Math 620 Algebraic Number Theory Fall 2014

What is algebraic number theory:

- study arithmetic properties of number fields and systems of polynomial equations over number fields, including zeta and L-functions of arithmetic nature

Standard materials in a first year graduate course on number theory:

(1) local fields, ramification theory (local method)

(2) finiteness properties of global fields

(3) local / global class-field theory

(4) L-functions and functional equation via Tate's method

(5) Artin L-functions & generalization

(6) non-vanishing of L-values + applications

Fall 2014:

(1), (2), (4) perhaps

- appreciation of L-functions as the litmus test

$\mathrm{Res}_{s=1}\, \zeta_K(s) = |D_K|^{-1/2} \cdot 2^{r_1} \cdot (2\pi)^{r_2} \cdot h_K \cdot R / w$

$L(s)\big|_{s=0} \neq 0 \rightsquigarrow$ Dirichlet's theorem

zero-free region along $\mathrm{Re}(s) = 1 \Rightarrow$ prime number theorem

bigger zero-free region $\dashrightarrow$ march toward RH

class field theory = identify abelian Artin L-function with Hecke L-functions for Hecke characters of finite order

Langlands program $\longleftrightarrow$ identify L-functions from arithmetic with automorphic L-functions for algebraic automorphic representations

$\parallel$

non-abelian reciprocity law

Review of Dedekind domains

Prop A commutative ring is a DVR if and only if it is a noetherian local ring whose max. ideal is given by a non-nilpotent element

Prop' A noetherian local integral domain is a DVR iff it is integrally closed in its fraction field and it has one non-zero prime ideal

A: noetherian integral domain

A is a Dedekind domain

$\overset{\text{def}}{\iff}$ $A_{\mathfrak{p}}$ is a DVR $\forall$ non-zero prime ideal $\mathfrak{p} \subseteq A$

$\iff$ A is integrally closed in $\mathrm{frac}(A)$ and $\dim(A) \leq 1$

Approximation lemma $\quad$ A: Dedekind domain

Given: $\mathfrak{p}_1, \dots, \mathfrak{p}_r$: distinct non-zero prime ideals

$x_1, \dots, x_r \in \mathrm{frac}(A) =: K$, $n_1, \dots, n_r \in \mathbb{N}$

$\Rightarrow$ $\exists\ x \in K$ s.t. $v_{\mathfrak{p}_i}(x - x_i) \geq n_i$ for $i = 1, \dots, r$

and $v_{\mathfrak{p}}(x) \geq 0$ $\forall$ non-zero prime ideal $\mathfrak{p}$ different from $\mathfrak{p}_1, \dots, \mathfrak{p}_r$

Behavior in finite extensions

L/K finite ext^n of fields $\quad$ $A \subset K$ noeth. integrally closed in K

B = integral closure of A in L

(finiteness assumption): B is a finite A-module

holds if L/K is <u>separable</u>

Prop: A is Dedekind $\Rightarrow$ B is Dedekind

In particular: no inclusion relation between prime ideals of B lying above the same prime ideal in A

Assume (finiteness cond^n)

Prop: $\mathfrak{p}$: non-zero prime ideal in A

$$\Rightarrow [L:K] = \sum_{\mathfrak{P} | \mathfrak{p}} e_{\mathfrak{P}} \cdot f_{\mathfrak{P}}$$

In particular, $\forall$ prime ideal $\mathfrak{p} \subseteq A$ $\exists$ $\mathfrak{P} \subseteq B$ prime ideal lying above A

$\rightsquigarrow$ $\exists$ extension of discrete valuations centered

$$\begin{array}{ccc} I_A = \begin{pmatrix}\text{the group of f.g.}\\ \text{invertible } A\text{-submodules in } K\end{pmatrix} & \underset{N}{\overset{i}{\rightleftarrows}} & \begin{pmatrix}\text{the group of f.g.}\\ \text{invertible } B\text{-submodules in } L\end{pmatrix} = I_B \\ \cup \qquad \quad \| & & \| \\ I_A^+ \quad \text{free group with basis } \{\text{non-zero prime ideals of } A\} & & \text{free group with basis } \{\text{non-zero prime ideals of } B\} \\ \mathfrak{p} & \longmapsto & \mathfrak{p}B = \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^{e_{\mathfrak{P}}} \\ \mathfrak{p}^{f_{\mathfrak{P}}} & \longleftarrow & \mathfrak{P} \end{array}$$

