16/01/14

Algebraic Number Theory ①

Algebraic Number Fields $K/\mathbb{Q}$, $[K:\mathbb{Q}] < \infty$

(often interested in infinite extensions e.g.
$\mathbb{Q}^{cyc} = \mathbb{Q}(\{\zeta_n = e^{2\pi i/n}, \forall n \geq 1\})$)

<u>Classical Approach has two parts:</u>

i) <u>Algebraic part</u> : $\mathcal{O}_K$, ring of algebraic integers of K

- study algebraic properties of this ring
- ideals in $\mathcal{O}_K$, Theorem: Every non-zero ideal can be uniquely written as a product of prime ideals ($\mathcal{O}_K$ a Dedekind domain)
- fractional ideal, a non-zero, finitely generated $\mathcal{O}_K$-submodule of K. These form a <u>group</u> under multiplication.

We have <u>principal fractional ideals</u> of the form $x\mathcal{O}_K$ ($x \in K$, $x \neq 0$)
These form a subgroup with quotient group $Cl(K)$, the class group of K.

- $\mathcal{O}_K^*$, the unit-group of K. Because $x\mathcal{O}_K = \mathcal{O}_K \iff x \in \mathcal{O}_K^*$, it is reasonable to expect a connection between $\mathcal{O}_K^*$ and $Cl(K)$.

(one such is the so-called <u>Analytic Class-Number Formula</u>)
Algebra alone says nothing about $Cl(K)$ and $\mathcal{O}_K^*$. To say more, we need some "analytic" input, geometry of numbers.

ii) <u>Second Part</u> K, $[K:\mathbb{Q}] = n$, $\exists n$ embeddings $\sigma_1, \dots, \sigma_n : K \hookrightarrow \mathbb{C}$
which can be ordered so that $\sigma_1, \dots, \sigma_{r_1} : K \hookrightarrow \mathbb{R}$

$\sigma_{r_1+1}, \dots, \sigma_{r_2} : K \hookrightarrow \mathbb{C}$

$2r_2 + r_1 = n$

$\overline{\sigma_{r_1+1}} = \sigma_{r_2+r_1+1}$, etc

1

These fit together to give $\sigma : (\sigma_1, \ldots, \sigma_{r_1+r_2}) : K \hookrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$
the <u>Minkowski embedding</u>

Key fact: $\sigma(\mathcal{O}_K)$ is a <u>lattice</u> (rank n, discrete subgroup.
This leads to proof that $Cl(K)$ is <u>finite</u> and
(considering action of K^* by multiplication) that
$\mathcal{O}_K^*$ is finitely generated of rank $r_1 + r_2 - 1$ (Dirichlet's Unit Theorem)

<u>"Modern" Approach</u>:

Starting point is that prime ideals and embeddings into $\mathbb{R}$ or $\mathbb{C}$ are two different cases of a general notion, that of <u>absolute value</u> (or <u>place</u>) of K.

<u>Example</u>

$K = \mathbb{Q}$, we have the usual Archimedean absolute value
$|x|_\infty = |x|$, absolute value in $\mathbb{R}$.

But for every prime number p, we have <u>p-adic absolute value</u>

$$|x|_p = \begin{cases} 0 & x = 0 \\ \frac{1}{p^r} & \text{if } x = p^r \frac{a}{b},\ r \in \mathbb{Z},\ a, b \in \mathbb{Z},\ (ab, p) = 1 \end{cases}$$

This also satisfies the triangle inequality, $|x+y|_p \leq |x|_p + |y|_p$
actually, $|x+y|_p \leq \max(|x|_p, |y|_p)$ (strong triangle inequality)

$\mathbb{R}$ = completion of $\mathbb{Q}$ w.r.t. $|\cdot|_\infty$

For every prime p, we also have completion w.r.t. $|\cdot|_p$, the field of p-adic numbers $\mathbb{Q}_p$

- replacement for Minkowski space is the embedding

$$\mathbb{Q} \hookrightarrow \prod_p \mathbb{Q}_p \times \mathbb{R} = \prod_{p \leq \infty} \mathbb{Q}_p \quad (\mathbb{Q}_\infty = \mathbb{R})$$

16/01/14

Algebraic Number Theory ①

Books

Cassels + Frohlich "Algebraic Number Theory", Chapters 1 + (especially) 2

Neukirch "Algebraic Number Theory"

Algebraic Preliminaries

1. (Galois Theory) Trace and Norm

L/K a finite extension, degree n ($L \cong K^n$ as a K-vector space)

Then $\forall x \in L$, $u_x : L \to L$, $y \mapsto xy$ is a K-linear endomorphism of L.

The norm of x is $\begin{cases} N_{L/K}(x) = \det_K u_x \in K & \text{multiplicative hom } L^\times \to K^\times \\ Tr_{L/K}(x) = \cancel{\det_K}\ tr_K\, u_x \in K & \text{additive hom } L \to K \end{cases}$
trace

If L/K is separable, then

$N_{L/K}(x) = \prod \sigma_i(x)$ where $\{\sigma_i\}$ is the set of

$Tr_{L/K}(x) = \sum \sigma_i(x)$ K-homs $\sigma_i : L \hookrightarrow \bar{K}$

$Tr_{L/K}$ is not identically zero (equivalent to separability)

For L/K separable, the map $L \times L \xrightarrow{\Psi} K$, $(x,y) \mapsto Tr_{L/K}(xy)$ is a non-degenerate, symmetric, K-bilinear form Ψ on L (i.e. Ψ induces an isomorphism between L and its dual $Hom_K(L,K)$).

This is called the trace form.

In particular, if L/K is a finite Galois extension, then (if we take $\bar{K}$ an algebraic closure of L) then each σ_i is given by composing an element of $Gal(L/K)$ with the embedding $L \hookrightarrow \bar{K}$, so $N_{L/K}(x) = \prod_{\sigma \in Gal(L/K)} \sigma(x)$

$$Tr_{L/K}(x) = \sum_{\sigma \in Gal(L/K)} \sigma(x)$$

18/01/14 Algebraic Number Theory (1)

2 Commutative Algebra

All rings are commutative with 1.

$R^* = \{\text{invertible elements of } R\}$

a) Integral Closure

$R \subset S$ rings, $x \in S$ is integral over R if $\exists f \in R[T]$ monic with $f(x) = 0$. Equivalent conditions:

i) $R[x]$ is a finite R-algebra (i.e. f.g. as an R-module)

ii) $\exists S' \subset S$ containing R, x which is a finite R-algebra

(exercise : these are equivalent) c.f. Commutative Algebra (8) 3-7 det type argument

$R' = \{x \in S \mid x \text{ integral } /R\}$ is then a ring, the integral closure of R in S.

If $R' = R$ then we say that R is integrally closed in S.

If R is a domain, integrally closed in Frac(R), then we say R is normal (or integrally closed)

Proposition

R a normal domain which is Noetherian (every ideal is f.g.)

$K = \text{Frac}(R)$, L/K a finite separable extension. If S is the integral closure of R in L, then S is a finite R-algebra. (Standard example: $R = \mathbb{Z}$, $K = \mathbb{Q}$, $[L:K] < \infty$, $S = \mathcal{O}_L$, S has a finite $\mathbb{Z}$-basis)

Proof

$n = [L:K]$. Then Frac$(S) = L$. In fact, $\forall x \in L$, $\exists a \in R \setminus \{0\}$ with $ax \in S$, so $x \in \text{Frac}(S)$.

(take $a = b^n$, b any common denominator for coefficients of the min. poly. of x over K)

If $x \in S$, then all of its conjugates will be integral over $\{\sigma(x) \mid \sigma : L \hookrightarrow \overline{K}\}$. So $\underbrace{Tr_{L/K}(x), N_{L/K}(x)}_{\in K}$ are integral over R, hence they are in R since R was normal.

Now, choose a basis (e_i) for L/K with all $e_i \in S$ can clear denominators by first line of proof.

The trace form $(x, y) \mapsto Tr_{L/K}(xy)$ is non-degenerate:

Let f_i be the dual basis. Now $f_i \in L$, $Tr_{L/K}(e_i f_j) = \delta_{ij}$

Let $x \in S$: write $x = \sum a_i f_i$, $a_i \in K$.

So as $e_i x \in S$, $R \ni Tr_{L/K}(xe_i) = a_i$

$\therefore S \subset \sum_i R f_i$, so because R is Noetherian, S is an f.g. R-module $\square$

b) Local Rings

R is a local ring if it has a unique maximal ideal.

e.g. R a field $\underset{(0)}{\text{or}}$ $R = k[[\underset{(x)}{x}]]$, k a field

Equivalent condition: R is local $\Updownarrow$ $R \setminus R^*$ is an ideal (the maximal ideal)

Localisation

Let R be an integral domain, $P \subset R$ a prime ideal.

$R_P = \{\frac{x}{y} \mid x, y \in R, y \notin P\}$, a local ring with maximal ideal $m_P = \{\frac{x}{y} \mid x \in P, y \in R \setminus P\}$

called the localisation of R at P.

e.g. $P = (0)$, $R_P = Frac(R)$

$\mathbb{Z}_{(p)} = \{\frac{x}{y} \mid x, y \in \mathbb{Z}, p \nmid y\}$

NOT $\mathbb{Z}_p$ the p-adics

18/01/14 Algebraic Number Theory ②

Notations

$\mathbb{N} = \{0, 1, 2, \dots\}$, $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.

"$\subset$" the same as "$\subseteq$" . "$\subsetneq$" for strict inclusion.

$a := b$, a defined to be b.

1 Valuations and absolute values

Definition

A (rank 1) valuation of a field K is a non-trivial homomorphism $v : K^* \to (\mathbb{R}, +)$ such that

~~kernel is 1 or K^*, so just $v(1) = 0$~~

(V) $\forall x, y \in K^*$ with $x \neq -y$, $v(x+y) \geq \min(v(x), v(y))$

Remark

By convention, we extend v to K by setting $v(0) = +\infty$

Some writers do not require v to be non-trivial.

There are valuations of higher rank (replace $\mathbb{R}$ by some totally ordered group) but we will not need those.

Examples

i) p-adic valuation $v_p : \mathbb{Q}^* \to \mathbb{Z}$, $v_p(p^n \frac{a}{b}) = n$ if $(ab, p) = 1$.

ii) K an alg. number field, $\underline{P} \subset \mathcal{O}_K$ a non-zero prime ideal.

Let $v_{\underline{P}}(x)$ = exponent of $\underline{P}$ occurring in the exponent of the prime factorisation of $x\mathcal{O}_K$.

This is obviously a homomorphism (unique factorisation of ideals).

To check that this satisfies (V), we replace x, y by xz, yz for any $z \in K^*$, so WLOG, we can assume $x, y \in \mathcal{O}_K$.

Then $v_{\underline{P}}(x) = n \iff x \in \underline{P}^n \setminus \underline{P}^{n+1} \Rightarrow$ (V) trivially.

since $x+y \in \underline{P}^n + \underline{P}^m = \underline{P}^{\min(n,m)}$ $v_{\underline{P}}(x) = n$, $v_{\underline{P}}(y) = m$

iii) K = field of meromorphic functions on $\mathbb{C}$.

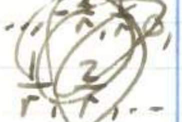
$v(f) = \mathrm{ord}_{z=0}(f)$ is a valuation.

We say that v is <u>discrete</u> if $v(K) \subset \mathbb{R}$ (the value group of v) is a discrete subgroup of $\mathbb{R}$, in which case $v(K) = \mathbb{Z}r$ for some $r > 0$. A discrete valuation is said

pick least $r>0$ in $\mathrm{Im}(v)$

to be <u>normalised</u> if $v(K) = \mathbb{Z}$.

i), ii), iii) are normalised discrete valuations. Later, we will see useful valuations with $v(K^*) = \mathbb{Q}$.



If v is any valuation and $\alpha > 0$, then αv is also a valuation. We say that v, αv are <u>equivalent</u> (so that every discrete valuation is equivalent to a normalised one).

$\ldots, -r, 0, r, 2r, \ldots$

<u>Proposition 1.1</u>

Let v be a valuation on K. Then if $v(x) \neq v(y)$,
$v(x+y) = \min(v(x), v(y))$.

<u>Proof</u>

WLOG, $v(x) < v(y)$, so $v(x) = v((x+y) + (-y))$

$$\geq \min(v(x+y), v(y))$$

Hence $v(x) \geq v(x+y) \geq v(x) \Rightarrow$ equality.

<u>Definition</u>

K a field, R a proper sub-ring. R is a <u>valuation ring</u> (of K) if $\forall x \in K \setminus R$, $x^{-1} \in R$.

<u>Remark</u>

If $x, y \in R \setminus \{0\}$, then this implies that at least

18/01/14 Algebraic Number Theory ②

one of x/y, y/x is in R, so in particular, $\mathrm{Frac}(R) = K$.

Theorem 1.2

Let R be a valuation ring of K.

i) R is local.

ii) R is normal

iii) Every finitely generated ideal of R is principal. In particular, if R is Noetherian, then it is a PID.

Proof

i) Let $m = R \setminus R^*$. Trivially, $x \in m$, $y \in R \Rightarrow xy \in m$

If $x, y \in m \setminus \{0\}$ then WLOG $y/x \in R$, hence

$$x + y = \underset{\substack{\cap \\ m}}{x}\,(1 + \underset{\substack{\cap \\ R}}{y/x}) \in m.$$

Hence m is an ideal, so R is local.

since $m = R \setminus R^*$ is as big as possible, must be unique maximal.

21/01/14

Algebraic Number Theory ③

Valuation Ring $R \subset K$ ($x \in K \setminus R \Rightarrow x^{-1} \in R$)

ii) We prove that R is integrally closed (normal)

Let $x \in K^*$ be integral over R, so $x^n + \sum_{i=0}^{n-1} a_i x^i = 0$, $a_i \in R$.

If $x^{-1} \notin R$, then $x \in R$ and we are done. Otherwise, $x^{-1} \in R$ and $1 = \underbrace{-x^{-1}}_{\in R}\underbrace{\left(\sum_{i=0}^{n-1} a_i (x^{-1})^{n-i-1}\right)}_{\in R}$ so $x^{-1} \in R^*$.

Hence $x \in R$.

iii) Every f.g. ideal of R is principal. If $x, y \in R$ then

$$xR + yR = \begin{cases} xR & \text{if } y/x \in R \\ yR & \text{if } x/y \in R \end{cases}$$

□

Theorem 1.3

K a field, v a valuation on K. Define $R_v = \{x \in K \mid v(x) \geq 0\}$

$m_v = \{x \in K \mid v(x) > 0\}$ [N.B. $0 \in m_v$ as $v(0) = +\infty$]

i) Then R_v is a valuation ring of K with maximal ideal m_v and v induces an isomorphism $K^*/R_v^* \xrightarrow{\sim} v(K^*) \subset \mathbb{R}$

ii) R_v is a maximal proper sub-ring of K, depending only on the equivalence class of v.

iii) If v, v' are valuations of K, and $R_v \subset R_{v'}$, then $R_v = R_{v'}$ and v, v' are equivalent. In particular, for any valuation ring R of K, $\exists$ at most one equivalence class of valuations v with $R = R_v$.

Remark

There are valuation rings which aren't of this form, R_v, and they are associated to valuations of rank >1.

Examples

1. $\mathbb{Z}_{(p)}$, R_v with $K=\mathbb{Q}$, $v = p$-adic valuation
2. $\mathcal{O}_{K,\mathfrak{p}}$, localisation of $\mathcal{O}_K$ at a prime $\mathfrak{p}$, valuation ring of $v_{\mathfrak{p}}$.

Proof

i) From the definition of valuation, R_v is a sub-ring of K, and $R_v \neq K$ as v is $\neq 0$. If $x \notin R_v$, then $v(x) < 0$ so $v(x^{-1}) = -v(x) > 0$ $\Rightarrow x^{-1} \in R_v$. So R_v is a valuation ring, with non-units m_v.
Finally, $\ker(v) = R_v^*$.

ii) Let $x \in K \setminus R_v$. Then $v(x) < 0$, hence $\forall y \in K$, $\exists n \in \mathbb{N}$ such that $v(y) > n\,v(x) \Rightarrow y/x^n \in R_v$, so $y \in R_v[x]$ i.e. $R_v[x] = K$. So R_v is maximal.
Trivially, v, v' equivalent $\Rightarrow R_v = R_{v'}$

iii) By maximality in ii), get $R_v = R_{v'}$ (hence $m_v = m_{v'}$).
So $\forall x, y \in K$, $v(x) \geq v(y)$

$$\Updownarrow$$
$$x/y \in R_v = R_{v'}$$
$$\Updownarrow$$
$$v'(x) \geq v'(y) \qquad (*)$$

Let $0 \neq \pi \in m_v$ (so $v(\pi) > 0$). Then $\forall p/q \in \mathbb{Q}$, $q > 0$,
$\frac{v(x)}{v(\pi)} \geq p/q \iff v(x^q) \geq v(\pi^p) \iff \frac{v'(x)}{v'(\pi)} \geq p/q$ by $(*)$
So $\frac{v(x)}{v(\pi)} = \frac{v'(x)}{v'(\pi)}$ for any $x \in K^*$, so v, v' are equivalent $\square$

Definition

i) R_v is called the <u>valuation ring</u> of v.

ii) A <u>discrete valuation ring</u> is the valuation ring of a discrete valuation.
DVR

21/01/14

Algebraic Number Theory ③

Proposition 1·4

A domain R is a DVR $\Leftrightarrow$ it is a PID with unique non-zero prime ideal.

Proof

($\Leftarrow$) R a PID with unique prime ideal $\pi R \neq 0$, $K = \mathrm{Frac}(R)$.

If $x \in R \setminus \{0\}$, $xR = \pi^n R$ for some $n \in \mathbb{N}$. $v(x) := n$

because a PID is also a UFD, $x = \pi^n u$, some n, unit u

For $\frac{x}{y} \in K$, $v(\frac{x}{y}) := v(x) - v(y)$. and all ideals are αR, so π exists

Easy to see that v is a normalised discrete valuation.

($\Rightarrow$) Let R be a DVR. Choose $\pi \in m_R$, non-zero, with $v(\pi)$ minimal (possible since v is discrete). Then $m_R = \pi R$.

$\pi R \subset m_R$ is clear. Now $v(x) = n v(\pi) \Rightarrow x = \pi^n u$

If $I \overset{\neq 0}{\subset} R$ is any ideal, then I contains π^m for some minimal $m \geq 1$, and it follows that $I = \pi^m R$.

Lemma 1·5

R a ring, $\pi \in R$ not a zero divisor. Then $\forall m, n \geq 0$, we have an R-module isomorphism $R/\pi^n R \xrightarrow[\times \pi^m]{\sim} \pi^m R / \pi^{m+n} R$

Proof (Obvious) Easy to check well-defined, injective, surjective

Theorem 1·6

A valuation of $\mathbb{Q}$ is equivalent to some v_p, p prime.

Any valuation of a number field K is equivalent to some $v_{\mathfrak{p}}$, $\mathfrak{p} \subset \mathcal{O}_K$ a prime ideal.

Proof

Integrally closed in its field of fractions

Let $\mathcal{O}_K$ be ring of integers of K, v a valuation on K.

R_v is normal and contains $\mathbb{Z}$, so $R_v \supset \mathcal{O}_K$. As $\mathrm{Frac}(\mathcal{O}_K) = K$,

closure polys in R_v closure polys in $\mathbb{Z}$

v is non-trivial on $\mathcal{O}_K$, so $\mathfrak{p} := m_v \cap \mathcal{O}_K$ is a non-zero

since $v(\mathcal{O}_K) = 0 \Rightarrow v(K) = 0$

prime ideal of $\mathcal{O}_K$. Then if $x \in \mathcal{O}_K \setminus \mathfrak{p} \subset R_v \setminus \mathfrak{m}_v = R_v^*$ then $v(x) = 0$. So $R_v \supset \mathcal{O}_{K,\mathfrak{p}}$. Therefore by 1.3 iii), as $\mathcal{O}_{K,\mathfrak{p}}$ is a valuation ring of $v_\mathfrak{p}$, $R_v = \mathcal{O}_{K,\mathfrak{p}}$ and v is equivalent to $v_\mathfrak{p}$ □

Definition

K a field. A map $|\cdot| : K \to \mathbb{R}_{\geq 0}$ is an absolute value (AV) if $\forall x, y \in K$,

(AV1) $|x| = 0 \Leftrightarrow x = 0$

(AV2) $|xy| = |x||y|$ so $|\cdot| : K^* \to \mathbb{R}_{>0}^*$ is a homomorphism

(AV3) $|x+y| \leq |x| + |y|$

(AV4) $\exists x$ with $|x| \neq 0, 1$.

If the stronger condition $|x+y| \leq \max(|x|, |y|)$ (AV3N) we say that $|\cdot|$ is non-Archimedean (NA), and otherwise $|\cdot|$ is Archimedean.

Example

Usual absolute value on $\mathbb{R}$ and modulus of $\mathbb{C}$ are examples of archimedean AVs.

23/01/14 Algebraic Number Theory ④

Non-Archimedean if $|x+y| \leq \max\{|x|, |y|\}$

Theorem 1·7

Fix $\rho \in (0,1)$ and let v be a valuation on K. Then

$$|x|_v = \begin{cases} 0 & \text{if } x=0 \\ \rho^{v(x)} & x \neq 0 \end{cases}$$ is a non-archimedean AV on K (NAAV)

$v \mapsto |\cdot|_v$ is a bijection (valuations) $\leftrightarrow$ (NAAVs on K)

Proof

Immediate from definitions (Note: Some people use "valuation" for "NAAV")

Example

v_p the p-adic valuation on $\mathbb{Q}$. We usually choose $\rho = \frac{1}{p}$ and get a p-adic AV, $|p^n \frac{u}{v}|_p = \frac{1}{p^n}$, $u, v \in \mathbb{Z}, (uv, p) = 1$

If $|\cdot|$ is a NAAV, then so is $|\cdot|^r$ for any $r > 0$
(not necessarily true for archimedean AVs).

We say that AVs $|\cdot|$, $|\cdot|'$ are equivalent if $|\cdot|' = |\cdot|^r$, some $r > 0$.

Proposition 1·8

Let $|\cdot|$ be an AV on K. Then the function $d(x,y) = |x-y|$ is a metric on K, translation invariant, for which field operations are continuous. Equivalent AVs give equivalent metrics (proof is the same as showing that $|x-y|_\infty$ is a metric on $\mathbb{R}$). Note that we use $|xy| = |x||y|$ to show that $\times$ and $(\cdot)^{-1}$ are continuous.

So $(K, |\cdot|)$ is a topological field.

Proposition 1.9

An AV $|\cdot|$ on K is non-archimedean $\iff |a \cdot 1_K| \leq 1 \ \forall a \in \mathbb{Z}$

If $|\cdot|$ is archimedean, then $|\cdot|$ is unbounded on $\mathbb{Z}\cdot 1_K \subset K$.

Proof

Write a for $a \cdot 1_K$. If $a \in \mathbb{N}$, then $|-a| = |a| = |1 + \dots + 1| \leq |1|$
$= 1$ if $|\cdot|$ is NA.

Suppose conversely that $|a| \leq 1 \ \forall a \in \mathbb{Z}$. Let $x, y \in K$.

$$|x+y|^n = |(x+y)^n| = \Big|\sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}\Big|.$$

$$\leq (n+1) \max(|x|^n, |y|^n) \quad \text{can drop terms } \left|\binom{n}{i}\right| \leq 1$$

Taking n^{th} roots and letting $n \to \infty \Rightarrow$ (AV3N).

For the last part, if $|a| > 1$ then $|a^n| \to \infty$. $\square$

It is convenient to weaken the definition of AV slightly, replacing (AV3) by (AV3'):

for some $\alpha \in (0, 1]$, $|x+y|^\alpha \leq |x|^\alpha + |y|^\alpha$ (AV3')

With this definition, the square of modulus on $\mathbb{C}$ is an AV (later we will see that this is a good idea).

If $|\cdot|$ satisfies (AV3') then $|\cdot|^\alpha$ satisfies AV, so we haven't really introduced anything new.

Remark

If $\mathrm{char}(K) = p > 0$, then any AV on K is NA, since $\mathbb{Z}\cdot 1_K$ is finite, so $|\cdot|$ is bounded.

23/01/14 Algebraic Number Theory ④

Theorem 1·10 (Ostrowski)

Every absolute value on $\mathbb{Q}$ is equivalent to $|\cdot|_\infty$ (usual archimedean AV) or some $|\cdot|_p$.

Proof 1·6, 1·7 deal with NAAVs
NAAVs are p-adic $\Longleftrightarrow$ p-adic valuations

It is enough to show that if $|\cdot|$ is an Archimedean AV, then it is equivalent to $|\cdot|_\infty$. We may assume that it satisfies (AV3): (triangle inequality)

If $a \in \mathbb{Z}_{>1}$, write $M_a = \max\{|1|, |2|, \dots, |a-1|\}$

Satisfies using AV3 and not just AV3' by swapping $|\cdot|$ and $|\cdot|^\alpha$

By 1·9, $\exists b > 1$ ($\in \mathbb{Z}$) with $|b| > 1$.

Therefore it is sufficient to prove that if $\forall a > 1$, $a \in \mathbb{Z}$, $|a| = |b|^{(\log a / \log b)}$ ($= \log_b a$), then $|a| = |a|_\infty$.

