

(in terms of matrices; $\mathcal{U} \mapsto {}^t U Q U$, U = an $n \times n$ matrix). Then the fiber of Q is (by def$^{\underline{n}}$!), O_n (w.r.t. Q).

Hence, by the general "recipe", need only specify invariant differential forms/K on $\mathrm{End}(V)$ and $\mathrm{Quad}(V)$ to get forms on the fibers. (in matrix form: $du = \prod du_{ij}$; quad form = sym form (a_{ij}) $\prod\limits_{i \le j} da_{ij}$). This differential form on the fiber O_n is in fact invariant, i.e. defines a Haar measure:

$$\begin{tikzcd} \mathrm{End}(V) \arrow[r, "\text{mult. by } g"', "\text{on left}"] \arrow[d, "f"] & \mathrm{End}(V) \arrow[d, "f"] \\ \mathrm{Quad}(V) \arrow[r, "1"'] & \mathrm{Quad}(V) \end{tikzcd} \qquad (\text{for fixed } g \in O_n)$$

$$\left(\begin{tikzcd} u \arrow[r, mapsto] \arrow[d] & gu \arrow[d] \\ Qu \arrow[r, mapsto] & Qu = Q \circ g \circ u \end{tikzcd} \right) \quad \checkmark$$

, g leaves the form on $\mathrm{End}\, V$ invariant

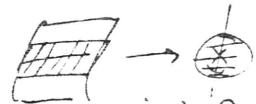
($(\det g)^n$ is the relevant factor: g acts linearly) ✓

This gives a Haar measure defined over K.

Choosing a basis of the lattice under consideration as a basis for V, then for this choice of measure,

$$\mathrm{vol}\,(G_\mu(O_v)) = \text{the Siegel volume}$$

(and similarly at ∞).

<u>Proof</u>: (cf. § 28): by computing volumes on fibers 
have already shown these formulas ok, i.e. agree with Siegel's formulas.

— o —

The two-groups game

Let $\begin{matrix} G \supset g \\ \cup \quad \cup \\ \Gamma \supset \gamma \end{matrix}$ be locally compact groups, (with given Haar measures) discrete subgroups (respectively), with $\gamma = \Gamma \cap g$ and suppose $\mathrm{vol}(g/\gamma)$, $\mathrm{vol}(G/\Gamma)$ are finite. Let

$$Y = G/g$$

be the homogeneous space. The Haar measures on G, g define a measure dy on Y.

We have the following integration formula (Weil, Adeles + Alg. Gps):

"Suppose φ is a continuous function on Y with compact support. Then

$$\mathrm{vol}(g/\gamma) \int_Y \varphi(y)\,dy = \int_{G/\Gamma} \Big\{ \sum_{y \in \Gamma/\gamma} \varphi(ty) \Big\} d\dot{t} \quad ."$$

(Proved as follows: $\begin{matrix} G/\gamma \\ \downarrow \\ Y = G/g \end{matrix}$ g/γ fiber so $\int$ above is $\int_{G/\gamma} \varphi(g)\,dg$

Using $G/\gamma \to G/\Gamma$, can compute this integral as the R.H.S. of the formula.)

Let Ω be open in G, and assume Ω is compact (the so-called "definite" case). Then

$$G/\Gamma = \coprod_{x \in I} \Omega x \Gamma/\Gamma = \coprod \Omega \bar{x} \qquad \bar{x} = \text{class of } x \text{ in } G/\Gamma$$

stab. of $\bar{x}$ = $\Gamma_x = \Omega \cap x\Gamma x^{-1}$

Il manque la page 146 dans le document original

Define

$$N_x(\varphi) = \sum_{y \in \Gamma/\gamma} \varphi(xy)$$

Then our formula becomes

$$\int_Y \varphi(y)\,dy = \frac{\mathrm{vol}(G/\Gamma)}{\mathrm{vol}(g/\gamma)} \; \frac{\sum_{x \in I} N_x(\varphi)/|\Gamma_x|}{\sum_{x \in I} \frac{1}{|\Gamma_x|}}$$

Defining the "average value" $N(\varphi)$ by

$$N(\varphi) = \Big\{ \sum_{x \in I} N_x(\varphi)/|\Gamma_x| \Big\} \Big/ \sum_{x \in I} \frac{1}{|\Gamma_x|},$$

the formula is simply

$$\int_Y \varphi(y)\,dy = \frac{\mathrm{vol}(G/\Gamma)}{\mathrm{vol}(g/\gamma)} N(\varphi)$$

or,

$$N(\varphi) = \frac{\mathrm{vol}(g/\gamma)}{\mathrm{vol}(G/\Gamma)} \cdot \int_Y \varphi(y)\,dy.$$

In the applications, G, g will be adelic groups, Γ, γ the rational points, $Y = G/\gamma$ and φ a continuous function on Y invariant by the "auxiliary" Ω.

<u>Application</u>: <u>Positive Definite Quadratic Forms over $\mathbb{Q}$</u>.

We first relate $N_x(\varphi)$ above to the number of representations by some quadratic form.

Let V be a quadratic space over $\mathbb{Q}$ with quadratic form Q_V, $m = \dim V$ and let M be a lattice in V. Set O_V = the orthogonal group. Let

$$G = O_V(\mathbb{A}) \quad \text{be the adelic points of } O_V \text{, and}$$
$$\Gamma = O_V(\mathbb{Q}) \quad \text{the rational points.}$$

Let

$$\Omega = O_V(\mathbb{R}) \times \prod_p \Omega_p$$

where $O_V(\mathbb{R}) = G_\infty$ and Ω_p is the subgroup of $O_V(\hat{\mathbb{Q}}_p)$ which stabilizes $M_p = M \otimes \mathbb{Z}_p$.

Recall (cf. p. 00) that for x a representative of $\Omega \backslash G / \Gamma$, $x^{-1}M$ is a lattice in the genus of M ($x^{-1}M$ is the lattice with $(x^{-1}M)_p = x_p^{-1} M_p$, x_p the p-component of x). Further, all lattices in the genus of M are obtained in precisely this way (up to isomorphism), and $\Gamma_x \cong \mathrm{Aut}(x^{-1}M)$.

Let now W be another quadratic space over $\mathbb{Q}$ of dimension n (with positive non-degenerate quad. form Q_W), $\underline{n \le m}$. Choose a lattice L in W.

By a "representation of W by V" we mean an <u>embedding</u> $W \to V$ compatible with the given quadratic forms i.e.

$$y : W \to V$$

with

$$Q_V \circ y = Q_W.$$

(in terms of matrices : $\begin{matrix} T \leftrightarrow Q_W \\ S \leftrightarrow Q_V \end{matrix}$ $\quad X \leftrightarrow y \quad$ then ${}^tXSX = T$, or

$S[X] = T$ in Siegel's notation).

If $\dim N = n = 1$, this is just the representation of scalars by quadratic forms ($S[x] = t$, x a column vector and t a scalar).

The collection of all maps $y : W \to V$ as above constitute an a variety isomorphic to $O_V / O_{W^\perp}$, where $W^\perp$ is the orthogonal complement of W in V (assuming such a y exists over $\mathbb{Q}$, say $y_0 : W \to V$, this defines $W^\perp$, and then Witt's theorem shows the map is an isomorphism).

The map y "represents L by M" if $yL \subset M$

Set then

$$g = O_{W^\perp}(A)$$

$$\gamma = O_{W^\perp}(\mathbb{Q}).$$

Then

$$Y = G/g = \mathcal{Y}(A)$$

where

$$\mathcal{Y} = \text{the variety } O_V/O_{W^\perp} \text{ described above.}$$

In addition, here

$$\mathcal{Y}(\mathbb{Q}) = \Gamma/\gamma,$$

as follows:

Take a rational point $y: W \to V$ in $\mathcal{Y}(\mathbb{Q})$. It is necessary to show y lifts, i.e. that there is an $x \in O_V(\mathbb{Q}) = \Gamma$ such that $xy_0 = y$.

$$\begin{array}{c} W \\ \searrow^{y_0} \\ y : W \to V \end{array} \qquad /\mathbb{Q}.$$

This is due to Witt's Theorem. /

Finally, set $y = (y_\infty, (y_p))$, $y_\infty \in Y_\infty = G_\infty/g_\infty = \mathcal{Y}(\mathbb{R})$, $y_p \in \mathcal{Y}(\mathbb{Q}_p)$ and define

$$\varphi(y) = \begin{cases} 1 & \text{if } y_p L_p \subset M_p \text{ for every } p \\ 0 & \text{otherwise} \end{cases}$$

The function φ is clearly continuous with compact support invariant under Ω.

(φ is the characteristic function of $Y_\infty \times \prod Y^\circ_{L,M}(\mathbb{Z}_p)$ where $Y^\circ_{L,M}(\mathbb{Z}_p)$ are the integral points when the bases of V, W are chosen to be bases of L, M. $\mathcal{Y} \subset \mathrm{Hom}(V,W) \simeq$ affine nm space)

Here

$$\mathrm{vol}(g/\gamma) = \tau(O_{W^\perp}) \quad \text{(the orthogonal group in } m-n \text{ variables)}$$

$$\mathrm{vol}(G/\Gamma) = \tau(O_V) \quad \text{(the orthogonal group in } m \text{ variables)}$$

and

$$\int_Y \varphi(y)\,dy = \mathrm{vol}(Y_\infty) \times \prod_p \mathrm{vol}(Y^\circ_{L,M}(\mathbb{Z}_p)) = \prod_{p,\infty} \delta_p(L,M)$$

($\delta_\infty(L,M) = \mathrm{vol}(Y_\infty)$, $\delta_p(L,M) = \mathrm{vol}(Y^\circ_{L,M}(\mathbb{Z}_p))$ by definition). But

$S_p(L,M)$ = the local density of Siegel

(the proof is the same as in the case of the mass: cf. p. 144)

Let

$$c = \frac{\tau(O_{W^\perp})}{\tau(O_V)}.$$

Then our integration formula becomes:

$$N(\varphi) = c \cdot \prod_{p,\infty} S_p(L,M).$$

Now,

$$N_x(\varphi) = \sum_{y \in \Gamma/\gamma} \varphi(xy)$$

where $y: W \to V$ is defined over $\mathbb{Q}$. Then

$$\varphi(xy) = \begin{cases} 1 & \text{if } x_p y_p (= x_p y) L_p \subset M_p \text{ for all } p \\ 0 & \text{otherwise} \end{cases}$$

and since $x_p y \cdot L_p \subset M_p \Leftrightarrow y L_p \subset x_p^{-1} M_p$, we see that $\varphi(xy) = 1$ if and only if $yL \subset x^{-1}M$, so

$N_x(\varphi)$ = the number of $y: W \to V$ with $yL \subset x^{-1}M$ (y defined over $\mathbb{Q}$), i.e.

$N_x(L)$ = the number of representations of the lattice L by the lattice $x^{-1}M$.

Hence

$N(L)$ = the "mean value" of the number of representations of L by lattices in the same genus as M.

This gives Siegel's formula in the definite case (Ω compact). It remains to consider the constant $c = \tau(O_{W^\perp})/\tau(O_V) = \tau(SO_{m-n})/\tau(SO_m)$

Recall that $\tau(O_n) = 1$ $(n \geq 2)$, $\tau(O_1) = \frac{1}{2}$. Hence

$$c = \begin{cases} 1 & \text{if } m > n+1 \\ \frac{1}{2} & \text{if } m = n+1 \end{cases}$$

<u>Proof that $\tau(SO_n) = 2$, $n \geq 3$.</u> ($\tau(SO_2) = 2$ if the form does not represent 0 and $\tau(SO_2) = 1$ if it splits).

For $n \geq 5$, a uniform proof can be given (see Igusa)

For $n = 2, 3, 4$:

$SO_2 \leftarrow$ 1 dim'l torus

$SO_3 \leftarrow A_1$

$SO_4 \leftarrow A_1 \times A_1$

(orthogonal Dynkin SO_n: o—o—o…—o—o=o odd n; o—o—o…—o—o< even n)

For SO_3:

D a quaternion algebra over K $\qquad$ $SL_1(D)$

The "multiplicative group" of D, $GL_1(D)_1$ is the kernel of the reduced norm map.

The center is $\mu_2 = \{\pm 1\}$ and $SL_1(D)/\mu_2$ is the orthogonal group in 3 variables, and $SL_1(D)$ is an unramified covering of SO_3. Then

$$\tau(SO_3) = 2 \cdot \tau(SL_1(D)) = 2$$

since $\tau(SL_1(D)) = 1$ (see Igusa), we shall see later that $\tau(SL_n) = 1$.

