Algebraic Number Theory

- Number Fields - integrality, norm and trace, Dedekind Domains, ideal factorization and class group. lattices and Minkowski bound, Dirichlet's Unit Theorem

- Local Theory - p-adic numbers, completions, valuations and absolute values, extensions of valuations, Hensel's lemma, local and global fields, ramification of extensions

- Class Field Theory - adeles and ideles, statements of local and global class field theory, statement of Artin Reciprocity, statement of Chebotarev density

Polynomial Irreducibility

Gauss's Lemma

- $f \in \mathbb{Z}[x]$ nonconstant
- f primitive in $\mathbb{Z}[x]$, i.e. $\gcd(a_1, \dots, a_n) = 1$

$$\left.\begin{array}{l} \bullet\ f \in \mathbb{Z}[x] \text{ nonconstant} \\ \bullet\ f \text{ primitive in } \mathbb{Z}[x] \text{, i.e.} \\ \quad \gcd(a_1,\dots,a_n)=1 \end{array}\right\} \quad \begin{array}{c} f \text{ irreducible in } \mathbb{Z}[x] \\ \Updownarrow \\ f \text{ irreducible in } \mathbb{Q}[x] \end{array}$$

Root Theorem

$$\begin{aligned} f(x) &= x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0 \\ &= (x-\alpha_1)\cdots(x-\alpha_n) \\ &= x^n + \dots + (-1)^n \alpha_1 \cdots \alpha_n \end{aligned}$$

Can extend to non monic w/ $\alpha = p/q$ w/ $p \mid a_0$ and $q \mid a_n$

If f has an integer root α, then $\alpha \mid a_0$.

Example: f quadratic or cubic: f reducible $\Longleftrightarrow$ f has a root then check all divisors of a_0.

Eisenstein's Criterion

$$\left.\begin{array}{l} f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0 \\ \exists p \text{ s.t. } p \mid a_0, a_1, \dots, a_{n-1} \\ \qquad\quad p^2 \nmid a_0 \end{array}\right\} \begin{array}{l} f \text{ irreducible} \\ \text{over } \mathbb{Q} \end{array}$$

Can extend to $\mathbb{Q}_p$ or any int. domain and some prime ideal.

Cyclotomic Polynomial Trick

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} \text{ irreducible} \Longleftrightarrow \Phi_p(x+1) = \frac{(x+1)^p - 1}{x} \text{ irreducible}$$

and
$$\frac{(x+1)^p - 1}{x} = \frac{x^p + \binom{p}{1}x^{p-1} + \dots + \binom{p}{1}x + 1 - 1}{x} = \underbrace{x^{p-1} + px^{p-2} + \dots + p}_{\text{satisfies Eisenstein!}}$$

Galois Review

↱ irred $f \in K[x]$ no roots or all roots in L

L/K Galois $\iff$ L/K normal and separable

↳ no repeat roots ∀ min poly of elts in L. true for $K/\mathbb{Q}$.

$\iff |\mathrm{Aut}(L/K)| = [L:K]$

$\iff$ L is splitting field of (separable) polynomial in $K[x]$.

$\mathrm{Gal}(L/K) := \mathrm{Aut}(L/K)$.

Then M/L always Galois (subgroup of $\mathrm{Gal}(M/K)$)

If $\mathrm{Gal}(M/K)$ is normal, L/K is Galois

$\mathrm{Gal}(L/K) \simeq \mathrm{Gal}(M/K)/\mathrm{Gal}(M/L)$.

$$H \le \mathrm{Gal}(L/K) \longmapsto L^H = \{\alpha \in L : \sigma(\alpha) = \alpha \ \forall \sigma \in H\}$$

Galois's correspondence

$$\mathrm{Aut}(L/M) \le \mathrm{Gal}(L/K) \longleftarrow\!\!\shortmid K \subseteq M \subseteq L$$

↑ subgroup fixing M

Structure Theorems

Finitely Generated Abelian Groups

G fin. gen. (or just finite)

$$G \simeq \underbrace{\mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z} \oplus \dots \oplus \mathbb{Z}/n_k\mathbb{Z}}_{\text{torsion}} \oplus \underbrace{\mathbb{Z}^r}_{\text{torsion-free}}$$

r = rank of G

may assume $n_1 | n_2 | \dots | n_k$

Finitely Generated Modules / PID or DD

R a PID (or DD)

M fin gen Rmodule

$$M \simeq R/I_1 \oplus R/I_2 \oplus \dots \oplus R/I_k \oplus R^r$$

I_j are nonzero ideals of R

r = rank of M

Units of Cyclic Groups

p odd $(\mathbb{Z}/p^k\mathbb{Z})^\times \simeq \mathbb{Z}/\varphi(p^k)\mathbb{Z} = \mathbb{Z}/p^{k-1}(p-1)\mathbb{Z}$

$p = 2$ $(\mathbb{Z}/2^k\mathbb{Z})^\times \simeq \mathbb{Z}/2^{k-2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

n $(\mathbb{Z}/n\mathbb{Z})^\times = (\mathbb{Z}/p_1^{e_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p_m^{e_m}\mathbb{Z})^\times \simeq (\mathbb{Z}/p_1^{e_1}\mathbb{Z})^\times \times \dots \times (\mathbb{Z}/p_m^{e_m}\mathbb{Z})^\times$

Integrality

Defns

$A \subset B$ rings

- $b \in B$ is integral over A if $\exists f \in A[x]$ monic s.t.
  $f(b) = b^n + a_{n-1}b^{n-1} + \dots + a_1 b + a_0 = 0$. $(\deg f \geq 1)$
- B is integral over A if every $b \in B$ is
- $\bar{A} = \{ b \in B \mid b \text{ integral over } A \}$ (forms a ring!)
- A is integrally closed if $A = \bar{A}$ in $\mathrm{Frac}(A)$

Facts

- UFD $\Rightarrow$ Integrally closed $\leftarrow$
- PID $\Rightarrow$ UFD

$\left(\frac{a}{b}\right)^n + \dots + a_1\left(\frac{a}{b}\right) + a_0 = 0$

$a^n + \dots + a_1 a b^{n-1} + a_0 b^n = 0$

$a^n = b(\sim)$

but WMA no primes divide a and b

so b a unit $\Rightarrow a \in A$

- setup $\begin{cases} A \text{ int closed in } K = \mathrm{Frac}(A) \\ L/K \text{ fin field ext} \\ B = \text{int clos of } A \text{ in } L \end{cases}$

$$\begin{tikzcd} B \arrow[r, phantom, "\subseteq"] \arrow[d, dash] & L \arrow[d, dash] \\ A \arrow[r, phantom, "\subseteq"] & K \end{tikzcd}$$

B is integrally closed,

$b \in L$ integral/$A \iff P_b(x) \in A[x]$

- Number Theory Set up:

integral closure of $\mathbb{Z}$ in K $\rightarrow$

$$\begin{tikzcd} \mathcal{O}_K \arrow[r, phantom, "\subset"] \arrow[d, dash] & K \arrow[d, dash] \\ \mathbb{Z} \arrow[r, phantom, "\subset"] & \mathbb{Q} \end{tikzcd}$$

Norm and Trace

Defn

$L|K$ field ext.

$x \in L \rightsquigarrow T_x(\alpha) = x\alpha$

view T_x as matrix op in K-vector space.

$$\boxed{Tr_{L|K}(x) = Tr(T_x)} \qquad \boxed{N_{L|K}(x) = \det(T_x)}.$$

Alternatively: $L|K$ separable (e.g. $K/\mathbb{Q}$) with $\sigma : L \to \overline{K}$ varying over K-embeddings

$$\boxed{Tr_{L|K}(x) = \sum_{\sigma} \sigma x} \qquad \boxed{N_{L|K}(x) = \prod_{\sigma} \sigma x}$$

Properties

- $Tr_{L|K}(x+y) = Tr_{L|K}(x) + Tr_{L|K}(y)$
- $N_{L|K}(xy) = N_{L|K}(x) N_{L|K}(y)$
- $M/L/K \Rightarrow$ $N_{M|K} = N_{L|K} \circ N_{M/L}$
  $Tr_{M|K} = Tr_{L|K} \circ Tr_{M/L}$

Thm

$\mathcal{O}_K$ is a finitely generated $\mathbb{Z}$-module.