Let $a > 1$. For $q \in \mathbb{N}$, let $p \in \mathbb{N}$ with $a^p \leq b^q < a^{p+1}$ $(*)$. Then

$b^q = \sum_{i=0}^{p} c_i a^i$, $c_i \in \{0, \dots, a-1\}$ and

$$|b|^q \leq \sum_{i=0}^{p} |c_i||a|^i \leq (p+1) M_a \max(1, |a|^p) \qquad (\dagger)$$

Since $q/p \to \log a / \log b$ (take logs of $(*)$) as $q \to \infty$, and $|b| > 1$, this forces $|a| > 1$. Taking p^{th} roots, and letting $q \to \infty$,

$$|b|^{\log a / \log b} \leq |a|$$

otherwise LHS of $(\dagger) \to \infty$ faster than RHS

As $|a| > 1$, we can swap a, b, so that this is an equality. □

so $|a| = |b|^{\log a / \log b}$
now use that $|b| = |b|_\infty^\lambda$, some λ

2 Completions

(X, d) a metric space, completion $(\hat{X}, \hat{d})$

$\hat{X} = $ Cauchy sequences in $X / \sim$

$(x_n) \sim (x'_n)$ iff $d(x_n, y_n) \to 0$.

$\hat{d}((x_n), (x'_n)) := \lim_{n \to \infty} d(x_n, y_n)$.

$\hat{X}$ is complete and $X \hookrightarrow \hat{X}$, an isometry. This is an isomorphism iff X is complete.

Let K be a field, $|\cdot|$ an AV. If $|\cdot|$ is NAAV, let R be the valuation ring of associated valuation. The metric $d(x,y) = |x-y|$ gives completions, $\hat{K}$, $\hat{R}$. $(R = \{x \in K : |x| \leq 1\})$

Theorem 2.1

i) $\hat{K}$ is a field, and $\hat{d}(x,y) = |x-y|^\wedge$ for an AV $|\cdot|^\wedge$ on $\hat{K}$ extending $|\cdot|$.

ii) $|\cdot|$ non-archimedean $\Rightarrow$ so is $|\cdot|^\wedge$ and $\hat{R}$ is the valuation ring of $\hat{K}$.

$|\cdot|_\infty$ on $\mathbb{Q}$ $\quad \hat{K} = \mathbb{R}$

$|\cdot|_p$ on $\mathbb{Q}$ $\quad \hat{K} = \mathbb{Q}_p$ p-adic

Proof

i) $\{\text{Cauchy Sequences in } K\} = S \subset K$ is easily seen to be a ring (by the axioms for AV) and $\hat{K} = S/I$ with $I = \{(x_n) \in K^{\mathbb{N}} \mid |x_n| \to 0\}$, an ideal. We extend $|\cdot|^\wedge$ by $|(x_n)|^\wedge = \lim |x_n|$, clearly an AV. It is sufficient to prove that I is maximal. Let $x = (x_n) \in S \setminus I$. As $x \notin I$, $|x_n|$ is bounded below by some $\varepsilon > 0$ (large enough $n > N$). Let $y_n = \frac{1}{x_n}$ for $n > N$. Then $|y_n - y_m| = \frac{|x_n - x_m|}{|x_n||x_m|} \leq \frac{1}{\varepsilon^2}|x_n - x_m|$, so $(y_n) \in S$. ($y_n = 1$ for $n \leq N$). $xy - 1 \in I$. so $\hat{K} = S/I$ a field

$|xy| = |x||y|$ is crucial here.

ii) First part follows from 1.9 (bounded on $\mathbb{Z}$). Second part: we have $|x|^\wedge \leq 1$ $\forall x \in \hat{R}$ by taking limits so $\hat{R} \subset$ valuation ring of $\hat{K}$. Suppose $x \in \hat{K}$, represented by $(x_n) \in S$, and $|x|^\wedge = \lim |x_n| \leq 1$. By (AV3N), since $|x - x_n|^\wedge \to 0$, $|x_n| = |x|^\wedge$ for n sufficiently large (if $x \neq 0$)

$|x|^\wedge \leq \max(|x-x_n|^\wedge, |x_n|^\wedge)$

$|x_n|^\wedge \leq \max(|x-x_n|^\wedge, |x|^\wedge)$

Now $x_n \in R$ for $n >> 0 \Rightarrow$ so $x \in \hat{R}$.

25/01/14 Algebraic Number Theory (5)

$\mathbb{Q}$, $|\cdot|_p$ p-adic AV, completion $\mathbb{Q}_p$, valuation ring $\mathbb{Z}_p$ p-adic integers

Proposition 2·2

Every element of $\mathbb{Z}_p$ has a unique representation as a series

$$x = a_0 + a_1 p + \sum_{n \geq 2} a_n p^n \quad , \quad a_i \in \{0, 1, \ldots, p-1\}$$

Every element of $\mathbb{Q}_p$ has a unique representation

$$x = \frac{a_{-N}}{p^N} + \ldots + \frac{a_{-1}}{p} + \sum_{n \geq 0} a_n p^n \qquad (1)$$

In either case, $v_p(x) = \min\{n \in \mathbb{Z} \mid a_n \neq 0\}$

Proof. First assume we have representations

- (1) is Cauchy, so converges to an element of $\mathbb{Q}_p$, and the strong triangle inequality applied to its partial sums, $\underbrace{v_p(x) = \min\{n \in \mathbb{Z} \mid a_n \neq 0\}}_{\text{distinguishes } \mathbb{Z}_p, \mathbb{Q}_p}$
- Given two representations $\sum_{n \geq -N} a_n p^n = \sum_{n \geq -N} b_n p^n$ of $x \in \mathbb{Q}_p$, multiplying by powers of p, we may assume that $N = 0$.

$\Rightarrow a_0 - b_0 = \sum_{n \geq 1} (b_n - a_n) p^n \Rightarrow v_p(a_0 - b_0) \geq 1 \Rightarrow a_0 = b_0$

$\Rightarrow a_n = b_n \; \forall n.$

$v(a_0) = v(b_0) = 0$

$v(x+y) = \min(v(x), v(y))$

- It remains to show that every element of $\mathbb{Q}_p$ has a representation (1).

The set of partial sums of series (1) is precisely

$\mathbb{Z}[\frac{1}{p}]_{\geq 0} = \{x \in \mathbb{Z}[\frac{1}{p}] \mid x \geq 0\}$.

This means that $\mathbb{Z}[\frac{1}{p}]_{\geq 0}$ is dense in $\mathbb{Q}_p$ so each element of $\mathbb{Q}_p$ is a limit of partial sums (1)

As $\mathbb{Q}$ is dense in $\mathbb{Q}_p$, it is sufficient to prove that $\mathbb{Z}[\frac{1}{p}]_{\geq 0}$ is dense in $\mathbb{Q}$ (for the topology induced by $|\cdot|_p$). Let $x = p^{-n}\frac{a}{b}$, $(p, b) = 1$, $b > 0$.

Let $m > 0$ and choose $c \in \mathbb{N}$ with $bc \equiv a \mod p^{m+n}$.

Then $|x - p^{-n}c|_p = |\frac{a-bc}{p^n b}|_p \leq p^{-m}$, and $p^{-n}c \in \mathbb{Z}[\frac{1}{p}]_{\geq 0}$

$\therefore \mathbb{Z}[\frac{1}{p}]_{\geq 0}$ is dense in $\mathbb{Q}$. $\square$

In elementary terms, p-adic numbers are "backwards decimals" and it is easy to see what arithmetic operations are.

For the remainder of the section we will only consider NAAV $|\cdot|$, associated to some valuation v.

so $0 < v(\pi) < \infty$

K a field, R its valuation ring. If $\pi \in R$ with $0 < |\pi| < 1$ (so $\pi \in m_v = m$)

then $\pi^n R = \{x \in K \mid |x| \leq |\pi|^n\}$ is open for the topology induced by $|\cdot|$;

"looks closed"

- If $x \in \pi^n R$, and $0 < \varepsilon < |\pi|^n$, then $\forall y$ with $|y| < \varepsilon$, $|x+y| \leq |\pi|^n$ (by AV3N) strong Δ inequality
- Then $x + y \in \pi^n R$, so $\pi^n R$ is open.

<u>Remark</u> this says that for each $x \in \pi^n R$, $\exists \varepsilon > 0$ $(\varepsilon < |\pi|^n)$ such that open ball $B_x(\varepsilon) \subseteq \pi^n R$. c.f. definition of open set for metric space.

Analysis is much easier (in some ways) for NAAVs. For example, the series $\sum x_n$ converges (in a complete field w.r.t. NAAV) $\Leftrightarrow x_n \to 0$ (by the strong triangle inequality).

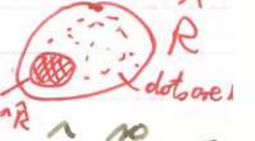
<u>Proposition 2.3</u>

Let R be the valuation ring of $(K, |\cdot|)$, $\hat{R}$ the completion.

Let $\pi \in R$ with $0 < |\pi| < 1$. Then for every $n \geq 1$, the canonical map $R/\pi^n R \to \hat{R}/\pi^n \hat{R}$ is an isomorphism.

for the same reasons as $\pi^n R \subset R$

visualise $\hat{R}$



trivial since $\hat{R}$ is the completion of R

<u>Proof</u>

$R \subset \hat{R}$ is dense, and $\pi^n \hat{R} \subset \hat{R}$ is open, so $R + \pi^n \hat{R} = \hat{R}$, so surjective.

Also, $R \cap \pi^n \hat{R} = \{x \in R \mid |x| \leq |\pi|^n\} = \pi^n R$, so this is an isomorphism. $\square$

5/01/14 Algebraic Number Theory (5)

Remark

$\pi^n R \subset R$ is open, and so is every $x + \pi^n R$, so $\pi^n R$ is also closed

(or see this directly by continuity of $|\cdot|$)

$\therefore$ Induced topology on $R/\pi^n R$ is discrete. because $x+\pi^n R$ is open AND closed $\forall x \in R$.

Digression (Inverse Limits)

Let $(X_n)_{n\in\mathbb{N}}$ be a collection of sets (say), $\pi_n : X_{n+1} \to X_n$,

a collection of maps. This (π_n, X_n) is called an inverse system.

Its inverse limit is defined to be

$$\varprojlim (X_n, \pi_n)_n = \varprojlim X_n = \{(x_n)_{n\in\mathbb{N}} \mid \pi(x_{n+1}) = x_n \ \forall n\} \subset \prod_n X_n$$

$$\begin{array}{ccccccc} \cdots\cdots \to & X_2 & \to & X_1 & \to & X_0 \\ & \Uparrow & & \Uparrow & & \Uparrow \\ & x_2 & \longmapsto & x_1 & \longmapsto & x_0 \end{array}$$

Typically, we consider such systems where all of the π_n are surjective.

If X_n are groups (or rings) and the π_n are homomorphisms, then

$\varprojlim X_n$ is a group (or ring), in fact, a subgroup (ring) of $\prod_n X_n$.

Example

1. $X_n = \mathbb{Z}/p^n\mathbb{Z}$, $\pi_n : \mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$, reduction mod p^n.

Claim : $\varprojlim \mathbb{Z}/p^n\mathbb{Z} = \mathbb{Z}_p$

Using the standard bijection $\mathbb{Z}/p^n\mathbb{Z} = \{0, 1, \dots, p^n - 1\}$ and

writing in base p, this follows from 2·2.

2. I-adic completion

R a ring, I an ideal. Consider the family R/I^n with maps

$R/I^{n+1} \to R/I^n$ with π_n the canonical maps

$\left(IJ = \left\{ \sum_{k=1}^{n} x_k y_k \mid x_k \in I, y_k \in J, n \in \mathbb{N} \right\}\right)$

The I-adic completion of R is $\hat{R}_I = \varprojlim R/I^n$.

For example $\hat{\mathbb{Z}}_{(p)} = \mathbb{Z}_p$ as we just saw.

We have a canonical map $R \to \hat{R}_I$, $x \mapsto ((x \bmod I^n) \in R/I^n)_n$ with kernel $= \bigcap I^n$.

We have a topology on $\hat{R}_I$ given as follows:

(More generally) suppose $X = \varprojlim (X_n, \pi_n)$ (inverse limit of sets)

Let $p_m : X \to X_m$ be the map $((x_n) \in \varprojlim X_n) \mapsto x_m$

The <u>inverse limit topology</u> is the smallest topology for which the maps p_n are continuous (for the discrete topology on X_m).

i.e. open sets in $\varprojlim X_n$ are arbitrary unions of sets of the form $U_{m,a} = p_m^{-1}(\{a\})$.

$$\cdots \to X_m \to \cdots \to X_1 \to X_0$$

e.g. $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$

$$p_m : \mathbb{Z}_p \longrightarrow \mathbb{Z}/p^m\mathbb{Z}$$
$$(a_n)_{n\geq 0} \longmapsto a_m$$

$p_m^{-1}(\{a\}) = \{ (a_n)_{n\geq 0} \mid a_m = a \}$

fixes a_k for $k \leq m$ but can vary for $k > m$

$\Rightarrow p_m^{-1}(\{a\}) = \{$all elements within $\frac{1}{p^{m+1}}$ of $(a_0, a_1, \ldots, a_m, 0, 0, \ldots)\}$

$\therefore$ Inverse Limit Topology on $\mathbb{Z}_p$ is the same as the topology induced by $|\cdot|_p$.

8/10/14 Algebraic Number Theory ⑥

Proposition 2.4

i) $\varprojlim X_n$ is totally disconnected only singletons are connected.

ii) Suppose that each X_n is finite. Then $\varprojlim X_n$ is compact.

Proof

i) $x = (x_n) \neq (y_n) = y$, both in $\varprojlim X_n$. Choose m with $x_m \neq y_m$.

Then $\varprojlim X_n$ = the disjoint union of the open sets given by

U_{m,x_m} and $U_{m,x_m}^c = \bigcup_{\substack{a \in X_m \\ a \neq x_m}} U_{m,a} \ni y$. So X is totally disconnected

ii) X_n finite $\Rightarrow X_n$ is compact (for discrete topology)

$\Rightarrow \prod_n X_n$ is compact (Tychonoff's Theorem)

$\Rightarrow \varprojlim X_n$ is compact, since it is closed in $\prod_n X_n$. □

e.g. $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$ is compact and totally disconnected.

Remarks

1. We can define inverse limits more generally (replacing the index set $\mathbb{N}$ by another partially ordered set satisfying some properties

e.g. G an infinite group. Consider the family of Normal subgroups of finite index, partially ordered by (reverse) inclusion. If $N \subset N'$ we have $G/N \to G/N'$ and can form $\varprojlim_N G/N$; called the profinite completion of G.

2. Sometimes it is useful to consider some other topology on $\{X_n\}$.

We can then form an induced topology on $\prod_n X_n$ (product)

and also on $\varprojlim X_n$ (assuming that the π_n are continuous.

e.g. $X_n = \mathbb{R}/\mathbb{Z}$ with usual topology $\forall n$.

$\pi_n : \mathbb{R}/\mathbb{Z} \xrightarrow{2} \mathbb{R}/\mathbb{Z} \Rightarrow \varprojlim (\mathbb{R}/\mathbb{Z}, 2)$ is a topological group.

This is called the "2-adic solenoid".

Theorem 2·5

K, valuation v, AV $|\cdot|$, valuation ring R, completions $\hat{K}$, $\hat{R}$.

Choose any $\pi \neq 0$, $\pi \in R$, $|\pi| < 1$.

i) K is already complete i.e. $K = \hat{K} \iff R$ is π-adically complete

i.e. $R = \varprojlim R/\pi^n R$

ii) In general, $\hat{R}$ equals the π-adic completion of R.

Proof

kernel of $R \to \varprojlim R/\pi^n R$ $\parallel$

i) First assume that $K = \hat{K}$. Obviously $\bigcap_n \pi^n R = \bigcap_n \{x \in R \,|\, |x| < |\pi|^n\} = \{0\}$

So $R \to \varprojlim R/\pi^n R$ is injective. Let $(x_n) \in \varprojlim R/\pi^n R$. Pick $y_n \in R$ with $y_n \bmod \pi^n = x_n$. Then $y_{n+1} \equiv y_n \bmod \pi^n$ $\Rightarrow (y_n)$ is a Cauchy sequence with limit y say. So it is sufficient to prove that $y \bmod \pi^n = x_n \; \forall n$. If not, say $y \not\equiv y_m \bmod \pi^m$, then $\forall n \geq m$, $y \not\equiv y_n \bmod \pi^m$ so $|y - y_n| \not\to 0$ $\divideontimes$

Hence R is π-adically complete.

ii) What we just proves shows that $\hat{R}$ is π-adically complete.

i.e. $\hat{R} \cong \varprojlim \hat{R}/\pi^n\hat{R} \cong \varprojlim R/\pi^n R$ by 2·3.

i.e. $\hat{R}$ is the π-adic completion of R. In particular, if R is π-adically complete then $R = \hat{R}$ so $K = \hat{K}$ is complete, and we have finished proving (i). $\square$

The origin of completion and of p-adic numbers goes back to Hensel (see Borevic and Shafarevic)

28/01/14

Algebraic Number Theory ⑥

Problem

$f \in \mathbb{Z}[T]$. Suppose we have $a \in \mathbb{Z}$ with $f(a) \equiv 0 \mod p^n$.

When does there exist b with $f(b) \equiv 0 \mod p^{n+1}$ with $b \equiv a \mod p^n$

Variant: $f(T_1, \dots, T_r)$, $a \in \mathbb{Z}^r$.

Example

$p = 2$, $f(T) = T^2 + 1$. $f(1) \equiv 0 \ (2)$ but there are no solutions mod 4.

Suppose we have $a_n \in \mathbb{Z}$ with $f(a_n) \equiv 0 \ (p^n)$, $a_{n+1} \equiv a_n \ (p^n)$ $\forall n$.

Then $x = \lim (a_n) \in \mathbb{Z}_p$ with $f(x) = 0$

(Conversely, if $x \in \mathbb{Z}_p$ has $f(x) = 0$ we get the a_n as above)

$|f(a_n) - 0|_p \leq \frac{1}{p^n}$, so reminiscent of successive approximation (Newton's Method)

Theorem 2.6 (Hensel's Lemma)

Let R be a complete DVR, with πR the unique maximal ideal. (We say that πR is a uniformiser of R). Suppose that $f, g_1, h_1 \in R[T]$ such that

i) g_1 monic

ii) $f \equiv g_1 h_1 \ (\pi)$

iii) $(\bar{g_1}, \bar{h_1})$ are coprime ($\bar{g_1}$ is the image of g_1 in $k[T] = R/\pi R[T]$)

Then $\exists!$ $g, h \in R[T]$ with ~~g monic~~.

i) g monic

ii) $f = gh$

iii) $g \equiv g_1$, $h \equiv h_1 \ (\pi)$

N.B. we do not assume that f is monic.

Proof

only require $f \equiv g_1 h_1 \ (\pi)$, can remove excess coefficients

Let $N = \deg(f)$, $d = \deg(g_1)$. WLOG, $\deg(h_1) \leq N - d$.

We will inductively construct $g_n, h_n \in R[T]$ such that g_n is monic of degree d, $\deg(h_n) \leq N-d$, $f \equiv g_n h_n \ (\pi^n)$ and $g_{n+1} \equiv g_n \ (\pi^n)$ $h_{n+1} \equiv h_n \ (\pi^n)$, and such that (g_n, h_n) is unique mod π^n.

This does not use the completion.

Suppose we have constructed $g_n h_n$, so $f - g_n h_n = \pi^n q$ for $q \in R[T]$, some n. $\deg(q) \leq N$, (g_n, h_n) unique mod π^n.

u, v to be determined

Let $g_{n+1} = g_n + \pi^n u$, $h_{n+1} = h_n + \pi^n v$ where $\deg(u) \leq d-1$, $\deg(v) \leq N-d$. $f \equiv g_{n+1} h_{n+1} \ (\pi^{n+1}) \iff g_n v + h_n u \equiv q \pmod{\pi}$

$\therefore$ it is sufficient to prove that $\exists! \ \bar{u}, \bar{v} \in k[T]$ such that $\bar{g}_1 \bar{v} + \bar{h}_1 \bar{u} = \bar{q}$, $\deg(\bar{u}) \leq d-1$, $\deg(\bar{v}) \leq N-d$.

But $(\bar{g}_1, \bar{h}_1) = 1$, so $\exists \ \bar{u}, \bar{v}$ as above, unique up to transformations $(\bar{u}, \bar{v}) \mapsto (\bar{u} + \bar{r}\bar{g}_1, \bar{v} - \bar{r}\bar{h}_1)$, $\bar{r} \in k[T]$.

By Bezout or Extended Euclidean Algorithm

So $\bar{u}, \bar{v}$ are unique with this condition on degrees.

To complete the proof, $g = \lim g_n$, $h = \lim h_n$ (unique by uniqueness at every stage). note g_n obtained $\deg(g_n) = \deg(g)$

N.B. we used DVR at least to know that $R \cong \varprojlim R/\pi^n R$

31/02/14 Algebraic Number Theory 7

Corollary 2.7

$f \in R[T]$, $a \in R$ with $f(a) \equiv 0 \bmod \pi$, $f'(a) \not\equiv 0 \bmod \pi$.

$R = \hat{R_I}$

Then $\exists!\, b \in \mathbb{Z}_p$ with $f(b) = 0$, $b \equiv a \ (\pi)$

Proof

$g_1 = T - a$, h_1 any poly with $\bar{f} \doteq (T - \bar{a})\bar{h}_1$.

As $\bar{f}'(a) \neq 0$, $(T - \bar{a}, \bar{h}_1) = 1$. Then apply Hensel.

Example

i) $f = T^{p-1} - 1 \equiv (T-1)(T-2)\ldots(T-(p-1)) \bmod p$

so that each $a \in \mathbb{F}_p^*$ has a unique lifting to a $(p-1)^{st}$ root of unity $[a] \in \mathbb{Z}_p$, (so that $\mathbb{Z}_p$ contains all $(p-1)^{st}$ roots of unity).

ii) Similarly, for R a complete DVR with residue field k, k contains a finite field $\mathbb{F}_q$. The same applied to $T^{q-1} - 1$ shows that R has all $(q-1)^{st}$ roots of unity.

Remark

There is a wider class of (discrete valuation, or more generally, local (rings for which Hensel's Lemma holds (mod $\pi \Rightarrow$ mod m_R). They are called Henselian rings (and the definition is what was just given).

Example

$R = \{$elements of $\mathbb{Z}_p$ that are algebraic over $\mathbb{Q}\}$

3 Extensions of Local Fields

For now, a local field = a field complete w.r.t. an AV. (Usually, people are more restrictive).

Theorem 3·1

Let k be complete w.r.t. an AV $|\cdot|$, and L/k an algebraic extension.

i) There exists a unique AV $|\cdot|_L$ extending $|\cdot|$.

ii) If $[L:k] = n < \infty$ and $x \in L$, then $|x|_L = |N_{L/k}(x)|^{1/n}$

iii) Suppose that $|\cdot|$ is NA, with valuation ring R. Then $|\cdot|_L$ is also NA and its valuation ring is the integral closure of R in L (In particular, the integral closure of R in L is local).

Proof

If k is $\mathbb{R}$ or $\mathbb{C}$, this is an easy exercise. We will prove for for discretely valued NAAV (general case requires an appropriate version of Hensel's Lemma. See Cassels, "Local Fields").

Lemma 3·2

Let R be a DVR, $K = \mathrm{Frac}(R)$, π a uniformiser, $k = R/(\pi)$.

Assume that K is complete.

i) Let $f \in K[T]$ be monic, irreducible. Suppose that $f(0) \in R$. Then $f \in R[T]$.

ii) If L/K is finite, $z \in L$ with $N_{L/K}(z) \in R$, then z is ~~in the valuation ring of L~~ integral over R.

Proof $\quad R = \mathbb{Z}$, $L = \mathbb{Q}(i)$, $z = \frac{1+2i}{1-2i}$, $N_{L/K}(z) = 1 \in \mathbb{Z}$ but z is not integral over $\mathbb{Z}$.

i) Let $d = \deg(f)$, and let m be minimal with $\pi^m f = f^*(T)$ $= \sum_{i=0}^{d} a_i T^i$ in $R[T]$. (since $K = \mathrm{Frac}(R) = R[\frac{1}{\pi}]$) If $m \leq 0$ we are finished (since $f \in R[T]$).

Otherwise, $m > 0$, so let j be the largest integer with $a_j \in R^*$. (indeed $a_j \in R^*$ for some j since we only use π to clear denominators as far as necessary)

So in $k[T]$, $\overline{f^*(T)} = \overline{a_j} T^j + \dots + \overline{a_0}$. Note that $(0 < j < d)$ by

01/02/14 Algebraic Number Theory (7)

hypothesis. So $\overline{f^*(T)} = \bar{g}\bar{h}$

$\bar{g} = (\bar{a}_j T^j + \dots + \bar{a}_0)$, $\bar{h} = (0 \cdot T^{d-j} + \dots + 1)$

or better $\bar{g} = (T^j + \frac{\bar{a}_{j-1}}{\bar{a}_j} T^{j-1} + \dots + \frac{\bar{a}_0}{\bar{a}_j})$, $\bar{h} = (0 \cdot T^{d-j} + \dots + 0 \cdot T + \bar{a}_j)$

We may apply Hensel's Lemma to f^* (as $a_j \in R^*$), so we get a non-trivial factorisation of f. since K is complete, Hensel's Lemma lifts to a factorisation in $R[T]$

ii) Apply i) to the min. poly. of z over K.