(e.g. x^2+yz, $D = M_2$, $SO_3 = SL_2/\mu_2$)

FOR SO_4:

Use the universal covering $\widetilde{SO_4}$ = the spin group:

$$\widetilde{SO_4} = \begin{cases} SL_1(D) \times SL_1(D') , & D, D' \text{ quaternion algebras } /K \\ \text{or} & \\ R_{K'/K}\, SL_1(D') , & D' \text{ quaternion algebra } /K' . \end{cases}$$

K' = quad extension, separable of K

(the Dynkin diagram consists of only two points over the algebraic closure).

Hence $\tau(\widetilde{SO_4}) = 1$, so $SO_4 = \widetilde{SO_4}/\mu_2$ (diagonally embedded) $\Rightarrow \tau(SO_4) = 2$

For SO_2:

SO_2 is isomorphic either to $\mathbb{G}_m$ (when the quadratic form is equiv. to X_1X_2, i.e. represents 0)

or

a one-dimensional torus T not isomorphic to $\mathbb{G}_m$

(the character group is $\simeq \mathbb{Z}$ with $Gal(\bar{k}/k)$ acting by a quadratic character $\chi: gal(\bar{k}/k) \twoheadrightarrow \{\pm 1\}$, kernel defines K'/k quadratic).

Then

$1 = \tau(\mathbb{G}_m)$ in the first case

$2 = \tau(T)$ in the second case.

-3-81 When the binary form does not represent 0: E/k quadratic, $gal(E/k) = \{\pm 1\}$ and $SO_2 = T$, a one-dimensional torus with character group $\simeq \mathbb{Z}$ with an obvious action of $g = gal(E/k)$. There are two exact sequences:

(a) $$1 \to \mathbb{G}_m \to \underbrace{R_{E/k}\,\mathbb{G}_m}_{\text{a torus, } \Theta\text{, say}} \to T \to 1$$

(b) $$1 \to T \to R_{E/k}\,\mathbb{G}_m \to \mathbb{G}_m \to 1$$

which can be used to compute $\tau(T)$, as follows:

(these are dual to the sequences:

the "$\circlearrowleft$" denotes non-trivial g-action, i.e. the twisted form of $\mathbb{Z}$

$$0 \leftarrow \overset{\text{trivial action}}{\mathbb{Z}} \leftarrow \mathbb{Z}[g] \leftarrow \underset{\circlearrowleft}{\mathbb{Z}} \leftarrow 0$$

and $$0 \leftarrow \underset{\circlearrowleft}{\mathbb{Z}} \leftarrow \mathbb{Z}[g] \leftarrow \mathbb{Z} \leftarrow 0$$

).

Hence

$$1 \to \mathbb{G}_m(\mathbb{A}) \to \Theta(\mathbb{A}) \to T(\mathbb{A}) \to 1$$
$$1 \to \mathbb{G}_m(K) \to \Theta(K) \to T(K) \to 1$$

and then

$$1 \to \mathbb{G}_m^1(\mathbb{A})/\mathbb{G}_m(K) \to \Theta^1(\mathbb{A})/\Theta(K) \to T(\mathbb{A})/T(K) \to 1$$

(the surjectivity follows as $\mathbb{G}_m$ has trivial cohomology).
(T contains no $\mathbb{G}_m$, so need not pass to "T^1" to compute Tamagawa numbers.

The compatibility of the Tamagawa measures must be checked: the factors of the discriminant and L-factors are all right, but $G/G^1 \cong (\mathbb{R}_+^\times)^2 \ldots \left(\frac{dt}{t}\right)^2$ so restriction to $\mathbb{G}_m^1(\mathbb{A})/\mathbb{G}_m(K)$ is the square, so define instead $\mu'_{\mathbb{G}_m} = \frac{1}{2}\mu_{\mathbb{G}_m}$. Then in the sequence, the measures $(\mu'_{\mathbb{G}_m}, \mu_\Theta, \mu_T)$ are compatible.
Computing volumes then gives

$$\tau(\Theta) = \tau(T) \cdot \tfrac{1}{2}\tau(\mathbb{G}_m)$$

and $\tau(\mathbb{G}_m) = 1$ gives $\tau(\Theta) = \frac{1}{2}\tau(T)$ and since Tamagawa numbers are invariant under restriction of scalars, also $\tau(\Theta) = 1$. Hence

$$\tau(T) = 2 \quad \checkmark$$

For the second sequence:

$$1 \to T(\mathbb{A})/T(K) \to \Theta^1(\mathbb{A})/\Theta(K) \to \mathbb{G}_m^1(\mathbb{A})/\mathbb{G}_m(K)$$
$$\qquad\qquad\qquad\qquad \| \qquad\qquad\qquad\qquad \|$$
$$\qquad\qquad\qquad I_E^1/E^\times \xrightarrow{\text{Norm}} I_K^1/K^\times$$

Exactness follows because:

For $u \in I_E^1$, $Nu = \lambda \in k^\times \Rightarrow Nu = Nu'$, $u' \in E^\times$ (since for quadratic extensions, a local norm is a global norm (quadratic extensions are cyclic!)). Then $N(uu'^{-1}) = 1$ so $uu'^{-1} \in T$ shows exactness.

The image is determined by class field theory: $C_K/NC_E \simeq \{\pm 1\}$.
so again $\tau(\Theta) = \tau(T) \cdot \frac{1}{2}\tau(G_m)$ gives $\tau(T) = 2$.

—o—

Proof of Siegel's formula

We return to consideration of Siegel's formula: we have the formula (p. 151)
$N(\varphi) = c \cdot \prod_{p,\infty} \delta_p(L,M)$, $c = \tau(O_W)/\tau(O_V)$.

Let

$N_{L,M}$ = the mean value of the number of representations of a lattice L by a lattice in the genus of M ($= N(\varphi)$ above).

so our formula reads

$$(*) \qquad N_{L,M} = c \cdot \prod_{p,\infty} \delta_p(L,M) \qquad c = \frac{\tau(SO_{W^\perp})}{\tau(SO_V)}$$

Observe that c is <u>independent</u> of L.

We shall prove $\tau(O_V) = 1$ for $\dim V \geq 2$, $\tau(O_V) = \frac{1}{2}$ for $\dim V = 1$, by induction on n:

We shall use the formula above for $\dim W = 1$ (representation of numbers by quadratic forms, as explained before). It remains to show that formula $(*)$ implies $c = 1$ for $m = \dim V \geq 3$ (and that $c = \frac{1}{2}$ for $m = 2$).

Explication of Formula when $\dim W = 1$:

Recall M is a lattice, and let $t \in \mathbb{Z}$, $t > 0$, and set

$$N_M(t) = \left| \{ x \in M \mid Q(x) = t \} \right|$$

(where $Q(x)$ is the quadratic form on V, $Q(x) = {}^t x Q x$ with a matrix Q having integral coefficients).

Then

$$\begin{aligned} N(t) &= N(t, M) \\ &= \text{the mean value of } N_M(t) \text{ over the genus of } M \\ &= \frac{\sum_x N_{x^{-1}M}(t) / |\Gamma_x|}{\sum_x \frac{1}{|\Gamma_x|}} \end{aligned}$$

so formula $(*)$ reads

$$N(t) = c \prod_{p,\infty} \delta_p(t, M)$$

where $\delta_p(t, M)$ is the local density of representation of t by M.

The idea is to avoid the (difficult) problem of counting points (for example on a sphere) by getting approximations to this number by considering $\sum_{t \leq T} N(t)$.

<u>Remark</u>: the formula we are proving shows

$$\text{the "expected number of representations of } t\text{"} \left(= \prod_{\text{all } p} \delta_p(t, M)\right) = \begin{cases} 1; & \dim V \geq 3 \\ 2; & \dim V = 2 \end{cases} \times \begin{array}{l}\text{mean value of} \\ \text{the number} \\ \text{of representations}\end{array}$$

<u>example</u>: $x^2+y^2=1$: 4 solutions, but the value on the left is 8 (see below)
(but this "anomaly" occurs only for binary quadratic forms)

<u>exercise</u>: show $\prod_{\text{all } p} \delta_p(1) = 8$ by showing $\delta_\infty(1) = \pi$, $\delta_p(1) = \frac{p - \left(\frac{-1}{p}\right)}{p}$ (p odd) since the number of pts / $\mathbb{F}_p$ on a conic $x^2+y^2=1$ is $p+1$: when the point at ∞ is rational (i.e. -1 a square) therefore, there are only $p-1$ solutions of $x^2+y^2=1 \bmod p$, otherwise $p+1$, and that $\delta_2(1) = 2$ [compute solutions $x^2+y^2 \equiv 1 \bmod 8$ and divide by 8]. Hence $\prod \delta_p = \pi \cdot 2 \cdot \prod_{p>2} \left(1 - \frac{\left(\frac{-1}{p}\right)}{p}\right) = 2\pi \cdot L(1,\chi)^{-1}$, and $L(1,\chi) = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + - \ldots = \frac{\pi}{4} \Rightarrow \prod_{\text{all } p} \delta_p = 8$ ✓ done.

For m an integer, $m \geq 2$, let

$$\omega_m = \text{the volume of the unit ball in } \mathbb{R}^m \quad \left(\sum_{i=1}^m x_i^2 \leq 1\right)$$

$$= \pi^{m/2} / \Gamma\left(1 + \tfrac{m}{2}\right) \qquad \text{so if } \left(m = 2k,\ \omega_{2k} = \frac{\pi^k}{k!}\right)$$

If $Q(x) = {}^t x Q x$ with Q a symmetric non-degenerate $m \times m$ positive definite matrix, $\Delta = \det Q$, then

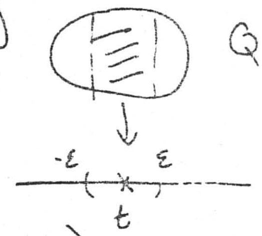
$$\mathrm{vol}(\{Q(x) \leq t\}) = \omega_m \Delta^{-1/2} t^{m/2}$$

(by transforming to the quad. form $\sum_{i=1}^m x_i^2$ and using homothety).

Let

$$\delta_{\infty}(Q,t) = \text{value at } t \text{ of } \frac{d}{dt}\left(\omega_m \Delta^{-1/2} t^{m/2}\right)$$
$$= \frac{m}{2}\omega_m \Delta^{-1/2} t^{m/2-1}.$$

(the density is defined by



take ratio of volumes as $\varepsilon \to 0$,

which is the derivative above)

Now let Λ be a lattice in $\mathbb{R}^m$, and set

$$S_\Lambda(t) = \text{the number of } x \in \Lambda \text{ s.t. } Q(x) \le t.$$

Then

$$\sum S_\Lambda(t) = \frac{1}{\mathrm{vol}(\Lambda)}\,\omega_m \Delta^{-1/2} t^{m/2} + o(t^{m/2})$$

(the error is even $O(t^{\frac{m}{2}-\frac{1}{2}})$)

($\mathrm{vol}(\Lambda) = \mathrm{vol}(\mathbb{R}^m/\Lambda)$ of course)

(Remark: this is an "average" representation statement, and avoids having to count precisely the number of $x \in \Lambda$ with $Q(x) =$ some given t.).

The proof involves considering $\frac{1}{\sqrt{t}}\Lambda$, considering pts with $Q(x) \le 1$ and then approximating by the Riemann integral (which exists here).

Observe that with Λ given and $x_0 \in \mathbb{R}^m$, then

$$S_{\Lambda+x_0}(t) = \sum_{\substack{x\in x_0+\Lambda \\ Q(x)\le t}} 1 \sim \frac{1}{\mathrm{vol}(\Lambda)}\, w_m\, \Delta^{-1/2}\, t^{m/2}$$

What can be said regarding the δ_p ? Recall that (p. 19)

$$\delta_p(t,M) = \text{the (stable) value of } \left(\text{the number of representations of } t \text{ by } Q \bmod p^n\right) \Big/ p^{n(m-1)} .$$

(stable means the value computed is fixed for n large)

Call a p "good" if $p\neq 2$ and $p\nmid\Delta$, the discriminant of Q. Then <u>for good</u> <u>p</u>, <u>$\delta_p(t,M)$ can be computed</u> (see Siegel, Lemma 16). An indication of the values:

(1) Assume t is a $p$adic unit. Then

if $m=2k$; $\quad \delta_p = \delta_p(t,M) = 1-\chi(p)p^{-k}$

where $\chi(p) = \left(\frac{(-1)^k\Delta}{p}\right)$. $\quad$ (corresponds to the character of the quadratic extension given by the action on Dynkin:

if $m=2k+1$, $\quad \delta_p = (1-p^{-2k})(1-\chi(p)p^{-k})^{-1}$

where $\chi(p) = \left(\frac{(-1)^k\Delta t}{p}\right)$

(indication of the proof: homogeneous space: want # of pts in orthogonal gps such as $\frac{SO_m}{SO_{m-1}}$, and the formulas given before give the values above)

(2) Suppose $t = up^{\ell}$, u a p-adic unit. Then

if $m=2k$; $\delta_p = (1-\chi(p)p^{-k})\left(\sum_{p^\alpha | t} \chi(p)^\alpha p^{-\alpha(k-1)}\right)$

if $m=2k+1$; formula is more complicated, see Siegel, lemma 16.