$$\mathcal{C}_A = \begin{Bmatrix}A\text{-modules}\\ \text{of finite length}\end{Bmatrix} \qquad \qquad \mathcal{C}_B = \begin{Bmatrix}B\text{-modules of}\\ \text{finite length}\end{Bmatrix}$$

$$\begin{tikzcd} \mathcal{C}_A \arrow[r, "\chi_A"] \arrow[d] & I_A^+ \arrow[d, hook] \\ K(\mathcal{C}_A) \arrow[r] & I_A \end{tikzcd}$$

Same for B

Prop
- M: finite length B-module $\rightsquigarrow$ $\chi_A(M) = N(\chi_B(M))$
- N: finite length A-module $\rightsquigarrow$ $\chi_B(M \otimes_A B) = i(\chi_A(M))$
- $N(\underset{\substack{\uparrow \\ L}}{x} B) = N_{L/K}(x) \cdot A$

unramified = ramification index = 1 + separable residue field ext^{n}

What happens when L/K is finite Galois:

1) $Gal(L/K)$ operates transitively on the non-empty set of all prime ideals in B above a given prime ideal $\mathfrak{p} \subseteq A$

In particular, all $e_{\mathfrak{P}}$'s are equal and all $f_{\mathfrak{P}}$'s are equal

$$+ \qquad n = e_{\mathfrak{p}} \cdot f_{\mathfrak{p}} \cdot \left(\begin{array}{c} \text{\# of prime of } B \\ \text{above } \mathfrak{p} \end{array} \right) \qquad \forall\, \mathfrak{p} \subset A \text{ prime}, \ \mathfrak{p} \neq 0$$

2) $\mathfrak{P} \rightsquigarrow D = D_{\mathfrak{P}}, \quad I = I_{\mathfrak{P}}$

$$\begin{array}{c} \mathfrak{P} \\ | \\ \mathfrak{p} \end{array}$$

$$\begin{tikzcd}
L \arrow[d, dash] \arrow[d, bend left, phantom, "I"] \arrow[dd, bend right=60, dash, "D"'] \\
K_I \arrow[d, dash] \\
K_D \arrow[d, dash, "\text{\# of prime ideals above } \mathfrak{p}"] \\
K
\end{tikzcd}$$

def^{n} of I

$$1 \to I \to D \to Gal(\kappa_L / \kappa) \to 1$$

$[K_I : K_D] = [\kappa_L : \kappa]_{sep}$ separable part of $[\kappa_L : \kappa]$

$[K_D : K] = $ # of prime ideals of B above A

$[L : K_I] = e \cdot p^{i}$

$$p^{i} = [\kappa_L : \kappa]_{insep}$$

3) Frobenius attached to an unramified prime:

unramified $\Leftrightarrow$ $I =$ trivial

i.e.
$$\begin{array}{ccc} D_{\mathfrak{P}} & \xrightarrow{\sim} & Gal(\kappa_{\mathfrak{P}} / \kappa) \\ \Psi & & \Psi \\ Fr_{\mathfrak{P}} & \longmapsto & \text{arith. Frob} \end{array} \qquad \forall\, \mathfrak{P} \text{ above } \mathfrak{p}$$

Note: $Fr_{\mathfrak{P}}$ and $Fr_{\mathfrak{P}'}$ are conjugate in $Gal(L/K)$

$\rightsquigarrow \left(\frac{L/K}{\mathfrak{a}}\right)$, or $(\mathfrak{a}, L/K)$ (unramified)

$\mathfrak{a}$: all primes in $\mathfrak{a}$ unramified in L/K

Artin symbol

arithmetically normalized

Consequence of Artin reciprocity law: existence of conductor for Artin map.