Proof (of Theorem 3·1, continued)

For (discrete) NAAVs.

$|\cdot|$ non-archimedean $\Rightarrow$ bounded on $\mathbb{Z} \cdot 1_K \subset K$

So $|\cdot|_L$ is bounded on $\mathbb{Z} \cdot 1_L$ if it exists.

First assume that $[L:K] = n < \infty$.

- Existence

Define $|x|_L = |N_{L/K}(x)|^{1/n}$. We check the Δ-inequality to show that this is an AV. Let $x, y \in L$ with $|x|_L \leq |y|_L$. It is sufficient to prove that

$N_{L/K}(z)$ $|x+y|_L \leq |y|_L$.

$= N_{K(z)/K}(z)$

$= N_{L/K(z)} \circ N_{K(z)/K}(z)$ Equivalently, it is sufficient to prove that if $|z|_L \leq 1$ then

$= N_{L/K(z)}(f(0))$ $|z+1|_L \leq 1$ (dividing by y).

$= f(0)^{\frac{n}{m}}$

Let f = min. poly. of z/K, $m = \deg f$.

Then $|f(0)|^{1/m} = |z|_L$, so $|z|_L \leq 1 \Rightarrow |f(0)| \leq 1$

$\Rightarrow f(0) \in R \Rightarrow f \in R[T]$, and $f(T-1)$ is the min. poly. of $z+1$, so $|1+z|_L = |f(-1)|^{1/m} \leq 1$.

04/02/14 Algebraic Number Theory 8

Proof (3·1 continued)

R_L = valuation ring of $|\cdot|_L = \{x \in L \mid N_{L/K}(x) \in R\}$

where R is the valuation ring of K. $\Rightarrow f \in R[T]$

Recall 3·2ii) : $N_{L/K}(x) \underset{= f(0)}{\in} R \Rightarrow x$ integral over R.

So every element of R_L is integral over R, and R_L is normal (as a valuation ring) so R_L is the integral closure of R in L.

If $|\cdot|'$ is any other AV on L extending $|\cdot|$, let R' be its valuation ring. As $|\cdot|'$ extends $|\cdot|$, $R' \supset R$. R' is normal, so contains R_L. So by 1·3iii), $R' = R_L$ and $|\cdot|', |\cdot|$ are equivalent.

valuation rings are maximal proper sub-rings

L/K an arbitrary algebraic extension. Then $L = \bigcup$ (subfields finite over K) $= \bigcup L_\alpha$ say. Define $|x|_L$, for $x \in L$, to be $|x|_{L_\alpha}$, for any L_α containing x. If $x \in L_\alpha, L_\beta$, then $|x|_{L_\alpha} = |x|_{L_\beta}$ because this doesn't depend on α: if $K(x) \subset L_\alpha$, $|\cdot|_{K(x)}, |\cdot|_{L_\alpha}$ are two extensions of $|\cdot|$ to $K(x)$ which are therefore the same. So this is well defined and is an AV. $\square$

Consequence :

Let $\bar{K}$ = algebraic closure of K. Then $\exists!$ extension of $|\cdot|$, to $\bar{K}$.

e.g. $K = \mathbb{Q}_p$, $|\cdot| = |\cdot|_p$. There is a unique AV on $\overline{\mathbb{Q}_p}$ extending $|\cdot|_p$, also denoted $|\cdot|_p$. It is not discrete :

$|p^{\frac{1}{n}}|_p = |p|_p^{\frac{1}{n}} = \frac{1}{p^{\frac{1}{n}}}$

(In fact, it is easy to see that $|\mathbb{Q}_p^*| = p^{\mathbb{Z}}$, $|\overline{\mathbb{Q}}_p^*| = p^{\mathbb{Q}}$

Proposition 3.3

Let K be complete with respect to a discrete valuation, L/K a finite, separable extension. Then L is unique (with respect to the unique extension of the valuation) and discretely valued.

First proposition; comm. alg. section

Moreover $R_L \cong R^{[L:K]}$ as an R-module.

Proof

$n = [L:K]$. Then $|L^*| \subset |K^*|^{\frac{1}{n}}$, so L is discretely valued.

As R_L = integral closure of R in a finite separable extension, R_L is a finite R-module. R is a DVR, so a PID, so R_L is free (being torsion-free) and $\operatorname{rank}_R R_L = \dim_K L = n$. structure theorem

i.e. for $r_L \in R_L$ non-zero, $\mathrm{Ann}(r_L) = \{0\}$

True because R a PID $\Rightarrow$ R an integral domain

Suppose $r \in \mathrm{Ann}(x)$, $x^n + \dots + a_0 = 0$, $a_i \in R$, $a_0 \neq 0$. Multiply by r $\Rightarrow ra_0 = 0 \Rightarrow r = 0$

$\pi_K \in R$, $\pi_L \in R_L$ uniformisers. Then $\pi_K R_L = \pi_L^e R_L$ for some $e \geq 1$ as R_L is a DVR. (Theorem 3.1 $_{\text{val discrete}}$)

So $\varprojlim_m R_L/\pi_L^m R_L = \varprojlim_m R_L/\pi_L^{em} R_L = \varprojlim_m R_L/\pi_K^m R_L \cong \varprojlim_m \left(R/\pi_K R\right)^n$

as R-modules. So $R_L \cong R^n$ as R is π-adically complete.

i.e. R_L is complete.

Remarks

i) L/K finite $\Rightarrow$ L complete (without assumption that the valuation is discrete)

For L/K infinite, L/K is typically not complete, e.g. $\overline{\mathbb{Q}_p}$ is not complete

ii) If L/K is finite and the valuation is not discrete, then R_L need not be a finitely generated R-module. or even free

We examine (algebraically) finite separable extensions of complete discretely valued fields (CDVF).

04/02/14

Algebraic Number Theory (8)

Let K be such a field.

Notation

$\mathcal{O}_K$ = valuation ring of K (also called "ring of integers of K")

π_K a uniformiser.

v_K the normalised valuation on K ($v_K(\pi_K) = 1$).

Residue field $k_K = \mathcal{O}_K / \pi_K \mathcal{O}_K$

L/K a finite extension. We have the same notation for L, and $\mathcal{O}_L \supseteq \mathcal{O}_K$. As $\pi_K \in \pi_L \mathcal{O}_L$, the inclusion $\mathcal{O}_K \to \mathcal{O}_L$ induces an extension $k_K \hookrightarrow k_L$.

Definition

Residue class degree $f = f(L/K) = [k_L : k_K]$

Ramification degree $e = e(L/K) = v_L(\pi_K)$

i.e. $\pi_L^e \mathcal{O}_L = \pi_K \mathcal{O}_L$

N.B. as they are normalised, $v_L|_K$ is not necessarily v_K.

Proposition 3.4

L/K a finite separable extension. Then

i) $e(L/K) f(L/K) = [L:K]$

ii) $L \cong K^{[L:K]}$ as a topological K-vector space.

Proof

i) $\pi_K \mathcal{O}_L = \pi_L^e \mathcal{O}_L \subset \pi_L^{e-1} \mathcal{O}_L \subset \dots \subset \pi_L \mathcal{O}_L \subset \mathcal{O}_L$

$\Rightarrow 0 \subset \dfrac{\pi_L^{e-1}\mathcal{O}_L}{\pi_L^e \mathcal{O}_L} \subset \dots \subset \dfrac{\mathcal{O}_L}{\pi_L^e \mathcal{O}_L}$, k_K-vector spaces.

$\Rightarrow \dim_{k_K} \dfrac{\mathcal{O}_L}{\pi_K \mathcal{O}_L} = \sum_{i=0}^{e-1} \dim_{k_K} \dfrac{\pi_L^i \mathcal{O}_L}{\pi_L^{i+1}\mathcal{O}_L} = \sum_{i=0}^{e-1} \dim_{k_K} \dfrac{\mathcal{O}_L}{\pi_L \mathcal{O}_L}$ (Lemma 1.5)

$W \supset V$ $\dim W = \dim W/V + \dim V$ $\qquad \dfrac{\pi_L^i \mathcal{O}_L}{\pi_L^{i+1}\mathcal{O}_L} \cong \dfrac{\mathcal{O}_L}{\pi_L \mathcal{O}_L}$ $\qquad = e \cdot f$

3

$\nearrow \mathcal{O}_L \cong \mathcal{O}_K^{[L:K]}$

But $\frac{\mathcal{O}_L}{\pi_K \mathcal{O}_L} \cong \frac{\mathcal{O}_K^n}{\pi_K \mathcal{O}_K^n}$ with k_K dimension n.

ii) Follows from the proof of 3·4 i)?
or
3·3?

$$R_L \cong R^{[L:K]}$$

$$L = \mathrm{Frac}(R_L)$$

$$K = \mathrm{Frac}(R)$$

05/02/14

Algebraic Number Theory 9

We will assume (until the end of the section) that all valuations are discrete. K complete wrt normalised v_K, $\mathcal{O}_K, \pi_K, k_K$.

8-2-2 L/K finite, $e(L/K) = v_L(\pi_K)$, $f(L/K) = [k_L : k_K]$

$$[L:K] = f(L/K)\, e(L/K)$$

Definition

We say that L/K is unramified if

i) $e(L/K) = 1$ (i.e. π_K is also a uniformiser of L) $\pi_K \mathcal{O}_L = \pi_L \mathcal{O}_L$

ii) k_L/k_K separable

(in most cases of interest here, k_K will be finite so ii) is automatic). as finite extensions of $\mathbb{F}_q$ are Galois

These are easy to classify.

Proposition 3.5

L/K finite separable. The following are equivalent:

i) L/K is unramified.

ii) $L = K(x)$, some $x \in \mathcal{O}_L$, whose min. poly. $/K$ is separable mod π_K.

If so, then $\mathcal{O}_L = \mathcal{O}_K[x]$ for any x as in ii).

Proof

i) $\Rightarrow$ ii) Let L/K be unramified, degree n. So k_L/k_K is separable of degree n. by definition of unramified So $k_L = k_K(\bar{x})$, $\bar{x}$ separable over k_K.

Let $x \in \mathcal{O}_L$ be any lifting of $\bar{x}$ to $\mathcal{O}_L$, with min. poly. $g \in \mathcal{O}_K[T]$. $\deg g \leq n$ Then $\bar{g}(\bar{x}) = 0 \Rightarrow \bar{g} =$ min. poly. of $\bar{x}$, so is separable, and g has degree n, because now, $\deg \bar{g} = n$ so $L = K(x)$.

if $\bar{g}$ was not the min. poly. of $\bar{x}$ then since $\bar{g}$ has degree $\leq n$, min. poly $\neq \bar{g}$ reduces min. poly. degree ✗✗

ii)$\Rightarrow$i) Conversely, suppose that we have x as in ii), with min. poly. $f \in \mathcal{O}_K[T]$. As $\bar{f}$ is separable, it must be irreducible, since if not, Hensel's Lemma lifts to a factorisation of f ※

So if $\bar{x} \in k_L$ is the image of x, $\bar{f}(\bar{x}) = 0$, $\bar{f}$ irreducible, and separable of degree n.

$\Rightarrow k_L = k_K(\bar{x})$ is separable of degree n i.e. L/K is unramified. $n = ef$

If $\mathcal{O}_L \supsetneq \mathcal{O}_K[x]$, then $\exists\, y \in \mathcal{O}_L$ with $\pi_K y \in \mathcal{O}_K[x]$ but $y \notin \mathcal{O}_K[x]$ ~~(viewing $\mathcal{O}_K[x]$ as an $\mathcal{O}_K$-submodule of $\mathcal{O}_L$).~~ $L = K(x)$. Write $y = \sum_{i=0}^{n-1} a_i x^i$, $a_i \in \mathcal{O}_K$

Multiply by π_K until $v(\pi_K^{j} a_i) \geq 0$

$\pi_K y = \sum_{i=0}^{n-1} a_i x^i$, $a_i \in \mathcal{O}_K$. Then $1, \bar{x}, \dots, \bar{x}^{n-1}$ is a basis for k_L/k_K. As $y \in \mathcal{O}_L$, $\overline{\pi_K y} = 0$ in k_L

$\Rightarrow$ all $\bar{a_i} = 0$ i.e. all a_i are divisible by π_K. since $1, \bar{x}, \dots, \bar{x}^{n-1}$ is a basis

$\Rightarrow y \in \mathcal{O}_K[x]$ ※ $\square$

Let L/K, M/K be finite, separable extensions with K as above. Any K-homomorphism $L \to M$ maps $\mathcal{O}_L$ to $\mathcal{O}_M$, so induces a map $k_L \to k_M$ (k_K-homomorphisms). So $L \to k_L$ is a functor:

(unramified) $\longrightarrow$ (finite separable)

$\begin{pmatrix}\text{finite separable}\\ \text{extensions of } K\end{pmatrix} \longrightarrow \begin{pmatrix}\text{finite extensions}\\ \text{of } k_K\end{pmatrix}$

<u>Theorem 3.6</u>

i) Let L/K be unramified, M/K any finite separable extension. Then $\mathrm{Hom}_{K\text{-algebra}}(L, M) \to \mathrm{Hom}_{k_K\text{-algebra}}(k_L, k_M)$ is <u>bijective</u>.

05/02/14 Algebraic Number Theory 9

ii) Let k'/k_K be any finite separable extension. Then $\exists\, L/K$ unramified with $k_L \cong k'$ (as k_K-algebras), and L is unique up to isomorphism.

Proof $k_L = k_K(\bar{x})$, $x \in \mathcal{O}_L$ $\in \mathcal{O}_K[T]$

i) Write $L = K(x)$ as in 3·5 ii), with f = min. poly. of x/K. — we fix K, and y = Image (x) determines the Hom completely

$\mathrm{Hom}_{K\text{-algebra}}(L, M) = \{y \in M \mid f(y) = 0\}$

$= \{y \in \mathcal{O}_M \mid f(y) = 0\}$ — since $f \in \mathcal{O}_K[T]$, monic, any such y must be in $\mathcal{O}_M$

$\simeq \{\bar{y} \in k_M \mid \bar{f}(\bar{y}) = 0\}$ by Hensel, as $\bar{f}$ is separable Hensel gives a unique lift back to $\mathcal{O}_M$

$= \mathrm{Hom}_{k_K\text{-algebra}}(k_L = k_K(\bar{x}), k_M)$.

ii) Let $k' = k_K(\bar{x})$, $\bar{x}$ separable over k_K with min. poly. $\bar{g} \in k_K[T]$. Lift $\bar{g}$ to some monic $g \in \mathcal{O}_K[T]$. Let $L = K(x)$, $g(x) = 0$.

Then by 3·5(ii), this is unramified of degree $\deg g = [k' : k_K]$. If L' is any other unramified extension with $k_{L'} \cong k'$, applying i) shows that any k_K-isomorphism $k_L \xrightarrow{\sim} k_{L'}$ lifts to a unique isomorphism $L \xrightarrow{\sim} L'$. □

Consequence

$L \rightsquigarrow k_L$ is an <u>equivalence of categories</u>

$\left(\begin{array}{l}\text{finite unramified}\\ \text{extensions of } K\end{array}\right) \xrightarrow{\sim} \left(\begin{array}{l}\text{finite separable}\\ \text{extensions of } k_K\end{array}\right)$ preserving degrees.

Remark

L/K arbitrary separable algebraic extensions (L need not be complete).

We can extend the normalised valuation v_K to a valuation v_K of K (not necessarily discrete or normalised). We say that L/K is <u>unramified</u> if $v_K(L^*) = \mathbb{Z}$ and k_L/k_K is separable (equivalent to requiring that every finite sub-extension is unramified. $L \supset L' \underset{\text{finite}}{\supset} K$). The same equivalence holds (delete "finite").

<u>Corollary 3.7</u>

Suppose $k_K = \mathbb{F}_q$ is finite. Then K has a <u>unique</u> (up to isomorphism) unramified extension of degree $n \geq 1$ for every such n, namely $\mathrm{spl}(X^{q^n-1} - 1)$.

<u>Proof</u>

These are exactly the finite extensions of $\mathbb{F}_q$. $\square$

<u>Corollary 3.8</u> (use the equivalence on the previous page)

i) L/K unramified. Then L/K is Galois $\iff$ k_L/k_K is Galois. If so, $\mathrm{Gal}(L/K) \xrightarrow{\sim} \mathrm{Gal}(k_L/k_K)$ canonically.

ii) $k_K = \mathbb{F}_q$ finite. Then every finite unramified extension L/K is Galois, and $\exists!\ \sigma_{L/K} \in \mathrm{Gal}(L/K)$ (<u>the arithmetic Frobenius</u>) such that $\forall x \in \mathcal{O}_L$, $\sigma_{L/K}(x) \equiv x^q \pmod{\pi_L}$; it generates $\mathrm{Gal}(L/K)$.

08/02/14

Algebraic Number Theory (10)

L/K <u>unramified</u> if $e(L/K) = 1$ $(\pi_K \mathcal{O}_L = \pi_L \mathcal{O}_L)$ and k_L/k_K <u>separable</u>.

<u>Remark</u>

$K/\mathbb{Q}_p$ finite, complete w.r.t v_p, $|\cdot|_p$, $k_K = \mathbb{F}_q$ say.

$\bar{\mathbb{F}}_q = \bigcup \mathbb{F}_{q^n} = \bigcup \mathbb{F}_q(\mu_m)$, $\mu_m = m^{th}$ roots of unity.

$\Rightarrow$ If $K^{nr} = \bigcup_{(m,p)=1} K(\mu_m)$, we see that K^{nr} is the union of all finite unramified extensions of K. It is called the <u>maximal unramified extension of K</u> (not complete!).

$$\mathrm{Gal}(K^{nr}/K) \cong \mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q) = \varprojlim \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \cong \varprojlim \mathbb{Z}/n\mathbb{Z} \cong \hat{\mathbb{Z}}$$

$$\varphi_K \in \mathrm{Gal}(K^{nr}/K) \quad \Leftrightarrow \quad (x \mapsto x^q)$$

φ_K is the arithmetic Frobenius of K^{nr}/K, and generates a dense subgroup of $\mathrm{Gal}(K^{nr}/K)$. Often it is more convenient to consider $F_K = \varphi_K^{-1}$ instead, called the <u>geometric Frobenius</u>.

<u>Ramification</u>

We will assume (for considerable simplification) that all L/K have k_L/k_K <u>separable</u> (e.g. k_K perfect or finite).

<u>Theorem 3.9</u>

L/K finite, separable, k_L/k_K separable. Then $\exists!$ intermediate field $K \subset L_0 \subset L$ such that L_0/K is <u>unramified</u> and L/L_0 is <u>totally ramified</u> (i.e. $\overbrace{f(L/L_0)}^{=[k_L:k_{L_0}]} = 1$).

If $K \subset F \subset L$, then $L_0 \supset F \Leftrightarrow F/K$ is unramified.

We call L_0 the <u>maximal unramified subfield</u> of L/K.

<u>Proof</u>

By 3.8ii) $\exists\, K'/K$ unramified with $k_{K'} \cong k_L$, and this induces a map $K' \hookrightarrow L$; let L_0 be the image.

L_0/K is unramified of degree $[k_L : k_K] = f(L/K)$,

so $f(L/L_0) = [k_L : k_{L_0}] = 1$.

$$\begin{tikzcd} & & L \arrow[d, dash] \\ k_L \arrow[rr, dashed, dash] \arrow[d, dash, "\text{finite separable}"'] & & L_0 \arrow[d, dash] \\ k_K \arrow[rr, dashed, dash] & & K \end{tikzcd}$$

$$\begin{tikzcd} L \arrow[d, dash] \arrow[dr, dash] & \\ F \arrow[d, dash] & L_0 \arrow[dl, dash] \\ K & \end{tikzcd}$$

If $F \subset L_0$ ($K \subset F \subset L$), then F is unramified (or L_0 is).

Conversely, if F/K is unramified, $k_F \subset k_{L_0} = k_L$ and 3.6 then gives $F \hookrightarrow L_0$

<u>Totally Ramified Extensions</u>

<u>Definition</u>

A monic polynomial $g = T^n + \sum_{i=0}^{n-1} a_i T^i \in \mathcal{O}_K[T]$ is said to be <u>Eisenstein</u> if $v_K(a_i) \geq 1\ \forall i$ and $v_K(a_0) = 1$

(so g is <u>irreducible</u> by Eisenstein's Criterion)

<u>Theorem 3.10</u>

i) If $g \in \mathcal{O}_K[T]$ is an Eisenstein polynomial and $g(x) = 0$ then $L = K(x)/K$ is totally ramified.

$\mathcal{O}_L = \mathcal{O}_K[x]$, $v_L(x) = 1$.

ii) Conversely, if L/K is totally ramified, and π_L is any uniformiser of L, then its minimal polynomial is Eisenstein and $\mathcal{O}_L = \mathcal{O}_K[\pi_L]$.

In particular, $L = K(\pi_L)$!!

<u>Example</u>

$K = \mathbb{Q}_p$, $L = \mathbb{Q}_p(\mu_q) = \mathbb{Q}_p(\zeta_q)$, $\zeta_q^{\,q} = 1$, $q = p^r$

Now ζ_q is a root of $\Phi_q(T) = \frac{T^q - 1}{T^{q/p} - 1}$

and $\Phi_q(T+1)$ is an Eisenstein polynomial $\Rightarrow \mathcal{O}_L = \mathbb{Z}_p[\zeta_q]$

and $\pi_L = \zeta_q - 1$ is a uniformiser of L.

<u>Proof</u>

i) $g = T^n + a_{n-1}T^{n-1} + \dots + a_1 T + a_0$. Let v_K be the normalised (discrete) valuation on K, extended to a valuation on L (not necessarily $\mathbb{Z}$-valued), $L = K(x)$, $x \in \mathcal{O}_L$

$v_K(x+y) \geq \min(v(x), v(y))$

$x^n = -\sum_{i=0}^{n-1} a_i x^i \Rightarrow v_K(x) > 0$ (as $v_K(a_i) \geq 1\ \forall i$).

$\Rightarrow \forall i \neq 0,\ v_K(a_i x^i) > 1$, and $v_K(a_0) = 1$.

So $v_K(\text{RHS}) = 1$ by Δ-inequality $\Rightarrow v_K(x) = \frac{1}{n}$.

where $n = [L:K]$. $e(L/K) = v_L(\pi_K)$ forced since $e_i \leq n$

$\Rightarrow$ since $ef = n$, this implies $e = n$ (i.e. x is a uniformiser) $\uparrow$ $x = \varepsilon\pi_L^i$, $i=1$ is forced

and $f=1$, so L/K is totally ramified. Say $\pi_L = x$. $v_L = n v_K$

Consider $y = \sum_{i=0}^{n-1} b_i \pi_L^i$, $b_i \in K$. Then

$v_L(b_i \pi_L^i) = i + n v_K(b_i) \equiv i \mod n$

$\uparrow$ because of this

In particular, the $v_L(b_i\pi_L^i)$ are <u>distinct</u> (†). So ~~$v_L(y) = \min v_L(b_i$~~

$v_L(y) = \min v_L(b_i \pi_L^i)$.

$i + n v_K(b_i)$

So $y \in \mathcal{O}_L \Leftrightarrow v_L(y) \geq 0 \Leftrightarrow$ all $v_L(b_i\pi_L^i) \geq 0$ $\quad 0 \leq i \leq n-1$

$\Rightarrow$ forces $v_K(b_i) \geq 0$ as $b_i \in K \Rightarrow v_K(b_i) \in \mathbb{Z}$

So $y \in \mathcal{O}_L \Leftrightarrow y \in \mathcal{O}_K[\pi_L]$.

ii) L/K totally ramified, degree n, $g = T^m + \sum a_i T^i \in \mathcal{O}_K[T]$ the min. poly. of π_L ($m \leq n$).

$v_K(\pi_L) = \frac{1}{n}$

$(*)\ -\pi_L^m = \sum_{i=0}^{m-1} a_i \pi_L^i$. ~~The RHS has $v_K = v_K(a_0) = 1$.~~

$v_K(\pi_L) = \frac{1}{n}$ as L/K is totally ramified, so $m = n$.

Take v_K of $(*)$. $(\dagger) \Rightarrow \frac{m}{n} \geq \min\left(\frac{i}{n} + v_K(a_i)\right)$

$m < n \Rightarrow$ unattainable as $v_K(a_i) \in \mathbb{Z}$, $i < m$. $\Rightarrow m = n$. Only attainable if $v_K(a_0) = 1$, $v_K(a_i) \geq$

as π_L now has degree n.

So $L = K(\pi_L)$ and the rest follows from i).

Remark

Suppose that $K/\mathbb{Q}_p$ is finite, $k_K = \mathbb{F}_q$. One way to normalise an AV on K is $|x|_K = \frac{1}{q^{v_K(x)}}$ (called normalised AV or modulus).

K is a topological field, locally compact ($\mathcal{O}_K$ is compact).

Every locally compact topological group has a Haar measure (positive functional on continuous functions of compact support), which is translation invariant: $\int f(hg)\,dg = \int f(g)\,dg$

Examples

$K = \mathbb{R}$, Lebesgue measure dx $(d(x+a) = dx)$

$K = \mathbb{C}$, $(2)\,dx\,dy$

$K/\mathbb{Q}_p$ finite. It is enough to integrate functions of the form $\mathbb{1}_{a+\pi^m\mathcal{O}_K}$. So we need an invariant measure μ on $a + \pi^m\mathcal{O}_K$.