<u>Remark</u>: for $m \geq 5$, these values are very close to 1:

$$\delta_p = 1 + O\left(\frac{1}{p^2}\right) \quad \text{(uniformly in } t\text{)}$$

(so in particular $\prod_p \delta_p$ converges).

Want to consider $\sum_{t \leq T} N(t)$. First reduce to a situation involving only good primes:

Choose a value t_0 which is represented by one of the forms in the genus. Choose then a $P \geq 1$ divisible by $8\Delta t_0^3 \ldots$ (suitably), and consider

$$\sum_{\substack{t \leq T \\ t \equiv t_0 \bmod P}} N(t) = F(T), \text{ say.}$$

This will be estimated in two ways. Let

F = the mean value of the $F_{x^{-1}M}$ where $x^{-1}M$ is in the genus of M.

Let $x_0, \ldots, x_a$ be representatives mod P of the solutions of $Q(x) \equiv t_0 \bmod P$

so

$$F_M(t) = \sum_i \sum_{\substack{x \equiv x_i \bmod P \\ Q(x) \le T}} 1 \sim a \cdot \omega_m \Delta^{-1/2} T^{m/2} P^{-m} \quad \text{as } T \to \infty.$$

since we are working with points mod P.

using the volumes above.

For P large enough (highly divisible by the bad primes),

$$\frac{a}{P^{m-1}} = \delta_P(t_0) = \prod_{p \mid P} \delta_p(t_0) \quad \text{since } \delta_P(t) = \delta_p(t) \text{ for } p \mid P.$$

Hence, since the dependence on the lattice disappears,

$$F(T) \sim \Big\{ \prod_{p \mid P} \delta_p(t_0) \Big\} P^{-1} \omega_m \delta^{1/2} T^{\frac{m}{2}} \quad \text{as } T \to \infty.$$

i.e.

$$(1) \qquad \frac{F(T)}{\prod_{p \mid P} \delta_p(t_0)} \sim \lambda T^{m/2} \quad \text{with } \lambda = \omega_m \Delta^{-\frac{1}{2}} P^{-1}.$$

(Notice that $\delta_p(t_0) \neq 0$ for all p, since t_0 is "represented".)

Now we compute another way, using

$$F(T) = c \sum_{\substack{t \equiv t_0 \bmod P \\ t \le T}} \Big(\delta_\infty(t) \prod_p \delta_p(t) \Big)$$

(by formula (*)). For $p \mid P$, the local constancy of the δ_p gives as above $\delta_p(t) = \delta_p(t_0)$, so

$$(2) \qquad F(T) = c \cdot \prod_{p \mid P} \delta_p(t_0) \cdot \frac{m}{2}\,\omega_m \Delta^{1/2} \sum_{\substack{t \le T \\ t \equiv t_0 \bmod P}} t^{\frac{m}{2}-1} \prod_{p \nmid P} \delta_p(t)$$

using our value for δ_∞.

Consider the function $G(T) = \dfrac{\lambda^{-1} F(T)}{\prod_{p \mid P} \delta_p(t_0)}$. Then

(1) implies $G(T) \sim T^{m/2}$ as $T \to \infty$

(2) implies $G(T) = c \cdot P \cdot \frac{m}{2} \cdot \sum_{\substack{t \equiv t_0 \bmod P \\ t \le T}} t^{\frac{m}{2}-1} \prod_{p \nmid P} \delta_p(t)$.

We use the estimates for the δ_p.

<u>Case</u>: $m \geq 5$. Choose P divisible by so many primes that $\prod_{p \nmid P} \delta_p(t)$ is within ε of 1 (see the Remark on p. 161). Then estimate

$$\sum_{\substack{t \equiv t_0 \bmod P \\ t \le T}} t^{\frac{m}{2}-1}$$

(the powers of an integer in an arithmetic progression), which is

$$\sim \frac{1}{P} \frac{2}{m} T^{m/2}.$$

Hence, asymptotically,
$$G(T) \le c \cdot P \cdot \frac{m}{2} \cdot \frac{1}{P} \cdot \frac{2}{m} \cdot T^{\frac{m}{2}} (1+\varepsilon)$$
$$G(T) \geq c \cdot P \cdot \frac{m}{2} \cdot \frac{1}{P} \cdot \frac{2}{m} \cdot T^{m/2} (1-\varepsilon)$$

which forces

$$c = 1 \quad (!). \qquad /$$

—o—

-8-81 For a lattice M, let $M_1, \dots, M_h$ be representatives for the genus of M, and set

$$w_i = |\mathrm{Aut}(M_i)|$$

Recall the definition $N_{M_i}(t)$ = the number of representations of the integer t (>0) by M_i, i.e. $\displaystyle\sum_{\substack{x \in M_i \\ Q(x) = t}} 1$.

and

$$N(t) = \text{the mean value of } N_{M_i}(t) = \frac{\sum_{i=1}^{h} \frac{N_{M_i}}{w_i}}{\sum_{i=1}^{h} \frac{1}{w_i}}$$

(so the Siegel formula reads $N(t) = c \prod_{p,\infty} \delta_p(t, M) = c \prod_{p,\infty} \delta_p(t)$).

We are trying to show:

$$c = 1 \quad \text{if} \quad \dim V = m \geq 3$$
$$c = \tfrac{1}{2} \quad \text{if} \quad \dim V = m = 2.$$

We have shown $c = 1$ for $m \geq 5$, and that

$$T^{\frac{m}{2}} \sim c \cdot P \cdot \frac{m}{2} \cdot \sum_{\substack{t \equiv t_0 \bmod P \\ t \leq T}} t^{\frac{m}{2}-1} \prod_{p \nmid P} \delta_p(t) \quad \text{as } T \to +\infty.$$

(the auxiliary elements t_0 and P are defined above (p. 161).)

The proof for $m \geq 5$ does not apply for $m = 2, 3, 4$; so ad hoc proofs are given:

$\underline{c = 1 \text{ when } m = 4}$;

$$\delta_p(t) = (1 - \chi(p)p^{-2}) \sum_{p^\alpha | t} \frac{\chi(p^\alpha)}{p^\alpha} \quad \text{for } p \nmid P.$$

where $\chi(p) = \left(\frac{\Delta}{p}\right)$, Δ = the discriminant of the form.

Hence

$$\prod_{p \nmid P} \delta_p(t) = L_P(2, \chi)^{-1} \cdot \sum_{\substack{d | t \\ (d, P) = 1}} \frac{\chi(d)}{d}$$

(where $L_P(s, \chi) = \prod_{p \nmid P} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$, the L-series with P-factors removed).

This gives

$$G(T) = c \cdot P^{\frac{m}{2}} \cdot L_P(2, \chi)^{-1} \cdot \sum_{\substack{t \equiv t_0 (P) \\ t \leq T}} t \cdot \sum_{\substack{d | t \\ (d, P) = 1}} \frac{\chi(d)}{d}.$$

Writing $t = dd'$,

$$\sum_{\substack{t \equiv t_0 (P) \\ t \leq T \\ d | t \\ (d, P) = 1}} t \frac{\chi(d)}{d} = \sum_{\substack{d \leq T \\ (d, P) = 1}} \chi(d) \sum_{\substack{d' \leq \frac{T}{d} \\ d' \equiv \frac{t_0}{d} \bmod P}} d'.$$

The inner sum on the right is the sum of the elements in an arithmetic progression: $\displaystyle\sum_{\substack{d' \leq T/d \\ d' \equiv \frac{t_0}{d} (P)}} d' = \frac{1}{2P}\left(\frac{T}{d}\right)^2 + O\left(\frac{T}{d}\right)$.

$\Big(\displaystyle\sum_{\substack{n \leq x \\ n \equiv n_0 \bmod P}} n = n_0 + (n_0 + P) + \dots + (n_0 + mP)$, $m = \frac{x}{P} + O(1) \Rightarrow \sum \sim \frac{x^2}{2P} + O(x)\Big)$

This gives

$$G(T) = c\cdot P\cdot \tfrac{m}{2}\cdot L_P(2,\chi)^{-1}\left\{ \sum_{\substack{d\le T\\(d,P)=1}} \chi(d)\left[\frac{T^2}{2d^2P} + O\left(\frac{T}{d}\right)\right]\right\}$$

Now, using $|\chi(d)|\le 1$, the sum in $\{\ \}$ becomes

$$\sum_{\substack{d\le T\\(d,P)=1}} \frac{T^2}{2P}\cdot\frac{\chi(d)}{d^2} + O\left(\frac{T}{d}\right)$$

$$= \frac{T^2}{2P}\left(L_P(2,\chi) + o(1)\right) + T\cdot \underbrace{O\left(\sum_{d\le T}\frac{1}{d}\right)}_{O(T\cdot\log T).}$$

Hence

$$G(T) \sim c\cdot P\cdot\tfrac{m}{2}\cdot L_P(2,\chi)^{-1}\cdot\frac{T^2}{2P}\cdot L_P(2,\chi) \qquad \text{as } T\to+\infty$$

$$= cT^2$$

which again forces

$$c = 1.\ \checkmark$$

<u>$c=\frac{1}{2}$ when $m=2$:</u>

$$S_p(t) = \left(1-\frac{\chi(p)}{p}\right)\sum_{p^\alpha | t}\chi(p^\alpha) \qquad \text{where } \chi = \left(\frac{-\Delta}{p}\right)$$

Here there is no absolute convergence, so products are taken for increasing p:

$$\prod_{\substack{p \nearrow \\ p \nmid P}} \delta_p(t) = L_P(1,\chi)^{-1} \sum_{\substack{d \mid t \\ (d,P)=1}} \chi(d)$$

Then

$$G(T) = c \cdot P \cdot L_P(1,\chi)^{-1} \sum_{\substack{t \equiv t_0 (P) \\ t \leq T \\ d \mid t \\ (d,P)=1}} \chi(d).$$

Let $\Sigma = \sum_{\substack{t \equiv t_0 (P) \\ t \leq T,\, d \mid t \\ (d,P)=1}} \chi(d)$, and we estimate Σ. The method above gives an error term on the order of the main term!, so the sum is split: $\Sigma = \Sigma_1 + \Sigma_2$, where Σ_1 sums over $d \leq T^{1/2}$, and Σ_2 the sum over $d' < T^{1/2}$ $(dd' = t)$. Then

$$\Sigma_1 = \sum_{\substack{d \leq T^{1/2} \\ (d,P)=1}} \chi(d) \cdot \sum_{\substack{d' \\ d' \leq \frac{T}{d} \\ d' \equiv \frac{t_0}{d} \bmod P}} 1 .$$

Here

$$\sum_{\substack{d' \\ \text{as above}}} 1 = \frac{T}{dP} + O(1)$$

so

$$\Sigma_1 = \sum_{\substack{d \leq T^{1/2} \\ (d,P)=1}} \chi(d) \left[\frac{T}{dP} + O(1) \right]$$

$$= \frac{T}{P} \cdot \sum_{\substack{d \leq T^{1/2} \\ (d,P)=1}} \frac{\chi(d)}{d} + O(T^{1/2})$$

$$= \frac{T}{P}\left(L_P(1,\chi) + o(1) \right) + O(T^{1/2})$$

so

$$\Sigma_1 \sim \frac{T}{P} L_P(1,\chi).$$

The integer P was chosen to be divisible by t_0, so $t = dd'$, $t \equiv t_0 \bmod P$ implies $t_0 | t$, $(t_0, d) = 1$, so $t_0 | d'$, hence $d' = t_0 \delta$. Then

$$\Sigma_2 = \sum_{\substack{\delta \leq T^{1/2}/t_0 \\ \delta \equiv \frac{1}{d} \bmod P/t_0 \\ (\delta, P) = 1.}} \chi(\delta) \sum_{\substack{d \\ d \leq T/\delta t_0 \\ d \equiv \delta^{-1} \bmod P/t_0}} 1.$$

We may assume χ is defined mod P/t_0 (enlarging P, if necessary), and then $\chi(d) = \chi(\delta)$ since δ is quadratic.