Pf $(x,y) \longmapsto Tr(xy)$ is nondegenerate bilinear pairing [use $(Tr(x_i x_j))$ for a basis $\{x_i\}$ and show $\det \neq 0$]
so take a basis $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$ of $K/\mathbb{Q}$. The pairing gives a dual basis $\alpha_1^*, \ldots, \alpha_n^*$ of $K/\mathbb{Q}$ with $Tr(\alpha_i \alpha_j^*) = \delta_{ij}$.
Take $\beta \in \mathcal{O}_K$ then $\beta = y_1\alpha_1^* + \ldots + y_n\alpha_n^*$ and $Tr(\alpha_i \beta) = y_i \in \mathbb{Z}$
so $\beta \in \mathbb{Z}\alpha_1^* + \ldots + \mathbb{Z}\alpha_n^*$ and since this is a $K/\mathbb{Q}$ basis
$\mathcal{O}_K$ is a finitely generated $\mathbb{Z}$-module (and also free)

Discriminant

Defns

- L/K separable, basis $\alpha_1, \dots, \alpha_n$, $\sigma_i : L \to \overline{K}$ embeddings

$$\boxed{d(\alpha_1, \dots, \alpha_n) = \det((\sigma_i \alpha_j))^2}$$

- If basis $1, \theta, \theta^2, \dots, \theta^{n-1}$

$$d(1, \theta, \dots, \theta^{n-1}) = \prod_{i<j} (\theta_i - \theta_j)^2 = \prod_{i \neq j} (\theta_i - \theta_j)$$

where $\theta_i = \sigma_i \theta$

by Vandermonde Matrix

$$\det \begin{pmatrix} 1 & \theta_1 & \cdots & \theta_1^{n-1} \\ 1 & \theta_2 & \cdots & \theta_2^{n-1} \\ \vdots & & \ddots & \vdots \\ 1 & \theta_n & \cdots & \theta_n^{n-1} \end{pmatrix}^2 = \prod_{i<j} (\theta_i - \theta_j)^2$$

Pf: $\det V$ is polynomial in θ_i's. Sub θ_i for θ_j, two equal row gives zero of $\det$ so $\theta_i - \theta_j$ is a root. Repeat for all $i \neq j$. Then compare single term to get constant coeff of 1.

- $w_1, \dots, w_n$ is an integral basis of B over A if each $b \in B$ can be written uniquely as $b = a_1 w_1 + \dots + a_n w_n$ for $a_i \in A$. (makes B a free A-module)
- $K/\mathbb{Q}$ number field with integral basis w_i of $\mathcal{O}_K / \mathbb{Z}$,

$$\boxed{d_K = \mathrm{disc}(K/\mathbb{Q}) = d(w_1, \dots, w_n) = \det((\sigma_i w_j))^2}$$

is the discriminant of $K/\mathbb{Q}$

Discriminant (cont.)

$f(x) = ax^2+bx+c \quad \Delta_f = b^2-4ac$

$f(x) = x^3+bx+c \quad \Delta_f = -4b^3-27c^2$

Relationship to Disc(f)

$$\mathrm{Disc}(f) = \prod_{i\neq j}(x_i-x_j) = \prod_{i<j}(x_i-x_j)^2 \text{ where } f(x) = \prod_{i=1}^{n}(x-x_i).$$

For $\mathbb{Z}[\alpha]/\mathbb{Z}$ with min poly $f(x)$ then

$$\mathrm{Disc}(\mathbb{Z}[\alpha]/\mathbb{Z}) = \pm\,\mathrm{Disc}(f).$$

and

$$\mathrm{Disc}(f) = \pm\,\mathrm{Disc}(\mathbb{Z}[\alpha]/\mathbb{Z}) = \pm(\mathcal{O}_K:\mathbb{Z}[\alpha])^2\,\mathrm{Disc}(\mathcal{O}_K/\mathbb{Z})$$

so

$$\boxed{|\mathrm{Disc}(f)| = (\mathcal{O}_K:\mathbb{Z}[\alpha])^2\,|\mathrm{Disc}(K/\mathbb{Q})|}$$

General Discriminant

$$\begin{tikzcd} & B \arrow[r, phantom, "\subset"] \arrow[d, dash] & L \arrow[d, dash] \\ \text{PID} \arrow[r] & A \arrow[r, phantom, "\subset"] & K \end{tikzcd}$$

$\Big\}$ then B is a free A-module, has an integral basis.

If no integral basis, let $n=[L:K]$ take all collections $\omega_1, \omega_2, \dots, \omega_n \in \mathcal{O}_L$

$$\mathrm{Disc}(L/K) = \big(d(\omega_1,\dots,\omega_n)\big)_{\{\omega_i\}} \longleftarrow \text{ideal!}$$

For any $\alpha_1,\dots,\alpha_n$, $\mathrm{Disc}(L/K) \mid (d(\alpha_1,\dots,\alpha_n))$ [use to get bounds on the ideal]

Special Case

$K=\mathbb{Q}(\alpha)$ with min poly $f(x)$ and $\mathcal{O}_K = \mathbb{Z}[\alpha]$

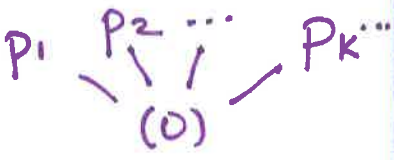
$$\mathrm{Disc}(K/\mathbb{Q}) = \pm\,\mathrm{Disc}(f) = \pm\prod_{i<j}(\alpha_i-\alpha_j)^2 = \pm N_{K/\mathbb{Q}}(f'(\alpha))$$

If $f(x)=x^n-a$ then $f'(x)=nx^{n-1}$ so $\pm N_{K/\mathbb{Q}}(f'(\sqrt[n]{a})) = \pm n^* a^*$.

Dedekind Domains

Defn

A **Dedekind Domain** is
- Noetherian (ideals are fin gen'd).
- integrally closed integral domain
- nonzero primes are maximal



Fact: $\mathcal{O}_K$ for $K/\mathbb{Q}$ is a dedekind domain

Fact:
$$\begin{tikzcd} S \arrow[r, phantom, "\subset"] \arrow[d, dash] & L \arrow[d, dash, "n"] \\ R \arrow[r, phantom, "\subset"] & K \end{tikzcd}$$
R Dedekind domain $\Longrightarrow$ S a dedekind domain
(Example $\mathcal{O}_L$ a dedekind domain)

Non-Examples

- Noetherian
- Integrally Closed
- NOT 1-dim

} $K[x,y]$
- R Noeth $\Longrightarrow$ (Hilberts Basis Thm) $R[x_1,\dots,x_n]$ Noeth
- R UFD $\Longrightarrow$ $R[x_1,\dots,x_n]$ UFD $\Longrightarrow$ $R[x_1,\dots,x_n]$ integrally closed
- $(0) \subsetneq (x) \subsetneq (x,y)$ prime, nonzero, not maximal

- NOT Noetherian
- integrally closed
- 1-dim

} $K[x^{1/2}, x^{1/4}, x^{1/8}, \dots]$ ↳ $\mathcal{O}_K$ over $\mathbb{Z}$
- $(x^{1/2}) \subsetneq (x^{1/4}) \subsetneq \dots$ breaks ACC
- int closure of $\mathbb{Z}$ $\Rightarrow$ int closed

Unique Ideal Factorization

(Fractional) Ideals have unique factorization $a = \prod_p p^{v_p}$.

Pf Sketch:

Exist $\mathcal{M} = \{a : a \text{ ideal w/o prime factorization}\}$ $\xrightarrow{\text{Noeth}}$ "maximal" ideal $a \in \mathcal{M}$ then $a \subseteq p$ and ap^{-1} ideal $\notin \mathcal{M}$ so has factor $\longrightarrow$ $a = p \prod p^{v_p}$.

Unique: Same as integers, $\prod p^{v_p} = \prod q^{v_q}$ then $p \mid q$ for some q. (both maximal so $p = q$)
$pp^{-1} = \mathcal{O}$ cancels product.

Ideal Class Group

Defns

- A *fractional ideal* $\mathfrak{a}$ is a fin gen'd $\mathcal{O}$-submodule of K. Equivalently, an $\mathcal{O}$-submodule of K with $c \in \mathcal{O}$ $(c \neq 0)$ s.t. $c\mathfrak{a} \subseteq \mathcal{O}$, is an ideal.
- The *ideal group* is J_K, set of all fractional ideals, $(\mathfrak{a})^{-1} = \mathfrak{a}^{-1}$ and identity (1).
  $\mathfrak{a}\mathfrak{b} = \{ \sum_i a_i b_i : a_i \in \mathfrak{a}, b_i \in \mathfrak{b} \}$
- The *ideal class group*, let P_K = principal frac ideals
  $\boxed{Cl_K = J_K / P_K}$ $\boxed{h_K = |Cl_K|}$ is the *class number*

Fact Class groups are finite

Pf: Minkowski Bound $\Rightarrow \forall [\cdot]\ \exists\, \mathfrak{a} \in [\cdot] \in Cl_K$ s.t. $\mathfrak{N}(\mathfrak{a}) \leq M_K$.
$\mathfrak{N}$ multiplicative so determine primes $\mathfrak{N}(\mathfrak{p}) = p^f \leq M_K$.
only finitely many $p^f \leq M_K$, and fin many $\mathfrak{p}$ over each p.

Example Nontrivial class group $\mathbb{Q}(\sqrt{-5})$, $Cl_K \simeq \mathbb{Z}/2\mathbb{Z}$

$M_K = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|d_K|} < 3$ so only $2^1 \leq M_K$,

check primes over 2 → Dedekind Kummer
→ Discriminant -20 $\}$ 2 ramifies as $\mathfrak{p}^2$.

so $\{[(1)], [\mathfrak{p}]\}$ generate Cl_K, and $[\mathfrak{p}]$ has order 2

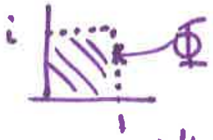
so $Cl_K \simeq \mathbb{Z}/2\mathbb{Z}$.