If $\mu(\mathcal{O}_K) = 1$, then $\mathcal{O}_K = \bigcup_{a \bmod \pi^m} (a + \pi^m\mathcal{O}_K)$

so $\mu(a + \pi^m\mathcal{O}_K) = \mu(\pi^m\mathcal{O}_K) = \frac{1}{(\mathcal{O}_K : \pi^m\mathcal{O}_K)} = \frac{1}{q^m}$

Take $a \in K^*$. What is $d(ax)$? This is still invariant under translation and therefore, with ~~the~~ we have uniqueness of Haar measure

$K = \mathbb{R}$, $d(ax) = |a|\,dx$

$K = \mathbb{C}$, ~~d~~ $\mu(az) = |a|^2\mu(z)$

$K/\mathbb{Q}_p$, $\mu(a\mathcal{O}_K) = \mu(\mathcal{O}_K)$, $a \in \mathcal{O}_K^*$.

$$d(ax) = \underbrace{|a|_K}_{\text{normalised}}\,dx$$

11/02/14

Algebraic Number Theory ⑪

4 Ramification Theory

Setup : K a complete, discretely valued field, $\mathcal{O}_K, \pi_K, k_K, v_K$

L separable, finite $/K$, $\mathcal{O}_L, \pi_L, k_L, v_L$. Assume k_L/k_K separable.

$[L:K] = n = e(L/K)\, f(L/K)$, $f = [k_L : k_K]$

$v_K(\pi_K) = 1 = v_L(\pi_L)$, $e = v_L(\pi_K)$.

Definition

The *inverse different* of L/K is $\mathcal{D}_{L/K}^{-1} = \{x \in L \mid tr_{L/K}(x\mathcal{O}_L) \subset \mathcal{O}_K\} \supset \mathcal{O}_L$.

This is the *dual* of $\mathcal{O}_L$ with respect to the trace form

$(x, y) \mapsto tr_{L/K}(xy)$, $L \times L \to K$.

Since the trace-form is non-degenerate, $\mathcal{D}_{L/K}^{-1}$ is f.g. as an $\mathcal{O}_K$-module (take a dual basis for the basis of $\mathcal{O}_L$)

Obviously $\mathcal{D}_{L/K}^{-1}$ is an $\mathcal{O}_L$-submodule of L, containing $\mathcal{O}_L$.

So $\mathcal{D}_{L/K}^{-1} = \pi_L^{-\delta}\mathcal{O}_L$ for some $\delta = \delta(L/K) \geq 0$

(as it is a fractional ideal) because $\mathcal{O}_L$-submodules of L = Fractional Ideals of L

The *different* of L/K is $\mathcal{D}_{L/K} = \pi_L^{\delta}\mathcal{O}_L$. δ is called the *differential exponent*.

Theorem 4.1

i) If $M/L/K$, $\mathcal{D}_{M/K} = \mathcal{D}_{M/L}\mathcal{D}_{L/K}$

ii) Suppose that $\mathcal{O}_L = \mathcal{O}_K[x]$ for some $x \in L$, with min. poly. $g(T)$. Then $\mathcal{D}_{L/K} = (g'(x))$

iii) L/K is unramified $\iff \mathcal{D}_{L/K} = \mathcal{O}_L$ (i.e. $\delta_{L/K} = 0$).

If $\mathrm{char}(k_K) = 0$, or $\mathrm{char}(k_K) = p > 0$ and $p \nmid e(L/K)$, then $\delta_{L/K} = e - 1$, and we say L/K is *tamely ramified*.

In the remaining case where $p \mid e(L/K)$, $\delta_{L/K} \geq e$, and we say that L/K is <u>wildly ramified</u>.

<u>Proof</u>

i) It is sufficient to prove that $\mathcal{D}_{M/K}^{-1} = \mathcal{D}_{M/L}^{-1}\mathcal{D}_{L/K}^{-1}$. This follows from the definition and the fact that $tr_{M/K} = tr_{L/K} \circ tr_{M/L}$.
Easy to see that $\mathcal{D}_{M/L}^{-1}\mathcal{D}_{L/K}^{-1} \subset \mathcal{D}_{M/K}^{-1}$. Also $\mathcal{D}_{M/K}^{-1} \subset \mathcal{D}_{M/L}^{-1}$

ii) Let $x = x_1, \dots, x_n$ be roots of g in $\bar{K}$. L/K separable $\Rightarrow x_i \neq x_j$ and using partial fractions, $\frac{1}{g(T)} = \sum_{i=1}^{n} \frac{1}{(T-x_i)g'(x_i)}$

Expand each side in powers of $\frac{1}{T}$. $g = T^n + \dots + a_1 T + a_0$.

$$T^{-n} - a_{n-1}T^{-n-1} + \dots = \sum_i g'(x_i)^{-1}(T^{-1} + x_i T^{-2} + x_i^2 T^{-3} + \dots)$$
$$= \sum_{r=0}^{\infty} tr_{L/K}[g'(x)^{-1}x^r]\, T^{-r-1}$$
$$\Rightarrow tr_{L/K}(g'(x)^{-1}x^r) = \begin{cases} 0 & 0 \leq r < n-1 \\ 1 & r = n-1 \\ \in \mathcal{O}_K & \forall r \end{cases}$$

$\mathcal{O}_L = \mathcal{O}_K[x]$

$$\mathcal{O}_L = \bigoplus_{r=0}^{n-1} \mathcal{O}_K x^r \Rightarrow \mathcal{D}_{L/K}^{-1} = \bigoplus_{r=0}^{n-1} \mathcal{O}_K g'(x)^{-1} x^r$$
$$= g'(x)^{-1}\mathcal{O}_L$$

$$\Rightarrow \mathcal{D}_{L/K} = (g'(x))$$

iii) If L/K is unramified, $\mathcal{O}_L = \mathcal{O}_K[x]$ with $\bar{g}$ separable over k_K, so $g'(x)$ is a unit. $\Rightarrow \mathcal{D}_{L/K} = \mathcal{O}_L$. by (ii)
because $\bar{g}'(x)$ is a unit i.e. non-zero in k_K

In general, by i), this gives $\mathcal{D}_{L/K} = \mathcal{D}_{L/L_0}$ where L_0/K is the maximum unramified subfield. $\mathcal{D}_{L/K} = \underbrace{\mathcal{D}_{L/L_0}}_{\text{a ideal}} \underbrace{\mathcal{D}_{L_0/K}}_{=\mathcal{O}_{L_0}} = \mathcal{D}_{L/L_0}$

So it is enough to consider the case L/K totally ramified.

$\Rightarrow \mathcal{O}_L = \mathcal{O}_K[\pi_L]$, and the min. poly.

$g = T^e + \sum a_i T^i$ is <u>Eisenstein</u> ($v_K(a_i) \geq 1$, $V_K(a_0) = 1$)
$e = e(L/K)$, L/K totally ramified

11/02/14

Algebraic Number Theory (11)

$\Rightarrow g'(\pi_L) = e\pi_L^{e-1} + \sum_{i=1}^{e-1} i a_i \pi_L^{i-1}$ $\quad v_K(a_i) \geq 1 \Rightarrow v_L(a_i) \geq e$

$v_L(i a_i \pi_L^{i-1}) \geq e + (i-1) \quad (i \geq 1)$ $\quad v_L(\pi_L^{i-1}) = i-1$

If $\mathrm{char}(k_L) = 0$ or p and $p \nmid e$, then $v_L(e\pi_L^{e-1}) = e-1$.

want $v_L(e) = 0$

$\Rightarrow v_L(g'(\pi_L)) = e-1$.

True since in these cases, $\bar{e} \neq 0$ in k_L so $v_K(e) = v_L(e) = 0$

Otherwise, $v_L(e\pi_L^{e-1}) \geq e$. Hence $v_L(g'(\pi_L)) \geq e$.

(In particular, if $L \neq K$, then $\delta_{L/K} > 0$). $\square$

Remark

We have a module of Kähler differentials $\Omega_{B/A}$ for a ring homomorphism $A \to B$. $\Omega_{B/A}$ is the B-module generated by $\{db \mid b \in B\}$, ~~quotiented out by~~ subject to $(d(a) = 0, a \in A)$ and $(d(b_1 b_2) = (db_1) b_2 + b_1 (db_2))$

iii) shows that $\Omega_{\mathcal{O}_L/\mathcal{O}_K}$ is cyclic, generated by dx, annihilator $g'(x)\mathcal{O}_L$.

Example

$K_n = \mathbb{Q}_p(\zeta_{p^n})$, $p > 2$. $\pi_n = \zeta_{p^n} - 1$ is a uniformiser,

$K_n/\mathbb{Q}_p$ is totally ramified, degree $(p-1)p^{n-1}$

ζ_{p^n} is a root of $f(X) = X^{(p-1)p^n} + X^{(p-2)p^n} + \dots + 1$

π_n is a root of $f(1+X)$. This is Eisenstein.

$n = 1 \Rightarrow K_1/\mathbb{Q}_p$ is tamely ramified, $e = p-1$

$\Rightarrow \mathcal{D}_{K_1/\mathbb{Q}_p} = \pi_1^{p-2}\mathcal{O}_{K_1}$ $\qquad \mathcal{D}_{L/K} = (g'(x))$ for $\mathcal{O}_L = \mathcal{O}_K[x]$

$n > 1 \Rightarrow K_n/K_{n-1}$ has degree p. $\mathcal{O}_{K_n} = \mathcal{O}_{K_{n-1}}[\zeta_{p^n}]$.

ζ_{p^n} has min. poly. $T^p - \zeta_{p^{n-1}}$ over K_{n-1}.

$\Rightarrow \mathcal{D}_{K_n/K_{n-1}} = (p\zeta^{p-1}) = p\mathcal{O}_{K_n}$.

$\Rightarrow \mathcal{D}_{K_n/\mathbb{Q}_p} = (p^{n-1}\pi_1^{p-2})$

$\mathcal{D}_{K_n/\mathbb{Q}_p} = \mathcal{D}_{K_n/K_{n-1}} \cdot \mathcal{D}_{K_{n-1}/K_{n-2}} \cdots \mathcal{D}_{K_1/\mathbb{Q}_p}$

13/02/14

Algebraic Number Theory 12

L/K Galois.

k_L/k_K separable. $G = Gal(L/K) \ni \sigma$. $|x|_L = |N_{L/K}(x)|^{\frac{1}{n}}$

σ preserves the AV on L (by uniqueness of extension of AVs).

So $\sigma(\mathcal{O}_L) = \mathcal{O}_L$, $\sigma(m_L^i) = m_L^i \ \forall i \geq 1$.

$\therefore \sigma$ acts on the quotients $\mathcal{O}_L/m_L^{i+1}$ $(i \geq 0)$.

<u>Definition</u>

The <u>ramification subgroups</u> of L/K are $G_i = G_i(L/K)$

$G_i = \ker(G \to Aut(\mathcal{O}_L/m_L^{i+1}))$ $(i \geq 0)$.

It is convenient to set $G_{-1} = G$. Clearly $G_i \trianglelefteq G$, because it is a kernel

$G_i \supset G_{i+1} \supset \dots$

inverse limits

$\bigcap_i G_i = \bigcap_i \ker(G \to Aut(\mathcal{O}_L/m_L^{i+1})) = \ker(G \to \mathcal{O}_L) = \{1\}$

So, as G is finite, $G_i = \{1\}$ for $i \gg 0$.

<u>Definition</u>

$I = I(L/K) = G_0(L/K)$, the <u>inertia group</u> of L/K. ($= \ker(G \to Aut(\underbrace{\mathcal{O}_L/m_L}_{= k_L}))$)

$P = P(L/K) = G_1(L/K)$, the <u>wild ramification sub group</u>.

L | totally ramified | L_0 | unramified | K

$I = \ker(G \to Aut(k_L)) = \ker(G \to \underbrace{Gal(k_L/k_K)}_{= Gal(L_0/K)})$

$= Gal(L/L_0)$

In particular, L/K is <u>unramified</u> (i.e. $L = L_0$) $\iff I = \{1\}$ so all G_i are trivial in this case

$G/I = Gal(k_L/k_K)$, and also

$\forall i \geq 0$, $G_i(L/K) = G_i(L/L_0)$. So to study G_i, the essential case is when L/K is totally ramified.

<u>Proposition 4.2</u>

Assume that L/K is totally ramified. Fix π_L a uniformiser of L.

i) $\forall i \geq 0$, $G_i(L/K) = \{\sigma \in Gal(L/K) \mid v_L(\sigma(\pi_L) - \pi_L) \geq i+1\}$

ii) Define maps $\Theta_i : G_i \to \begin{cases} k_L^* & \text{if } i=0 \\ m_L^i / m_L^{i+1} & \text{if } i>0 \end{cases}$

by $\Theta_0(\sigma) = \frac{\sigma(\pi_L)}{\pi_L} \bmod m_L$, $\Theta_i(\sigma) = \frac{\sigma(\pi_L)}{\pi_L} - 1 \bmod m_L^{i+1}$ for $i>0$

(well defined by (i)). Then Θ_i is a homomorphism independant of the choice of π_L, with kernel G_{i+1}.

Proof

i) $\mathcal{O}_L = \mathcal{O}_K[\pi_L]$, so σ acts trivially on $\mathcal{O}_L / m_L^{i+1}$

$\Leftrightarrow \sigma(\pi_L) \equiv \pi_L \bmod m_L^{i+1}$ σ already fixes $\mathcal{O}_K$

ii) $\sigma \in G_i$. If $u \in \mathcal{O}_L^*$, then $\sigma(u) \equiv u \bmod m_L^{i+1}$.

$\Rightarrow \frac{\sigma(u)}{u} \equiv 1 \bmod m_L^{i+1}$.

So $\frac{\sigma(u\pi_L)}{u\pi_L} \overset{\sigma \text{ an automorphism}}{=} \frac{\sigma(u)}{u}\frac{\sigma(\pi_L)}{\pi_L} \equiv \frac{\sigma(\pi_L)}{\pi_L} \bmod m_L^{i+1}$

This shows that Θ_i is independant of choice of π_L. So if $\sigma, \tau \in G_i$,

$\Theta_i(\sigma) = \frac{\sigma(\tau(\pi_L))}{\tau(\pi_L)} \overset{??}{(-1)}$

If $i=0$, $\sigma, \tau \in G_0$, then $\Theta_0(\tau)\Theta_0(\sigma) = \frac{\tau(\pi_L)}{\pi_L}\frac{\sigma(\tau(\pi_L))}{\tau(\pi_L)}$

$= \frac{\sigma\tau(\pi_L)}{\pi_L} = \Theta_0(\sigma\tau)$ $(\in k_L^* = (\mathcal{O}_L/m_L)^*)$

For $i>0$, then $\Theta_i(\sigma)\Theta_i(\tau) = 0$ as $m^i m^i \subset m^{i+1}$,

and $\Theta_i(\sigma\tau) = \frac{\sigma\tau(\pi_L)}{\pi_L} - 1 = \frac{\sigma\tau(\pi_L)}{\tau(\pi_L)}\frac{\tau(\pi_L)}{\pi_L} - 1$

$= (\Theta_i(\sigma)+1)(\Theta_i(\tau)+1) - 1$

$= \Theta_i(\sigma) + \Theta_i(\tau)$.

So Θ_i is a homomorphism in all cases and by i),

$\ker(\Theta_i) = G_{i+1}$.

So $G_0/G_1 \hookrightarrow k_L^*$ and $\forall i > 0$,

$G_i/G_{i+1} \hookrightarrow m_L^i/m_L^{i+1} \simeq k_L$
$\pi_L^i \longleftrightarrow 1$

Corollary 4.3

i) In every case, G_0/G_1 is cyclic, of order prime to char(k_K) (if $\neq 0$) since $G_0/G_1 \leq k_L^*$, $|k_L^*| = p^r - 1$, char$(k_K) = p$

ii) If char$(k_K) = 0$, then $G_1 = 0$ (since $G_i/G_{i+1} \hookrightarrow k_L$, torsion free) ← finite, has torsion, so $G_i/G_{i+1} = 0$ so $G_i = G_{i+1} = \ldots \Rightarrow G_1 = 0$, $\overset{\shortparallel}{G_2}$, $\overset{\shortparallel}{G_3}$ etc

iii) If char$(k_K) = p > 0$, then each G_i/G_{i+1} is an elementary abelian p-group (i.e. $\cong (\mathbb{Z}/p\mathbb{Z})^n$) (since $G_i/G_{i+1} \hookrightarrow k_L$, an $\mathbb{F}_p$-vector space)

iv) If k_K is finite, and L/K is arbitrary Galois (i.e. not necessarily totally ramified) then $\mathrm{Gal}(L/K)$ is soluble.

$G \supset G_0 \supset G_1 \supset$ ~~...~~ $= \{id\}$, G_1 a p-group, G_0/G_1 cyclic (see (i) above)

because $G_1/G_2, G_2/G_3, \ldots$ all p-groups and $G_i = \{id\}$ for $i >> 0$

G/G_0 cyclic ($\overset{\text{because}}{\cong} \mathrm{Gal}(k_L/k_K)$ cyclic) □

In particular, if $f \in \mathbb{Q}_p[T]$ is an irreducible polynomial of degree $n \geq 5$, its Galois group is never S_n (or A_n).

Example

$K_n = \mathbb{Q}_p(\zeta_{p^n})$, $(p > 2)$. $K_n/\mathbb{Q}_p$ is totally ramified, and $G = G_0$ (because $k_L = k_K$ so $\mathrm{Gal}(k_L/k_K)$ trivial)

$G = G_0 \xrightarrow{\sim} (\mathbb{Z}/p^n\mathbb{Z})^*$ (as the cyclotomic polynomial is irreducible over $\mathbb{Q}_p$)

$(\sigma_a : \zeta_{p^n} \mapsto \zeta_{p^n}^a) \longleftrightarrow a$

$\pi_n = \zeta_{p^n} - 1$ a uniformiser of K_n.

Let $a \neq 1 \in (\mathbb{Z}/p^n\mathbb{Z})^*$, $a - 1 \equiv p^{n-m} b \pmod{p^n}$

for some b with $(b, p) = 1$ and $0 < m \leq n$.

$v_{K_n}(\sigma_a(\pi_n) - \pi_n) = v_{K_n}(\sigma_a(\zeta_{p^n}) - \zeta_{p^n})$

$= v_{K_n}(\zeta_{p^n}^a - \zeta_{p^n}) = v_{K_n}(\zeta_{p^n}^{a-1} - 1) = v_{K_n}(\zeta_{p^m}^b - 1)$

apply element of Gal

$$= v_{K_n}(\zeta_{p^m} - 1) = v_{K_n}(\pi_m) = [K_n : K_m] = p^{n-m}$$

$(m > 0)$

So by 4.2(i), putting $r = n - m$,

$$G_i = \ker\left(\left(\mathbb{Z}/p^n\mathbb{Z}\right)^* \to \left(\mathbb{Z}/p^r\mathbb{Z}\right)^* \right)$$

if $p^{r-1} \leq i < p^r$.

$a \equiv 1 \ (p^{n-m})$

15/02/14 Algebraic Number Theory (13)

5 Places

2pm Wed MR3

Definition

Let K be a field. A place of K is an equivalence class of AVs on K. It is finite if the AV is non-archimedean and infinite otherwise.

Notation

$\Sigma_K = \{\text{places of } K\} = \underbrace{\Sigma_{K,f}}_{\text{finite}} \cup \underbrace{\Sigma_{K,\infty}}_{\text{infinite}}$.

We typically denote places $v, w, \ldots$ (shouldn't cause confusion) and $|\cdot|_v$ for an AV in the class (possibly suitably normalised).

$K = \mathbb{Q}$: Every AV is equivalent to $|\cdot|_\infty$ (Euclidean AV) [Analysis II] or some $|\cdot|_p$ [Ostrowski]. Write p, ∞ for the corresponding place.

$\Sigma_{\mathbb{Q}} = \{p \mid p \text{ prime}\} \cup \{\infty\}$

$v \in \Sigma_K$: write K_v for completion with respect to v (so $\mathbb{Q}_\infty = \mathbb{R}$).

Extensions

L/K separable, algebraic, $v \in \Sigma_K$, $w \in \Sigma_L$. We say that w lies over v if the restriction of $|\cdot|_w$ to K is equivalent to $|\cdot|_v$.

If K is not complete, there are typically several w lying over v (if K is complete, $\exists!\, w$ by Theorem 3·2). $|N_{L/K}(x)|^{\frac{1}{n}}$

Notation: $w|v$ for "w lies over v".

Suppose $w|v$, and assume that $|\cdot|_w$ and $|\cdot|_v$ are equal on K.

Let $(K_v, |\cdot|_v)$, $(L_w, |\cdot|_w)$ be completions.

Then $K \subset L \subset L_w$, so by uniqueness of extensions of AVs, $\exists!\, K_v \hookrightarrow L_w$, a K-algebra homomorphism, such that

$|\cdot|_w$ extends $|\cdot|_v$.

Lemma 5·1

Suppose $L = k(x)/k$ is finite. Then $L_w = k_v(x)$ is finite over K_v.

Proof

because L/k is and $k_v \supset k$

Let $F = k_v(x) \subset L_w$. $[F : k_v] < \infty$, so $\exists!$ extension of $|\cdot|_v$ from k_v to F, and F is complete. But $L \subset F \subset L_w$, so $|\cdot|_w$ is another such extension. Therefore $F = L_w$. by uniqueness $\square$

Suppose now that L/k is finite. By the lemma, if $w|v$ the numbers $f(w|v) := f(L_w/k_v)$, $e(w|v) := e(L_w/k_v)$ are defined and $e(w|v)f(w|v) = [L_w : k_v]$.

Let $L = k(x)$. To each $w|v$ we can associate an irreducible factor $g \in k_v[T]$ of the minimal polynomial f of x over k; take g = min. poly. of x over k_v. (*)

$$\begin{tikzcd} & L_w \arrow[d, dash] \\ L=k(x) \arrow[ur, dash] \arrow[d, dash] & K_v \\ K \arrow[ur, dash] & \end{tikzcd}$$

Conversely, let $g \in k_v[T]$ be irreducible, monic, with $g|f$. Then $F = k_v[T]/(g)$ is finite $/k_v$.

So $\exists!$ extension $|\cdot|_F$ of $|\cdot|_v$ from k_v to F.

$$\begin{tikzcd} F \arrow[d, dash] \\ k_v \end{tikzcd}$$

$S = g\,k_v[T] \cap k[T] = f\,k[T]$ as $g|f$, f irreducible over K.
because $h \in S \Rightarrow g|h$, $h \in k[T]$, h has some roots of f so $f|h$.

$\exists!$ k-homomorphism $L = k(x) \to F$ mapping x to $(T \bmod g)$.

Then Lemma 5·1 $\Rightarrow F = L_w$, for w = place containing $|\cdot|_F \circ i$.
as F is complete already and $L_w \subset F$, see 5·1

Summarising:

Theorem 5·2

$L = K(x) = K[T]/(f)$, $f = \prod_{i=1}^{k} g_i$, factorisation in $k_v[T]$.

15/02/14

Algebraic Number Theory 13

Then we have a bijection $\{g_i\} \xrightarrow{\sim} \{w \in \Sigma_L, w | v\}$, $g_i \mapsto w_i$

surjective by (*)

where $L_{w_i} = k_v[T]/(g_i)$. ~~Since (1)~~ injective by uniqueness of the AV extensions and k-homs used.

Since $[L_{w_i} : k_v] = \deg(g_i)$, we have

<u>Corollary 5·3</u>

$$[L:K] = \sum_{w|v} [L_w : k_v] = \sum_{w|v} e(w/v) f(w/v)$$

Write more canonically using <u>tensor products</u>.

$L = K[T]/(f)$. Then $L \otimes_K k_v \underset{= K[T]/(f) \otimes_K k_v}{=} k_v[T]/(f)$.

$$L \otimes_K k_v = \prod_i k_v[T]/(g_i) \quad (CRT) \quad = \prod_i L_{w_i} \ (\text{by } 5{\cdot}2)$$

This is a finite dimensional k_v-algebra of dimension $= [L:K] = \deg(f)$.

So Theorem 5·2 can be restated as:

<u>Theorem 5·4</u>

$L \otimes_K k_v = \prod_{w|v} L_w$ (for each $w|v$, $K \hookrightarrow L \hookrightarrow L_w$, $K \hookrightarrow k_v \hookrightarrow L_w$, so that $L \otimes_K k_v \twoheadrightarrow L_w$).

<u>Corollary 5·5</u>

L/K finite, $v \in \Sigma_K$, $x \in L$.

$$N_{L/K}(x) = \prod_{w|v} N_{L_w/k_v}(x), \quad Tr_{L/K}(x) = \sum_{w|v} Tr_{L_w/k_v}(x)$$

<u>Proof</u>

If $u_x \in End_K(L)$ is $u_x(y) = xy$, then

$N_{L/K}(x) = \det_K u_x$, $Tr_{L/K}(x) = tr_K u_x$.

u_x extends by k_v-linearity to an endomorphism of $L \otimes_K k_v$ ($= k_v[T]/(f)$), also given by multiplication by x, and $L \otimes_K k_v \cong \bigoplus L_w$ as k_v-vector spaces $\Rightarrow$ the formula. properties of traces and dets over direct sums $\square$

In the case that L/K is finite Galois:

$\sigma : L \to L$ an automorphism, $|\cdot|$, $|\cdot|'$ AVs on L. Then σ defines an isometry $(L, |\cdot|) \xrightarrow{\sim} (L, |\cdot|') \Leftrightarrow \underbrace{|\sigma(x)|' = |x| \;\forall x}_{\text{definition of isometry}}$.