The inner sum on the right is as before $\frac{T}{\delta P} + O(1)$, so

$$\Sigma_2 = \sum_{\substack{\delta < T^{1/2}/t_0 \\ (\delta, P) = 1}} \chi(\delta)\left(\frac{T}{\delta P} + O(1)\right)$$

$$= \frac{T}{P}\left(L_P(1,\chi) + o(1) \right) + O(T^{1/2})$$

Hence

$$\Sigma_1 \sim \Sigma_2 \sim \frac{T}{P} L_P(1,\chi) \quad \text{as } T \to +\infty.$$

giving

$$T \sim G(T) \sim 2 \cdot c \cdot P \cdot L_P(1,\chi)^{-1} \cdot \frac{T}{P} L_P(1,\chi) \quad \text{as } T \to +\infty$$

i.e.

$$c = \frac{1}{2}\,! \quad \checkmark.$$

$c=1$ when $m=3$: This proof is different from the previous proofs:

(1) If Q and Q' are two quadratic forms and $Q' = \lambda Q$, then $\tau(O_Q) = \tau(O_{Q'})$ since $O_Q = O_{Q'}$.

(2) If Q and Q' have the same discriminant up to a square (in the field) and the same dimension (≥ 3), then $c_Q = c_{Q'}$. (see below)

These imply

(3) If the dimension m is odd and $m \geq 3$, then c is independent of the quadratic form, since λQ has discriminant λ^m times that of Q, so modulo squares, we may obtain any discriminant ✓

Hence it will suffice to show $c=1$ for a single form Q.

Proof of (2): Suppose Q, Q' have the same discriminant and $m \geq 3$. Then there are two formulas; giving c_Q and $c_{Q'}$.

Claim: one can choose the same t_0, P for both forms, and $\delta_p(t) = \delta'_p(t)$ for all $p \nmid P$ ($\delta'_p(t)$ the density for Q').

Pf: An indefinite quadratic form in at least 5 variables represents 0 non-trivially over the field (so over $\mathbb{Z}$).

Form the expression

$$Q(x_1, \dots, x_m) - Q'(y_1, \dots, y_m)$$

which represents 0 non-trivially. This defines t_0 ✓.

P can clearly be chosen the same for both ✓

That $\delta_p(t) = \delta_p(t')$ follows from the formulae for these expressions (they depend only on the discriminant), or ;

M, M' lattices in the same genus, then $M_p \simeq M_p'$ for all $p \nmid 2$, since M_p is determined by its reduction, hence by its discriminant mod p. ✓ This proves the Claim.

Since now the formulae involving c_Q, $c_{Q'}$ are otherwise independent of Q, Q', it follows that $c_Q = c_{Q'}$, and (2) follows. ✓

It is enough now to check $c = 1$ for the form

$$x^2 + y^2 + z^2.$$

There is only one class in the genus of this form (quadratic forms of discriminant 1 can be classified by reduction theory and for $m < 8$ there is only one (for $m = 9$ there are two), and being in the same genus $\Rightarrow$ having the same discriminant). Hence the Siégel formula is:

$$N(t) = \# \text{ of representations of } t \text{ as a sum of 3 squares}$$

$$= c \cdot \prod_p \delta_p(t).$$

Choose $t = 1$: $N(1) = 6$. We compute $\delta_\infty(1)$, $\delta_2(1)$, and $\delta_p(1)$, $p \neq 2$.

$$\delta_\infty(1) = \frac{d \operatorname{vol}(x^2+y^2+z^2 \leq t)}{dt}\Big|_{t=1} = \frac{d}{dt}\left(\tfrac{4}{3}\pi \cdot t^{3/2}\right)\Big|_{t=1}$$

$$= 2\pi.$$

$\delta_2(1)$ can be computed by counting mod 8.

Computation (mod 8) : $x^2 \equiv 0 \ (8)$ if $x \equiv 0, 4$

$x^2 \equiv 4 \ (8)$ $x \equiv 2, 6$

$x^2 \equiv 1 \ (8)$ $x \equiv 1, 3, 5, 7$.

And $x^2+y^2+z^2 \equiv 1 \ (8)$ is possible only if (up to permutation)

$x^2 \equiv 1 \ (8)$ and $\begin{cases} y^2 \equiv z^2 \equiv 0 \ (8) \\ \text{or} \\ y^2 \equiv z^2 \equiv 4 \ (8) \end{cases}$. This gives $3 \times 2 \times 4 \times 2 \times 2 = 3.2^5$

possibilities. Hence $\delta_2(1) = \frac{1}{8^2} \cdot 3.2^5 = 3/2$.

Computation mod $p \neq 2$

$x^2+y^2+z^2 \sim -x^2+yz$ (mod p).

Sol. of $-x^2+yz \equiv 1 \pmod p$:

a) $y \equiv 0$; z arb ; $x^2 \equiv -1$;

number $= p\,(1+\chi(p))$

b) $y \not\equiv 0$; $z = \dfrac{1+x^2}{y}$; x arb ; y arb. $\neq 0$;

$p(p-1)$ sol.

Hence number of sol $= p(p-1) + p + p\chi(p) = p\,(p+\chi(p))$

$\delta_p(1) = 1 + \chi(p)/p = \left(1 - \frac{1}{p^2}\right) / (1 - \chi(p)/p)$.

$$\delta_2(1) = \frac{1}{8^2} \cdot \#\text{ solutions of } x^2+y^2+z^2 \equiv 1 \bmod 8$$

$$= \frac{3}{2}$$

Finally, we compute $\delta_p(1)$ for $p>2$ (the prime 2 is bad for this quadratic form):

$$\delta_p(1) = \frac{1}{p^2}\#\{\text{solutions of } x^2+y^2+z^2 \equiv 1 \bmod p\}$$

$$= 1 + \frac{\chi(p)}{p}.$$

($SO_3/SO_2 = (1-\frac{1}{p^2})/(1-\frac{\chi(p)}{p})$ since SO_2 is for x^2+y^2, so depends on $\chi(p) = (\frac{-1}{p})$)

Hence

$$6 = c \cdot \prod_{p,\infty} \delta_p(1) = c \cdot 2\pi \cdot \frac{3}{2} \cdot \prod_{p\neq 2} (1-\frac{1}{p^2})/(1-\frac{\chi(p)}{p})$$

$$\frac{3}{4} \prod_{p\neq 2}(1-\frac{1}{p^2}) = 3\zeta(2)^{-1} = \frac{6}{\pi^2}$$

$$\prod_{p\neq 2} \frac{1}{1-\frac{\chi(p)}{p}} = L(1,\chi) = 1 - \frac{1}{3} + \frac{1}{5} - + \ldots = \frac{\pi}{4}.$$

Hence

$$6 = c \cdot 2\pi \cdot \frac{3}{2} \cdot \frac{4}{3} \frac{6}{\pi^2} \cdot \frac{\pi}{4}$$

$$\Rightarrow \quad c = 1 \; ! \qquad \checkmark \qquad \text{done}$$

-10-81 **Remarks on Siegel's Proof:**

(1) $m=3$ (ternary forms) The proof showed c was independent of the choice of ternary form and $c=1$ for the form $x^2+y^2+z^2$.

For an odd number of variables, the orthogonal groups are inner forms of each other, hence the proof shows the groups have the same Tamagawa number - the Weil conjecture could be solved if this same statement could be made for arbitrary inner forms of arbitrary groups.

(2) Also of importance in the proof were the use of summation arguments (i.e. the sums $\sum_{\substack{t \le T \\ t \equiv t_0 \\ \text{etc}}}$), i.e. volume arguments. These arguments have origins as far back as Gauss (D.A.), used extensively by Dirichlet, and a "standard" approach for class number formulas.

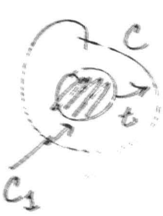
These are related to the Poisson formula:

$$\sum_{x \in \mathbb{Z}^n} \varphi(x) = \sum_{x \in \mathbb{Z}^n} \hat{\varphi}(x) = \mathrm{vol}(C) + \sum_{\substack{x \in \mathbb{Z}^n \\ x \neq 0}} \hat{\varphi}(x)$$

$\varphi = 1$ on C
$= 0$ outside

so the "volume argument" asserts that the remainder is negligible.
This is frequently applied to homothetic balls:

$$\sum_{x \in \frac{1}{t}\mathbb{Z}^n} \varphi_1(x) \underset{\text{Poisson}}{\sim} \sum_{x \in t\mathbb{Z}^n} \hat{\varphi}_1(x) = \hat{\varphi}(0) + \sum_{\substack{x \neq 0 \\ x \in t\mathbb{Z}^n}} \hat{\varphi}_1(x).$$



Nowadays, the Poisson formula is "always" used instead of the volume approach (in the adelic formulation).

(3) The history of this theory is 'cloudy': certainly a progression exists: Gauss, Eisenstein, Smith, Minkowski, Siegel...
For example, when did the notion of $N(t)$ = the mean value of representations of t by forms in a genus first arise? Minkowski gives a formula for it, but the 'idea' is 'probably' not original to him. It would be of interest to trace the development of these ideas.

Applications of Siegel's formula:

(1) The mass formula:
$$\sum_{\substack{M_i \text{ in a} \\ \text{given genus}}} \frac{1}{|\mathrm{Aut}(M_i)|} = \prod_{p,\infty} S_p^{-1}$$

The computation of S_p is a local problem ($p \nmid 2\Delta$ easier than others). Even for the "unit form" $\sum_{i=1}^{m} x_i^2$, the computation of S_2 is not so simple (cf. Magnus, Math Ann, 1936?) – depends on the congruence of m mod 8.

The mass formula can be used to verify that a set of classes in a genus is a complete set of representatives for the genus; e.g. let $\mathfrak{m}_m$ be the mass of the form $\sum_{i=1}^{m} x_i^2$. Then (cf. Magnus)

$$\mathfrak{m}_m = \frac{1}{2^m m!} \quad \text{for } m \leq 8$$
$$> \frac{1}{2^m m!} \quad m \geq 9$$

The automorphism gp. of the unit form is $S_m \cdot \{\pm 1\}$, so the mass formula implies immediately:

for $m \leq 8$, there is only one class in the genus of $\sum_{i=1}^{m} x_i^2$

for $m \geq 9$, there exist at least two classes.

(if $m=9$, there is only one additional form $x_1^2 + \phi_8(x_2, \dots, x_9)$)

where ϕ_8 is a quadratic form of E_8 (takes even values and has disc. 1)).

— o —

(cf. Conway's computation – p. 174 bis)

— o —

The Growth of M_m (cf. Milnor - Hösemoller):

$$m = 27 \quad M_m < 1$$
$$= 28 \quad > 100$$
$$= 29 \quad > 100{,}000$$

($\Rightarrow \exists$ at least 200,000 classes in the genus!)

— o —

Forms of discriminant 1, representing even values; $Q(x) \in 2\mathbb{Z}$ for all x, positive definite ($\Rightarrow m \equiv 0 \bmod 8$; arise from 4 manifolds; $H_2(M,\mathbb{Z})$; signature; cf. Milnor ~1956).

The mass formula here involves products of Bernoulli numbers:

$m = 8$: one form; ϕ_8

$= 16$: $\phi_8 \oplus \phi_8$, ϕ_{16}

$= 24$: (Niemeier) there are 24 forms; one of them gives the Leech lattice - automorphism gp. gives the sporadic group of Conway

$\vdots$

cf. Conway's computation. – note this verifies Niemeier's computation.

Locally at $p \neq 2$, all these forms are in the same genus:

$$x_1x_2 + x_3x_4 + \dots + x_{m-1}x_m \quad \left(\text{matrix} - \begin{pmatrix} \frac{1}{2}\begin{pmatrix}0&1\\1&0\end{pmatrix} & \\ & \frac{1}{2}\begin{pmatrix}0&1\\1&0\end{pmatrix} \\ & & \ddots \end{pmatrix}\right)$$

at $p=2$; $\quad 2(x_1x_2 + \dots + x_{m-1}x_m) \quad \left(\text{matrix} - \begin{pmatrix} \begin{pmatrix}0&1\\1&0\end{pmatrix} & \\ & \begin{pmatrix}0&1\\1&0\end{pmatrix} \\ & & \ddots \end{pmatrix}\right)$

— o —

Conway.