Lattice s

Defns

- A <u>lattice</u> in V (n-dim $\mathbb{R}$-vec. sp.) is a subgroup $\Gamma = \mathbb{Z}v_1 + \dots + \mathbb{Z}v_m$ linearly independent v_i
- $v_1, \dots, v_m$ are a <u>basis</u>, Γ <u>complete</u> when $m = n$
- The <u>fundamental mesh/region</u> $\Phi = \left\{ \begin{matrix} x_1v_1 + \dots + x_mv_m : \\ x_i \in \mathbb{R},\ 0 \le x_i < 1 \end{matrix} \right\}$
- Lattices are <u>discrete</u> subgroups, each $\gamma \in \Gamma$ has a nbhd in which $\mathcal{U} \cap \Gamma = \{\gamma\}$.
  lattice $\Longleftrightarrow$ discrete for subgroups of V
- the <u>volume of Γ</u> is $\boxed{\mathrm{vol}(\Gamma) = \mathrm{vol}(\Phi) = |\det(\langle v_i, v_j \rangle)|^{1/2}}$
- $X \subseteq V$ is <u>centrally symmetric</u> if $x \in X \Rightarrow -x \in X$
  <u>convex</u> if $x, y \in X \Longrightarrow$ line connecting $x, y \in X$ $\{tx + (t-1)y : t \in [0,1]\} \in X$

Examples



fundamental mesh

- $\mathbb{Z}[i] \subset \mathbb{C}$ is complete ($n=2$),
  $\mathrm{vol}(\Gamma) = \mathrm{vol}(\Phi) = \left|\det \begin{pmatrix} \langle 1,1 \rangle & \langle 1,i \rangle \\ \langle i,1 \rangle & \langle i,i \rangle \end{pmatrix}\right|^{1/2} = \left|\det \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\right|^{1/2} = 1$
- $\mathbb{Z} + \mathbb{Z}[\sqrt{2}] \subseteq \mathbb{R}$ is <u>not</u> a lattice (can get arbitrarily close)

Minkowski lattice Theorem

Γ complete lattice in V
$X \subseteq V$ centrally sym & convex
$\mathrm{vol}(X) > 2^n \mathrm{vol}(\Gamma) \Rightarrow \exists\, 0 \ne \gamma$
$\gamma \in \Gamma \cap X$.

Sharpness of Bound

$\Gamma = \mathbb{Z}[i]$ $X = (-1,1) \times (-1,1) \subseteq \mathbb{C}$
then $\mathrm{vol}(\Gamma) = 1$ $\mathrm{vol}(X) = 4 = 2^2 \mathrm{vol}(\Gamma)$
and $\Gamma \cap X = \{0\}$.

Minkowski Bounds

Set up $K \longrightarrow \prod_{\tau} \mathbb{C}$ for τ embeddings $K \hookrightarrow \overline{\mathbb{Q}}$.

$a \longmapsto (\tau a)_\tau$ — n dim $\mathbb{R}$-vector space once restricted to $\mathbb{R}$ for all real embeddings

(nonzero) $\mathfrak{a}$ ideal $\longmapsto$ complete lattice with volume $\sqrt{|d_K|}\,(\mathcal{O}_K : \mathfrak{a})$

$X = \{(z_\tau) : |z_\tau| < c_\tau\}$ for c_τ s.t. $\prod c_\tau > \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}\,(\mathcal{O}_K : \mathfrak{a})$

Minkowski Lattice Thm $\Rightarrow \exists\, \alpha \in \mathfrak{a}$, $|N_{K/\mathbb{Q}}(\alpha)| < \prod c_\tau \downarrow M_K(\mathcal{O}_K : \mathfrak{a})$.

Better space $X = \{(z_\tau) : \sum |z_\tau| < t\}$ gives better bound.

Minkowski Bound

Every nonzero ideal $\mathfrak{a}$ has a nonzero element α with

$$|N_{K/\mathbb{Q}}(\alpha)| \leq M_K(\mathcal{O}_K : \mathfrak{a}) = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|d_K|}\,(\mathcal{O}_K : \mathfrak{a}).$$

Class Group Minkowski Bound

Every $[\mathfrak{a}] \in Cl_K$ has an ideal rep with $\eta(\mathfrak{a}) \leq M_K$.

where $\eta(\mathfrak{a}) = (\mathcal{O}_K : \mathfrak{a})$ and $\eta(\mathfrak{p}) = p^f$

with $M_K = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|d_K|}$

Pf Idea:

Take any $\mathfrak{a} \in [\mathfrak{a}]$ and $\gamma \in \mathcal{O}_K$ s.t. $\gamma \mathfrak{a}^{-1} \subseteq \mathcal{O}_K$ is an ideal, $\mathfrak{b} = \gamma \mathfrak{a}^{-1}$.

Minkowski Bound gives $\alpha \in \mathfrak{b}$ s.t. $|N(\alpha)|\,\eta(\mathfrak{b})^{-1} \leq M_K$

$\mathfrak{c} = \alpha \mathfrak{b}^{-1} = \alpha \gamma^{-1} \mathfrak{a}$ has $\eta(\mathfrak{c}) = |N(\alpha)|\,\eta(\mathfrak{b}^{-1}) \leq M_K$

and $\alpha, \gamma \in \mathcal{O}_K$ so $[\mathfrak{c}] = [\mathfrak{a}]$.

Dirichlet's Unit Theorem

Theorem

$K/\mathbb{Q}$ number field

$\mathcal{O}_K$ ring of integers

r # of real embeddings

s # of complex embed pairs

$\mu(K)$ roots of unity in K

$$\boxed{\mathcal{O}_K^\times \simeq \mu(K) \times \mathbb{Z}^{r+s-1}}$$

Pf Sketch:

$$\begin{tikzcd}
\mathcal{O}_K^* \arrow[r] \arrow[d, phantom, sloped, "\subseteq"] & \{N(y)=\pm 1\} \arrow[r] \arrow[d, phantom, sloped, "\subseteq"] & \mathrm{Ker}(\mathrm{Tr}) \arrow[d, phantom, sloped, "\subseteq"] \\
K^* \arrow[r, "\alpha \mapsto (\tau\alpha)_\tau"] \arrow[d, "N_{K/\mathbb{Q}}"] & \prod_\tau \mathbb{C}^* \arrow[r, "(\alpha)_\tau \mapsto (\log|\alpha|)_\tau"] \arrow[d, "N"] & \prod_\tau \mathbb{R}^+ \arrow[d, "\mathrm{Tr}"] \\
\mathbb{Q}^* \arrow[r] & \mathbb{R}^* \arrow[r, "z \mapsto \log|z|"] & \mathbb{R}
\end{tikzcd}$$

1) $1 \to \mu(K) \to \mathcal{O}_K^* \xrightarrow{\lambda} \lambda(\mathcal{O}_K^*) = \Gamma \to 1$ exact.

$\mu(K) \subseteq \ker(\lambda)$: $\zeta \longmapsto \lambda(\zeta) = (\log|\tau\zeta|)_\tau = (\log|\zeta'|)_\tau = (\log|1|) = 0.$

$\ker(\lambda) \subseteq \mu(K)$: $\alpha \in \ker(\lambda)$ means $|\tau\alpha| = 1$ $\forall \tau$ embeddings (all conjugates)
If $m = \deg f_\alpha$ then only fin many poly with $\deg \leq m$
and coefficients bounded by roots, so the set
$\{1, \alpha, \alpha^2, \dots\}$ is finite (all roots of such polynomials)
and so α is a root of unity

2) $\dim \mathrm{Ker}(\mathrm{Tr}) = r+s-1$ and $\lambda(\mathcal{O}_K^*) = \Gamma$ is a complete lattice in $\mathrm{Ker}(\mathrm{Tr})$ so $\Gamma \simeq \mathbb{Z}^{r+s-1}$.

Example

$K = \mathbb{Q}(\sqrt{2})$ $\quad \varepsilon_1 = 1+\sqrt{2}$ $\quad \mathcal{O}_K^\times = \pm(1+\sqrt{2})^n \quad n \in \mathbb{Z}$

$r=2 \; s=0$

$r+s-1 = 1$

$\mu(K) = \{\pm 1\}$ $\quad \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$

Quadratic Reciprocity

Defn

- Given p odd prime $\left(\frac{a}{p}\right) = \begin{cases} 1 & a=\square \bmod p \ (a\neq 0 \bmod p) \\ -1 & a\neq\square \bmod p \\ 0 & a=0 \bmod p \end{cases}$

  Legendre Symbol $\nearrow$

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p \qquad \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

Quadratic Reciprocity

p, q distinct odd primes

$$\boxed{\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}}$$

Pf Idea $\tau_p = \sum_{k=1}^{p-1}\left(\frac{k}{p}\right)\zeta_p^k \in \mathbb{Q}(\zeta_p)$ Quadratic Gauss Sum

Express τ_p^q two ways using ① binomial theorem and ② Euler's criterion of $\left(\frac{k}{p}\right) = k^{\frac{p-1}{2}} \bmod p$.