$G = Gal(L/K)$, $w \in \Sigma_L$. For $\sigma \in G$, define $\sigma w \in \Sigma_L$ by the AV $x \mapsto |\sigma^{-1}(x)|_w$ (σ^{-1} to make a left action).

Then $w | v \Leftrightarrow \sigma w | v$ as $\sigma|_K = id$, and if so, σ extends to a K_v-isomorphism $L_w \xrightarrow{\sim} L_{\sigma w}$.

<u>Theorem 5.6</u>

$\forall w | v$, L_w / K_v is Galois, and $Gal(L_w/K_v) \xrightarrow{\sim} G_w \subset G$ (G_w = stabiliser of w) under restriction $L \subset L_w$.

Moreover, G acts <u>transitively</u> on $\{w | v\}$.

18/02/14 Algebraic Number Theory (14)

Theorem 5·6

For every place $w|v$, L_w/K_v is Galois, and the map

$\mathrm{Gal}(L_w/K_v) \xrightarrow[\text{to } L]{\text{restriction}} G = \mathrm{Gal}(L/K)$ is an isomorphism

onto $G_w = \{\sigma \in G \mid \sigma w = \overset{w}{0}\}$ = stabiliser of w

should be w?

Proof

We saw that any $\sigma \in G_w$ extends to an automorphism of L_w/K_v. On the other hand, if $\sigma \in \mathrm{Aut}(L_w/K_v)$, then $\sigma(L) = L$, (σ maps conjugates of $x \in L$ to L) (L/K Galois), so $\sigma|_L \in G$ ($= \mathrm{Gal}(L/K)$). By uniqueness of extensions of AVs, $\sigma w = w$, so $\sigma|_L \in G_w$

σ fixes K so $\sigma v = v$
v extends to w
So σv extends to $\sigma w = w$

because normal σ extend to automorphisms $L_w \xrightarrow{\sim} L_{\sigma w}$ and here $\sigma w = w$

$\therefore \mathrm{Aut}(L_w/K_v) \xrightarrow{\sim} G_w$ (*)

Now by Corollary 5·3, $\#G = [L:K] = \sum_{w|v} [L_w : K_v]$

$$\geq \sum_{\sigma \in G/G_w} [L_{\sigma w} : K_v] \qquad (\dagger)$$

$$= (G:G_w)[L_w : K_v] \text{ as } L_{\sigma w} = L_w$$

So $[L_w : K_v] \leq \#G_w$, with equality $\Leftrightarrow$ G acts transitively on $\{w|v\}$ (i.e. orbits every $w|v$). So by (*), L_w/K_v is Galois and we have equality.

$[L_w : K_v] \geq |\mathrm{Aut}(L_w/K_v)| = |G_w|$
$\Rightarrow$ equality everywhere in ($\dagger$)
$|\mathrm{Aut}(L_w/K_v)| = [L_w : K_v] \Rightarrow$ Galois and G transitive on $w|v$

Corollary 5·7

L/K finite Galois. Then $f(w|v) = [L_w : K_v]$ ($= f_v$) and $e(w|v) = e(L_w/K_v)$ ($= e_v$) depend only on v (and not on w), and $[L:K] = e_v f_v g_v$ where $g_v = \#\{w|v\}$.

Proof

$w, w'|v \Rightarrow w' = \sigma w$ for some $\sigma \in G$ (by 5·6), inducing a K_v isomorphism $L_w \xrightarrow{\sim} L_{\sigma w}$.

Now $[L:K] = \sum [L_w : K_v] = \sum [L_{\sigma w} : K_v] = g_v [L_w : K_v$

Remark

1. If L/K is algebraic, then if $v \in \Sigma_K$, $w \in \Sigma_L$, $w|v$, define $L'_w = \bigcup_{\substack{K \subset F \subset L \\ \text{finite}}} F_{(w|F)} \subset L_w$

$F_{(w|F)}$ = completion of F with respect to the AV induced by w.
Then if L/K is Galois, so is L'_w/K_v, and
$Gal(L'_w/K_v) = G_w \underset{\text{closed}}{\subset} G$.
All places $w|v$ are conjugate under G (Proof by passage to limit over F).

2. If the residue field of K_v is finite, then we have a canonical generator of the Galois group of residue fields.
If L_w/K_v is unramified, then this equals $Gal(L_w/K_v)$, so we have a canonical element ("Frobenius of w") of G, whose conjugacy class depends only on v.

Section 5 applies usefully to:

- Algebraic extensions of $\mathbb{Q}$
- Algebraic extensions of $k(t)$, where we consider only AVs which are trivial on k.

6 Number Fields

From now on, k, L etc will be number fields.
Places of $\mathbb{Q}$ = $\{p\}_{\text{prime}} \cup \{\infty\} = \Sigma_{\mathbb{Q}}$
Let $p \leq \infty$ (i.e. $p \in \Sigma_{\mathbb{Q}}$). Denote by $\overline{\mathbb{Q}_p}$ an algebraic closure of $\mathbb{Q}_p$ ($= \mathbb{C}$ if $p = \infty$)

18/02/14

Algebraic Number Theory (14)

Extend $|\cdot|_p$ to $\overline{\mathbb{Q}}_p$. $|\cdot|_\infty = |z|$.

Let K be a number field, $v \in \Sigma_K$, $v | p$. Then $[K_v : \mathbb{Q}_p] < \infty$, so $\exists$ a $\mathbb{Q}_p$-embedding of K_v into $\overline{\mathbb{Q}}_p$, $i_v : K_v \hookrightarrow \overline{\mathbb{Q}}_p$, with any 2 i_vs conjugate (just by knowledge of Galois Theory) under $\mathrm{Gal}(\overline{\mathbb{Q}}_p / \mathbb{Q}_p)$. Conversely, if $i : K_v \hookrightarrow \overline{\mathbb{Q}}_p$ is a $\mathbb{Q}_p$-homomorphism, then $|\cdot|_p \circ i$ is an AV on K_v.

As $|\cdot|_p$ is invariant under $\mathrm{Gal}(\overline{\mathbb{Q}}_p / \mathbb{Q}_p)$, this AV depends only on the $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ conjugacy class of i.

$\Rightarrow$ <u>Proposition 6.1</u>

$v \mapsto i_v$ is a bijection

$$\{\text{places } v \text{ of } K \text{ over } p\} \xleftrightarrow{\sim} \left\{\begin{matrix}\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \text{ conjugacy classes of} \\ \mathbb{Q}_p\text{-embeddings } K \hookrightarrow \overline{\mathbb{Q}}_p\end{matrix}\right\}$$

$p = \infty$, RHS $= \{$embeddings $K \hookrightarrow \mathbb{C}$ up to complex conjugation$\}$

<u>Conventions and Notations</u>

K a number field, $v \in \Sigma_K$, $v | p$ (finite). Write

i) $\mathcal{O}_v \subset K_v$ completion and

ii) (slight abuse of notation) v = normalised discrete valuation $v : K_v^* \twoheadrightarrow \mathbb{Z}$

iii) π_v = any element of K (not just in K_v) with $v(\pi_v) = 1$

(this exists, because K is dense in K_v, so take any uniformiser π_{K_v} of K_v, and choose π_v with $v(\pi_v - \pi_{K_v}) > 1$)

iv) q_v = order of the residue field $k_v = \mathcal{O}_v / \pi_v \mathcal{O}_v$

v) $|x|_v = |N_{K_v/\mathbb{Q}_p}(x)|_p = q_v^{-v(x)}$, normalised AV

(c.f. end of section 3)

v infinite we say that v is real (complex) if $k_v \cong \mathbb{R}$ (resp $\mathbb{C}$)

In this case, $e_v = e(v/\infty) := 1$ (resp. 2).

(so that complex places are "ramified").

$$|x|_v = \begin{cases} |x|, & k_v \cong \mathbb{R} \\ |x|^2 & \text{if } k_v \cong \mathbb{C} \end{cases} \qquad (\text{so } |x|_v = |N_{k_v/\mathbb{R}}(x)|$$

Theorem 5·2

k a number field, $x \in k^*$.

i) For all but finitely many $v \in \Sigma_k$, $|x|_v = 1$.

ii) (Product Formula) $\prod_{v \in \Sigma_k} |x|_v = 1$ (well defined by (i)).

Proof

- $k = \mathbb{Q}$, $x = \varepsilon \prod_{p \in S} p^{r(p)} \in \mathbb{Q}^*$, $\varepsilon = \pm 1$

$$|x|_p = \begin{cases} \varepsilon x & p = \infty \\ p^{-r(p)} & p \in S \\ 1 & \text{otherwise} \end{cases} \Rightarrow \text{i) and ii)}$$

- In general, consider the min. poly. f of x over $\mathbb{Q}$.

For all but finitely many primes p, $f \in \mathbb{Z}_p[T]$ and

$|f(0)|_p = 1$, hence x is integral over $\mathbb{Z}_p$, and $|x|_p = 1$. (i)

$v | p \leq \infty \Rightarrow |x|_v = |N_{k_v/\mathbb{Q}_p}(x)|_p$,

so $\prod_{\text{all } v} |x|_v = \prod_{p \leq \infty} \prod_{v|p} |x|_v = \prod_{p \leq \infty} \left| \prod_{v|p} N_{k_v/\mathbb{Q}_p}(x) \right|$

$= \prod_{p \leq \infty} |y|_p$, $y = N_{k/\mathbb{Q}}(x)$ by 5·3 (ii)

$= 1$ by the case $k = \mathbb{Q}$.

20/02/14

Algebraic Number Theory (15)

Recall

$x \in K^*$, $|x|_v = 1$ for all but finitely many v, and

$\prod_v |x|_v = 1$.

Theorem 6·3

Let $L = K(x)/K$ be number fields. Then, $\exists$ finite $S \subset \Sigma_{K,f}$ such that $\forall v \in \Sigma_{K,f} \setminus S$, $w|v$, L_w / K_v is unramified and $\mathcal{O}_{L_w} = \mathcal{O}_{K_v}[x]$.

Proof

Let f be the min. poly. of x. By 6·2 ii), $\exists$ a finite set S such that $\forall v \in \Sigma_{K,f} \setminus S$, $f \in \mathcal{O}_v[T]$ and $\boxed{\text{disc}(f) \in \mathcal{O}_v^*.}$ Then any irreducible factor $g \in K_v[T]$ of f has $\underbrace{g \in \mathcal{O}_v[T]}_{\text{Gauss' Lemma}}$ and $\underbrace{\text{disc}(g) \in \mathcal{O}_v^*}_{\text{so } g \text{ is separable in } K_v}$.

because disc$(f) \in K^*$ non-zero as f is a min. poly.

$\Rightarrow$ If w = place corresponding to g, then $\mathcal{O}_w = \mathcal{O}_v[x]$ and L_w / K_v is unramified by 3·6.

Places and Ideals

By 1·6, finite places of $K \longleftrightarrow$ prime ideals P of $\mathcal{O}_K$.

$$v \longmapsto P_v$$

Given $x \in K^*$, $x\mathcal{O}_K = \prod_{v \in \Sigma_{K,f}} P_v^{v(x)}$

If $I = \prod_v P_v^{m_v}$ is any fractional ideal, then $x \in I$ $\Leftrightarrow v(x) \geq m_v \;\forall v$ ($m_v = 0$ for all but finitely many v)

Define $I(K)$ = group of fractional ideals $\cong$ Free abelian group on $\Sigma_{K,f}$.

$P(K)$ = subgroup of principal ideals $x\mathcal{O}_K$, $x \in K^*$.

$Cl(K)$ = ideal class group $= I(K)/P(K)$.

Study using <u>all</u> embeddings $K \hookrightarrow K_v$, $v \in \Sigma_K$.

7 Ideles and Adeles

$K \hookrightarrow K_v$ ($v \in \Sigma_K$). We want to consider all v simultaneously. Our obvious first try is $K \hookrightarrow \prod_v K_v$ but this is a bad choice as $\prod_v K_v$ is not locally compact. But, if $x \in K$, then $x \in \mathcal{O}_v$ for all but finitely many v.

Convention: "almost all v" means "all but finitely many v".

<u>Definition</u>

i) The ring of <u>adeles of K</u> is "Almost all x_v are integers"

$$A = A_K = \left\{ (x_v) \in \prod_{v \in \Sigma_K} K_v \;\middle|\; x_v \in \mathcal{O}_v \text{ for almost all } v, (|x_v|_v \leq 1 \right.$$

ii) The group of <u>ideles of K</u> is $J_K = A_K^*$

Equivalently, $J_K = \left\{ (x_v) \in \prod_{v \in \Sigma_K} K_v^* \;\middle|\; \begin{matrix} x_v \in \mathcal{O}_v^* \\ |x_v|_v = 1 \end{matrix} \text{ for almost all } v \right\}$

"Almost all x_v are units"

<u>Remarks</u>

1. A is a ring (condition $|x|_v \leq 1$ for almost all v is stable under $+$ and $\cdot$)

2. We have the <u>obvious</u> diagonal embeddings $K \hookrightarrow A_K$ and $K^* \hookrightarrow J_K$ (ring/group homomorphisms). Particularly important is $C_K := J_K/K^*$, the idele class group. This "contains" both $Cl(K)$ and $\mathcal{O}_K^*$.

i.e. $x \mapsto (x)_v$

22/02/14 Algebraic Number Theory 15

Idele Norm

$x = (x_v)_v \in J_K$, so $|x_v|_v = 1$ for almost all v.

So, define $|x| = |x|_{\mathbb{A}} = \prod_{v \in \Sigma_K} |x_v|_v$, a homomorphism $J_K \to \mathbb{R}^*_{>0}$

$\ker |\cdot|_{\mathbb{A}} = J_K'$, the ideles of norm 1.

The product formula $\Rightarrow K^* \subset J_K'$.

Content Map

$$c : J_K \longrightarrow I(K) \quad \text{is a homomorphism}$$

$$x = (x_v)_v \longmapsto c(x) = \prod_{v \in \Sigma_{K,f}} p_v^{v(x_v)} \text{ or } \sum_{v \in \Sigma_{K,f}} v(x_v)[v]$$

(ideals) (free abelian group on $\Sigma_{K,f}$)

If $x \in K^*$, $c(x) = x\mathcal{O}_K$, a fractional ideal.

So $c(K^*) = P(K)$ $\quad \overset{\shortparallel}{\prod_{v \in \Sigma_{K,f}}} p_v^{v(x)}$

Variant

$S \subset \Sigma_K$, $I_S(K) =$ subgroup of $I(K)$ generated by all $v \in \Sigma_{K,f} \setminus S$

Obvious Projection: $I(K) \xrightarrow[v \in S]{\text{ignore}} I_S(K)$ "forgetful map"

Compose this with c to get to get $c_S : J_K \longrightarrow I_S(K)$

$$(x_v)_v \longmapsto \sum_{v \in \Sigma_{K,f} \setminus S} v(x)[v]$$

Topology on J_K

$$U_K = \ker(c) = \prod_{v \in \Sigma_{K,\infty}} K_v^* \times \prod_{v \in \Sigma_{K,f}} \mathcal{O}_v^*$$

"unit ideles"

Define topology on J_K by declaring that U_K has product topology and that it is an open subgroup.

As $J_K = \coprod$ (cosets of U_K), this determines the topology on J_K.

?

Concretely, a basis of open sets is given by $\prod X_v$ where $X_v \subset K_v^*$ is open for all v and $X_v = \mathcal{O}_v^*$ for almost all $v \in \Sigma_{K,f}$.

- U_K is locally compact, so J_K is locally compact, and is a topological group.
- $c : J_K \to I(K)$ is continuous for the discrete topology on $I(K)$ (ker c is open) $\to$ hence all translates of ker c are. So preimage of a point of $I(K)$ is open
- Projections $J_K \to K_v^*$ are continuous, so $|\cdot|_{\mathbb{A}}$ is continuous and $x_v \mapsto |x_v|_v$ continuous (for the usual topology on $\mathbb{R}^*$, with the caveat that this topology is not the restriction of the product topology on $\prod K_v^*$)

Theorem 7.1

$K^* \subset J_K$ is a discrete subgroup.

Proof

Let $X = \prod X_v \subset J_K$, given by $X_v = \begin{cases} \{x \in K_v^* \mid |x|_v < 2\} & v \text{ infinite} \\ \{x \in K_v^* \mid |x|_v = 1\} & \text{“}\mathcal{O}_v \setminus \{0\}\text{”}, v \text{ finite} \end{cases}$

X is an open neighbourhood of 1.

If $x \in K^* \cap X$, then $x \in \mathcal{O}_K$ (since $x \in \mathcal{O}_v$ $\forall$ finite v).

for all infinite v, $|x|_v < 2$.

$\Rightarrow$ coefficients of the minimal polynomial of x over $\mathbb{Q}$ are bounded independent of x. conjugates have the same absolute values

Min. poly. $\in \mathbb{Z}[T] \Rightarrow K^* \cap X$ is finite $\Rightarrow K^*$ is discrete $\square$

because $x \in \mathcal{O}_K$ finitely many choices for coefficients

In particular $K^* \subset J_K$ is closed$^{(*)}$. Hence $J_K/K^* = C_K$ is Hausdorff and locally compact, and similarly for J_K'/K^*.

$$1 \longrightarrow J_K'/K^* \underset{\text{inclusion}}{\longrightarrow} \overset{C_K}{\overset{\shortparallel}{J_K/K^*}} \xrightarrow[|\cdot|_A]{} \mathbb{R}^*_{>0} \longrightarrow 1$$

Important Theorem : J_K'/K^* is compact.

(*) ~~J_K locally compact~~

~~$K^* \subset J_K$ discrete~~

~~Then let $x \in J_K$, $x \notin K^*$.~~

~~x has a compact neighbourhood V.~~

~~Each $y \in K^*$ has an open neighbourhood U_y with $U_y \cap K^* = \{y\}$~~

~~$\bigcup_y U_y$ open. $W = J_K \setminus \bigcup_y U_y$ closed.~~

$$\mathcal{U} = \{\alpha \in I_K \mid |\alpha_v|_v = 1 \text{ for } v \in \Sigma_{K,f},\ |\alpha_v - 1|_v < 1 \text{ for } v \in \Sigma_{K,\infty}\}$$

(*) $(x, y) \mapsto xy^{-1}$ continuous

$\therefore \exists$ a neighbourhood V of 1 with $VV^{-1} \subseteq \mathcal{U}$

Then $\forall y \in I_K$, yV contains at most one $x \in K^*$

since if $x_1 = yv_1$, $x_2 = yv_2 \in K^*$, $x_1 \neq x_2$

then $x_1 x_2^{-1} = v_1 v_2^{-1} \in \mathcal{U}$ ⋇

(Since K^* discrete, $\mathcal{U}$ contains only 1 from K^*
$\mathcal{U} \cap K^* = \{1\}$)

$J_K/K^* = C_K$ Hausdorff + Locally compact:

$\theta : J_K \to C_K$

i) Locally compact:

$\theta(x) \in C_K$, look at x.

x has a compact neighbourhood

$\Rightarrow \theta(x)$ does, so C_K locally compact

ii) $K^* = \ker\theta$ closed.

Let $y_1 \neq y_2$, $y_1, y_2 \in C_K$

$\theta(x_i) = y_i$

$\theta^{-1}(y_i) = x_i + K^*$, closed

$x_i + K^*$ are disjoint, otherwise $\theta(x_1) = \theta(x_2)$ ※

Take a compact neighbourhood of each x_i and intersect with $x_i + K^*$, result is closed + compact.

Can separate by open sets

Images of these are open sets separating y_1, y_2.

22/02/14

Algebraic Number Theory (16)

8 Geometry of Numbers

Theorem 8.1 (Minkowski's Theorem, Blichfeldt's Lemma)

$\Lambda \subset \mathbb{R}^n$ a lattice (discrete subgroup such that $\mathbb{R}^n/\Lambda$ is compact)

$\mu_\Lambda = \mathrm{vol}(\mathbb{R}^n/\Lambda) = R$

Let $X \subset \mathbb{R}^n$ be a compact subset which is convex and symmetric about 0. Then if $\mathrm{vol}(X) > 2^n R$, then $X \cap \Lambda \neq \{0\}$.

Remarks

Λ a lattice $\Leftrightarrow \Lambda = \bigoplus_{1 \le i \le n} \mathbb{Z} e_i$, e_i $\mathbb{R}$-linearly independent.

Convex: $x, y \in X \Rightarrow \lambda x + (1-\lambda) y \in X \quad \forall \lambda \in [0,1]$.

Symmetric about 0: $x \in X \Rightarrow -x \in X$.

Proof projection

$X \xrightarrow{\pi} \mathbb{R}^n/2\Lambda$, $\mathrm{Vol}(X) > \mathrm{vol}(\mathbb{R}^n/2\Lambda)$ because $\mathrm{vol}(X) > 2^n R$

$\Rightarrow \exists$ distinct $x, y \in X$ with $x - y \in 2\Lambda$ (because π cannot be injective)

$\Rightarrow \frac{x-y}{2} \in X \cap \Lambda \setminus \{0\}$ because $0 \in X$, and X convex $\square$

We usually apply as follows:

For k a number field, $\sigma : k \hookrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$

$r_1 = \#$ real embeddings $\quad r_2 = \#$ complex embeddings (for each such, pick an embedding $k \hookrightarrow \mathbb{C}$)

If $I \subset k$ is a fractional ideal, then $\sigma(k) \subset \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ (Minkowski Space) is a lattice.

We apply this to show that J_k^1/k^* is compact.

Theorem 8·2

$\exists$ a constant $C_K > 0$ such that :

For $(d_v)_{v\in\Sigma_K} \subset \mathbb{R}_{>0}$ with $\begin{cases} d_v \in |K^*|_v & \forall v \\ d_v = 1 & \text{for almost all } v \\ \prod_v d_v > C_K \end{cases}$

~~then~~ we have $\{x \in K \mid \forall v, |x|_v \le d_v\} \ne \{0\}$

Proof Finite places $\rightsquigarrow$ Lattice

Infinite places $\rightsquigarrow$ ~~Open~~ closed Ball X about 0.

$\forall$ finite v, put $d_v = q_v^{-n_v}$, $n_v \in \mathbb{Z}$, as $|K^*|_v = |K_v^*| = \langle q_v \rangle$

Then $I = \{x \in K \mid \forall \text{finite } v, |x|_v \le d_v\}$

is the fractional ideal $\prod_v P_v^{n_v}$

$\sigma : K \hookrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \cong \mathbb{R}^n$ — Check

$\mu_{\sigma(I)} = \mu_{\sigma(\mathcal{O}_K)} N(I) \; (*)$, where $N(I) = \prod q_v^{n_v}$

(if $I \subset \mathcal{O}_K$ then $N(I) = (\mathcal{O}_K : I)$, so the above becomes obvious ; in general consider J with $\mathcal{O}_K \supset J \subset I$).

Let $X = \{x \in \prod_{v\in\Sigma_{K,\infty}} K_v \cong \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \mid \forall v|\infty, |x_v|_v \le d_v\}$

$$= \prod_{v \text{ real}} [-d_v, d_v] \times \prod_{v \text{ complex}} \{|z|^2 \le d_v\}$$

$|z|^2$ means area $= \pi r^2$, $r = \sqrt{d_v}$

So $\mathrm{vol}(X) = 2^{r_1}\pi^{r_2} \prod_{v|\infty} d_v > 2^n \left(\prod_{v \text{ finite}} d_v\right)^{-1} \mu_{\sigma(\mathcal{O}_K)}$

$= 2^n \mu_{\sigma(I)}$ by $(*)$

This holds $\Leftrightarrow \prod_{\text{all } v} d_v > \left(\frac{4}{\pi}\right)^{r_2} \mu_{\sigma(\mathcal{O}_K)} =: C_K$

If so, then by Minkowski's Theorem,

$\sigma(I) \cap X \ne \{0\} \Rightarrow \exists x \ne 0$ in K satisfying

$|x|_v \le d_v \;\; \forall v.$ $\square$

22/02/14 Algebraic Number Theory (16)

Theorem 8·3

J_K^1 / K^* is compact.

First, we prove:

Proposition 8·4

Let $(\rho_v)_{v \in \Sigma_K}$, $\rho_v > 0$, with $\rho_v = 1$ for almost all v.

Then $X = \{x \in J_K^1 \mid \forall v, |x_v|_v \leq \rho_v\}$ is compact.

Proof

We want to get a lower bound on $|x_v|_v$ as well.

ok since $\rho_v = 1$ for almost all v.