L/K finite abelian ext^n of number fields

$\exists$ an ideal $I \subseteq \mathcal{O}_A$, containing all ramified places

s.t. $(x\mathcal{O}_A, L/K) = 1$ $\forall x \in K$ s.t. $v_{\mathfrak{p}}(x-1) \geq v_{\mathfrak{p}}(I)$ $\forall$ ramified places

and $\alpha(x) > 0$ $\forall$ real embedding $\alpha: K \hookrightarrow \mathbb{R}$

Completion & local fields

- complete discretely valued fields
- **Lemma**: K complete discretely valued field

  K is locally compact $\iff \# \mathcal{O}_K/\mathfrak{m}_K < \infty$

  normalized absolute value:

  $$\mu(xE) = \|x\| \cdot \mu(E) \quad \forall E \text{ measurable}$$

  $\|x\|$: normalized abs. value

  μ: Haar measure

Prop: $K = \text{frac } \mathcal{O}_K$ $\mathcal{O}_K$ = complete dvr

L/K finite ext^n, $\mathcal{O}_L$ = integral closure of

$\rightsquigarrow$ $\mathcal{O}_L$ is a free $\mathcal{O}_K$-module of rank $[L:K]$

and $\mathcal{O}_L$ is a complete dvr

esp. - $[L:K] = e_{L/K} \cdot f_{L/K}$

- $\exists!$ valuation on L extending v_K

$\implies$ Galois conjugate elements have the same valuation

$$v_L(x) = \frac{1}{f} v_K(N_{L/K}(x)) \quad \forall x \in L$$

$v_L(\pi_L) = 1$

$$\|x\|_L = \|N_{L/K}(x)\|_K \qquad \forall x \in L$$

normalized absolute values

Krasner's lemma

K: complete under a valuation (not nec. discrete)

$\alpha, \beta \in K^{alg}$, α separable over $K(\beta)$

Assume: $\forall \underset{\neq id}{\sigma} : K(\alpha) \xhookrightarrow[K\text{-linear}]{} K^{alg}$

have: $|\beta - \alpha| < |\sigma\alpha - \alpha|$ ("β very close to α")

Then: $K(\alpha) \subset K(\beta)$

Pf $\forall \tau : K(\alpha, \beta) \xhookrightarrow[K(\beta)\text{-linear}]{} K^{alg}$

Have $|\beta - \alpha| = |\beta - \tau(\alpha)|$

$$\Rightarrow |\tau(\alpha) - \alpha| = |\tau(\alpha) - \beta + \beta - \alpha| \leq |\beta - \alpha|$$
$$< |\tau(\alpha) - \alpha|$$

unless $\tau(\alpha) = \alpha$ q.e.d.

Hensel's lemma

How to solve polynomial equations in complete field

$f(T) \in K(T)$

$|f(\alpha_0)| < |f'(\alpha_0)^2| \qquad \alpha_0 \in \mathcal{O}_K$

$\rightsquigarrow$ Construct $(\alpha_i)_{i \geq 1}$: $\alpha_{i+1} = \alpha_i - \frac{f(\alpha_i)}{f'(\alpha_i)}$

$$f(\alpha_{i+1}) = f\left(\alpha_i - \frac{f(\alpha_i)}{f'(\alpha_i)}\right) \equiv f(\alpha_i) - \frac{f(\alpha_i)}{f(\alpha_i)} \cdot f'(\alpha_i) \mod \left(\frac{f(\alpha_i)}{f'(\alpha_i)}\right)^2 \mathcal{O}_K$$

Inductive assumption:

$$\left|\frac{f(\alpha_i)}{f'(\alpha_i)^2}\right| \leq \left|\frac{f(\alpha_0)}{f'(\alpha_0)^2}\right|^{2^i} \quad \underset{\text{Want}}{\Longrightarrow} \quad \left|\frac{f(\alpha_{i+1})}{f'(\alpha_i)}\right| \leq \left|\frac{f(\alpha_0)}{f'(\alpha_0)}\right|^{2^{i+1}}$$

$$c = \left|\frac{f(\alpha_0)}{f'(\alpha_0)^2}\right| < 1$$

Need to check

$$f'(\alpha_{i+1}) \equiv f'(\alpha_i) - \underbrace{f''(\alpha_i)\frac{f(\alpha_i)}{f'(\alpha_i)}} \quad \text{mod} \quad \underbrace{O_K \cdot \left(\frac{f(\alpha_i)}{f'(\alpha_i)}\right)^2}_{|\cdot| \leq c^{2^{2^i}}}$$

$$|\cdot| \leq |f'(\alpha_i)| \cdot c^{2^{2^i}} \qquad \text{by induction}$$
$$< |f'(\alpha_i)|$$