Supplemental Laws

$$\boxed{\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}} \qquad \boxed{\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}}$$

Extensions of Number Fields

Set up

$$\begin{tikzcd} \mathcal{O}_L \arrow[r, phantom, "\subseteq"] \arrow[d, dash] & L \arrow[d, dash, "\text{finite}"] \\ \mathcal{O}_K \arrow[r, phantom, "\subseteq"] & K \end{tikzcd}$$

$\mathfrak{p}$ prime ideal of $\mathcal{O}_K$

$\mathfrak{q}_i \cap \mathcal{O}_K = \mathfrak{p}$
$\mathfrak{q}_i$ lies over $\mathfrak{p}$

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r}$$

factorization into primes in $\mathcal{O}_L$

e_i is the ramification index

$f_i = [\mathcal{O}_L/\mathfrak{q}_i : \mathcal{O}_K/\mathfrak{p}]$ is the inertia degree

Thm (L/K separable)

$$\boxed{[L:K] = n = \sum_{i=1}^{r} e_i f_i .}$$

← fundamental identity

Pf: By Chinese Remainder Thm $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \simeq \bigoplus_{i=1}^{r} \mathcal{O}_L/\mathfrak{q}_i^{e_i}$.

$\kappa = \mathcal{O}_K/\mathfrak{p}$ show

$\dim_\kappa(\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L) = n$
↓
take basis and lift to L, show basis of L/K.

$$\dim_\kappa(\mathcal{O}_L/\mathfrak{q}_i^{e_i}) = e_i f_i$$
↓
$$= \sum_{\nu=0}^{e_i-1} \dim(\mathfrak{q}_i^{\nu}/\mathfrak{q}_i^{\nu+1})$$
$$= \sum_{\nu=0}^{e_i-1} \dim(\mathcal{O}_L/\mathfrak{q}_i) = e_i f_i$$

Defns

- split completely means $r = [L:K]$ $e_i = f_i = 1$ $\mathfrak{p} = \mathfrak{q}_1 \cdots \mathfrak{q}_n$.
- ramified means some $e_i > 1$, totally ramified $e = n$ $\mathfrak{p} = \mathfrak{q}^n$.
- unramified means every $e_i = 1$, $\mathfrak{p} = \mathfrak{q}_1 \cdots \mathfrak{q}_r$.

Thm $p \in \mathbb{Q}$ ramifies in $K \iff p \mid \operatorname{Disc}(K/\mathbb{Q})$

Pf: In power basis case, $d_K = \prod_{i<j}(\theta_i - \theta_j)^2 = 0 \bmod p \iff \theta_i = \theta_j \bmod p$ for some $i \neq j$
$\iff p(x)$ repeat root
$\iff p$ ramifies (Ded-Ku)

Dedekind Kummer Theorem

Basic Theorem

$K = \mathbb{Q}(\alpha)$ with $\mathcal{O}_K = \mathbb{Z}[\alpha]$ and min poly $f(x)$.

$f(x)$ splits mod p the same as (p) splits in $\mathcal{O}_K$

$\left[\bar{f}(x) = f_1^{e_1}(x) \cdots f_r^{e_r}(x) \text{ then } q_i = (p)\mathcal{O}_K + f_i(\alpha)\mathcal{O}_K\right]$

and the inertia degrees is the degree of f_i.

Pf Idea:

$$\mathcal{O}_K/(p) \underset{\substack{\uparrow \\ \mathbb{Z}[x]/(f(x))/(p)}}{\cong} \mathbb{F}_p[x]/(\bar{f}(x)) \underset{\substack{\uparrow \\ \text{CRT}}}{\cong} \bigoplus_{i=1}^{r} \mathbb{F}_p[x]/(f_i^{e_i}(x))$$

Extension

Holds for other K as long as $p \nmid \underbrace{[\mathcal{O}_K : \mathbb{Z}[\alpha]]}_{\text{conductor of } \mathbb{Z}[\alpha].}$

Example

Q: How does (2) split in $\mathbb{Q}(\sqrt{7})$?

A: $\mathcal{O}_K = \mathbb{Z}[\sqrt{7}]$ since $7 \equiv 3 \bmod 4$

so $f(x) = x^2 - 7 \equiv x^2 + 1 = (x+1)^2 \bmod 2$

so $(2) = \mathfrak{p}^2$ in $\mathcal{O}_K$ for $K = \mathbb{Q}(\sqrt{7})$.

Galois Extensions

Set up

$$\begin{tikzcd}
q_1^{e_1}\cdots q_r^{e_r} \subseteq \arrow[d, dash] & O_L \arrow[d, dash] \subseteq & L \arrow[d, dash, "\text{fin Galois}"] \\
p \subseteq & O_K \subseteq & K
\end{tikzcd}$$

$G = Gal(L/K)$

$G \curvearrowright \{q_1, \dots, q_r\}$ transitively

so $e_i = e, f_i = f \ \forall i$ $\boxed{[L:K] = ref}$

Defns

- Given $q \subseteq O_L$, $G_q = \{\sigma \in Gal(L/K) : \sigma(q) = q\}$ is the decomposition group of q. The subfield of L fixed by G_q is its decomposition field
- Take $\sigma \in G_q$ then σ acts on O_L/q and fixes O_K/p so $G_q \longrightarrow Gal(O_L/q \,/\, O_K/p)$ surjective map. The kernel is $I_q \subseteq G_q$ ($I_q = \{\sigma : \sigma(\alpha) = \alpha \bmod q \ \forall \alpha \in O_L\}$) the inertia subgroup of q.

Properties

$$\begin{tikzcd}
q \in \arrow[d, dash] & M \arrow[d, dash] \\
p \in \arrow[d, dash] & L \arrow[d, dash] \\
p \in & K
\end{tikzcd}$$

$$\left[\begin{array}{l} G_q(M/L) = G_q(M/K) \cap Gal(M/L) \\ I_q(M/L) = I_q(M/K) \cap Gal(M/L) \end{array}\right.$$

$$\left[\begin{array}{l} G_p(L/K) = G_q(M/K)/Gal(M/L) \\ I_p(L/K) = I_q(M/K)/Gal(M/L) \end{array}\right.$$

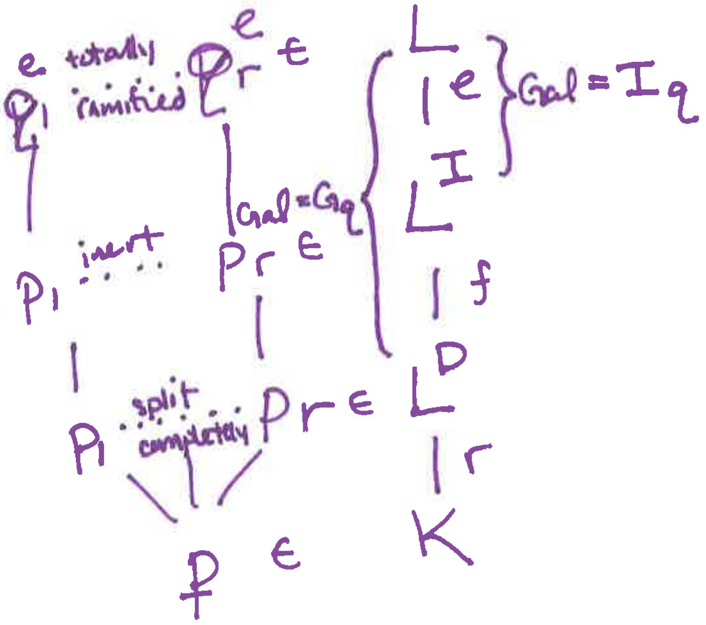
Recall $Gal(L/K) \cong Gal(M/K)/Gal(M/L)$.

If $K/\mathbb{Q}$, $G_q/I_q \simeq Gal(O_K/q/\mathbb{F}_p) = \underline{\underline{cyclic}}$

$$G_{\sigma q} = \sigma G_q \sigma^{-1}$$

More generally, if L/K

$$G_p(L/K) \simeq Gal(L_p/K_p)$$



$|I_q| = e$

$|G_q| = ef$

Quadratic Fields

Set up

D a □-free integer $(D \neq 0,1)$

$K = \mathbb{Q}(\sqrt{D})$.

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right] & D \equiv 1 \bmod 4 \\ \mathbb{Z}[\sqrt{D}] & D \equiv 2,3 \bmod 4 \end{cases} \qquad d_K = \begin{cases} D \\ 4D \end{cases}$$

Pf: Take $\frac{a}{b} + \frac{c}{d}\sqrt{D} \in \mathbb{Q}(\sqrt{D})$ find minimal polynomial modular conditions to determine if $\frac{a}{b}, \frac{c}{d} \in \mathbb{Z}$ or $b = d = 2$ and $a \equiv c \bmod 2$. Then use integral basis to compute discriminant.

Pell's Equation (Application)

$1 = x^2 - y^2 n$ for n positive nonsquare integer.