Let $R = \prod_v \rho_v$, $S = \Sigma_{K,\infty} \cup \{v \mid \rho_v \neq 1\} \cup \{v \in \Sigma_{K,f} \mid q_v \leq R\}$

If $v \notin S$, $x \in X$, then $\rho_v = 1$ so

$$\rho_v = 1 \geq |x_v|_v = \prod_{w \neq v} |x_w|_w^{-1} \geq \prod_{w \neq v} \rho_w^{-1} = R^{-1} > \frac{1}{q_v}$$

As $q_v > R$, $|x_v|_v = 1$ since $|K^*|_v = \langle q_v \rangle$

Hence $X = X' \times \prod_{v \notin S} \mathcal{O}_v^*$ with $X' = \{(x_v) \in \prod_{v \in S} K_v^* \mid \prod_{v \in S} |x_v|_v = 1, \forall v \in S, |x_v|_v \leq \rho_v\}$

But X' is a closed subset of $X'' = \{(x_v) \in \prod_S K_v^* \mid \forall v \in S, \frac{\rho_v}{R} \leq |x_v|_v \leq \rho_v\}$

which is compact. So X is compact. ↑because $\prod |x_v|_v = 1$ □

X'' closed + bounded

Proof (Theorem 8·3)

trivially possible $y \in J_K$. would be hard for $y \in K$ c.f. 8·2

Let c_K be as in 8·2. Pick $y \in J_K$ with $|y|_{\mathbb{A}} > c_K$.

Let $X = \{x \in J_K^1 \mid \forall v, |x_v|_v \leq |y_v|_v\}$

By (8·4), X is compact. So it is sufficient to prove that

$J_K^1 = X K^*$.

$|y|_{\mathbb{A}} |z|_{\mathbb{A}}$

Let $z \in J_K^1$. Then $|z|_{\mathbb{A}} = 1$, hence $\prod_v |y_v z_v|_v > c_K$.

Then by 8·2, $\exists b \in K^*$ with $|b|_v \leq |y_v z_v|_v \quad \forall v$.

↑direct application

3

$\nearrow$ so J_K'/K^* is compact

Then $bz^{-1} \in X$. Hence $z^{-1} \in b^{-1}X \subset XK^*$. $\square$

Corollary 8.5

The class group $Cl(K) = I(K)/P(K)$ is *finite*.

Proof

Content map $c : J_K' \twoheadrightarrow I(K)$ is surjective and continuous for the discrete topology on $I(K)$.

$c(K^*) = P(K)$, so c induces a continuous surjection $J_K'/K^* \twoheadrightarrow Cl(K)$. So $Cl(K)$ is compact, hence finite. $\square$

Remark

This argument shows that *any* discrete quotient of J_K'/K^* is finite (since $\underset{(y_v)}{J_K} \cong \underset{\longleftrightarrow (r>0,}{\mathbb{R}^*_{>0}} \times \underset{(x_v))}{J_K'}$, where $y_v = \begin{cases} x_v & v \text{ finite} \\ r^{\frac{1}{n}} x_v & v \text{ infinite} \end{cases}$ where $n = [K:\mathbb{Q}]$.

So $|y|_{\mathbb{A}} = \underset{1}{|x|_{\mathbb{A}}} \times \prod_{v \text{ real}} r^{\frac{1}{n}} \times \prod_{v \text{ complex}} r^{2/n} = r$)

This applies more generally to "ray class groups" (apply congruence conditions to $P(K)$)

25/02/14

Algebraic Number Theory (17)

$J_K' = \{x = (x_v) \in J_K \mid |x|_{\mathbb{A}} = \prod |x_v|_v = 1\} \underset{\text{discrete}}{\supseteq} K^*$, $U_K' = U_K \cap J_K'$

We saw that J_K'/K^* is compact.

$$1 \longrightarrow U_K \longrightarrow \overset{K^*}{\overset{\cap}{J_K}} \xrightarrow{c} I(K) \longrightarrow 0 \qquad (*)$$

$\ker c = \prod_{v|\infty} K_v^* \times \prod_{v\nmid\infty} \mathcal{O}_v^*$ $\qquad U_K \cap K^* = \{x \in K^* \mid \forall \text{finite } v, |x|_v = 1\} = \mathcal{O}_K^*$

so $1 \to U_K'/\mathcal{O}_K^* \to J_K'/K^* \xrightarrow{c} Cl(K) \to 0$ quotient $(*)$ by K^* and its images

So compactness may give us information about $\mathcal{O}_K^*$.

<u>Corollary 8.6</u>

$S \supset \Sigma_{K,\infty}$ a finite set of places of K.

$\mathcal{O}_{K,S}$ = "ring of S-integers of K" $= \{x \in K \mid \forall v \notin S, |x|_v \leq 1\}$

"S-integers" $\mathcal{O}_{K,\Sigma_{K,\infty}} = \mathcal{O}_K$ e.g. "v-invertible" for all finite v

"S-units" We have that $\mathcal{O}_{K,S}^* = \{x \in K \mid \forall v \notin S, |x|_v = 1\}$ is a f.g. abelian group of rank $(\#S - 1)$

If $S = \Sigma_{K,\infty}$, then $\mathcal{O}_K^*$ has rank $r_1 + r_2 - 1$ (Dirichlet's Unit Theorem)

<u>Proof</u>

Logarithmic Map :

$\lambda_S : J_K \to \mathbb{R}^S$, $(x_v) \mapsto (\log |x_v|_v)_{v \in S}$

Let $\mathbb{R}^{S,0} = \{(y_v) \in \mathbb{R}^S \mid \sum y_v = 0\}$, hyperplane

trace zero hyperplane

Then $\lambda_S(\mathcal{O}_{K,S}^*) \subset \mathbb{R}^{S,0}$, by the product formula.

$x \in \mathcal{O}_{K,S}^*$, $\prod_v |x_v|_v = 1$, $|x_v|_v = 1 \ \forall v \notin S$

So it is sufficient to prove that

i) $\ker \lambda_S \cap \mathcal{O}_{K,S}^*$ is finite. and therefore each element of $\mathbb{R}^{S,0}$ has finitely many pre-images in $\mathcal{O}_{K,S}^*$

ii) $\lambda(\mathcal{O}_{K,S}^*)$ is a lattice in $\mathbb{R}^{S,0}$ (discrete subgroup with compact quotient) and so is f.g.

Case $S = \Sigma_{K,\infty}$:

$U_K' = U_K \cap J_K' \simeq \left(\prod_{v|\infty} K_v^*\right)' \times \prod_{v \text{ finite}} \mathcal{O}_v^*$

since $K^* \subset J_K$ discrete   by the exact sequence on the previous page

$\mathcal{O}_K^* = U_K' \cap K^*$ discrete $\subset U_K'$, $U_K'/\mathcal{O}_K^*$ compact   clear

$U_K' \cap \ker\lambda = \prod_{v\ \text{real}} \{\pm 1\} \times \prod_{v\ \text{complex}} (\text{circle}) \times \prod_{v\ \text{finite}} \mathcal{O}_v^*$ is compact

so $\ker\lambda \cap \mathcal{O}_K^*$ is finite, yielding i).   discrete $\subset$ compact is finite

---

$\lambda : U_K' \twoheadrightarrow \mathbb{R}^{S,0}$ has a continuous section (with right inverse σ)

with $\underset{\substack{\| \\ G}}{\mathrm{im}(\sigma)} = \left(\prod_{v|\infty} \mathbb{R}_{>0}^*\right)^1 \times \prod_{v\ \text{finite}} \{1\} \xrightarrow[\lambda]{\sim} \mathbb{R}^{S,0}$

So $U_K' = G \times \ker\lambda|_{U_K'}$.

If $B \subset (\mathbb{R}^r)^0$ is a compact neighbourhood of 0

then $\lambda^{-1}(B) \cong B \times \underbrace{\ker\lambda|_{U_K'}}_{\text{compact - stated above}}$, so $\lambda^{-1}(B)$ is also compact,

and then $\lambda(\mathcal{O}_K^*) \cap B = \lambda(\underbrace{\mathcal{O}_K^*}_{\text{discrete}} \cap \underbrace{\lambda^{-1}(B)}_{\text{compact}})$ is finite.

So $\lambda(\mathcal{O}_K^*)$ is discrete, and as $\lambda : U_K'/\mathcal{O}_K^* \twoheadrightarrow \mathbb{R}_S^0/\lambda(\mathcal{O}_K^*)$ compact quotient

is continuous and $U_K'/\mathcal{O}_K^*$ is compact, so we obtain ii).

General Case:

Either repeat the argument, replacing $\mathbb{R}^S$ by

$\prod_{v\in\Sigma_{K,\infty}} \mathbb{R} \times \prod_{v\in S\cap\Sigma_{K,f}} \mathbb{Z}(\log q_v)$, so that the argument is

only notationally different,

Or $\quad 1 \longrightarrow \mathcal{O}_K^* \longrightarrow \mathcal{O}_{K,S}^* \xrightarrow[\mu]{(v)_{v\in S\cap\Sigma_{K,f}}} \mathbb{Z}^{S\cap\Sigma_{K,f}}$

Then it is sufficient to prove that $\mathrm{im}(\mu)$ has finite index.

But if $h = \#Cl(K)$, then $\forall$ finite $v \in S$,

$P_v^h = z_v \mathcal{O}_K$ for some $z_v \in \mathcal{O}_K$, then $w(z_v) \neq 0$

$\forall$ finite $w \neq v \Rightarrow z_v \in \mathcal{O}_{K,S}^* \Rightarrow \mathrm{Im}(\mu) \supset h \cdot \mathbb{Z}^{S\cap\Sigma_{K,f}}$ $\square$

Later, we will compute (for an appropriate measure) the

volume of J_K'/K^* (analytic class number formula) and relate to ζ_K

25/02/14

"Strong Approximation Theorem"

Recall the Chinese Remainder Theorem in K: we can solve simultaneous congruences $x \equiv y_i \pmod{P_i^{m_i}}$, $P_1, \dots, P_k$ distinct prime ideals, $m_i \geq 1$, $y_i \in \mathcal{O}_K$ with $x \in \mathcal{O}_K$.

Let $P_i \leftrightarrow v_i$. Then CRT $\Leftrightarrow$ $\exists x \in K$ with

$|x - y_i|_{v_i} \leq q_i^{-m_i}$ $\forall i$, $|x|_v \leq 1$ $\forall v \in \Sigma_{K,f} \setminus \{v_i\}$

Here, we can replace $\Sigma_{K,\infty}$ by any non-empty subset of Σ_K:

Theorem 8.7 (Strong Approximation Theorem)

Let $S \subset \Sigma_K$ be non-empty, and for all $v \notin S$, given $y_v \in K_v$, $\delta_v > 0$, such that for almost all $v \notin S$,

$|y_v| \leq 1$ and $\delta_v = 1$.

Then $\exists x \in K$ such that $\forall v \notin S$

$|x - y_v|_v \leq \delta_v$ (if $S = \Sigma_{K,\infty}$, this is CRT)

Remark

This is false if $S = \emptyset$, because then we know that using Q12, Sheet 2, K is discrete in $\mathbb{A}_K$.

Lemma 8.8 (compactness of $\mathbb{A}_K / K$)

There exists R (depending on K) such that

$\forall x = (x_v) \in \mathbb{A}_K$, $\exists y \in K$ with

$$|y - x_v|_v \leq \begin{cases} 1 & v \text{ finite} \\ R & v \text{ infinite} \end{cases}$$

Proof

Recall that $(x_v) \in \mathbb{A}_K \Rightarrow |x_v|_v \leq 1$ for almost all v.

i) First assume that $x_v = 0$ $\forall$ finite v. So we require

then $|y - x_v|_v = |y|_v \leq 1$ for all finite v

$y \in \mathcal{O}_K$ such that $|y - x_v|_v \leq R$ $\forall v | \infty$

$$B_\infty = \prod_{v|\infty} \{ z \in K_v \mid |z|_v \leq R \} \subset \prod_{v|\infty} K_v \xrightarrow{\sim} \mathbb{R}^n$$

$$K \xrightarrow{\sigma} \mathbb{R}^n \quad \text{Minkowski Embedding}$$

$\sigma(\mathcal{O}_K) \subset \mathbb{R}^n$ is a lattice. So $\exists R$ such that B_∞ contains a fundamental domain for $\sigma(\mathcal{O}_K)$ i.e. $B_\infty \twoheadrightarrow \mathbb{R}^n / \sigma(\mathcal{O}_K)$

i.e. $\mathrm{Im}(B_\infty)$, $\sigma(\mathcal{O}_K)$ generate $\mathbb{R}^n$

$\Rightarrow \prod_{v|\infty} K_v = B_\infty + \mathcal{O}_K$, which implies the result.

$\prod_{v|\infty} K_v \xrightarrow{\sim} \mathbb{R}^n$

27/02/14 Algebraic Number Theory (18)

Class Wed 5 2pm

Extralecture Thu 11 1:15pm

Proof (Lemma 8.8, continued)

i) Case $x_v = 0$ $\forall$ finite x_v done last time

ii) x arbitrary. As $|x_v|_v \leq 1$ for almost all v, $\exists N \in \mathbb{Z}$, $N \geq 1$ such that $\forall$ finite v, $|N x_v|_v \leq 1$ ($N = \prod q_v^{m_v}$ for the v with $|x_v|_v > 1$). Then by the Chinese Remainder Theorem, $\exists z \in \mathcal{O}_K$ such that $\forall$ finite v with $v(N) > 0$, $z \equiv N x_v \mod \pi_v^{v(N)} \mathcal{O}_v$.

Then $y' := \frac{z}{N} \in K$ satisfies $|y' - x_v|_v \leq 1$ for all finite v.

Now the proof of i) $\Rightarrow \exists w \in \mathcal{O}_K$ with $|w - (x_v - y')|_v \leq R$ $\forall$ infinite v.

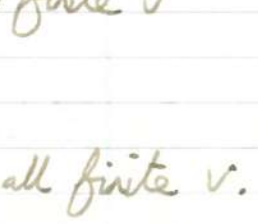
strong triangle inequality $\Rightarrow |w + y' - x_v|_v \leq 1$ $\forall$ finite v

Then $y = y' + w$ satisfies the conditions of the lemma. $\square$

Proof (Strong Approximation Theorem)

or this is just CRT

$S \neq \emptyset$. $\forall v \notin S$, we are given y_v, $\delta_v > 0$ such that for almost all v, $|y_v|_v \leq 1$ and $\delta_v = 1$. We want $x \in K$ with $\forall v \notin S$, $|x - y_v| \leq \delta_v$.



A_K

Let $\delta_v' = \begin{cases} \delta_v & v \notin S, \text{ finite} \\ R^{-1}\delta_v & v \notin S, \text{ infinite} \end{cases}$

with R as in the Lemma.

We claim that $\exists w \in K^*$ such that $\forall v \notin S$, $|w|_v \leq \delta_v'$. This follows from Theorem 8.2:

since $S \neq \emptyset$, we can take $d_v \in |K^*|_v$ (all $v \in \Sigma_K$) such that $d_v = 1$ for almost all v, $d_v \leq \delta_v'$ $\forall v \notin S$, and $\prod_{\text{all } v} d_v > C_K$. $\rightarrow$ because for $v \in S$, we could make d_v very large

Then $8.2 \Rightarrow \exists x \in K^*$ with $|x|_v \leq d_v$ $\forall v$

By Lemma 8·8, $\exists\, z \in K$ such that
$$\left|z - \frac{y_v}{w}\right|_v \leq \begin{cases} 1 & v \notin S \text{ finite} \\ R & v \notin S \text{ infinite} \end{cases}$$
$\Rightarrow x = wz$ has $|x - y_v|_v \leq \delta_v \;\; \forall v \notin S$. $\square$

9 Dedekind ζ-Function

Recall $\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s}$, $s \in \mathbb{C}$, $Re(s) > 1$
$$= \prod_{p \text{ prime}} \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \ldots\right) = \prod_{p \text{ prime}} \frac{1}{1 - p^{-s}} \quad \text{(Euler Product)}$$

$$Z(s) := \pi^{-\frac{s}{2}} \Gamma\left(\tfrac{s}{2}\right) \zeta(s)$$

has a meromorphic continuation with simple poles at $s = 0, 1$ and has "functional equation" $Z(1-s) = Z(s)$

$Res_{s=1} = 1 = -Res_{s=0}$.

Let K be a number-field. We define the Dedekind Zeta Function of K:

$\zeta_K(s) := \sum_{I \subset \mathcal{O}_K} (NI)^{-s}$ where I runs over non-zero ideals $I \subset \mathcal{O}_K$ and $NI = (\mathcal{O}_K : I) < \infty$.

Proposition 9·1

$\zeta_K(s)$ is absolutely convergent for $Re(s) > 1$ and
$$\zeta_K(s) = \prod_{v \text{ finite}} \frac{1}{1 - q_v^{-s}} \quad (Re(s) > 1).$$

Proof

$\#\{I \subset \mathcal{O}_K \mid NI < M\}$ is finite, so $\zeta_K(s)$ is a formal Dirichlet series, $\zeta_K(s) = \sum_{n \geq 1} \frac{c_n}{n^s}$ (here $c_n \in \mathbb{Z}$).

Formally, writing $I = \prod P_v^{n_v}$ we have

$\cancel{N(I)}\, (NI)^{-s} = \prod q_v^{-n_v s}$ hence $\zeta_K(s) = \prod_v (1 + q_v^{-s} + q_v^{-2s} + \ldots)$

27/02/14

Algebraic Number Theory (18)

so $\zeta_K(s) = \prod_v \frac{1}{1-q_v^{-s}}$

But $\#\{v \in \Sigma_{K,f} \mid v|p\} \leq n = [K:\mathbb{Q}]$

Also, $q_v \geq p$ if $v|p$.

each factor $\frac{1}{1-q_v^{-s}}$ compares to some $\frac{1}{1-p^{-s}}$ and no more than n of them compare to the same p

So the product for $\zeta_K(s)$ is absolutely convergent by comparison with $\prod_p \left(\frac{1}{1-p^{-s}}\right)^n = \zeta(s)^n$ for $Re(s) > 1$.

$\Rightarrow$ the series is also absolutely convergent as well (in this range) $\square$

Define $\Gamma_{\mathbb{R}}(s) = \pi^{-\frac{s}{2}}\Gamma(\frac{s}{2})$

$\Gamma_{\mathbb{C}}(s) = 2(2\pi)^{-s}\Gamma(s)$

$\Gamma(s) = \int_0^\infty e^{-t} t^s \frac{dt}{t}$, analytic for $Re(s) > 0$

$s\Gamma(s) = \Gamma(s+1)$, $\Gamma(n) = (n-1)!$ if $n \geq 1$.

Meromorphic continuation to $\mathbb{C}$ with simple poles at $s = 0, -1, -2, \dots$.

(The factor 2 in $\Gamma_{\mathbb{C}}$ is chosen so that $\Gamma_{\mathbb{R}}(s)\Gamma_{\mathbb{R}}(s+1) = \Gamma_{\mathbb{C}}(s)$)

d_K = discriminant of K = discriminant of the trace form $\mathcal{O}_K \times \mathcal{O}_K \to \mathbb{Z}$

$|d_K| = \prod_{\text{finite } v} N\delta_{K_v/\mathbb{Q}_p}$

Theorem 9.2

i) $Z_K(s) = |d_K|^{\frac{s}{2}}\Gamma_{\mathbb{R}}(s)^{r_1}\Gamma_{\mathbb{C}}(s)^{r_2}\zeta_K(s)$

$r_1 = \#$ real v, $r_2 = \#$ complex v

This has an analytic continuation to $\mathbb{C}$ with simple poles at $0, 1$.

ii) $\zeta_K(s)$ has a zero of order $r_1 + r_2 - 1$ ($=$ rank $\mathcal{O}_K^*$)

and $\lim_{s \to 0} s^{-(r_1+r_2-1)}\zeta_K(s) = -\frac{h_K R_K}{w_K}$

Here, $h_K = \# Cl(K)$ | $w_K = \#(\mathcal{O}_K^*, \text{torsion})$

$= \#(\text{roots of unity in } K)$

If $\mathcal{O}_K^* = (\text{finite}) \times \langle \varepsilon_1, \dots, \varepsilon_r \rangle$, $r = r_1 + r_2 - 1$

then in the $r \times (r+1)$ matrix $(\log |\varepsilon_i|_v)_{1 \le i \le r,\, v \in \Sigma_{K,\infty}}$

∞ places is $r_1 + r_2 = r+1$

the sum of the columns is 0 because $\forall i$,

$\sum_{v \in \Sigma_{K,\infty}} \log |\varepsilon_i|_v = \sum_{\text{all } v} \log |\varepsilon_i|_v = 0$ by the product formula.

R_K = absolute value of any $(r-1)\times(r-1)$ minor of this matrix.

det of

~~e.g. if r = 1 then~~ R_K is called the <u>regulator</u> of K.

$\varepsilon_i \in \mathcal{O}_K^*$

so $|\varepsilon_i|_v = 1 \quad \forall v \in \Sigma_{K,f}$

01/03/14 Algebraic Number Theory (19)

$$\zeta(s) = \prod_p \frac{1}{1-p^{-s}}, \quad Z(s) = \underbrace{\pi^{-s/2}\Gamma(s/2)}_{=\Gamma_{\mathbb{R}}(s),\ p=\infty \text{ factor}}\zeta(s) = Z(1-s)$$

Let p be prime, dx a Haar measure on $\mathbb{Q}_p$.

$$\int_{\mathbb{Z}_p} |x|_p^{s-1}\,dx = \sum_{n\geq 0}\int_{p^n\mathbb{Z}_p \setminus p^{n+1}\mathbb{Z}_p} |x|_p^{s-1}\,dx$$

On our sets of choice, $|x|_p^{s-1} = p^{-n(s-1)}$

$$\int_{\mathbb{Z}_p} |x|_p^{s-1}\,dx = \sum_{n\geq 0} p^{-n(s-1)}\text{measure}(p^n\mathbb{Z}_p \setminus p^{n+1}\mathbb{Z}_p)$$

$$\text{measure}(\mathbb{Z}_p) = \sum_{a \bmod p^n}(a+p^n\mathbb{Z}_p) = \sum_{a \bmod p^n}\text{measure}(p^n\mathbb{Z}_p)$$
$$= p^n\,\text{measure}(p^n\mathbb{Z}_p)$$

as the Haar-measure is translation invariant.

$$\Rightarrow \text{measure}(p^n\mathbb{Z}_p) = p^{-n}\text{measure}(\mathbb{Z}_p).$$

So $\int_{\mathbb{Z}_p} |x|_p^{s-1}\,dx = \sum_{n\geq 0}(p^{-n}-p^{-n-1})p^{-n(s-1)}\text{measure}(\mathbb{Z}_p)$

$$= \underbrace{(1-p^{-1})\text{measure}(\mathbb{Z}_p)}_{\text{other factor}}\underbrace{\frac{1}{1-p^{-s}}}_{\text{Euler Factor for }\zeta(s)}$$

This suggests:

i) $\zeta(s) = \prod_p$ (p-adic integrals)

ii) $\Gamma_{\mathbb{R}}(s)$ should be the analogous integral over $\mathbb{R}$.

iii) We should choose the normalisation of dx carefully to remove the other factors for almost all p.

Approach of Tate (and Iwasawa):

("Tate's Thesis", last chapter of Cassels - Frohlich)

<u>Fourier Analysis</u>

On $\mathbb{R}$, a <u>Fourier - transform</u> of f is

$$\hat{f}(y) = \int_{-\infty}^{\infty} \underset{\substack{\uparrow \\ \text{homomorphism} \\ \text{to } S}}{e^{-2\pi i x y}} \underset{\substack{\uparrow \\ \text{function}}}{f(x)} \underset{\substack{\nwarrow \\ \text{measure}}}{dx}$$

We will generalise this to local fields F ($F = \mathbb{R}, \mathbb{C}, F/\mathbb{Q}_p$ finite)

Ingredients:

1. An <u>additive character</u> $\Psi : F \to U(1) = \{|z| = 1\} \subset \mathbb{C}^*$, $\Psi(x+y) = \Psi(x)\Psi(y)$

$$\Psi_\infty \begin{cases} - F = \mathbb{R}, \ \Psi(x) = e^{-2\pi i x}, & \mathbb{R}/\mathbb{Z} \xrightarrow{\sim} U(1) \\ - F = \mathbb{C}, \ \Psi(z) = e^{-2\pi i (z + \bar{z})}, & \end{cases}$$

- $F/\mathbb{Q}_p$, $\mathbb{Q}_p = \mathbb{Z}[\frac{1}{p}] + \mathbb{Z}_p$ $\quad \Psi(x+y) = \Psi(x)\Psi(y)$

We define $\Psi_p : \mathbb{Q}_p/\mathbb{Z}_p \hookrightarrow \mathbb{C}^*$

For $x = y + z$, $y \in \mathbb{Z}[\frac{1}{p}]$, $z \in \mathbb{Z}_p$, $\Psi_p(x) := e^{2\pi i y}$

i.e. if $x = \sum_{n \geq -N} a_n p^n$, p-adic expansion

$$\Psi_p(x) = \exp\left(2\pi i \sum_{n=-N}^{-1} a_n p^n\right)$$

$$\Psi := \Psi_p \circ \mathrm{Tr}_{F/\mathbb{Q}_p} : F \to \mathbb{C}^*$$

N.B. we have chosen the signs in the exponentials so that if $x \in \mathbb{Q}$, say, then $\prod_{p \leq \infty} \Psi_p(x) = 1$.

2. <u>Haar Measure</u> : $d_F x$

A translation invariant positive functional on some class of functions of F (e.g. continuous of compact support).

- $F = \mathbb{R}$, $d_F x$ = Lebesgue Measure
- $F = \mathbb{C}$, $d_F z = 2 \times$ Lebesgue Measure $= 2 dx\, dy$

$$= |dz\, d\bar{z}|$$

- $F/\mathbb{Q}_p$. We will usually only integrate locally constant functions.