Lattice	g	d/g	
Leech	$2^{22}3^{9}.5^{4}7^{2}11.13.......23$	15570 57285 23304 96000	Conway
A_{24}^{1}	$2^{23}3^{10}5^{6}7^{3}11^{2}13.17.19.23$	417 36889 95840	$\lvert\mathfrak{S}_{25}\rvert\cdot\lvert\mathbb{F}_2\rvert$
D_{24}^{1}	$2^{45}3^{10}5^{4}7^{3}11^{2}13.17.19.23$	248 77125	$=\lvert\mathfrak{S}_{24}\ltimes\mathbb{F}_2^{23}\rvert$
A_{12}^{2}	$2^{22}3^{10}5^{4}7^{2}11^{2}13^{2}$	834 78595 71179 52000	$\lvert\mathfrak{S}_{13}\rvert^2\times 2^2$
D_{12}^{2}	$2^{43}3^{10}5^{4}7^{2}11^{2}$	6727 16268 31500	$\lvert\mathfrak{S}_{12}\ltimes\mathbb{F}_2^{11}\rvert^2\times\lvert\mathbb{F}_2\rvert$
A_{8}^{3}	$2^{23}3^{13}5^{3}7^{3}$	2 25800 76768 65740 80000	$\lvert\mathfrak{S}_9\rvert\lvert\mathbb{F}_2\rvert\,\lvert\mathfrak{S}_3\rvert$
D_{8}^{3}	$2^{43}3^{7}.5^{3}7^{3}$	156 98314 63275 07500	$\lvert\mathfrak{S}_8\ltimes\mathbb{F}_2^{7}\rvert^3\cdot\lvert\mathfrak{S}_3\rvert$
E_{8}^{3}	$2^{43}3^{16}5^{6}7^{3}$	6 38045 60820	$\lvert W(E_8)\rvert\,\lvert\mathfrak{S}_3\rvert$
A_{6}^{4}	$2^{19}3^{9}.5^{4}7^{4}$	83 61079 85490 85716 48000	$\lvert\mathfrak{S}_7\rvert^4\cdot\lvert\mathfrak{S}_4\rvert$
D_{6}^{4}	$2^{39}3^{9}.5^{4}$	19144 96682 32302 48000	$\lvert\mathfrak{S}_6\ltimes\mathbb{F}_2^{5}\rvert\cdot\lvert\mathfrak{S}_4\rvert$
E_{6}^{4}	$2^{32}3^{17}5^{4}$	373 50339 17655 04000	$\lvert W(E_6)\rvert^4\lvert\mathfrak{S}_4\rvert\lvert\mathbb{F}_2\rvert$
A_{4}^{6}	$2^{22}3^{7}.5^{7}$	1806 74574 58471 93247 41632	$\lvert\mathfrak{S}_5\rvert^6\,\lvert\mathfrak{S}_5\rvert\lvert\mathbb{F}_2\rvert$?
D_{4}^{6}	$2^{40}3^{9}.5$	11 96560 42645 18905 00000	$\lvert\mathfrak{S}_4\ltimes\mathbb{F}_2^{3}\rvert^6\cdot\lvert\mathfrak{S}_6\rvert\lvert\mathbb{F}_3\rvert$?
A_{3}^{8}	$2^{31}3^{9}...7$	4375 99241 67383 42400 00000	$\lvert\mathfrak{S}_4\rvert^8\cdot(2^7.3.7)$
A_{2}^{12}	$2^{19}3^{15}5...11$	3129 27932 59189 86240 00000	$\lvert\mathfrak{S}_3\rvert^{12}\cdot 2\,\lvert M_{12}\rvert$?
A_{1}^{24}	$2^{34}3^{3}.5.7.11...........23$	315 22712 17195 90080 00000	$=\lvert M_{24}\rvert\cdot\lvert\mathbb{Z}/2\mathbb{Z}\rvert^{24}$
$A_{17}^{1}E_{7}^{1}$	$2^{27}3^{12}5^{4}7^{3}11.13.17$	3 48314 63546 88000	$\lvert\mathfrak{S}_{18}\rvert\,\lvert W(E_7)\rvert\lvert\mathbb{F}_2\rvert$
$D_{16}^{1}E_{8}^{1}$	$2^{44}3^{11}5^{5}7^{3}11.13$	27 10578 37050	$\lvert\mathfrak{S}_{16}\ltimes\mathbb{F}_2^{15}\rvert\,\lvert W(E_8)\rvert$
$A_{15}^{1}D_{9}^{1}$	$2^{31}3^{10}5^{4}7^{3}11.13$	33 30758 70167 04000	$\lvert\mathfrak{S}_{16}\rvert\cdot\lvert\mathfrak{S}_9\ltimes\mathbb{F}_2^{8}\rvert\lvert\mathbb{F}_2\rvert$
$A_{11}^{1}D_{7}^{1}E_{6}^{1}$	$2^{28}3^{11}5^{4}7^{2}11$	8082 64111 60535 04000	$\lvert\mathfrak{S}_{12}\rvert\lvert\mathbb{F}_2\rvert\lvert\mathfrak{S}_7\ltimes\mathbb{F}_2^{6}\rvert\lvert W(E_6)\rvert\lvert\mathbb{F}_2\rvert$
$D_{10}^{1}E_{7}^{2}$	$2^{38}3^{12}5^{4}7^{3}$	4 13453 55411 36000	$\lvert\mathfrak{S}_{10}\ltimes\mathbb{F}_2^{9}\rvert\cdot\lvert W(E_7)\rvert^2\lvert\mathbb{F}_2\rvert$
$A_{9}^{2}D_{6}^{1}$	$2^{27}3^{10}5^{5}7^{2}$	1 06690 86273 19062 52800	$\lvert\mathfrak{S}_{10}\rvert^2\lvert\mathfrak{S}_6\ltimes\mathbb{F}_2^{5}\rvert\cdot\lvert\mathbb{F}_2\rvert^2$
$A_{7}^{2}D_{5}^{2}$	$2^{31}3^{6}.5^{4}7^{2}$	27 00612 46290 13770 24000	$\lvert\mathfrak{S}_8\rvert^2\lvert\mathbb{F}_2\rvert^2\lvert\mathfrak{S}_5\ltimes\mathbb{F}_2^{4}\rvert\cdot\lvert\mathbb{F}_2\rvert$
$A_{5}^{4}D_{4}^{1}$	$2^{26}3^{10}5^{4}$	522 78522 73863 40638 72000	$\lvert\mathfrak{S}_6\rvert^4\lvert\mathfrak{S}_4\rvert\lvert\mathbb{F}_2\rvert\cdot\lvert\mathfrak{S}_4\ltimes\mathbb{F}_2^{3}\rvert$?
		Total = 10276 37932 58606 15209 60267	

$$M = \frac{n}{d} = \frac{691^2.3617.43867.174611.77683}{2^{45}3^{17}5^{7}7^{4}11^{2}13^{2}17.19.23} = \frac{10276\ 37932\ 58606\ 15209\ 60267}{1294\ 77933\ 34002\ 68515\ 60636\ 14861\ 31200\ 00000}$$

The verification of the Mass-formula for the Niemeier forms.

In 8k dimensions the value of the mass-constant is $B_{4k}B_2B_4B_6\ldots B_{8k-2}/2^{8k-1}(4k)!$,

where the B's are the Bernoulli numbers in the notation $B_2=1/6$, $B_4=1/30$, ...

In 8 dimensions we have $M = 1/2^{14}3^{5}5^{2}7$.

In 16 dimensions we have $M = 691/2^{30}3^{10}5^{4}7^{2}11.13 = 1/2^{15}(16!) + 1/2^{29}3^{10}5^{4}7^{2}$.

$B_2 = 1/6$ $B_4 = 1/30$ $B_6 = 1/42$ $B_8 = 1/30$ $B_{10} = 5/66$ $B_{12} = 691/2730$ $B_{14} = 7/6$

$B_{16} = 3617/510$ $B_{18} = 43867/798$ $B_{20} = 174611/330$ $B_{22} = 11.77683/138$.

283.617 11.131.593

a 28. Schenk.

(2) Representations of $t \in \mathbb{Z}$ by a genus:

If $Q(x)$ is unique in its genus, then $N_Q(t)$ is precisely the number of representations of t by Q, so $= \prod_{p,\infty} \delta_p(t)$.

In particular this applies to $\sum_{i=1}^{m} x_i^2$ for $m \le 8$.

Remark (Siegel): "If M_p is a $\mathbb{Z}_p$-lattice, then $\delta_p(M_p, t)$ (for $t \in \mathbb{Z}_p$, say) is defined. Knowledge of $t \mapsto \delta_p(M_p, t)$ in fact characterizes M_p (up to $\mathbb{Z}_p$-isomorphism)." Siegel attributes this to Minkowski: Serre and Igusa non-commital.

(3) Applications to Values of Zeta Functions of Totally Real Fields

For totally real number fields: m(genus) is certainly a rational number. On the other hand, for $m = 2k+1$, one finds

$$m\,(\text{genus}) = (\text{rat'l number})\, d_k^{1/2}\, \pi^{rN}\left[\zeta_K(2)\zeta_K(4)\ldots\zeta_K(2k)\right]$$

$N = k(k+1)$

$(r = [K:\mathbb{Q}])$. Hence:

$$\zeta_K(2) = d_K^{1/2} \cdot \pi^{2r} \cdot (\text{rational number})$$

$$\vdots$$

$$\zeta_K(2k) = d_K^{1/2} \cdot \pi^{2kr} \cdot (\text{rational number}).$$

This result was stated (without proof) by Hecke, first proved by Siegel.

Equivalently,

$$\zeta_K(1-2k) \in \mathbb{Q}, \quad k = 1, 2, 3, \ldots \qquad (!).$$

Using the orthogonal group in an even number of variables, one obtains;

$$L_K(1-k,\chi) \in \mathbb{Q} \quad , \quad k \geq 1$$

where χ is a quadratic character of K, corresponding to K_χ/K where either

k is even, and K_χ is totally real

or

k is odd, and K_χ is totally complex.

(4) Application of Siegel's formula to Modular Forms:

Let M be a lattice and $M_1, \ldots, M_h$ representatives for the lattices in the genus of M. (positive definite, integral valued (say)).

Define the theta series Θ_M by

$$\Theta_M(z) = \sum_{x \in M} e^{\pi i (x,x) z} \qquad [\text{writing } Q(x) = x \cdot x].$$

$$= \sum_{t=0}^{\infty} N_M(t) e^{\pi i t z} \qquad [N_M(t) = \text{the number of representations of } t \text{ by } M \text{ as before}]$$

Then $\Theta_M(z)$ is holomorphic in $\mathfrak{h} = \{z \mid \operatorname{Im}(z) > 0\}$, and is a modular form of weight $\frac{m}{2}$ ($m = \operatorname{rk} M$) on a congruence subgp of $SL_2(\mathbb{Z})$.

Let $w_i = |\operatorname{Aut}(M_i)|$, $N(t) = \dfrac{1}{\sum \frac{1}{w_i}} \cdot \sum \dfrac{N_{M_i}(t)}{w_i}$, and set

$$E_M = \frac{\sum \frac{\Theta_{M_i}}{w_i}}{\sum \frac{1}{w_i}} = \sum_{t=0}^{\infty} N(t) e^{\pi i t z}, \quad \text{again modular of weight } \frac{m}{2}.$$

(the "mean value of the theta series over the genus")

" **Theorem** E_M is an Eisenstein series

(Siegel: $m \geq 5$, o.k. for $m = 4$: Serre: should be true for all m)

Furthermore:

$$E_M - \Theta_{M_i} \text{ is a cusp form } \quad (i = 1, 2, \dots, h). \text{ "}$$

Hence ;

$$\Theta_M = E + f_M$$ where E is Eisenstein for the genus and f_M is a cusp form.

and

$$\sum_{i=1}^{h} \frac{1}{w_i} f_{M_i} = 0$$

example: Consider the forms in $8k$ variables described above which are even ($\Rightarrow e^{\pi i (x \cdot x) z} = q^{x \cdot x/2}$ for $q = e^{2\pi i z}$) and of discriminant 1. Then Θ is modular on $SL_2(\mathbb{Z})$, of weight $4k$. Here

$$E = 1 + \lambda_k \sum_{t=1}^{\infty} \sigma_{4k-1}(n) q^n \qquad \left(\lambda_k = -\frac{8k}{B_?} \right)$$

Bernoulli number

Then, looking at the n^{th} coefficient; of order n^{4k-1} for E. For a cusp form, the n^{th} coefficient is on the order of $O(n^{2k - 1/2 + \varepsilon})$ for all $\varepsilon > 0$ (Deligne). Hence the cusp form contributes much less than the Eisenstein series.