So $|f'(\alpha_{i+1})| = |f'(\alpha_i)|$

$$f(\alpha_{i+1}) \in O_K \cdot \left(\frac{f(\alpha_i)}{f'(\alpha_i)}\right)^2$$

$$\Rightarrow \left|\frac{f(\alpha_{i+1})}{f'(\alpha_{i+1})^2}\right| \leq \frac{|f(\alpha_i)|^2}{|f'(\alpha_i)|^2 \cdot |f'(\alpha_i)|^2} = \left|\frac{f(\alpha_i)}{f'(\alpha_i)^2}\right|^2$$

Note: The solution α we get is
$$\alpha \equiv \alpha_0 \left(\text{mod } \frac{f(\alpha_0)}{f'(\alpha_0)}\right)$$

Example: $f(T) = x^2 - p \qquad p \equiv 1 \pmod{2^4}$

Start with approximate solution $3 \in \mathbb{Q}_2$.

$$\alpha_0 = 3. \qquad \alpha_1 = 3 - \left(\frac{9-p}{6}\right) = 3 - \frac{1}{3}\cdot\underbrace{\left(\frac{9-p}{2}\right)}_{\equiv 0 \pmod 4}$$

e.g. if $p = 17$. $\alpha_1 = 3 - \frac{4}{3} \equiv -1 \pmod 8$

Thus α_1 and α_0 are NOT congruent mod 8 only mod 4

Conclusion: If $\left|\frac{f(\alpha_0)}{f'(\alpha_0)^2}\right| < 1$, $\exists!$ solution/root α of $f(T)$

s.t. $\alpha \equiv \alpha_0 \left(\text{mod } \frac{f(\alpha_0)}{f'(\alpha_0)} \cdot O_K\right)$

Different and discriminant

L/K separable

$B = \mathcal{O}_L$ $\quad$ $B =$ normal closure of A in frac(L)

$A = \mathcal{O}_K$ $\quad$ $\mathcal{D}_{L/K}^{-1} = \mathcal{D}_{\mathcal{O}_L/\mathcal{O}_K}^{-1} = \{ x \in L \mid \mathrm{Tr}_{L/K}(x\mathcal{O}_L) \subseteq \mathcal{O}_K \}$

$$\mathrm{disc}_{L/K} = N_{L/K}(\mathcal{D}_{L/K}) = \chi_A(\mathcal{D}_{L/K}^{-1}/\mathcal{O}_L)$$

Computation: $\mathcal{O}_L = x_1\mathcal{O}_K \oplus \cdots \oplus x_d\mathcal{O}_K$

$$\rightsquigarrow \underset{M =}{\left(\mathrm{Tr}(x_i x_j)\right)_{i,j}} \rightsquigarrow \mathcal{D}_{L/K}^{-1} = \left\{ \sum_{i=1}^d a_i x_i \;\middle|\; a_i \in K,\ M\cdot\begin{pmatrix} a_1 \\ \vdots \\ a_d \end{pmatrix} \subseteq \mathcal{O}_K^d \right\}$$

$$\rightsquigarrow \chi_A(\mathcal{D}_{L/K}^{-1}/\mathcal{O}_K) = \det(M)\cdot\mathcal{O}_A$$

i.e. computation if we know the trace pairing for a basis

Euler: $f(T)$ = irred. poly of a generator of L, x_1 = a root $\quad$ L/K : separable ext^{n}

$$\frac{1}{f(T)} = \sum_{i=1}^d \frac{1}{f'(x_i)(T-x_i)}$$

$x = x_1, \dots, x_d$ = roots of $f(T)$

Assume : $f(T) \in \mathcal{O}_K[T]$

Want : $$\mathrm{Tr}_{L/K}\left(\frac{x^j}{f'(x)}\right) = \sum_{i=1}^d \frac{x_i^j}{f'(x_i)}$$

$$\sum_{i=1}^d \frac{1}{f'(x_i)\,(T-x_i)} = \sum_{j=0}^\infty \sum_{i=1}^d \frac{1}{f'(x_i)} \cdot \frac{x_i^j}{T^{j+1}} \quad \Rightarrow \quad \sum_{i=1}^d \frac{x_i^j}{f'(x_i)} = \begin{cases} 0 & \text{if } 0 \le j \le d-1 \\ 1 & \text{if } j = d-1 \end{cases}$$