Take $K = \mathbb{Q}(\sqrt{n})$. Dirichlet's Unit Theorem says $\mathcal{O}_K^* = \mu(K) \times \mathbb{Z}^{r+s-1} = \mu(K) \times \mathbb{Z}$ so $\exists\, \varepsilon \in \mathcal{O}_K^*$ with $N(\varepsilon) = N(a+b\sqrt{n}) = (a+b\sqrt{n})(a-b\sqrt{n}) = a^2 - b^2 n = \pm 1$.

If -1, taking even powers gives infinitely many solutions to the Pell Equation. [If $n=1 \bmod 4$ may need higher powers to clear denominator of $1/2$].

Cyclotomic Fields

Defns

- ζ_n is a primitive n^{th} root of unity if $\zeta_n^n = 1$ and ζ_n generates all other roots (ζ_n^k $k=1,\dots,n$) $\boxed{\zeta_n = e^{2\pi i/n}}$
- Φ_n is the n^{th} cyclotomic polynomial, the minimal polynomial for ζ_n. $x^n - 1 = \prod_{d|n} \Phi_d$.

$$\boxed{\Phi_p(x) = 1 + x + x^2 + \dots + x^{p-1}} \longrightarrow = \frac{x^p - 1}{x - 1}$$

$\boxed{\deg \Phi_n = \varphi(n)}$ pf by counting primitive roots.

$\varphi(n) = \#\{1 \le d \le n : \gcd(d,n) = 1\}$ $\boxed{\varphi(p^k) = p^{k-1}(p-1)}$

Cyclotomic Fields

$K = \mathbb{Q}(\zeta_n)$

$\mathcal{O}_K = \mathbb{Z}[\zeta_n]$

$\mathrm{Gal}(K/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$

$p \mid \mathrm{Disc}(K/\mathbb{Q}) \Rightarrow p \mid n$

$K = \mathbb{Q}(\zeta_p)$

$\mathcal{O}_K = \mathbb{Z}[\zeta_p]$

$\Phi_p = 1 + x + \dots + x^{p-1} = \frac{x^p - 1}{x - 1}$

$\mathrm{Gal}(K/\mathbb{Q}) \simeq (\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{Z}/p-1\mathbb{Z}$.

$\mathrm{Disc}(K/\mathbb{Q}) = p^\ell$ for some $\ell \in \mathbb{Z}^+$.

$\mu(K) = \{$all p^{th} roots of unity$\}$

p-adic Numbers

Defns

$\leftarrow$ formal sum

- p-adic integer $\alpha = \underbrace{a_0 + a_1 p + a_2 p^2}_{} + \dots = \sum_{n=0}^{\infty} a_n p^n \in \mathbb{Z}_p$ $a_i \in [0,1,\dots,p-1]$
  $\alpha \in \mathbb{Z}$ or $\mathbb{Z}_{(p)} \to \mathbb{Z}_p$. unique rep mod p^n
- p-adic number $\alpha = a_{-m}p^{-m} + \dots + a_{-1}p^{-1} + a_0 + a_1 p + \dots = \sum_{n=-m}^{\infty} a_n p^n \in \mathbb{Q}_p$ $a_i \in [0,1,\dots,p-1]$
  $\alpha = p^{-m}\beta$ for some $\beta \in \mathbb{Z}_p$.
- p-adic valuation $\nu_p(a) = \nu_p(p^m \frac{b}{c}) = m$ where $p \nmid b,c$
  $|a|_p = p^{-\nu_p(a)}$

Representations of $\mathbb{Z}_p$

	formal sums	projective limit	p-adic completion
$\mathbb{Z}_p$	$\alpha = \sum_{n=0}^{\infty} a_n p^n$ $\simeq$ $a_i \in [0,1,\dots,p-1]$	$\varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$ $\simeq$ represent by residues mod p^n	$\{x \in \mathbb{Q}_p : \lvert x \rvert_p \leq 1\}$ w/ $\mathbb{Q}_p$ completion of $\mathbb{Q}$ w.r.t. p-adic val.
$\mathbb{Q}_p$	$\beta = p^{-m}\alpha$	field of frac of $\mathbb{Z}_p$	completion of $\mathbb{Q}$

Structure of $\mathbb{Z}_p$

- $\mathbb{Z}_p^* = \{x \in \mathbb{Z}_p \mid |x|_p = 1\}$
- $\mathbb{Q}_p^*$ unique reps by $p^m u$
  w/ $m \in \mathbb{Z}$ $u \in \mathbb{Z}_p^*$
- $|\cdot|_p$ extends to $\mathbb{Q}_p$ by
  $x = \{x_n\}$
  $|x|_p = \lim_{n\to\infty} |x_n|_p$

and $\nu_p(\mathbb{Q}_p) = \mathbb{Z} \cup \{\infty\}$

- max/prime ideal in $\mathbb{Z}_p$
  $p\mathbb{Z}_p = \{x \in \mathbb{Z}_p : |x|_p < 1\}$
- all ideals are $p^n\mathbb{Z}_p$ for $n \in \mathbb{N}$.
  $\mathbb{Z}_p/p^n\mathbb{Z}_p \simeq \mathbb{Z}/p^n\mathbb{Z}$.
- $\mathbb{Q}_p$ is complete, meaning every cauchy sequence (wrt $|\cdot|_p$) converges to a limit in $\mathbb{Q}_p$.

Valuations

Multiplicative Valuations (Absolute Values)

$|\cdot| : K \to \mathbb{R}$

(i) $|x| \geq 0$, $|x| = 0 \iff x = 0$

(ii) $|xy| = |x||y|$

(iii) $|x+y| \leq |x| + |y|$ Triangle Inequality

$|\cdot|_1 \sim |\cdot|_2 \iff \exists s \in \mathbb{R}^+$ s.t. $|x|_1 = |x|_2^s$ $\forall x \in K$.

$|x| = q^{-\nu(x)}$ for fixed $q > 1$

Additive Valuations (Exponential Valuations)

$\nu : K \to \mathbb{R} \cup \{\infty\}$

(i) $\nu(x) = \infty \iff x = 0$

(ii) $\nu(xy) = \nu(x) + \nu(y)$

(iii) $\nu(x+y) \geq \min\{\nu(x), \nu(y)\}$

$\nu_1 \sim \nu_2 \iff \exists s \in \mathbb{R}^+$ s.t. $\nu_1 = s\nu_2$.

$\nu(x) = -\log|x|$ ($\nu(0) = \infty$)

Defns

- $|\cdot|$ is nonarchimedean if $|n|$ bounded for all $n \in \mathbb{N}$ (e.g. $|\cdot|_p$)
- $|\cdot|$ is archimedean if $|n|$ unbounded for $n \in \mathbb{N}$ (e.g. $|\cdot|_{\mathbb{R}}$)
- Strong Triangle Inequality $|x+y| \leq \max\{|x|, |y|\}$ & $|x+y| = \max\{|x|, |y|\}$ when $|x| \neq |y|$
- ν is discrete if $\nu(K^\times) = s\mathbb{Z}$ (admits smallest positive value s)
- ν is normalized if $\nu(K^\times) = \mathbb{Z}$ (smallest pos. value is 1)

Facts

- $|\cdot|$ is nonarchimedean $\iff$ $|\cdot|$ satisfies strong triangle inequality
- Valuations on $\mathbb{Q}$ (up to equivalence) are $|\cdot|_p$ for primes p and $|\cdot|_\infty$.
- Approximation Theorem (generalizes CRT)

  $|\cdot|_1, |\cdot|_2, \dots, |\cdot|_n$ pairwise inequivalent on K

  $a_1, a_2, \dots, a_n \in K$. $\forall \varepsilon > 0$ $\exists x \in K$ s.t. $|x - a_i|_i < \varepsilon$ $\forall i = 1, 2, \dots, n$.
- Product Formula: for $a \neq 0$ $\prod_p |a|_p = 1$ all places of K (in $\mathbb{Q}$, $|\cdot|$ and $|\cdot|_p$ $\forall p$ prime)

  Pf: $\dfrac{\prod_{\infty} |a|}{\prod_{fin} |a|} = \dfrac{N(a)}{N(a)} = 1.$

Completions

Defns

- $(K, |\ |)$ is a complete valued field (wrt $|\ |$) if every cauchy sequence (wrt $d(x,y) = |x-y|$) converges to $\alpha \in K$.
- Given K with absolute value $|\ |$, let R = all cauchy sequences, and $\mathfrak{m}$ = all nullsequences ($\to 0$), then the completion is $\hat{K} = R/\mathfrak{m}$ w/ $K \to \hat{K}$ by $a \mapsto (a, a, a, \dots)$. and extend $|\ |$ to $\hat{K}$ by $|\{x_n\}| = \lim_{n \to \infty} |x_n|$.

Facts

- $\hat{K}$ is complete wrt the extension of $|\cdot|$.
- completions are unique up to isomorphism
- Ostrowski's Theorem: the only complete fields wrt an archimedean valuation are $\mathbb{R}$ and $\mathbb{C}$ (up to isomorphism).
- K is complete wrt $|\cdot|_K$, and L/K a finite alg ext, then $|\cdot|_K$ extends uniquely to $|\alpha|_L = \sqrt[n]{|N_{L/K}(\alpha)|_K}$.