In particular, given t, it is represented by some M_i $\Leftrightarrow$ it is locally representable, so as a consequence, if $m \geq 4$, t is represented by each form (since E depends only on the genus).

Indication of the proof that $E_M = E$ is Eisenstein: By Siegel:

$$E = 1 + \sum_{t=1}^{\infty} \prod_{p,\infty}' \delta_p(t)\, e^{\pi i t z}.$$

Estimate the coefficients:

$$\prod_{p,\infty} \delta_p(t) = \lambda \cdot t^{\frac{m}{2}-1} \prod_{p} \delta_p(t)$$ (see p. 159 for λ)

To consider δ_p, we consider the Gauss sums attached to a genus: let $\alpha \in \mathbb{Q}/\mathbb{Z}$, of order $\mathrm{den}(\alpha)$, and define

"denominator of α in lowest terms"

$$G(\alpha, M) = \sum_{x \in M/\mathcal{D}\cdot M} e^{2\pi i \alpha (x\cdot x)}.$$

If q is an integer, $q \geq 1$, define

$$d_q(t, M) = \frac{1}{q^{m-1}}$$ # of representations of t by M modulo q, i.e. the number of $x \in M/qM$ with $x\cdot x \equiv t \bmod q$.

(m = the rank of M, as usual).

By taking Fourier series (on M/qM), easily

$$d_q(t, M) = \sum_{\substack{\alpha \in \mathbb{Q}/\mathbb{Z} \\ q\alpha = 0}} \frac{G(\alpha, M)}{\mathrm{den}(\alpha)^m} e^{-2\pi i \alpha t}$$

(sum is finite, since sum is over $q \cdot \alpha = 0$)

The Gauss sums $G(\alpha, M)$ are relatively small:

$$|G(\alpha, M)| \leq (2\,\mathrm{den}(\alpha))^{m/2} \Delta^{1/2} = O(\mathrm{den}(\alpha)^{m/2}).$$

Assume now that $m \geq 5$ and take a sequence of q tending to ∞ multiplicatively (e.g. $1, 2, 3!, 4!, \dots, n!, \dots$). Then

$$\lim d_q(t,M) = \sum_{\alpha \in \mathbb{Q}/\mathbb{Z}} \frac{G(\alpha,M)}{(\operatorname{den}\alpha)^m} e^{-2\pi i \alpha t}, \text{ a "singular series",}$$

which is absolutely convergent, since it is majorized by $\sum_b \frac{1}{b^{\frac{m}{2}-1}}$ (the integers b are the $\operatorname{den}(\alpha)$ above).

But

$$\lim d_q(t,M) = \prod_p \delta_p(t) \quad !$$

Hence

$$E = 1 + \lambda \sum_{\substack{n=1 \\ \alpha \in \mathbb{Q}/\mathbb{Z}}}^{\infty} n^{\frac{m}{2}-1} e^{\pi i n(z-2\alpha)} \frac{G(\alpha,M)}{\operatorname{den}(\alpha)^{m/2}}$$

The dependence on n is through a sum of the form $\sum n^{\delta} e^{nz}$ and these sums can be estimated by a formula of Lipschitz:

$$\sum_{n=1}^{\infty} n^{\rho-1} e^{-nx} = \Gamma(\rho)\Big(\sum_{-\infty}^{\infty}{}_{\ell} (x+2\pi i \ell)^{-\rho}\Big) \qquad \rho > 1,\ \operatorname{Re}(x) > 0.$$

This gives

$$E = 1 + \lambda\, \Gamma\!\left(\tfrac{m}{2}\right) \sum_{\beta \in \mathbb{Q}} \frac{G(\beta,M)}{(\operatorname{den}\beta)^m} \left(\pi i (z-2\beta)\right)^{-\frac{m}{2}}$$

This is an Eisenstein series. //

Remark: one can also show directly that $\sum \frac{1}{w_i} \Theta_{M_i}$ is an eigenfunction for the Hecke operators ($\Rightarrow$ Eisenstein), using

$$\Theta_M | T_p = \text{combination of } \Theta\text{'s of "}p\text{-neighborhoods" of } M.$$

This is the point of view of Weil proving a similar result for more general Θ's. - proving certain "functoriality" properties for mean values.

12-15-81

§ III. SL_n

(1) The Minkowski - Hlawka Theorem

Minkowski was interested in lattices Λ of given volume in $\mathbb{R}^n$ and their intersection with "bodies" S in $\mathbb{R}^n$: $(\Lambda - \{0\}) \cap S$ (circa 1905).

Hlawka (1944) considered this problem from the point of view of volumes.
This was taken up by Siegel (1945), who gave another procedure for computing $\mathrm{vol}(SL_n(\mathbb{R})/SL_n(\mathbb{Z}))$, which shows $\tau(SL_n) = 1$.

Let $V = \mathbb{R}^n$, and Λ a lattice in $\mathbb{R}^n$. Set

$$\mathcal{M}_\delta = \text{the set of all lattices } \Lambda \text{ with } \mathrm{vol}(\mathbb{R}^n/\Lambda) = v(\Lambda) = \delta$$

(where $\delta > 0$).

Then $\mathcal{M}_\delta$ is a homogeneous space over $SL_n(\mathbb{R})$: $g \in G = SL_n(\mathbb{R})$, then $v(g\Lambda) = v(\Lambda)$. Let

$$\mathcal{M} = \bigcup_\delta \mathcal{M}_\delta \quad , \text{ a homogeneous space over } GL_n(\mathbb{R}).$$

Measure on $\mathcal{M}_\delta$:

If $\Lambda_0 \in \mathcal{M}_\delta$, let the stabilizer in SL_n of Λ_0 be $\Gamma_{\Lambda_0} \simeq SL_n(\mathbb{Z})$ (e.g.: $\delta = 1$, $\Lambda_0 = \mathbb{Z}^n$, $\Gamma = SL_n(\mathbb{Z})$), so $\mathcal{M}_\delta = G/\Gamma$. Now, $SL_n(\mathbb{R})$ has a natural measure, defined by any of the following:

(i) The exact sequence $\quad 1 \to SL_n \to GL_n \xrightarrow{\det} \mathbb{G}_m \to 1$

with measures: $\qquad \dfrac{\prod d(a_{ij})}{\det(a_{ij})} \qquad \dfrac{dt}{t}$

induces the natural measure ω on SL_n, ω "=" $\dfrac{\prod d(a_{ij})}{d(\det a_{ij})}$

(ii) Or, from the Lie algebra point of view:

$$\text{a } \underline{\text{basis}} \text{ of } \mathrm{Lie}(Sl_n) = \left\{ \begin{array}{ll} e_{ij} & \text{elementary matrices } i \neq j \\ e_{11} - e_{22} & \\ e_{22} - e_{33} & \\ \vdots & \\ e_{n-1,n-1} - e_{n,n} & \end{array} \right.$$

Then the differential form is dual to $\Lambda(e_\alpha)$.

(iii) View Sl_n as a scheme over $\mathbb{Z}$, so $\exists$ a $\mathbb{Z}$-structure on the Lie algebra, hence a differential form.

<u>Remark</u>: for any reductive group G, $\mathrm{Aut}(G)$ acts on $\det(\mathrm{Lie}\, G)$ (diff. forms of max. degree) by ± 1, hence the Haar measures on a reductive group are invariant by any automorphism.

Hence $\mathcal{M}_8$ has a <u>standard measure</u>, so integration on $\mathcal{M}_8$ is defined (we shall see later that $\mathrm{vol}(\mathcal{M}_8) < \infty$).

— o —

Suppose now that $n \geq 2$, and let $\varphi(x)$ be a function on $\mathbb{R}^n$ sufficiently well-behaved (e.g. bounded, compact support, and Riemann integrable; or even Schwartz-Bruhat with compact support...)

If Λ is a lattice, consider the function

$$\Sigma_\Lambda(\varphi) = \sum_{\substack{x \in \Lambda \\ x \neq 0}} \varphi(x).$$

note

Then we have the

Theorem (Siegel) – (1) The volume c_n of $Sl_n(\mathbb{R})/Sl_n(\mathbb{Z})$ is finite; in fact

$$c_n = \zeta(2)\zeta(3)\ldots\zeta(n)$$

(2) For every φ (as above), we have

$$\frac{1}{c_n}\int_{\mathcal{M}_\delta} \Sigma_\Lambda(\varphi)\, d\Lambda = \frac{1}{\delta}\int_{\mathbb{R}^n} \varphi(x)\,dx$$

(3) Let $\Sigma_\Lambda^{pr}(\varphi) = \sum_{\substack{x\in\Lambda \\ x \text{ primitive}}} \varphi(x)$ (where $x\in\Lambda$ is "primitive" if $x \notin m\Lambda$ for $m \geq 2$, i.e. x is not 'divisible in the lattice Λ'), then

$$\frac{1}{c_n}\int_{\mathcal{M}_\delta} \Sigma_\Lambda^{pr}(\varphi)\, d\Lambda = \frac{1}{\delta\,\zeta(n)}\int_{\mathbb{R}^n} \varphi(x)\,dx$$

(Remark: $n \geq 2$ since $Sl_n(\mathbb{R})$ acts transitively on $\mathbb{R}^n - \{0\}$).

Remark: (2) "means" that the mean value of $\Sigma_\Lambda\varphi$ (the left hand side in (2)) is $\frac{1}{\delta}\int_{\mathbb{R}^n}\varphi(x)\,dx$.

Remark: if we take the 'complete' sum $\Sigma_\Lambda^c\varphi = \sum_{x\in\Lambda}\varphi(x) = \varphi(0) + \sum_{x\neq 0}\varphi(x)$ then we have the equivalent formula

$$\text{mean value of } \Sigma_\Lambda^c\varphi = \varphi(0) + \hat{\varphi}(0)$$

where $\hat{\varphi}$ is the Fourier transform of φ.

<u>Corollary 1</u>: Let S be a bounded set in $\mathbb{R}^n$ which is Jordan measurable ($\Leftrightarrow$ the boundary has Lebesgue measure 0, or the characteristic function is Riemann integrable). Let $\delta > \mathrm{vol}(S)$. Then there is a $\Lambda \in \mathcal{M}_\delta$ with

$$(\Lambda - \{0\}) \cap S = \emptyset$$

<u>Proof</u>: Take φ = characteristic function of S, so $\int \varphi = \mathrm{vol}(S)$. If the statement of the Corollary were false, then

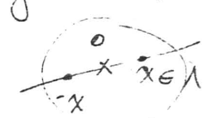
$$\sum_\Lambda \varphi \geqslant 1 \quad \text{for all } \Lambda$$

and hence the mean value is $\geqslant 1$, so $\frac{\mathrm{vol}(S)}{\delta} \geqslant 1$, which is a contradiction.

<u>Corollary 2</u>: Assume S is a "symmetric star body" (i.e. $x \in S$, $|t| \leq 1 \Rightarrow tx \in S$). Let $\delta > \frac{1}{2\zeta(n)} \mathrm{vol}(S)$. Then there exists a $\Lambda \in \mathcal{M}_\delta$ with

$$(\Lambda - \{0\}) \cap S = \emptyset.$$

<u>Proof</u>: Use the formula in (3) of the Theorem: assume the Corollary is false, i.e. any Λ intersects S non-trivially. Then $\sum_\Lambda^{pr} (\varphi) \geqslant 2$; Then



mean value of $\sum_\Lambda^{pr}(\varphi) \geqslant 2$, so $\frac{1}{\delta\zeta(n)} \mathrm{vol}(S) \geqslant 2$, a contradiction.

<u>Remark</u>: this is the Minkowski-Hlawka Theorem – Hlawka stated his result in a less precise form, namely that there is a lattice Λ in $\mathcal{M}_\delta$ with $\sum_\Lambda \varphi \geqslant \frac{1}{\delta} \int_{\mathbb{R}^n} \varphi(x)\,dx$

— o —

<u>References</u>:

J. Cassels - <u>An Introduction to the Geometry of Numbers</u>, Springer-Verlag, 1959

C. Lekkerkerker - <u>Geometry of Numbers</u>, North Holland, 1969

Remark: W. Schmidt has given improvements, e.g. for $n=2$, the bound $\frac{\delta}{vol(S)} > 1$ has been replaced by $\frac{15}{16}$, etc.