$$\frac{1}{f(T)} = T^{-d}(1 + \text{higher powers of } T^{-1})$$

Have computed the matrix $$\left(\mathrm{Tr}\left(x^i \cdot \frac{x^j}{f'(x)}\right)\right)_{0 \le i, j \le d-1} = \begin{pmatrix} 0 & & 1 \\ & \cdot^{\cdot^{\cdot}} & \\ 1 & & \underset{\text{in } \mathcal{O}_K}{*} \end{pmatrix} \in GL_d(\mathcal{O}_K)$$

$$\Rightarrow \left\{ y \in L \;\middle|\; \mathrm{Tr}_{L/K}(y \cdot \mathcal{O}_A[x]) \right\} = \sum_{j=0}^{d-1} \frac{x^j}{f'(x)} = \frac{1}{f'(x)}\cdot\mathcal{O}_A[x]$$

Conclude: If $\mathcal{O}_B = \mathcal{O}_A[x]$, $f(T) =$ irred poly. for x over K,

then $\mathcal{D}_{L/K} = f'(x)\cdot\mathcal{O}_L$

and $\mathrm{disc}_{L/K} = N_{L/K}(f'(x))\cdot\mathcal{O}_K$

Example $\mathbb{Q}_2(\sqrt{d})/\mathbb{Q}_2$ is ramified if $d \equiv 0\ (2)$ or if $d \equiv -1 \pmod 4$

$0 \neq d =$ non-zero integer square-free

split $(= \mathbb{Q}_2)$ if $d \equiv 1 \pmod 8$

inert if $d \equiv 5 \pmod 8$

Note: When $d \equiv 1 \pmod{16} \rightsquigarrow \sqrt{d} \equiv \pm 1 \bmod 8$

$d \equiv 9 \pmod{16} \rightsquigarrow \sqrt{d} \equiv \pm 3 \bmod 8$

1) Suppose: $d \equiv -1 \pmod 4$

$\rightsquigarrow (\sqrt{d}+1)^2 = p+1+2\sqrt{d} = 2\big(\underbrace{\sqrt{d} + 2\cdot\tfrac{d+1}{4}}_{\text{a unit}}\big)$

$\Rightarrow \mathbb{Z}_2[\sqrt{d}] = \mathcal{O}_{\mathbb{Q}_2[\sqrt{d}]}$ and $\mathbb{Q}_2(\sqrt{d})/\mathbb{Q}_2$ is ramified.

2) Suppose $d \equiv 1 \pmod 4$

$\dfrac{\sqrt{d}+1}{2}$ and $\dfrac{-\sqrt{d}+1}{2}$ are root of $x^2 - x + \left(\frac{1-d}{4}\right) = 0$

(2a) If $d \equiv 1 \pmod 8 \underset{\text{Hensel's lemma}}{\Longrightarrow} \mathbb{Q}_2(\sqrt{d}) = \mathbb{Q}_2$ split

(2b) If $d \equiv 5 \pmod 8$

$\rightsquigarrow$ In $\mathcal{O}_{\mathbb{Q}_2(\sqrt{d})}/\mathfrak{m} = \tilde{\kappa}$, $\exists$ a root of $x^2 - x + \underbrace{\tfrac{d-1}{4}}_{\equiv 1 \bmod 2}$

So: $[\bar{\kappa} : \mathbb{F}_2] = 2$ inert

Note: May replace d by any element in $\mathbb{Z}_2$, either a unit or $2\cdot$(a unit)

What about $\mathbb{Q}_p(\sqrt{d})$ d = square-free

$p \geq 3$

(1) $d \equiv 0 \pmod{p} \iff \mathbb{Q}_p(\sqrt{d})/\mathbb{Q}_p$ is ramified ("$\Longrightarrow$" obvious)

(2) if d is a quad residue mod $p \Rightarrow \mathbb{Q}_p(\sqrt{d})/\mathbb{Q}_p$ is split

(Hensel's lemma)

(3) if d is a quad non-residue mod p

$\Rightarrow \mathbb{Q}_p(\sqrt{d})/\mathbb{Q}_p$ is inert (again = obvious)