This measure is ~~[illegible]~~ determined by

$$\text{measure}(a + \pi^n \mathcal{O}_F) = (\mathcal{O}_F : \pi^n \mathcal{O}_F)^{-1} \text{measure}(\mathcal{O}_F)$$

$$:= q^{-n-\delta/2}, \quad \delta = \delta_{F/\mathbb{Q}_p} = \text{valuation of the } \underline{\text{different}}$$

($q^{-\delta/2}$ is put in to make things work better)

If $F/\mathbb{Q}_p$ is unramified then $\delta = 0$, so measure$(\mathcal{O}_F) = 1$.

In all cases, if $a \in F^*$, $d_F(ax) = |a| d_F(x)$,

$|a|$ the normalised AV.

~~Aside~~

~~Notation for integration is terrible.~~

~~For example, dx means two things:~~

~~i) A differential form on $\mathbb{R}$, to be integrate on an oriented segment.~~

~~$\int_a^b f(x)\,dx$, $\quad d(-x) = -dx$.~~

~~ii) Lebesgue measure (functional on $L^1(\mathbb{R})$).~~

~~This time, $d(-x) = dx$.~~

~~$f = \mathbb{1}_{[-1,1]}$, $f(x) = f(-x)$, $\int_{\mathbb{R}} f(x)\,dx = \int_{\mathbb{R}} f(-x)\,d(-x)$~~

~~We really should use $|dx|$ for the measure associated to a differential form dx.~~

~~For general spaces, we should never use d for measure, but everybody does!~~

3. A suitable class of functions

We use the Schwartz Space $\mathcal{S}(F)$.

- For $F=\mathbb{R}$ or $\mathbb{C}$, $S(F)=\{C^\infty$ functions $F\to\mathbb{C}$ such that $\forall n\geq 1, \forall \alpha\in\mathbb{N}$ or $\mathbb{N}^2$ ($\mathbb{N}$ for $\mathbb{R}$, $\mathbb{N}^2$ for $\mathbb{C}$), $|x|^n|\partial^\alpha F|\to 0$ as $|x|\to\infty\}$

e.g. e^{-x^2}.

- $F/\mathbb{Q}_p$, $S(F)=\{$locally constant functions of compact support$\}$

$=$ span of characteristic functions $\mathbb{1}_{a+\pi^n\mathcal{O}_F}$

Fourier Transforms

The Fourier-Transform of $f\in S(F)$ is $\hat{f}(y)=\int_F\Psi(xy)f(x)d_F(x)$

(e.g. the usual Fourier Transform for $F=\mathbb{R}$).

$$\hat{f}(y)=\int_{\mathbb{R}}e^{-2\pi i xy}f(x)\,dx$$

Lemma

Let $\underline{a}\in F$ be a fractional ideal. Then

$$\int_a \Psi(x)\,d_F(x)=\begin{cases}\text{measure}(\underline{a}) & \text{if } a\subset\mathcal{D}^{-1}_{F/\mathbb{Q}_p}\\ 0 & \text{otherwise}\end{cases}$$

See bottom of page

Proof

$\Psi=\Psi_p\circ\mathrm{Tr}_{F/\mathbb{Q}_p}$; $\mathrm{Tr}_{F/\mathbb{Q}_p}(\mathcal{D}^{-1}_{F/\mathbb{Q}_p})\subseteq\mathbb{Z}_p$,

$\Psi_p(\mathbb{Z}_p)=\{1\}$, hence the first part.

If $\underline{a}\not\subset\mathcal{D}^{-1}_{F/\mathbb{Q}_p}$, then by definition, $\exists x\in\underline{a}$ with

$\mathrm{Tr}_{F/\mathbb{Q}_p}(x)\notin\mathbb{Z}_p$ (as a is an ideal). i.e. not just the whole of $\underline{a}$

c.f. definition of Ψ_p note $\Psi=\Psi_p\circ\mathrm{Tr}_{F/\mathbb{Q}_p}$

$\Rightarrow H=\ker(\Psi:\underline{a}\to\mathbb{C}^*)\subsetneq\underline{a}$ is a proper subgroup

(of finite index as $p^n\underline{a}\subset\mathcal{D}^{-1}$ for $n>>0$) ~~if H had finite index~~ then $p^n\underline{a}$ has finite index and is contained in H.

So $\Psi:\underline{a}/H\xrightarrow{\sim}\langle\zeta_m\rangle$, $\zeta_m=e^{2\pi i/m}$, $m>1$ as H is proper so $\underline{a}/H$ non-trivial

Then $\displaystyle\int_a\Psi(x)\,d_F(x)=\sum_{b\in a/H}\int_{b+H}\Psi(x)\,d_F(x)$

$\displaystyle=\sum_{b\in a/H}\Psi(b)\underbrace{\text{measure}(b+H)}_{=\text{measure}(H)}=\text{measure}(H)\underbrace{\sum_{j=0}^{m-1}\zeta_m^j}_{=0}$

Recall $\mathcal{D}^{-1}_{F/\mathbb{Q}_p}=\{x\in F\mid\mathrm{Tr}_{F/\mathbb{Q}_p}(x\mathcal{O}_F)\subset\mathbb{Z}_p\}\supset\mathcal{O}_F$

lecture 11

04/03/14 Algebraic Number Theory 20

$F = \mathbb{R}$

$F = \mathbb{C}$ $\quad \Psi(x) = \begin{cases} e^{-2\pi i \underline{\mathrm{Tr}_{F/\mathbb{R}}}(x)} \\ \Psi_p(\mathrm{Tr}_{F/\mathbb{Q}_p}(x)) \end{cases}$ either x $F=\mathbb{R}$ or $2\mathrm{Re}(x)$ $F=\mathbb{C}$

$F/\mathbb{Q}_p$ finite

$\Psi_p\left(\frac{a}{p^n}\right) = e^{2\pi i b/p^n}$, $a \in \mathbb{Z}_p$, $b \in \mathbb{Z}$, $v_p(b-a) \geq n$ e.g. b is the first n p-adic digits of a

$d_F(x) = \begin{cases} [F:\mathbb{R}] \times (\text{Lebesgue Measure}) \\ q^{-\delta/2} \times (\text{measure with measure}(\mathcal{O}_F) = 1) \end{cases}$

Schwartz Space

$\mathcal{S}(F) = \begin{cases} \mathbb{C}^\infty \text{ functions that (along with derivatives)} \to \text{rapidly to } 0. \\ \text{Locally constant of compact support} \end{cases}$

Fourier Transform (for $f \in \mathcal{S}(F)$)

$$\hat{f}(y) = \int_F \Psi(xy) f(x)\, d_F x$$

Proposition 9.3

i) $F = \mathbb{R}$, $f(x) = e^{-\pi x^2} \in \mathcal{S}(F)$

Then $\hat{f}(x) = f(x)$

ii) $F = \mathbb{C}$, $f(z) = \frac{1}{\pi} e^{-2\pi z\bar{z}} \in \mathcal{S}(F)$

Then $\hat{f}(z) = f(z)$

iii) $F/\mathbb{Q}_p$, $n \in \mathbb{Z}$, $\mathbb{1}_{\pi^n \mathcal{O}_F}$ = (characteristic function of $\pi^n \mathcal{O}_F$)

Then $\hat{\mathbb{1}}_{\pi^n \mathcal{O}_F} = q^{-n-\delta/2} \mathbb{1}_{\pi^{-n} \mathcal{D}^{-1}_{F/\mathbb{Q}_p}}$

$q = \#(\mathcal{O}_F/\pi)$, $\mathcal{D}_{F/\mathbb{Q}_p} = \pi^\delta \mathcal{O}_F$

Proof

complete the square

move the contour

i) $\hat{f}(y) = \int_{-\infty}^{\infty} e^{-2\pi i xy - \pi x^2}\, dx$

$$= e^{-\pi y^2} \int_{-\infty}^{\infty} e^{-\pi(x+iy)^2}\, dx = e^{-\pi y^2} \int_{-\infty}^{\infty} e^{-\pi x^2}\, dx$$

$$= e^{-\pi y^2}$$

ii) Similar (exercise, to check that all the 2s cancel out)

$$2dx\,dy\ ,\ e^{-2\pi i(z+\bar{z})}\ ,\ e^{-2\pi z\bar{z}}$$

iii) $\hat{\mathbb{1}}_{\pi^n\mathcal{O}_F}(y) = \int_{\pi^n\mathcal{O}_F} \psi(xy)\, d_F x = \begin{cases} 0 & y \notin \pi^{-n}\mathcal{D}^{-1}_{F/\mathbb{Q}_p} \\ \operatorname{meas}(\pi^n\mathcal{O}_F) & y \in \pi^{-n}\mathcal{D}^{-1}_{F/\mathbb{Q}_p} \end{cases}$

by Lemma from last lecture

$\operatorname{meas}(\pi^n\mathcal{O}_F) = q^{-n}\operatorname{meas}(\mathcal{O}_F) = q^{-n-\delta/2}$ $\square$

<u>Fact</u>

$f \in \mathcal{S}(F) \Rightarrow \hat{f} \in \mathcal{S}(F)$ → c.f. Sheet 3

(For $F = \mathbb{R}$ or $\mathbb{C}$, this relies on the fact that $\widehat{f^{(n)}}(y) = (2\pi i y)^n \hat{f}(y)$)

then clear that we still have a Schwartz function

(For $F/\mathbb{Q}_p$, this is quite elementary)

<u>Fourier Inversion Theorem</u>

$f \in \mathcal{S}(F)$. $\hat{\hat{f}}(x) = f(-x)$

N.B this depends on the choice of ψ, $d_F x$. In general,

$\hat{\hat{f}}(x) = C_{\psi, d_F x}\, f(-x)$

constant independent of f.

9.3 i), ii) say that if $F = \mathbb{R}$ or $\mathbb{C}$, $\exists f \in \mathcal{S}(F)$ with $\hat{f} = f$ for this choice of $(\psi, d_F x)$. So with this choice, $C = 1$.

For $F/\mathbb{Q}_p$, we can check this by explicit computation.

All we need is $f = \mathbb{1}_{\mathcal{O}_F} \underset{9.3\,iii)}{\Rightarrow} \hat{\hat{\mathbb{1}}}_{\mathcal{O}_F} = q^{-\delta/2}\hat{\mathbb{1}}_{\mathcal{D}^{-1}_{F/\mathbb{Q}_p}}$

$$= q^{-\delta/2} q^{-\delta/2+\delta}\mathbb{1}_{\mathcal{O}_F}$$

$$= \mathbb{1}_{\mathcal{O}_F}$$

$\mathcal{D}^{-1}_F = \pi^{-\delta}\mathcal{O}_F$

explains the factor of $q^{-\delta/2}$ in our choice of measure.

04/03/14 Algebraic Number Theory 20

Remark

G any locally compact abelian topological group (write additively)

$\hat{G} = \mathrm{Hom}_{cts}(G, U(1))$, character group or Pontryagin Dual of G. This is also locally compact and $\hat{\hat{G}} \cong G$ (Pontryagin Duality).

Examples

i) $G = \mathbb{R}$, $\hat{G} \cong \mathbb{R}$ by $y \in \mathbb{R} \mapsto \chi_y(x) = e^{2\pi i x y}$

ii) $G = \mathbb{Z}$, $\hat{G} = U(1) \cong \mathbb{R}/\mathbb{Z}$ Haar measure dg on G, $d\chi$ on $\hat{G}$

Fourier Transform : (functions on G) $\to$ (functions on $\hat{G}$)

$$f \longmapsto \hat{f}(\chi) = \int_G \chi(g) f(g)\, dg$$

$f \in L^1(G)$

i) $G = \mathbb{R}$, $\hat{f}$ = usual Fourier Transform, identifying $\hat{G}$ with $\mathbb{R}$

ii) $G = \mathbb{R}/\mathbb{Z}$, $\hat{G} = \mathbb{Z}$, $\hat{f}(n)$ is the $(-n)^{th}$ Fourier coefficient of f.

$\hat{\hat{f}}(g) = c f(-g)$ for some constant $c > 0$ depending on measure

Lemma 9.4

$z \in F^*$, $g(x) = f(zx)$, $f \in S(F)$. Then $g \in S(F)$ and $\hat{g}(y) = |z|^{-1}\hat{f}(z^{-1}y)$

Proof

$$\hat{g}(y) = \int_F \Psi(xy) f(zx)\, d_F x \qquad t = zx, \quad d_F t = |z|\, d_F x$$

$$= \int_F \Psi(z^{-1}ty) f(t) \frac{d_F t}{|z|}$$

$$= |z|^{-1}\hat{f}(z^{-1}y) \qquad \square$$

Now choose a Haar measure on the multiplicative group F^*. As $d_F(ax) = |a|\, d_F(x)$, the measure on F^* is invariant

3

under $x \mapsto ax$, $a \in F^*$.

Define $d_F^* x = \dfrac{d_F x}{|x|}$ if $F = \mathbb{R}$ or $\mathbb{C}$ (|·| normalised AV)

$F/\mathbb{Q}_p$: $d_F^* x = \dfrac{q^{\delta/2}}{1-q^{-1}} \dfrac{d_F x}{|x|}$ so that

$$\text{measure}\,(\mathcal{O}_F^*, d_F^* x) = \int_{\underbrace{\mathcal{O}_F \setminus \pi\mathcal{O}_F}_{= \mathcal{O}_F^*}} \frac{q^{\delta/2}}{1-q^{-1}}\, d_F x$$

$$= \frac{q^{\delta/2}}{1-q^{-1}} \left(q^{-\delta/2} - q^{-1-\delta/2}\right) = 1 .$$

We can now define <u>Local-ζ-integrals</u>, for $f \in \mathcal{S}(F)$

$$\zeta(f,s) = \int_{F^*} f(x)\,|x|^s\, d_F^* x .$$

$$= \lim_{\varepsilon \to 0} \int_{\{x \in F \,|\, |x| \geq \varepsilon\}} f(x)\,|x|^{s-1}\, d_F x \times \begin{cases} 1 & \text{Archimedean} \\ \dfrac{q^{\delta/2}}{1-q^{-1}} & \text{Non Archimedean} \end{cases}$$

Since f is continuous and $\begin{cases} \text{rapidly} \to 0 \text{ as } |x| \to \infty \\ \text{has compact support in } F \end{cases}$

the limit certainly exists if $\mathrm{Re}(s) \geq 1$.

06/03/14

Algebraic Number Theory (21)

$f \in \mathcal{S}(F)$. $\zeta(f,s) = \int_{F^*} f(x)|x|^s d_F^* x$

$= \lim_{\varepsilon \to 0} \int_{\{x\in F \mid |x| \geq \epsilon\}} f(x)|x|^{s-1} d_F x \times \text{facto}$

<u>Proposition 9.5</u>

i) $F = \mathbb{R}$, $f(x) = e^{-\pi x^2}$ $\quad \zeta(f,s) = \Gamma_{\mathbb{R}}(s) = \pi^{-\frac{s}{2}}\Gamma(\frac{s}{2})$

ii) $F = \mathbb{C}$, $f(z) = \frac{1}{\pi}e^{-2\pi z\bar{z}}$ $\quad \zeta(f,s) = \Gamma_{\mathbb{C}}(s) = 2(2\pi)^{-s}\Gamma(s)$

iii) $F/\mathbb{Q}_p$ finite, $n \in \mathbb{Z}$. $\quad \zeta(\mathbb{1}_{\pi^n\mathcal{O}_F}, s) = \frac{q^{-ns}}{1-q^{-s}}$

In particular, $\zeta(\mathbb{1}_{\mathcal{O}_F}, s) = \frac{1}{1-q^{-s}}$

<u>Proof</u>

i) $\zeta(f,s) = 2\int_0^\infty e^{-\pi x^2} x^s \frac{dx}{x}$ $\qquad \left(\int_{\mathbb{R}^*} = 2\int_0^\infty\right)$

$= \int_0^\infty e^{-t}\left(\frac{t}{\pi}\right)^{\frac{s}{2}} \frac{dt}{t}$ $\qquad t = \pi x^2$

$= \Gamma_{\mathbb{R}}(s)$

ii) Similar, using polar coordinates. c.f. Sheet 3

iii) $\zeta(\mathbb{1}_{\pi^n\mathcal{O}_F}, s) = \int_{\pi^n\mathcal{O}_F\setminus\{0\}} |x|^s d_F^* x$

$= \sum_{m=n}^{\infty} \int_{\pi^m\mathcal{O}_F^*} q^{-ms} d_F^* x = \sum_{m=n}^{\infty} q^{-ms} \underbrace{\text{measure}(\pi^m\mathcal{O}_F^*, d_F^* x)}_{\text{measure}(\mathcal{O}_F^*, d_F^* x) \,=\, 1}$

because $d_F^*(ax) = d_F^*(x)$ and the normalisation of $d_F^*(x)$ has measure $(\mathcal{O}_F^*) = 1$

$= \frac{q^{-ns}}{1-q^{-s}}$

<u>Global Theory</u>

Let K be a number field. For $v \in \Sigma_K$, write

$\psi_v : K_v \to U(1)$, $d_v^{(*)}x = d_{K_v}^{(*)}x$, $\mathcal{S}(K_v)$.

$\mathbb{A}_K = \{(x_v) \in \prod K_v \mid x_v \in \mathcal{O}_v \text{ for almost all finite } v\}$

$= \bigcup_S \underbrace{\left(\prod_{v\in S} K_v \times \prod_{v\notin S} \mathcal{O}_v\right)}$, S running over finite sets of places containing $\Sigma_{K,\infty}$

1

Let $f_v \in \mathcal{S}(K_v)$ $(v \in \Sigma_K)$ such that $f_v = \mathbb{1}_{\mathcal{O}_v}$ and $x_v \in \mathcal{O}_v$ for almost all finite v.
for almost all finite v.

Then if $x = (x_v)_v \in \mathbb{A}_K$, then for almost all v, $f_v(x_v) = 1$,
so $f(x) = \prod_{\text{all } v} f_v(x_v)$ is a finite product.

Denote the resulting function $\mathbb{A}_K \to \mathbb{C}$ by $\prod_v f_v$ (or better, by $\bigotimes_v f_v$). This is:

- C^∞ in the archimedean variables x_v.
- locally constant in the p-adic variables x_v.

(Think of f as a C^∞ function on $\prod_{v | \infty} K_v$ together with some finite amount of congruence information).

Define $\mathcal{S}(\mathbb{A}_F)$ to be the ~~set~~ space of all finite linear combinations of such $f = \prod_v f_v$ (we should actually allow slightly more complicated functions at ∞ places).

We can now integrate $f \in \mathcal{S}(\mathbb{A}_F)$:

If $f = \prod f_v$, say $f_v = \mathbb{1}_{\mathcal{O}_v}$ $\forall v \notin S \supset \Sigma_{K,\infty}$

Then $f \neq 0$ outside $\prod_{v \in S} K_v \times \prod_{v \notin S} \mathcal{O}_v$ and we can define

$$\int_{\mathbb{A}_K} f(x)\, d_{\mathbb{A}} x := \prod_{\text{all } v} \int_{K_v} f_v(x)\, dx$$

$$= \prod_{v \in S} \int_{K_v} f_v(x)\, dx \quad \text{if } S \text{ also contains all finite } v \text{ ramified in } K/\mathbb{Q}.$$

(because if v is unramified, $\delta_v = 0$ then $\int_{\mathcal{O}_v} d_v x = 1$)

Let $\psi_{\mathbb{A}} = \prod_v \psi_v : \mathbb{A}_K \to U(1) \subset \mathbb{C}^*$

$$(x_v) \mapsto \prod_v \psi_v(x_v)$$

06/03/14 Algebraic Number Theory (21)

Proposition 9.6

$\Psi_{\mathbb{A}}$ is continuous, and $\Psi_{\mathbb{A}}(x) = 1$ if $x \in K \subset \mathbb{A}_K$ (embedded diagonally)

Proof

By definition, $\Psi_{\mathbb{A}}(x) = 1$ if $x \in \prod_{v \text{ finite}} \mathcal{O}_v \subset \mathbb{A}_K$,

so $\Psi_{\mathbb{A}}$ factors through the quotient:

$$\mathbb{A}_K \Big/ \prod_{v\text{ finite}} \mathcal{O}_v = \prod_{v|\infty} K_v \times \overbrace{\bigoplus_{v \nmid \infty} \left(K_v/\mathcal{O}_v\right)}^{\text{discrete}} \xrightarrow{\Psi_{\mathbb{A}}} U(1)$$

component $= 0$ for almost all v

because $x_v \in \mathcal{O}_v$ for almost all v

So as Ψ_v $(v|\infty)$ are continuous, $\Psi_{\mathbb{A}}$ is also continuous. because $K_v/\mathcal{O}_v$ disc so all maps are continuous

and we know the Ψ_v, $v|\infty$ are continuous from real/complex analysis

By definition of Ψ_v s, $\Psi_{\mathbb{A}_K}(x) = \Psi_{\mathbb{A}_\mathbb{Q}}\left(\underbrace{Tr_{K/\mathbb{Q}}(x)}_{\in \mathbb{Q}}\right)$ $x \in K$ because $\Psi_v = \Psi_p \circ Tr_{K_v/\mathbb{Q}_v}$

(as $\Psi_v = \Psi_p \circ Tr_{K_v/\mathbb{Q}_p}$ $\forall p \leq \infty$)

So it is enough to consider $x \in \mathbb{Q} = K$. Write x in "partial fractions":

$$x = b + \sum_{i=1}^{m} \frac{a_i}{p_i^{k_i}}, \quad k_i \geq 1, \; a_i, b \in \mathbb{Z}$$

p_i distinct primes. Can do by writing $\frac{a}{b} = \frac{a_1}{p_1^{k_1}} + \dots + \frac{a_r}{p_r^{k_r}}$ where $b = p_1^{k_1} \cdots p_r^{k_r}$ Bezout $\Rightarrow a_i$ exist since $p_i^{k_i}$ coprime

Then $\Psi_\infty(x) = e^{-2\pi i x} = \Psi_\infty(x-b)$ as $b \in \mathbb{Z}$

$\Psi_{p_i}(x) \overset{(=)}{=} \exp 2\pi i \left(\frac{a_i}{p^{k_i}}\right)$. Since $j \neq i$

we only take the negative p_i power fraction

$\Rightarrow \frac{a_j}{p_j^{k_j}} \in \mathbb{Z}_{p_i} \subset \ker(\Psi_{p_i})$

$\Psi_p(x) = 1$ if $p \notin \{p_i\}$ $\Rightarrow \prod_{p \leq \infty} \Psi_p(x) = 1$. $\square$

$\prod_{\{p_i\}} \exp 2\pi i(\dots) = \exp(2\pi i(x - b - \frac{a_1}{p_1^{k_1}} - \dots$

Now for $f = \prod f_v \in S(\mathbb{A}_K)$ define the Fourier Transform:

$$\hat{f}(y) = \int_{\mathbb{A}_K} \Psi_{\mathbb{A}}(xy) f(x) \, d\mathbb{A}(x)$$

$$= \prod_v \hat{f}_v(y_v) \in S(\mathbb{A}_K)$$

(as $\hat{\mathbb{1}}_{\mathcal{O}_v} = \mathbb{1}_{\mathcal{O}_v}$ for almost all v)

Theorem 9.7 (Poisson - Summation Formula)

$f \in \mathcal{S}(\mathbb{A}_K)$. Then $\sum_{a \in K} f(a) = \sum_{a \in K} \hat{f}(a)$

(and both sums are absolutely convergent).

Not proved here?

Example

i) Let $K = \mathbb{Q}$, $f = \prod f_v$ with $f_\infty \in \mathcal{S}(\mathbb{R})$, $f_p = \mathbb{1}_{\mathbb{Z}_p}$ for all p.

If $a \in \mathbb{Q}$, then $f(a) = 0$ unless $\forall p$, $|a|_p \leq 1$ i.e. unless $a \in \mathbb{Z}$

So the identity is equivalent to $\sum_{a \in \mathbb{Z}} f_\infty(a)$

(because $\hat{\mathbb{1}}_{\mathbb{Z}_p} = \mathbb{1}_{\mathbb{Z}_p}$) $\qquad = \sum_{a \in \mathbb{Z}} \hat{f}_\infty(a)$

This is the usual Poisson summation formula.

ii) For K arbitrary, $\exists S$ such that $f_v = \mathbb{1}_{\mathcal{O}_v}$ $\forall v \notin S$, and for finite $v \in S$, $f_v = 0$ outside $\pi_v^{-n_v} \mathcal{O}_v$.

So if $a \in K$, then $f(a) = 0$ unless $|a|_v \leq 1$ $\forall$ finite $v \notin S$,

and $|a|_v \leq q_v^{n_v}$ $\forall$ finite $v \in S$.

both true if and only if

$$a \in \underline{b} = \prod P_v^{-n_v} \subset K$$

fractional ideal

$\sigma : a \hookrightarrow \prod_{v | \infty} K_v \cong \mathbb{R}^n$, image a lattice.

$\Rightarrow$ Reduce to Poisson summation formula for a lattice in $\mathbb{R}^n$.