— o —

Proof of the Theorem: By induction on n. For $n=1$, there is nothing to prove.

We may assume $\delta = 1$ (by renormalizing, if necessary).

For $G = Sl_n(\mathbb{R})$ and H = the subgroup fixing $e_1 = (1,0,\ldots,0)$, then

$$\mathbb{R}^n = G/H$$

(in fact $H = \begin{pmatrix} 1 & * \\ 0 & \\ \vdots & * \\ 0 & \end{pmatrix} = G_{n-1} \cdot V_{n-1}$ (semi-direct product), with

$G_{n-1} = Sl_{n-1}$, $V_{n-1} \simeq \mathbb{R}^{n-1}$).

Then

$$\int_{\mathbb{R}^n} \varphi(x)\,dx = \int_{\mathbb{R}^n - \{0\}} \varphi(x)\,dx = \int_{G/H} \varphi(x)\,dx$$

with the following measures: (which are compatible)

(a) On $G = G_n = Sl_n$, the standard measure dg

(b) On $H = G_{n-1} \cdot \mathbb{R}^{n-1}$, the product of the standard measures on each factor (well-defined on the semi direct product since G_{n-1} stabilizes the Haar measure on $\mathbb{R}^{n-1}$ - any other action would define a character on Sl_{n-1} into $\mathbb{G}_m$, $\Rightarrow\Leftarrow$).

(c) On $\mathbb{R}^n - \{0\} = G/H$, the measure dx.

For $\Gamma_n = SL_n(\mathbb{Z})$, $\gamma = H(\mathbb{Z}) = SL_{n-1}(\mathbb{Z})\cdot \mathbb{Z}^{n-1}$,

$$\mathrm{vol}(H/\gamma) = \mathrm{vol}(G_{n-1}/\Gamma_{n-1})\cdot \mathrm{vol}(\mathbb{R}^{n-1}/\mathbb{Z}^{n-1})$$

$$= \begin{cases} 1 & \text{if } n=2 \\ c_{n-1} & \text{if } n \geq 3 \end{cases} \quad \text{by induction on } n.$$

$(c_n = \mathrm{vol}(SL_n(\mathbb{R})/SL_n(\mathbb{Z})),\ n \geq 1)$.

We have the inclusion $G \supset H \supset \gamma$, so define a function

$$F(g) = \varphi(ge_1) \quad \text{for } g \in G$$

so that

$$\int_{G/\gamma} F(g)\,dg = \mathrm{vol}(H/\gamma)\int_{G/H} F(\dot g)\,d\dot g \qquad (\dot g = \text{the class of } g \text{ in } G/H)$$

$$= c_{n-1}\int \varphi(x)\,dx.$$

Now since $G \supset \Gamma \supset \gamma$, the left hand side can be written

$$\int_{G/\gamma} F(g)\,dg = \int_{G/\Gamma}\Big\{\sum_{\xi\in\Gamma/\gamma} F(g\xi)\Big\}\,dg$$

$$G/\Gamma = SL_n(\mathbb{R})/SL_n(\mathbb{Z}) = \mathcal{M}_1.$$

The correspondence $SL_n(\mathbb{R})/SL_n(\mathbb{Z})$ is via $g \in G/\Gamma \longleftrightarrow \Lambda = g\Lambda_0$ $(\Lambda_0 = \mathbb{Z}^n)$.
Under this correspondence,

$$\sum_{\xi\in\Gamma/\gamma} F(g\xi) = \sum_{\Lambda}^{pr}(\varphi) \quad \text{for } \Lambda = g\Lambda_0,$$

since

$F(g\xi) = \varphi(g\xi e_1)$, with ξe_1 a primitive vector of Λ_0, so $g\xi e_1$ is primitive in $g\Lambda_0 = \Lambda$, and all primitive vectors are obtained uniquely in this way (by definition of γ).

Hence we obtain the formula

$$\int_{\mathcal{M}_1} \Sigma^{pr}_{\Lambda}(\varphi)\, d\Lambda = c_{n-1} \int_{\mathbb{R}^n} \varphi(x)\, dx .$$

To obtain a sum over all vectors in Λ (not necessarily primitive), observe that any $x \neq 0$ in Λ can be written uniquely as $x = m\tilde{x}$ for some $m \geq 1$, and $\tilde{x}$ primitive. Then

$$\sum_{\substack{x \in \Lambda \\ x \neq 0}} \varphi(x) = \sum_{m=1}^{\infty} \sum_{\substack{x \text{ primitive} \\ \text{in } \Lambda}} \varphi(mx)$$

Let $\varphi_m(x) = \varphi(mx)$. Then $\int \varphi_m(x)dx = \frac{1}{m^n}\int \varphi(x)dx$, so

$$\int_{\mathcal{M}_1} \Sigma_{\Lambda}(\varphi)\, d\Lambda = c_{n-1} \sum_{m=1}^{\infty} \frac{1}{m^n} \int_{\mathbb{R}^n} \varphi(x)\, dx$$

$$= c_{n-1}\, \zeta(n) \int_{\mathbb{R}^n} \varphi(x)\, dx .$$

It suffices now to prove $c_n = c_{n-1}\cdot\zeta(n)$, then induction finishes the proof.

<u>Sketch of Siegel's proof</u> that $c_n = c_{n-1}\cdot\zeta(n)$.

Let $t \in \mathbb{R}$ (think: t small!). Then

$$t^n \sum_{\substack{x \in t\Lambda \\ x \neq 0}} \varphi(x) \text{ tends to } \int \varphi(x)dx \quad \text{as } t \to 0,\ t > 0 .$$

Set $\psi_t(x) = t^n \varphi(tx)$, so $\sum_\Lambda(\psi_t) \underset{\text{as } t\to 0}{\longrightarrow} \int \varphi(x)dx = I(\varphi)$, say.

Then $\sum_\Lambda \psi_t$ is a function of Λ (and t) converging to the constant function $I(\varphi)$ as $t \to 0$.

If interchange of summation and integration is permissable, then

$$\int \sum_\Lambda \psi_t \, d\Lambda \to I(\varphi)\int 1 = I(\varphi)\, c_n .$$

Then

$$\int \psi_t(x)dx = \int \varphi(x)dx = I(\varphi)$$

and

$$\int_{M_1} \sum_\Lambda(\psi_t)\, d\Lambda = c_{n-1}\zeta(n) I(\varphi) = I(\varphi)c_n \Rightarrow c_n = c_{n-1}\zeta(n) \checkmark.$$

The interchange of summation and integration is valid by an argument using Lebesgue dominated convergence, and some serious work (cf. Siegel).

<u>Weil's Proof</u> Assume φ is Schwartz-Bruhat; then by Poisson:

$$\sum_{x\in\mathbb{Z}^n} \varphi(x) = \sum_{y\in\mathbb{Z}^n} \hat\varphi(y) \qquad \left(\hat\varphi(y) = \int_{\mathbb{R}^n} \varphi(x) e^{-2\pi i xy} dx\right).$$

More generally, for any lattice Λ with "dual" lattice Λ' (i.e. $\{y \in \mathbb{R}^n$ with $x\cdot y \in \mathbb{Z}$ for all $x \in \Lambda\}$ - more precisely - start with V and compute Λ' in V', the dual of V); the same formula holds.

Then

$$\sum_\Lambda(\varphi) = \sum_{\Lambda'}(\hat\varphi) + \hat\varphi(0) - \varphi(0)$$

(Here "$d\Lambda = d\Lambda'$" since under $\begin{matrix}\Lambda \leftrightarrow \Lambda' \\ g \leftrightarrow {}^tg^{-1}\end{matrix}$ and ${}^tg^{-1}$ preserves Haar measure - see the Remark above on Haar measures for reductive groups).

Hence,

$$\int_{M_1} \Sigma_\Lambda(\varphi)\,d\Lambda = \int \Sigma_\Lambda(\hat{\varphi})\,d\Lambda + \int \{\hat{\varphi}(0)-\varphi(0)\}\,d\Lambda$$

$$\begin{array}{ccc} \| & \| & \| \\ c_{n-1}\zeta(n)\hat{\varphi}(0) & c_{n-1}\zeta(n)\varphi(0) & c_n(\hat{\varphi}(0)-\varphi(0)) \end{array}$$

As a consequence, $c_n = c_{n-1}\cdot\zeta(n)$ (by choosing a φ with $\hat{\varphi}(0)\neq\varphi(0)$) ✓.

(Remark: a more careful analysis shows the c_n are in fact finite).

12-17-81 <u>Adelic proof of $\tau(SL_n)=1$ (and applications to vector bundles over curves (over finite fields))</u>

<u>Reference</u>: G. Harder - J. Crelle, 1970 (rank 2 vector bundles)
G. Harder and M.S. Narasimhan - Math. Ann. 1975 (arbitrary rank)

Let K be a global field (as usual!), and $G = SL_n$, acting on $X = Aff^n$ in the obvious way. Then G acts transitively on $X' = X - \{0\}$.

The proof that $\tau(SL_n)=1$ is by induction on n.

Let Φ be a Schwartz-Bruhat function on $X(\mathbb{A}) = \mathbb{A}^n$ Then

(1) $$\int_{X(\mathbb{A})} \phi(x)\,dx = \int_{X'(\mathbb{A})} \phi(x)\,dx$$

$(X'(\mathbb{A}) = G(\mathbb{A})/H(\mathbb{A})$ where $H =$ the stabilizer of $e_1 = (1,0,\dots,0)$).

(2) $$\int_{X'(\mathbb{A})} \phi(x)\,dx = \int_{G(\mathbb{A})/G(K)} \Big\{ \sum_{\xi\in X'(K)} \phi(g\xi) \Big\}\,dg$$

Let $\hat{\phi}$ be the Fourier transform of ϕ.

(3) $\int_{X'(\mathbb{A})} \hat{\phi}(x)\,dx = \int_{G(\mathbb{A})/G(K)} \{ \sum_{\xi \in X'(K)} \hat{\phi}({}^t g^{-1} \xi) \} dg$

(4) $\sum_{\xi \in X(K)} \phi(g\xi) = \sum_{\xi \in X(K)} \hat{\phi}({}^t g^{-1} \xi)$

(5) use (2) - (3), (4)

(6) $\hat{\phi}(0) - \phi(0) = \int_{G(\mathbb{A})/G(K)} (-\phi(0) + \hat{\phi}(0))\,dg$

$= \tau(G)\,(\hat{\phi}(0) - \phi(0))$

(7) $\tau(G) = 1$.

Justifications

(1) compute the integrals of $\phi = \otimes \phi_v$: both sides are $\prod_v \int \phi_v |dx|_v$ (because codim $\{0\} \geq 2$, so convergence) and at each local factor, have equality ✓

(2) Using subgroups $G \supset H$, $\Gamma = G(K)$, $\gamma \in H(K)$, apply the two-step integration technique (cf. p. 145), use induction for $\tau(H) = 1$, so $\operatorname{vol}(H/\gamma) = 1$.

(3) Replacing ϕ by $\hat{\phi}$, replacing g by ${}^t g^{-1}$, which leaves the measure invariant.

(4) Poisson. (H'): $\sum_{\xi \in X'(K)} \phi(g\xi) - \sum_{\xi \in X'(K)} \hat{\phi}({}^t g^{-1}\xi) = -\phi(0) + \hat{\phi}(0)$

(5) $\int \phi = \hat{\phi}(0)$

$\int \hat{\phi} = \phi(0)$

The remainder is clean (choose ϕ with $\hat{\phi}(0) \neq \phi(0)$ for (7)). //

— o —

Let now K be a function field over a finite field $k = \mathbb{F}_q$ (with k the field of constants in K), so

$$K = k(C)$$

where C is a smooth, projective, absolutely irreducible curve over k.

Let E be a vector bundle over C of rank $n = \operatorname{rank} E$. (so a locally free sheaf of rank n over the scheme C).

The line bundles (rank 1) of degree 0 over C correspond to the points in the Jacobian $\operatorname{Jac} C$ over $\mathbb{F}_q$, so consider bundles of rank ≥ 2.