Hensel's lemma

Basic Theorem

If $f \in \mathbb{Z}_p[X]$ and $a_0 \in \mathbb{Z}/p\mathbb{Z}$ s.t.
$$\left.\begin{array}{l} f(a_0) \equiv 0 \mod p \\ f'(a_0) \not\equiv 0 \mod p \end{array}\right\} \exists \alpha \in \mathbb{Z}_p \text{ unique lift of } a_0 \ (\alpha \equiv a_0 \bmod p) \text{ s.t. } f(\alpha) = 0 \text{ in } \mathbb{Z}_p.$$

Pf Idea: Newton's Method

$$f'(a_0) = \frac{f(a_0) - f(a_1)}{a_0 - a_1} \approx \frac{f(a_0)}{a_0 - a_1} \rightarrow a_1 = a_0 - \frac{f(a_0)}{\underbrace{f'(a_0)}_{\neq 0 \text{ so invertible.}}}$$

Iterate and define $\alpha = \lim_{n \to \infty} a_n$.

Generalizations

- $f \in \mathbb{Z}_p[x]$ $a_0 \in \mathbb{Z}/p\mathbb{Z}$ s.t. $|f(a_0)|_p < |f'(a_0)|_p^2$ $\Big\}$ $\exists \alpha \in \mathbb{Z}_p$ unique lift of a_0 ($\alpha \equiv a_0 \bmod p$) s.t. $f(\alpha) = 0$ in $\mathbb{Z}_p$
- $f \in \mathbb{Z}_p[x]$, $f \not\equiv 0 \bmod p$ $\bar{f}(x) = \bar{g}(x)\bar{h}(x)$ in $\mathbb{Z}/p\mathbb{Z}[x]$ w/ $\bar{g}, \bar{h}$ relatively prime $\Big\}$ $f = g \cdot h \in \mathbb{Z}_p[x]$ w/ $g = \bar{g} \bmod p$, $h = \bar{h} \bmod p$ $\deg(g) = \deg(\bar{g})$ $\deg(h) = \deg(\bar{h})$.

Examples

- $\sqrt{7} \in \mathbb{Q}_3$

  $f(x) = x^2 - 7 \equiv x^2 - 1 = (x+1)(x-1)$ in $\mathbb{Z}/3\mathbb{Z}$. ± 1 distinct (i.e. simple) roots in $\mathbb{Z}/3\mathbb{Z}$, so each lifts to $\alpha \in \overset{\mathbb{Z}_p}{\mathbb{Q}_3}$ s.t. $\alpha^2 = 7$.

- $\sqrt{5} \notin \mathbb{Q}_3$

  $f(x) = x^2 - 5 \equiv x^2 + 1$ has no roots so no $\alpha \in \mathbb{Z}_p$ w/ $\alpha^2 = 5$.

  If $\beta \in \mathbb{Q}_3$, w/ $\beta^2 = 5$ then $|\beta|_3^2 = |\beta^2|_3 = |5|_3 \leq 1$ so $|\beta| \leq 1 \Rightarrow \beta \in \mathbb{Z}_p$ ↯

Extensions of Valuations

$$\begin{tikzcd} |\cdot|_w \arrow[d, dash] & L \arrow[d, dash] \\ |\cdot|_v & K \end{tikzcd}$$

each embedding $\tau : L \hookrightarrow \overline{K_v}$ gives a valuation $|\alpha|_w = |\tau\alpha|_v$.

For $K = \mathbb{Q}$, $\overline{K_v} = \mathbb{C}, \overline{\mathbb{Q}_p}$.

Two valuations are equivalent if $\exists \sigma : \overline{K_v} \to \overline{K_v}$ such that $\tau = \sigma \circ \tau'$.

Theorem (Dedekind-Kummer-ish)

$L = K(\alpha)$ with min poly $f(x) \in K[x]$.

valuations $w_1, \ldots, w_r$ extending v correspond to irreducible factor $f_1, \ldots, f_r$ in $f(x) = f_1(x)^{m_1} \cdots f_r(x)^{m_r} \in K_v[x]$.

Pf Idea Each root of f gives a valuation, but roots that are conjugate over K_v (same $f_i(x)$ factor) give the same.

Fundamental Identity

if v discrete (e.g. p-adic)

$$[L:K] = \sum_{w|v} [L_w : K_v] = \sum_{w|v} e_w f_w = \sum_{w|v} (w(L^*) : v(K^*))[\lambda_w : K_v]$$

Tame Ramification

L/K with $p = \mathrm{char}(K/\mathfrak{p}) = \mathrm{char}(\kappa)$

tamely ramified if $(e, p) = 1$.

"Tame Inertia is cyclic". $I_q = \mathbb{Z}/e\mathbb{Z}$ when $p \nmid e$.

Profinite & Topological Groups

	Topological Groups	Profinite Groups
Defns	Group G with a topology s.t. $(x,y)\mapsto xy$ and $x\mapsto x^{-1}$ are continuous maps	A topological group that is Hausdorff () and compact w/ a basis of nbhds of $1\in G$ that are normal subgroups.
Examples	• $\mathbb{R}$ (or $\mathbb{R}^n$) w/ Euclidean topology under addition • Any group G w/ discrete top. • Galois Group $\mathrm{Gal}(L/K)$ with $\sigma\,\mathrm{Gal}(L/M)$ for fin M/K e.t. basis of nbhds for $\sigma\in\mathrm{Gal}(L/K)$ "Krull Topology"	• finite groups (w/ disc topology) • $\mathbb{Z}_p=\varprojlim_{n}\mathbb{Z}/p^n\mathbb{Z}$ and $\hat{\mathbb{Z}}=\varprojlim_{n}\mathbb{Z}/n\mathbb{Z}$ • $\mathrm{Gal}(K^{sep}/K)=\varprojlim_{\substack{L\text{ fin}\\ L/K\text{ sep}}}\mathrm{Gal}(L/K)$
Properties	• $H\simeq gH$ (homeomorphic) i.e. remains open/closed • open subgroups are closed $H^c=\bigcup_{g\notin H} gH$ = union of opens • closed finite index subgroups are open $H=(H^c)^c=(\underbrace{g_1H\cup\cdots g_nH}_{\text{closed}})^c$	• G profinite implies $G\cong\varprojlim_{N} G/N$ N over all fin. index open normal subgroups • The profinite completion $\hat{G}=\varprojlim_{N} G/N$ is profinite. • Given system of G_i's finite/profinite $\varprojlim_{i} G_i$ is profinite (ex: $\mathbb{Z}/n\mathbb{Z}$ or $\mathbb{Z}/p^n\mathbb{Z}$)

Adeles & Ideles

Defns $K/\mathbb{Q}$ a number field

- The Adele ring (or adeles) is the restricted product

$$\mathbb{A}_K = \prod_{p}{}' K_p \text{ w.r.t } \mathcal{O}_p$$

p ← all places, fin + infinite of K

restricted ↓ all but finitely many coordinates lie in $\mathcal{O}_p$, the valuation ring of K_p.

- The ideles are the unit group of $\mathbb{A}_K^\times$, i.e.

$$I_K = \prod_p{}' K_p^\times \text{ w.r.t } \mathcal{O}_p^\times$$

- Since $K \hookrightarrow K_p$ we define $K^\times \hookrightarrow I_K$ by $\alpha \longmapsto (\alpha_p)_p$ lies in the restricted product since $\alpha_p \notin \mathcal{O}_p^\times \Leftrightarrow \underbrace{p \mid \alpha_p^{-1}}_{\text{finite collection}}$

Then $C_K := I_K / K^\times$ is the idele class group

Properties:

- $\mathbb{C}_K \twoheadrightarrow Cl_K$ by $(\alpha_p)_p K^\times \longmapsto \prod_{p \text{ finite}} p^{v_p(\alpha_p)}$] finite product by restricted product.

- $N_{L/K} : C_L \to C_K$ for L/K where $\alpha = (\alpha_\beta) \in I_L$ maps to

$$N_{L/K}(\alpha) = \prod_p \Big(\prod_{\beta \mid p} N_{L_\beta / K_p}(\alpha_p) \Big)$$

This ① maps principal ideles to principal ideles (well-defined on C_L)

② composes in towers of extensions

③ $N_{L/K}(\alpha) = \prod_{\sigma \in Gal(L/K)} \sigma\alpha$ and $\alpha \in I_K$ then $N_{L/K}(\alpha) = \alpha^{[L:K]}$.

Structure Theorems for CFT

- $$\mathbb{Q}_p^\times = p^{\mathbb{Z}}\mathbb{Z}_p^\times \simeq p^{\mathbb{Z}} \times \mu_{p-1} \times 1+p\mathbb{Z}_p \cong \overbrace{\mathbb{Z}\times\mathbb{Z}/p-1\mathbb{Z}\times\mathbb{Z}_p}^{\text{w/ addition}}$$
  $$1+p\mathbb{Z}_p \xrightarrow{\log(\cdot)} \mathbb{Z}_p$$

K local field (e.g. $K/\mathbb{Q}_p$), uniformizer π, $q = \#\mathcal{K} = \#\mathcal{O}_K/(\pi)$.