08/03/14

Algebraic Number Theory (22)

Poisson Summation:

$f \in S(\mathbb{A}_K)$. Then $\sum_{a \in K} f(a) = \sum_{a \in K} \hat{f}(a)$

Remember that $f = \bigotimes_v f_v$

Corollary 9.8

$x \in J_K$. Then $\sum_{a \in K} f(ax) = |x|_{\mathbb{A}}^{-1} \sum_{a \in K} \hat{f}(x^{-1}a)$

(By Lemma 9.4) $\leftarrow$ $g(x) = f(zx) \Rightarrow \hat{g}(y) = |z|^{-1}\hat{f}(z^{-1}y)$ for a single component

Just

Global Zeta Integral

$f = \prod_v f_v \in S(\mathbb{A}_K)$, $f_v \in S(K_v)$, $f_v = \mathbb{1}_{O_v}$ for almost all finite v. Define $\zeta(f,s) = \int_{J_K} f(x)|x|_{\mathbb{A}}^s d_J^* x$

$$= \prod_v \int_{K_v^*} f_v(x)|x|_v^s d_v^* x = \prod_v \zeta(f_v, s)$$

Proposition 9.9

$\prod_v$ above converges for $Re(s) > 1$.

Proof

$\exists S \supset \Sigma_{K,\infty}$, a finite set such that $\forall v \notin S$, $f_v = \mathbb{1}_{O_v}$.

It is enough to prove the convergence of $\prod_{v \notin S} \zeta(f_v, s) = \prod_{v \notin S} \frac{1}{1-q_v^{-s}}$

(by 9.5), which converges for $Re(s) > 1$ by 9.1 $\square$

The rest is a finite product containing $\Gamma_{\mathbb{R}}, \Gamma_{\mathbb{C}}, \frac{q^{-ns}}{1-q^{-s}}$

Theorem 9.10

$\zeta(f,s)$ has a meromorphic continuation to $\mathbb{C}$, at worst simple poles at $s = 0, 1$, and satisfies $\zeta(f,s) = \zeta(\hat{f}, 1-s)$

$Res_{s=1}\zeta(f,s) = \hat{f}(0)K$

$Res_{s=0}\zeta(f,s) = -f(0)K$

where K = measure of J_K^1/K^* ($< \infty$ as J_K^1/K^* is complete).

Proof (begining)

Separate out the variable $|x|_{\mathbb{A}}$:

Embed $\mathbb{R}^*_{>0} \overset{i}{\hookrightarrow} J_K$ $\qquad i(t)_v = \begin{cases} t^{1/n} & \text{if } v|\infty,\ n=[K:\mathbb{Q}] \\ 1 & \text{if } v \text{ finite} \end{cases}$

$\qquad\quad t \longmapsto i(t)$

$i(t) = \prod_v i(t)_v$ really $\otimes$

so that $|i(t)|_{\mathbb{A}} = t$.

So we get an isomorphism $J_K' \times \mathbb{R}^*_{>0} \xrightarrow{\sim} J_K$

$$(x,t) \longmapsto i(t)x$$

(we will write t instead of $i(t)$ usually)

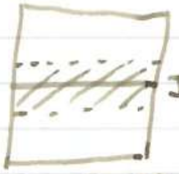
This enables us to define a measure on J_K'; $d^*_{J'}x$ such that

$$\int_{J_K} f\, d^*_J x = \int_0^t \int_{J_K'} f(tx)\, d^*_{J'}x\, \frac{dt}{t} \quad ①$$

If g is a function of J_K', choose any φ on $\mathbb{R}^*_{>0}$ of compact support, with $\int_0^\infty \varphi(t)\frac{dt}{t} \overset{②}{=} 1$. Then $tx \mapsto \varphi(t)g(x)$ $\quad g'(tx) =$

is a function g' on J_K, and define

$$\int_{J_K'} g(x)\, d^*_{J'}x = \int_{J_K} g'(y)\, d^*_J y$$



Works by ① and ②

It is easy to check that this is independent of φ.

So $\zeta(f,s) = \int_0^\infty \zeta_t(f,s)\frac{dt}{t}$ (where $\zeta_t(f,s)$

$= \cancel{|x|^s} t^s \int_{J_K'} f(tx)\, d^*_{J'}x$) $\quad$ (as $t^s = |tx|^s_{\mathbb{A}}$) $\quad |x|_{\mathbb{A}} =$

converges (at least for almost all t) for $\mathrm{Re}(s) > 1$, and so for every s (as the integrand is independent of s). $\square$

Write $J_K' = \coprod_{a\in K^*} aE$ for some $E \subset J_K'$ which we make explicit later, with $\kappa = \text{measure}(E) < \infty$.

Definition of this is

Local: $\zeta(f,s) := \int_{F^*} f(x)|x|^s d^*_F x = \lim \int_{F\setminus \text{ball of radius } \varepsilon} f(x)|x|^{s-1} d_F x$

2 Global $\zeta(f,s) := \int_{J_K} f(x)|x|^s_{\mathbb{A}} d^*_J x$ = product of local factors

08/03/14 Algebraic Number Theory (22)

Proposition 9·11

$$\zeta_t(f,s) + K f(0) t^s = \zeta_{1/t}(\hat{f},1-s) + K\hat{f}(0)t^{s-1}$$ "$(\frac{1}{t})^{1-s}$"

Proof

E given on previous page. Have simply split integral over J_K' into integral over cosets

Add $Kf(0)t^s$ into sum and change $\sum_{a\in K^*}$ to $\sum_{a\in K}$

$$LHS = t^s\int_E \sum_{a\in K^*} f(atx)\,d^*_{J'}x + \underbrace{K f(0) t^s}$$ K = measure of J_K'/K^*

$$= t^s\int_E \sum_{a\in K} f(atx)\,d^*_{J'}x = t^s\int_E \sum_{a\in K} |tx|_A^{-1}\hat{f}(a(tx)^{-1})\,d^*_{J'}x$$ (corollary 9·8)

$|x|_A = 1$

$$= t^{s-1}\int_E \sum_{a\in K^*}\hat{f}(at^{-1}x^{-1})\,d^*_{J'}x + t^{s-1}\hat{f}(0)K$$ — remove $a=0$ again, $\sum_{a\in K}\to\sum_{a\in K^*}$

Now on F_v^*, $d_v^*(\frac{1}{x}) = d_v^*x$ (invariant under $x\mapsto\frac{1}{x}$)

(On $\mathbb{R}^*_{>0}$ $d^*x = \frac{dx}{x}$, $d^*(\frac{1}{x}) = \frac{dx/x^2}{1/x} = \frac{dx}{x}$)

because measure $(\pi^n\mathcal{O}_v^*) = 1$ = measure $(\pi^{-n}\mathcal{O}_v^*)$

So $LHS = t^{s-1}\int_E \sum_{a\in K^*}\hat{f}(at^{-1}x)\,d^*_{J'}x + t^{s-1}\hat{f}(0)K$

$= RHS$ after change of variables □

Aside

Classical Proof for $\zeta(s) = \sum\frac{1}{n^s}$:

$$\pi^{-s/2}\Gamma(\tfrac{s}{2})\zeta(s) = \int_0^\infty e^{-y}(\tfrac{y}{\pi})^{s/2}\sum n^{-s}\frac{dy}{y}$$ $y = \pi n^2 t$

$$= \int_0^\infty \underbrace{\Big(\sum_{n=1}^\infty e^{-\pi n^2 t}\Big)}_{\frac{1}{2}(\Theta(t)-1)} t^{s/2}\frac{dt}{t}$$ $y=\pi n^2 t$

$\frac{1}{2}(\Theta(t)-1)t^{s/2} \leftarrow \zeta_t(f,s)$

$$\Theta(t) = \sum_{n=-\infty}^\infty e^{-\pi n^2 t} = \Theta(\tfrac{1}{t})t^{\frac{1}{2}}$$

So this proof is a variant on the "usual" proof for $\zeta(s)$.

Now $\zeta(f,s) = \int_0^\infty \zeta_t(f,s)\frac{dt}{t}$

$$= \int_1^\infty \zeta_t(f,s)\frac{dt}{t} + \int_0^1 \zeta_t(f,s)\frac{dt}{t} \quad (Re(s)>1)$$

and $\int_1^\infty \zeta_t(f,s)\frac{dt}{t} = \int_{\{x\in J_K \mid |x|_A\geq 1\}} f(x)|x|^s d^*_J x$

which converges for $Re(s)>1$ as $\zeta(f,s)$ does.

So as $|x|_{\mathbb{A}} \geq 1$ in the region of integration, it converges for all $s \in \mathbb{C}$.

2^nd term : $\int_0^1 \zeta_t(f,s)\frac{dt}{t} = \int_1^\infty \zeta_{1/t}(f,s)\frac{dt}{t}$ $\quad (\mathrm{Re}(s)>1)$

$$= \int_1^\infty \zeta_t(\hat{f},1-s) - Kf(0)t^{-s} + K\hat{f}(0)t^{1-s}\frac{dt}{t}$$

$$= \underbrace{\int_1^\infty \zeta_t(\hat{f},1-s)\frac{dt}{t}}_{\text{also converges } \forall s\in\mathbb{C}} + K\left(\frac{\hat{f}(0)}{s-1} - \frac{f(0)}{s}\right)$$

So $$\zeta(f,s) = \int_1^\infty \zeta_t(f,s) + \zeta_t(\hat{f},1-s)\frac{dt}{t} + K\left(\frac{\hat{f}(0)}{s-1} - \frac{f(0)}{s}\right)$$

where the integral is analytic $\forall s \in \mathbb{C}$.

Replacing f by $\hat{f}$ leaves the RHS unchanged since

$$\zeta_t(\hat{\hat{f}},s) = \zeta_t(f(-x),s) = \zeta_t(f,s)$$

as $d(-x) = dx$, $|-x| = |x|$

Local factors

$F=\mathbb{R}$, $\zeta(f,s) = \Gamma_{\mathbb{R}}(s) = \pi^{-s/2}\Gamma(\frac{s}{2})$

$F=\mathbb{C}$, $\zeta(f,s) = \Gamma_{\mathbb{C}}(s) = 2(2\pi)^{-s}\Gamma(s)$

11/03/14 Algebraic Number Theory (23)

$f \in \mathcal{S}(\mathbb{A}_K)$, $\zeta(f,s) = \zeta(\hat{f}, 1-s)$ (Theorem 9·11)

$\operatorname{Res}_{s=\{^1_0} \zeta(f,s) = \begin{cases} \kappa \hat{f}(0) \\ -\kappa f(0) \end{cases}$ $\kappa = \text{measure}\left(J_K^1 / K^*\right)$

<u>Theorem 9·12</u>

$\kappa = \dfrac{2^{r_1}(2\pi)^{r_2} h_K R_K}{w_K}$, $h_K = \# Cl(K)$, $R_K = \text{regulator}$

$w_K = \#$ roots of unity in K.

i) $Z_K(s) = |d_K|^{s/2}\, \Gamma_{\mathbb{R}}(s)^{r_1}\, \Gamma_{\mathbb{C}}(s)^{r_2}\, \zeta_K(s)$ has analytic continuation to $\mathbb{C}$ with simple poles at 0, 1

ii) $\zeta_K(s)$ has a zero of order r_1+r_2-1 at 0 and $\lim_{s\to 0} s^{-r_1-r_2+1} \zeta_K(s) = -\dfrac{h_K R_K}{w_K}$

Assuming this, we prove Theorem 9·2 by choosing suitable $f \in \mathcal{S}(\mathbb{A}_K)$

i) Take $f_v = \begin{cases} e^{-\pi x^2} & v \text{ real} \\ \frac{1}{\pi} e^{-2\pi z\bar{z}} & \text{complex} \\ \mathbb{1}_{\mathcal{O}_v} & \text{finite} \end{cases}$

so $\hat{f}_v = \begin{cases} f_v & v \text{ real} \\ f_v & \text{complex} \\ q_v^{-\delta_v/2}\, \mathbb{1}_{\mathcal{D}^{-1}_{K_v/\mathbb{Q}_p}} & \text{finite} \end{cases}$

We computed $\zeta(f_v, s)$ in 9·5, so

$\zeta(f,s) = \Gamma_{\mathbb{R}}(s)^{r_1}\, \Gamma_{\mathbb{C}}(s)^{r_2} \prod_{v \nmid \infty} (1-q_v^{-s})^{-1} = |d_K|^{-s/2} Z_K(s)$

v finite, $\zeta(\hat{f}, 1-s) = q_v^{-\delta_v/2 + \delta_v(1-s)} (1-q_v^{-(1-s)})^{-1}$ (by 9·5)

$= q_v^{\delta_v(\frac{1}{2}-s)}\, \zeta(f_v, 1-s)$

$Z_K(s) = |d_K|^{s/2} \zeta(f,s) = |d_K|^{s/2} \zeta(\hat{f}, 1-s)$ (9·11)

$= |d_K|^{s/2} \left(\prod_{v \text{ finite}} q_v^{\delta_v(\frac{1}{2}-s)} \right) \zeta(f, 1-s)$

$= |d_K|^{\frac{1}{2}-\frac{s}{2}} \zeta(f, 1-s) = Z_K(1-s)$

and has analytic continuation. (Proves 9·2(i) by properties of Γ and ζ)

ii) With f as above, $f(0) = \pi^{-r_2}$

So $\zeta(f,s) \underset{s=0}{\sim} -\kappa f(0) \frac{1}{s} = -\frac{1}{w_K} 2^{r_1+r_2} h_K R_K \frac{1}{s}$

$\Gamma(s) = \frac{1}{s}\Gamma(s+1) \underset{s=0}{\sim} \frac{\Gamma(1)}{s} = \frac{1}{s}$ so $\Gamma_{\mathbb{R}}(s) = \pi^{-\frac{s}{2}} \Gamma(\frac{s}{2}) \sim \frac{2}{s}$

$$\Gamma_{\mathbb{C}}(s) = 2(2\pi)^{-s}\Gamma(s) \sim \frac{2}{s}$$

and $|d_K|^{s/2} \to 1$ as $s \to 0$. So:

$$\zeta_K(s) = |d_K|^{-\frac{s}{2}} \Gamma_{\mathbb{R}}(s)^{-r_1} \Gamma_{\mathbb{C}}(s)^{-r_2} \zeta(f, s)$$

$$\sim -s^{r_1+r_2-1} \frac{h_K R_K}{w_K} \qquad \square$$

(It is trivial to obtain a similar expression for $\mathrm{Res}_{s=1} \zeta_K(s)$ and this is more classical)

<u>Computation of Volume</u> $\quad r = r_1 + r_2 - 1 = \operatorname{rank} \mathcal{O}_K^*$

$$J_\infty = \prod_{v|\infty} K_v^* \simeq (\mathbb{R}^*)^{r_1} \times (\mathbb{C}^*)^{r_2}$$

$$\supset J_\infty' = \{ (x_v)_v \in J_\infty \mid \prod_v |x_v|_v = 1 \}$$

Recall (unit theorem) $\lambda : J_\infty \to \mathbb{R}^\Sigma \cong \mathbb{R}^{r+1}$ $(\Sigma = \Sigma_{K,\infty})$

$$(x_v)_v \mapsto (\log |x_v|_v)_v$$

$\mathcal{O}_K^* \subset J_\infty$; the unit theorem shows that $\mathcal{O}_K^* \cap \ker \lambda$ is finite and $\lambda(\mathcal{O}_K)$ is a <u>lattice</u> in $\mathbb{R}^{\Sigma,0} = \{ (y_v) \in \mathbb{R}^\Sigma \mid \sum y_v = 0 \} = \lambda(J_\infty')$

Trace zero hyperplane

$$\mathcal{O}_K^* = \mu_K \times \langle \varepsilon_1, \dots, \varepsilon_r \rangle$$

R_K = absolute value of any $r \times r$ minor of $(\log |\varepsilon_i|_v)_{i,v}$

$$= \left\| \log|\varepsilon_1|_v \cdots\cdots \log|\varepsilon_r|_v \quad \frac{e_v}{n} \right\| \qquad e_v = [F_v : \mathbb{R}] = \begin{cases} 1 \\ 2 \end{cases} \quad \sum_v \frac{e_v}{n} = 1$$

So if $b = (e^{\frac{1}{n}}, \dots, e^{\frac{1}{n}}) \in J_\infty$ $(e = \exp(1))$

then $R_K = \mathrm{vol}\left(\dfrac{\mathbb{R}^\Sigma}{\lambda(\mathcal{O}_K^* \oplus \langle b \rangle)} \right)$

Consider $K_v^* \xrightarrow[\log|\cdot|_v]{} \mathbb{R}$ and left inverse $u \mapsto \begin{cases} e^u & \text{real} \\ e^{u/2} & \text{complex} \end{cases}$

This induces an isomorphism

$$\begin{array}{ccc} \mathbb{R} \times \{\pm 1\} & \xrightarrow{\sim} & \mathbb{R}^* \\ (u, \delta) & \longmapsto & \delta e^u \end{array}$$

$$du \times \begin{pmatrix} \text{counting measure} \\ \text{on } \{\pm 1\} \end{pmatrix} \longleftrightarrow d_{\mathbb{R}}^* x = \frac{dx}{|x|}$$

11/03/14

Algebraic Number Theory (23)

$$\mathbb{R} \times \left(\mathbb{R}/2\pi\mathbb{Z}\right) \xrightarrow{\sim} \mathbb{C}^*$$
$$(u, \theta) \longmapsto e^{u/2 + i\theta}$$

$$du\, d\theta \longleftrightarrow d_{\mathbb{C}}^* z = \frac{|dz\, d\bar{z}|}{z\bar{z}} = \frac{2}{r} dr\, d\theta \quad , z = re^{i\theta}$$

Consequence:

If $M \subset J_\infty$ is a discrete subgroup such that $\lambda : M \xrightarrow{\sim} \lambda(M)$, and $\lambda(M)$ is a lattice in $\mathbb{R}^\Sigma$, then

$$\text{measure}\left(J_\infty/M, \prod_v d_{K_v}^* x\right) = \text{vol}\left(\mathbb{R}^\Sigma/\lambda(M)\right) 2^{r_1} (2\pi)^{r_2}$$

Take $M = \langle \varepsilon_1, \dots, \varepsilon_r, b \rangle \subset M' = \langle \mathcal{O}_K^*, b \rangle$

$(M' : M) = w_K$

So $\text{Meas}\left(J_\infty/M'\right) = \frac{1}{w_K} \text{Meas}\left(J_\infty/M\right) = \frac{2^{r_1}(2\pi)^{r_2}}{w_K} \text{vol}\left(\frac{\mathbb{R}^\Sigma}{\lambda(M)}\right)$

$$= \frac{2^{r_1}(2\pi)^{r_2} R_K}{w_K}$$

Also, $J_\infty \cong J_\infty' \times \mathbb{R}_{>0}^*$, $(x, t) \mapsto (x_v t^{1/n})_v$, $x \in J_K'$, $t > 0$

$$\begin{matrix} J_\infty & \cong & J_\infty' & \times & \mathbb{R}_{>0}^* \\ \cup & & & & \cup \\ \langle b \rangle & \mapsto & 1 & \times & \langle e \rangle \end{matrix}$$

$\text{Meas}\left(\mathbb{R}_{>0}^*/\langle e \rangle, \frac{dt}{t}\right) = 1$

So $\text{Measure}\left(J_\infty/M'\right) = \text{Measure}\left(J_\infty'/\mathcal{O}_K^*\right)$

Finally, recall $U_K = J_\infty \times \prod_{v \nmid \infty} \mathcal{O}_v^*$, $U_K' = U_K \cap J_K' = J_\infty' \times \prod_{v \nmid \infty} \mathcal{O}_v^*$

and $1 \to U_K'/\mathcal{O}_K^* \to J_K'/K^* \to Cl(K) \to 1$

So $\text{measure}\left(J_K'/K^*\right) = h_K \times \text{measure}\left(U_K'/\mathcal{O}_K^*\right)$

$= h_K \times \text{measure}\left(J_\infty'/\mathcal{O}_K^*\right)$ as $\text{measure}(\mathcal{O}_v^*) = 1$

$$= 2^{r_1}(2\pi)^{r_2} \frac{h_K R_K}{w_K}$$

11/03/14

Algebraic Number Theory 24

"Fundamental Domain" for J_K'/K^*

$$\begin{array}{l} J_\infty^1 \xrightarrow{\lambda} \mathbb{R}^{\Sigma,0} \\ \cup \\ \mathcal{O}_K^* \\ \psi \\ \varepsilon_1, \dots, \varepsilon_r \end{array}$$

$\{\lambda(\varepsilon_j)\}$ a basis $/\mathbb{R}$

Let $P = \left\{ \sum_{j=1}^{r} \alpha_j \lambda(\varepsilon_j) \,\middle|\, 0 \leq \alpha_j < 1 \right\}$

Then $\mathbb{R}^{\Sigma,0} = \coprod_{y \in \lambda(\mathcal{O}_K^*)} (P+y)$

and $J_\infty^1 = \coprod_{\varepsilon \in \langle \varepsilon_1, \dots, \varepsilon_r \rangle} \lambda^{-1}(P)\,\varepsilon$

Let $Q \subset \lambda^{-1}(P) \subset J_\infty^1$ be $Q = \{x \in J_\infty^1 \mid \lambda(x) \in P, 0 \leq \arg x_{v_0} < \frac{2\pi}{w_K}$

with v_0 an infinite place of K, which is complex if $w_K > 2$.

(if v_0 is real, then $w_K = 2$ and this condition says that $x_{v_0} > 0$)

Then $J_\infty^1 = \coprod_{\varepsilon \in \mathcal{O}_K^*} Q \cdot \varepsilon$ (easy to see)

$E_0 = Q \times \prod_{v \nmid \infty} \mathcal{O}_v^*$, $U_K^1 = J_\infty^1 \times \prod \mathcal{O}_v^* = \coprod_{\varepsilon \in \mathcal{O}_K^*} E_0\,\varepsilon$

$U_K^1/\mathcal{O}_K^* \cong \ker(J_K^1/K^* \to Cl(K))$

Choose $x_1, \dots, x_h \in J_K^1$ whose images are all the elements of $Cl(K)$, and put $E = \coprod_{1 \leq i \leq h} E_0 x_i$

then $J_K^1 = \coprod_{x \in K^*} E x$. ($E$ is a measurable set of coset reps.)

L-Functions

$$\lim_{s \to 0} s^{-r} \zeta_K(s) = -\frac{h_K R_K}{w_K}$$

k_0 k_1

$\exists$ more general formulae e.g. leading coefficient of $\zeta_K(s)$ at $s = 1-m$ is (rational) $\times$ (higher regulator)

measure size of "K-groups" of $\mathcal{O}_K$.

For Abelian L-functions, see Sheet 3.

$\chi : J_K/K^* \to \mathbb{C}^*$ a continuous homomorphism (e.g. a hom $Cl(K) \to \mathbb{C}^*$)

$\chi((x_v)_v) = \prod_v \chi_v(x_v)$, and $\chi_v(\mathcal{O}_v^*) = 1$ for almost all v.

"χ_v unramified"

L-function of χ

$$L(\chi, s) = \prod_{\substack{v \nmid \infty \\ \text{unramified}}} \frac{1}{1 - \chi_v(\pi_v) q_v^{-s}}$$

$L(\chi, s)$ converges in some right half plane:

if $\chi : J_K/K^* \to U(1)$ converges for $Re(s) > 1$ (compare with $\zeta_K(s)$

Theorem

$L(\chi, s)$ has analytic continuation

$L(\chi, s) = (\ldots) L(\chi^{-1}, 1-s)$ $\quad (\chi = 1, \ L(\chi, s) = \zeta_K(s))$

How is this proved?

$\zeta(f, \chi, s) = \prod \zeta(f_v, \chi_v, s)$ $\qquad f \in S(\mathbb{A}_K)$

$\zeta(f_v, \chi_v, s) = \int_{K_v^*} f_v(x) \chi_v(x) |x|_v^s \, d_v^* x$

$\left(\chi(x) = |x|_{\mathbb{A}}^t, \ L(|\cdot|_{\mathbb{A}}^t, s) = \zeta_K(s+t) \right)$

$\zeta(f, \chi, s) = \zeta(\hat{f}, \chi^{-1}, 1-s)$ by Poisson Summation as before

It is slightly trickier to relate this to $L(\chi, s)$.

For "standard" f_v we can have $\zeta(f_v, \chi_v, s) = 0$

e.g. if v is real and $\chi_v(-1) = -1$, then

$$\zeta(e^{-\pi x^2}, \chi_v, s) = \int_{-\infty}^{\infty} e^{-\pi x^2} \chi_v(x) |x|^{s-1} dx = 0$$

since the integrand is odd.

A similar argument shows that $\zeta(\mathbb{1}_{\mathcal{O}_v}, \chi_v, s) = 0$

if χ_v is ramified (send $x \mapsto ax$ for some $a \in \mathcal{O}_v^*$ with $\chi_v(a) \neq 1$)

We must do 2 things:

i) Show that $\exists f_v$ such that $\zeta(f_v, \chi_v, s) \neq 0$

(e.g. $f_v = \mathbb{1}_{1+\pi^r \mathcal{O}_v}$ with $\chi_v|_{1+\pi^r \mathcal{O}_v} = 1$)

11/03/14 Algebraic Number Theory 24

ii) Compare $\zeta(f_v, \chi_v, s)$ and $\zeta(\hat{f}_v, \chi_v, s)$

For $\chi = 1$, ii) was easy, but in general, the <u>local functional equation</u>

$$\frac{\zeta_v(f_v, \chi_v, s)}{\zeta_v(\hat{f}_v, \chi_v^{-1}, 1-s)} = c(\chi_v, s) \quad \text{computable and independent of } f_v.$$

$\Rightarrow$ Functional equation for $L(\chi, s)$

$J_K = GL_1(\mathbb{A}_K)$

but for modular forms, we use $GL_2(\mathbb{A}_K)$

2