If E is a bundle of rank n, then $\overset{n}{\Lambda} E = \det E$ is a line bundle. We shall consider those E where $\det E$ is given:

Let L be a line bundle and define

S_L^n = the "set" of rank n vector bundles E with $\det E \simeq L$. (i.e. there exists an isomorphism)

Define $M = M_L^n$ = the mass of S_L^n, so

$$M_L^n = \sum_{\substack{E \in S_L^n \\ \text{(up to isomorphism)}}} \frac{1}{|\operatorname{Aut} E|} \Leftarrow \text{these are in fact finite.}$$

More restrictively, let

$$S^n_{L,1} = \text{the classes of } (E,\phi) \text{ where } \phi : \det E \simeq L$$

and then for $E \in S^n_{L,1}$, let $\mathrm{Aut}_1 E$ be the subgroup of $\mathrm{Aut}(E)$ consisting of elements which are compatible with ϕ. Then let

$$M^n_{L,1} = M_1 = \sum_{E \in S^n_{L,1}} \frac{1}{|\mathrm{Aut}_1 E|}.$$

Then in fact

$$M = \frac{1}{q-1} M_1 .$$

(follows from $\displaystyle \frac{1}{|\mathrm{Aut}\, E|} = \frac{1}{(q-1)} \sum_{\substack{(E,\phi) \\ \text{possible } \phi}} \frac{1}{|\mathrm{Aut}_1(E)|}.$)

<u>Theorem</u> (Harder) — $M_1 = q^{(n^2-1)(g-1)} \zeta_C(2) \dots \zeta_C(n)$

where ζ_C is the zeta function of the curve C and g is the genus of C. Equivalently,

$$M_1 = \zeta_C(-1) \dots \zeta_C(-n+1).$$

Explicitly, $\zeta_C(s) = Z(t)$ $(t = q^{-s})$ where

$$Z(t) = \frac{\prod_{\alpha=1}^{2g} (1 - \omega_\alpha t)}{(1-t)(1-qt)}$$

where the ω_α are the eigenvalues of Frobenius acting on $\mathrm{Jac}\, C$, with $|\omega_\alpha| = q^{1/2}$.

In particular:

$$\zeta_C(i) = \frac{\prod (1-\omega_\alpha q^{-i})}{(1-q^{-i})(1-q^{1-i})}$$

so

$$M_1 = q^{(n^2-1)(g-1)} \frac{\prod_{\alpha,\, 2\le i\le n} \left(1-\frac{\omega_\alpha}{q^i}\right)}{(1-q^{-1})\prod_{j=2}^{n-1}(1-q^{-j})^2 \cdot (1-q^{-n})}$$

The order of magnitude of M_1 can be read off from the formula above: $M_1 \sim q^{(n^2-1)(g-1)}$.

Proof of the Theorem: Use $\tau(SL_n)=1$: If Ω is an open, compact subgroup of $G(A)$, then acting on $G(A)/G(K)$ gives: (cf. p. 137)

$$1 = \sum_{\substack{x \text{ a representative} \\ \text{of } \Omega\backslash G(A)/G(K)}} \frac{\mathrm{vol}(\Omega)}{|\Gamma_x|}, \quad \text{with } \Gamma_x = \Omega \cap x\Gamma x^{-1}$$

$$(\Gamma = G(K))$$

$$= \mathrm{vol}(\Omega) \sum \frac{1}{|\Gamma_x|}.$$

Hence

$$\sum_x \frac{1}{|\Gamma_x|} = \frac{1}{\mathrm{vol}(\Omega)}.$$

We apply this as follows: let E_0 be a vector bundle of the type considered (so $\det E \simeq L$). View E_0 as a locally free sheaf. The closed pts correspond to the places v and the generic pt to K. Let

$V = V_0$ be the fibre at the generic pt (a vector space of dimension n / K).

Then viewing V as the rational sections, the corresponding E_v° can be viewed as lattices (over the local rings), $E_v^\circ \subset V$. (the superscript denotes dependence on E_0).

Another set of $E_v \subset V = V_0$ is of this type if $E_v = E_v^\circ$ for almost all v and $\det E_v = \det E_v^\circ$ for all v.

Then

$$S^n_{L,1} \quad \text{is the set of all } (E_v) \text{ modulo the action of}$$

$$G(K) = SL_n(K) \quad (= SL(V)).$$

Hence

$$S^n_{L,1} \text{ "consists" of double cosets modulo } G(K) \text{ and}$$

$$\Omega = \prod_v \underbrace{\mathrm{Aut}_1 E_v^\circ}_{}$$

the subgroup of $SL_n(K_v)$ preserving the lattice (an identification of ring with its completion is being used here).

It therefore remains to compute $\mathrm{vol}(\Omega)$ for this Ω.* With the correcting factor due to the Tamagawa measure, one obtains

$$\mathrm{vol}(\Omega) = q^{(1-g)\dim G} \prod_v \mathrm{vol}(\Omega_v)$$

with $\Omega_v \cong SL_n(\hat{O}_v) \leftarrow$ completion of the local ring. Here

$$\mathrm{vol}(\hat{O}_v) = \prod_{i=2}^{n} (1 - q_v^{-i}), \qquad q_v - N_v = q^{\deg v}.$$

Since $\dim G = n^2-1$ here, this gives the formula in the Theorem (modulo plus de details!)

— o —

Let now $n(E)$ denote the number of non-zero sections of E with an $E \in S_L^n$. (so $n(E) = q^{h^0(E)} - 1$ where $h^0(E) = \dim(H^0(C, E))$).

We shall give a formula for the mean value of $n(E)$, namely for

$$\frac{1}{M} \sum_E \frac{n(E)}{|\mathrm{Aut}\, E|} \qquad (E \in S_L^n).$$

<u>Theorem</u>: ($n \geq 2$) The mean value of $n(E)$, $E \in S_L^n$ $= \frac{1}{M} \sum_E \frac{n(E)}{|\mathrm{Aut}\, E|} = q^{c+n(1-g)}$

where c is the "Chern class" of L (or of E) $= \deg L$.

<u>example</u>: L trivial, $c = 0$, $g = 1$, then $q^{c+n(1-g)} = 1$, so the number of non-zero sections is ("in mean value") 1.

—o—

Let $n'(E)$ denote the number of sections of E which are <u>everywhere</u> non-zero.

<u>Theorem</u>: ($n \geq 2$) the mean value of $n'(E)$ is $q^{c+n(1-g)} / \zeta_C(n)$.

—o—

<u>Sketch of the Idea</u>: Take a function $\phi = \otimes \phi_v$ where $\phi_v = \begin{cases} 1 & \text{on } \hat{E}_v^0 \\ 0 & \text{outside} \end{cases}$

and apply the procedure of Weil above: $\int_{G(A)/G(K)} = \sum_{\text{orbits of } \Omega} n(E)$

$$= \mathrm{vol}(\Omega) \sum \frac{n(E)}{|\mathrm{Aut}\, E|}.$$

Remark: Observe that the mass is indep of the chosen line bundle, and the mean values above depend on L through its degree.

Example: $g=0$, $n=2$, so $C = \mathbb{P}_1/k$. By Grothendieck, a rank 2 vector bundle can be written

$$\mathcal{O}(n) \oplus \mathcal{O}(m) = L_n \oplus L_m$$

where L_n is the unique line bundle of degree n, and this decomposition is unique up to interchanging m and n.

Let $L = L_0$ be the trivial line bundle, so

$$E = L_n \oplus L_{-n} \qquad n = 0, 1, 2, \ldots$$

The automorphisms are given as follows

$$n = 0 \qquad GL_2(\mathbb{F}_q) \qquad \text{numbering } q(q-1)^2(q+1)$$

$$n \geq 1 \qquad (q-1)^2 q^{2n+1}$$

(since $L_n \oplus L_n$ $\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$ i.e. $\begin{pmatrix} \mathbb{F}_q^* & \text{polynomials of degree} \leq 2n \\ 0 & \mathbb{F}_q^* \end{pmatrix}$ $\rightleftarrows$ sections of L_{-n} to L_n)

The mass formula is then

$$M = \frac{1}{q(q-1)^2(q+1)} + \sum_{n=1}^{\infty} \frac{1}{(q-1)^2 q^{2n+1}}$$

$$= \frac{1}{(q-1)^2} \left\{ \frac{1}{q(q+1)} + \frac{1}{q} \cdot \frac{1}{q^2} \cdot \frac{1}{1-\frac{1}{q^2}} \right\}$$

$$= \frac{1}{(q-1)^2} \left\{ \frac{1}{q(q+1)} + \frac{1}{q(q+1)(q-1)} \right\}$$

$$= \frac{1}{(q-1)^3(q+1)}$$

The theorem gives the value $\frac{q^{-3}}{(q-1)} \cdot \zeta_C(2)$. Here

$$Z(t) = \frac{1}{(1-t)(1-qt)} \quad , \quad t = q^{-2} \text{ gives}$$

$$\zeta_C(2) = \frac{1}{(1-q^{-2})(1-q^{-1})}$$

so

$$q^{-3} \cdot \frac{1}{q-1} \cdot \zeta_C(2) = \frac{1}{(q-1)(q-1)(q^2-1)} \quad \checkmark$$

Suppose now we choose $L = L_1$. Then $E = L_n \oplus L_{1-n}$ $n \geq 1$, so $E = L_0 \oplus L_1$, $L_{-1} \oplus L_2, \ldots$, and

$$w_n = |\operatorname{Aut}(L_n \oplus L_{1-n})| \text{ computed as before for } L_{-n} \oplus L_n,$$
$$= (q-1)^2 q^{2n}$$

and so

$$M = \sum_{n=1}^{\infty} \frac{1}{(q-1)^2 q^{2n}} = \frac{1}{(q-1)^2 q^2 (1-\frac{1}{q^2})} = \frac{1}{(q-1)^2(q^2-1)} \checkmark$$

— o —

Application (Harder) to computing Betti numbers of varieties:

For simplicity, choose $n = 2$, $g \geq 2$, $c(L) \equiv 1 \bmod 2$.

Definition: E is a stable bundle (notion due to Mumford), which here $(n=2)$ means E does not contain a sub line bundle F with $c(F) > \frac{1}{2}c(E) = \frac{c}{2}$, $c(F) > c(E/F)$; stable and semistable are equivalent here as $c(L) \equiv 1 \bmod 2$

Here, $\underline{\text{stable}} \Leftrightarrow$ points over $\mathbb{F}_q$ of a moduli variety $\mathcal{M}_L$ (which is projective and non-singular), $\mathrm{Aut}\, E \cong \mathbb{F}_q^{\times}$),

so contribution of stable bundles in Mass M is $\frac{1}{q-1} |\mathcal{M}_L(\mathbb{F}_q)|$. For the remaining bundles,

unstable $\Leftrightarrow$ $\underline{\text{canonical}}$ extensions of two line bundles

so their contribution to the Mass can be computed (cf. Harder):

$$\text{"}M_{\text{unstable}}\text{"} = \frac{1}{(q-1)} \frac{h \cdot q^g}{(q-1)(q^2-1)}$$

where $h = |\mathrm{Jac}(\mathbb{F}_q)| = \prod_{\alpha=1}^{2g} (\omega_\alpha - 1)$.

Observe $M_{\text{unstable}} = O(q^{2g-4})$ since $h = O(q^g)$. Since we have $M = O(q^{3g-4})$ $\left(= \frac{1}{(q-1)} q^{3(g-1)} \ldots\right)$. Hence the contribution of unstable bundles is relatively slight w.r.t. q, i.e. "most" come from pts. $\mathcal{M}_L(\mathbb{F}_q)$. More precisely,

$$M_1 = |\mathcal{M}_L(\mathbb{F}_q)| + O(q^{2g-3}).$$
$$\|$$
$$q^{3g-3}\zeta(2).$$

so $\zeta(2) = \dfrac{\prod \left(1 - \frac{\omega_\alpha}{q^2}\right)}{(1-q^{-1})(1-q^{-2})} = 1 + \frac{1}{q} + \left(-\sum \frac{\omega_\alpha}{q^2}\right) + \ldots$ gives

$$|\mathcal{M}_L(\mathbb{F}_q)| = q^{3g-3} + q^{3g-4} - \sum \omega_\alpha q^{3g-5} + \ldots$$

Comparing this with Deligne's theorem, we see that the variety is connected. (it is known that the dimension is pure), and

$B_1(M_L) = 0$ (otherwise a term $q^{3g-4-\frac{1}{2}}$ would appear).

$B_2(M_L) = 1$

$B_3(M_L) = 2g$

∵ cf. Harder.