- $$K^\times = \pi^{\mathbb{Z}}\mathcal{O}_K^\times = \pi^{\mathbb{Z}} \times \mu_{q-1} \times \mathcal{U}^{(1)} = \pi^{\mathbb{Z}} \times \mu_{q-1} \times 1+\pi\mathcal{O}_K$$
  $$\simeq \mathbb{Z} \times \mathbb{Z}/q-1\mathbb{Z} \times \mathbb{Z}/p^a\mathbb{Z} \times \mathbb{Z}_p^{[K:\mathbb{Q}_p]} \quad \text{(for some } a\text{)}$$

- $$(\mathbb{Z}_p^\times)^2 \simeq 2\begin{cases}(\mathbb{Z}/p-1\mathbb{Z} \times \mathbb{Z}_p) \\ (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2)\end{cases} \cong \begin{cases} 2\mathbb{Z}/p-1\mathbb{Z} \times \mathbb{Z}_p & p \text{ odd} \\ 1 \times 2\mathbb{Z}_2 & p=2\end{cases}$$

so $$\mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^2 \simeq \begin{cases}\mathbb{Z}/2\mathbb{Z} & p \text{ odd} \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & p=2\end{cases}$$

- $$C_{\mathbb{Q}}/\overset{\substack{\text{connected}\\\text{component}\\\text{of } 1\in C_{\mathbb{Q}}}}{\mathbb{R}^+} \simeq \prod_p \mathbb{Z}_p^\times \quad (r\in\mathbb{R}^+ \longmapsto (1,\dots,1,r)\mathbb{Q}^\times \in C_{\mathbb{Q}} = \textstyle\prod_p{}' \mathbb{Q}_p^\times \times \mathbb{R}^\times/\mathbb{Q}^\times)$$

$$\prod_p \mathbb{Z}_p^\times \longrightarrow C_{\mathbb{Q}}/\mathbb{R}^+ = (\textstyle\prod_p{}' \mathbb{Q}_p^\times \times \mathbb{R}^\times/\mathbb{R}^+)/\mathbb{Q}^\times$$
$$(z_p)_p \longmapsto (z_p,\dots,z_p,1)\mathbb{Q}^\times$$

injective:

$(z_p,\dots,z_p,1)\mathbb{Q}^\times = (z_p',\dots,z_p',1)\mathbb{Q}^\times$ means $\exists\alpha\in\mathbb{Q}^\times$ s.t. $z_p = \alpha z_p'$ $\forall p$, and $\alpha>0$ (so $\alpha \to 1 \in \mathbb{R}^\times/\mathbb{R}^+$). In $\mathbb{Z}_p^\times$, $\alpha = z_p/z_p' \in \mathbb{Z}_p^\times$ so no primes divide α, and $\alpha>0$ so $\alpha=1$ and $(z_p)_p = (z_p')_p \in \prod_p \mathbb{Z}_p^\times$.

surjective:

take $(\alpha_p,\dots,\alpha_p,\pm1)\mathbb{Q}^\times \in C_{\mathbb{Q}}/\mathbb{R}^+$. can assume $+1$ by scaling by $\pm1\in\mathbb{Q}^\times$. By restricted product, only fin many $\alpha_p \in \mathbb{Q}_p^\times \setminus \mathbb{Z}_p^\times$. Take $q\in\mathbb{Q}^\times$ that puts $q\alpha_p \in \mathbb{Z}_p^\times$ for those p. Then $(q\alpha_p,\dots,q\alpha_p,1)\mathbb{Q}^\times = (\alpha_p,\dots,\alpha_p,1)\mathbb{Q}^\times$ and $(q\alpha_p)_p \in \prod_p \mathbb{Z}_p^\times \mapsto (\alpha_p,\dots,\alpha_p,1)\mathbb{Q}^\times$.

Local Class Field Theory

K a local field (e.g. $K/\mathbb{Q}_p$)

Local Artin Map

max abelian ext $= \varprojlim_{\substack{L \\ \text{fin ab.}}} \mathrm{Gal}(L/K)$

$$\Theta_K : K^\times \longrightarrow \mathrm{Gal}(K^{ab}/K) \qquad \left(\Theta_K : \widehat{K^\times} \xrightarrow{\sim} \mathrm{Gal}(K^{ab}/K)\right)$$

profinite completion

$$K^\times = \pi^{\mathbb{Z}} \mathcal{O}_K^\times \simeq \mathbb{Z} \times \mathcal{O}_K^\times \qquad \Theta_K(\mathcal{O}_K^\times) = \mathrm{Gal}(K^{ab}/K^{unr})$$

$= $ Inertia subgroup

Abelian Extensions

L/K finite abelian extension

$$K^\times \longrightarrow \mathrm{Gal}(K^{ab}/K) \xrightarrow{\text{res}} \mathrm{Gal}(L/K)$$

induces $\Theta_{L/K} : K^\times / N_{L/K}(L^\times) \simeq \mathrm{Gal}(L/K)$

inclusion reversing bijection:

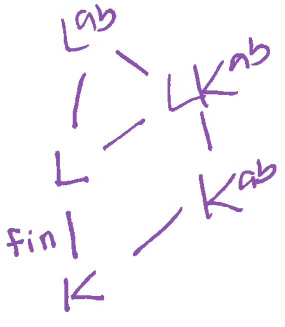
$$\left\{ \begin{matrix} \text{fin abel} \\ L/K \end{matrix} \right\} \underset{K^\times/N \simeq \mathrm{Gal}(L/K) \ \leftarrow\!\shortmid \ N}{\overset{L \ \mapsto \ N_{L/K}(L^\times)}{\longleftrightarrow}} \left\{ \begin{matrix} \text{fin.-index} \\ \text{open subgrps} \\ \text{of } K^\times \end{matrix} \right\}$$

- $N_{LM} = N_L \cap N_M$
- $N_{L\cap M} = N_L N_M$

$\Theta_{L/K}(\mathcal{O}_K^\times) = I_{L/K}$ inertia subgroup of $\mathrm{Gal}(L/K)$.

any π maps to a frobenius element of $\mathrm{Gal}(L/K)$

Functoriality



$$\begin{tikzcd} L^\times \arrow[r, "\Theta_L"] \arrow[d, "N_{L/K}"'] \arrow[dr, phantom, "\boxed{\text{commutes}}"] & \mathrm{Gal}(L^{ab}/L) \arrow[d, "\text{res.}"] \\ K^\times \arrow[r, "\Theta_K"] & \mathrm{Gal}(K^{ab}/K) \end{tikzcd}$$

Uniqueness

$\phi_K : K^\times \longrightarrow \mathrm{Gal}(K^{ab}/K)$ is the unique group hom s.t.

(i) $\forall\, L/K$ unramified, π unif of K

$\phi_K(\pi) \longrightarrow \mathrm{Frob} \in \mathrm{Gal}(L/K)$

(ii) L/K fin abelian

$\ker(K^\times \to \mathrm{Gal}(K^{ab}/K) \twoheadrightarrow \mathrm{Gal}(L/K))$

$= N_{L/K}(L^\times)$ inducing isom.

$\phi_{L/K} : K^\times / N_{L/K}(L^\times) \xrightarrow{\sim} \mathrm{Gal}(L/K)$.

Global Class Field Theory

$K/\mathbb{Q}$ a number field

Global Artin Map

max abelian ext.

$$\Theta_K : C_K = I_K/K^\times \twoheadrightarrow Gal(K^{ab}/K)$$

- kernel is connected component of $1 \in C_K$, and
- induces isomorphism $\hat{\Theta}_K : \hat{C}_K \xrightarrow{\sim} Gal(K^{ab}/K)$ [profinite completion]

Abelian Extensions

L/K finite abelian extension

$N_{L/K} : C_L \to C_K$ by $(\alpha_p)_p L^\times \mapsto \left(\prod_{p|q} N_{L_p/K_q}(\alpha_p)\right)_q K^\times$

$$C_K \longrightarrow Gal(K^{ab}/K) \overset{res}{\twoheadrightarrow} Gal(L/K)$$

induces $\Theta_{L/K} : C_K/N_{L/K}(C_L) \simeq Gal(L/K)$

inclusion reversing bijection: $\left\{\begin{matrix}\text{fin. abel.}\\ L/K\end{matrix}\right\} \overset{L \mapsto N_{L/K}(C_L)}{\underset{C_K/N \cong Gal(L/K) \leftarrow\!\shortmid\, N}{\longleftrightarrow}} \left\{\begin{matrix}\text{fin. index}\\ \text{open subgrps}\\ \text{of } C_K\end{matrix}\right\}$

- $D_p(L/K) = \Theta_{L/K}(K_p^\times)$
- $I_p(L/K) = \Theta_{L/K}(\Theta_p^\times)$

Functoriality

$$\begin{tikzcd}
L^{ab} \arrow[d, dash] \arrow[dr, dash] & \\
L \arrow[dd, dash] & LK^{ab} \arrow[d, dash] \\
 & K^{ab} \arrow[dl, dash] \\
K &
\end{tikzcd}$$

$$\begin{tikzcd}
C_L \arrow[r, "\Theta_L"] \arrow[d, "N_{L/K}"'] \arrow[dr, phantom, "\boxed{\text{commutes}}"] & Gal(L^{ab}/L) \arrow[d, "res."] \\
C_K \arrow[r, "\Theta_K"] & Gal(K^{ab}/K)
\end{tikzcd}$$

Local-to-Global

- $K_v^\times \hookrightarrow C_K$ by $\alpha \mapsto (1,\dots,1,\alpha,1,\dots)K^\times$

$$\begin{tikzcd}
K_v^\times \arrow[r, "\Theta_{K_v}"] \arrow[d, hook] \arrow[dr, phantom, "\boxed{\text{commutes}}"] & Gal(K_v^{ab}/K_v) \arrow[d, hook, "res."] \\
C_K \arrow[r, "\Theta_K"] & Gal(K^{ab}/K)
\end{tikzcd}$$

- Θ_K determines Θ_{K_v} $\forall$ places v and all Θ_{K_v} determine Θ_K.

$$\begin{matrix}
\Theta_{L/K}(K_v^\times) & = Gal(L_w/K_v) & \cong G_p(L/K) \\
\cup\!\shortmid & \cup\!\shortmid & \cup\!\shortmid \\
\Theta_{L/K}(\Theta_K^\times) & = I_{L_w/K_v} & \simeq I_p(L/K)
\end{matrix}$$

Enumerating Quadratics (CFT)

To find quadratic extensions $K/\mathbb{Q}$

$$\prod_p \mathbb{Z}_p^\times \simeq C_{\mathbb{Q}}/\mathbb{R}^+ \xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q}) \twoheadrightarrow \mathrm{Gal}(K/\mathbb{Q})$$
$$= \mathbb{Z}/2\mathbb{Z}$$

Each $\theta: \prod_p \mathbb{Z}_p^\times \twoheadrightarrow \mathbb{Z}/2\mathbb{Z}$ defines an $K/\mathbb{Q}$ (deg = 2).

Note: squares are in the kernel, and

$$\mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^2 \simeq \begin{cases} \mathbb{Z}/2\mathbb{Z} & p \text{ odd} \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & p = 2 \end{cases}$$

Since only finitely many primes ramify, and $\theta(\mathbb{Z}_p^*) = I_p$, only finitely many $\mathbb{Z}_p^\times$ have nontrivial image.

For each finite collection of primes, choose a surjective map $\mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^2 \twoheadrightarrow \mathbb{Z}/2\mathbb{Z}$, which determines a quadratic extension $K/\mathbb{Q}$ ramified at exactly those primes.

Note: 2 has more ramification options because it ramifies in 3 of the 4 extensions: $\mathbb{Q}(\sqrt{D})$, $\mathbb{Q}(\sqrt{-D})$, $\mathbb{Q}(\sqrt{2D})$, $\mathbb{Q}(\sqrt{-2D})$.

Chebotarev Density

Natural Density

M = set of primes in K $\qquad \eta(p) = \#(\mathcal{O}_K : p)$

$$\delta(M) = \lim_{x \to \infty} \frac{\#\{p \in M : \eta(p) \leq x\}}{\#\{p : \eta(p) \leq x\}}$$

Artin Symbols & Frobenius Elements

p unramified in $L|K \longrightarrow I_p = 1$ and $\overset{\text{(Decomposition)}}{D_p}$ is cyclic $\subseteq Gal(L|K)$.

$D_\beta = \langle \varphi_\beta \rangle$ for Frobenius elt φ_β

(well defined for p up to conjugacy)

The Artin Symbol is $\left(\frac{L|K}{\beta}\right) = \varphi_\beta$ $\left[\text{or } \left(\frac{L|K}{p}\right) = \{\tau \varphi_\beta \tau^{-1}\}\right]$

Fix $\sigma \in Gal(L|K)$

$$P_{L|K}(\sigma) = \left\{ \begin{array}{l} p \text{ prime in } K, \text{ unramified in } L|K \\ \text{w/ some } \beta | P \text{ s.t. } \left(\frac{L|K}{\beta}\right) = \sigma \end{array} \right\}$$

Chebotarev Density Theorem

$L|K$ Galois w/ $G = Gal(L|K)$

fix some $\sigma \in Gal(L|K)$

$$\boxed{\delta(P_{L|K}(\sigma)) = \frac{\#\{\tau \sigma \tau^{-1}\}}{\#Gal(L|K)}}$$

Example: p splits completely $\Longleftrightarrow D_p = 1 \Longleftrightarrow \varphi_\beta = 1 \ \forall \beta | p$

so then $\delta\left(\begin{smallmatrix}\text{split}\\ \text{completely}\end{smallmatrix}\right) = \delta(P_{L|K}(1)) = 1/\#G = 1/n$.

Note: If $L|K$ not Galois, let N be Galois closure, then

p split completely in $N \Longrightarrow p$ split completely in L

so $\delta\left(\begin{smallmatrix}\text{split}\\ \text{completely}\\ \text{in } L\end{smallmatrix}\right) \geq \delta\left(\begin{smallmatrix}\text{split}\\ \text{completely}\\ \text{in } N\end{smallmatrix}\right) = 1/[N:K] > 0$.

Application: If almost all p split completely then $L = K$.

"almost all" means $\delta(\text{sp. comp}) = 1$ but we also have $\delta(\text{sp comp}) = 1/n$

so then $n = 1$.

Ray Class Groups

Defn

- modulus is formal product $\prod_p p^{n_p}$ (may include infinite places)
- I_K^m restricts p^{th} place to $1+p^{n_p} = \mathcal{U}_p^{(n)}$ (for infinite places will be $\mathbb{R}_+^*$ or $\mathbb{C}^*$)
- ray class group is $C_K^m = I_K^m K^\times / K^\times$ and the ray class field K^m is an abel ext. s.t. $C_K^m \simeq Gal(K^m/K)$.
- Hilbert Class Field is K^1, maximal unramified abelian extension, and in this case $$Gal(H/K) \simeq Cl_K$$

Facts:

- Every (fin abel) L/K contained in some K^m (that is $C_K^m \subset N_L = \ker \Phi_{L/K}$)
- Every (fin abel) $L/\mathbb{Q}$ is contained in [Kronecker Weber Thm] so $\mathbb{Q}(\zeta)$ (not true for L/K)

Conductor

Local:

L/K local fields w/ max ideal p of K,

$\mathcal{U}_K^{(n)} = 1 + p^n$ (higher unit groups)

conductor is smallest n such that

$$\begin{tikzcd}
K^\times \arrow[rr, two heads, "\phi_K"] \arrow[dr] & & Gal(L/K) \\
& \mathcal{O}_K^\times / \mathcal{U}_K^{(n)} \arrow[ur] &
\end{tikzcd}$$

factors through,

that is $\phi_{L/K}$ is trivial on $\mathcal{U}_K^{(n)}$, i.e. $\mathcal{U}_K^{(n)} \subset N_L$.

Global

L/K global fields, the conductor $f(L/K)$ is gcd of all moduli m such that $C_K^m \subset N_L = \ker \Theta_{L/K}$

Facts:

- p ramifies $\Longleftrightarrow$ $p \mid f(L/K)$
- $f(L/K) = \prod_p p^{f(L_p/K_p)}$

Example:

$$f(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) = \begin{cases} |Disc(\mathbb{Q}(\sqrt{d})/\mathbb{Q})| & d>0 \text{ (real)} \\ \infty |Disc(\mathbb{Q}(\sqrt{d})/\mathbb{Q})| & d<0 \text{ (complex)} \end{cases}$$

Artin Reciprocity

Quadratic Reciprocity

$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$ ~ Does p split (completely) in $\mathbb{Q}(\sqrt{q})$ [or generally $\mathbb{Q}(\sqrt{D})$]?

Depends on modulo condition of p mod $4q$ [or $4D$]

"the primes that split completely in quadratic number fields are determined by a congruence condition modulo a value determined by the extension" ↪ disc $K|\mathbb{Q}$

Artin Reciprocity

"the primes that split completely in abelian extension $K|\mathbb{Q}$ are determined by a congruence condition modulo a value determined by the extension" ↪ conductor $K|\mathbb{Q}$

Artin ⇒ QR:

For $K = \mathbb{Q}(\sqrt{D})$ the discriminant is (essentially) the conductor and so we recover the original result.

From CFT Statements:

p split completely $\Longleftrightarrow$ trivial decomposition group $D_p(K|\mathbb{Q})$

$\Longleftrightarrow D_p(K|\mathbb{Q}) = D(K_{\mathfrak{P}}/\mathbb{Q}_p) = \Theta_{\mathbb{Q}}(\mathbb{Q}_p^\times) = 1$

$\Longleftrightarrow \Theta_{\mathbb{Q}}(p) = 1$ (unramified)

and $\Theta_{\mathbb{Q}}(\mathbb{Z}_p^\times) = 1 \leftarrow$ conductor condition