My CFT teacher only taught us formalism, but her final exam is full of concrete and wonderful number theoritic problems, all of my peers didn't know how to solve them. But I found these concrete problems are very attractive, this is a summary note before the exam for some review of final exam, and after the exam for some conclusions further

PART I Review of algebraic number theory

We are not talking about function fields, although most of results make sense, there're some distinguished features: the Grunald-Wang and some... as the function field ⊃ constant field as a transcental extension and the behavior of the constant field is important.

For global field $K/\mathbb{Q}$, we define its place by taking completion at each valuation, the study of global field in CFT is by study the behavior at each places.

The most important feature of CFT is ramification, the other conditions, which're also important, such as Abelian, is more technical, for imitate the cyclotomic extension $/\mathbb{Q}$.

Recall. Let L/K global fields, $[L:K]=3$, Galois extension

$\operatorname{Spec}\mathcal{O}_L$

$\downarrow$

$\operatorname{Spec}\mathcal{O}_K$

P_1 P_3 P_2 P_4

- P_1, P_2 are ramified: $P_1\mathcal{O}_L=\mathfrak{P}_1\mathfrak{P}_2$, $P_2\mathcal{O}_L=\mathfrak{P}_1^3$
- P_3 are unramified: $P_3\mathcal{O}_L=\mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3$
- P_4 are inerted: $P_4\mathcal{O}_L=\mathfrak{P}_1\mathfrak{P}_2$ $\quad e_1=1=e_2,\ f_1=2,\ f_2=1$

The inertia degree is the "multiplicity" by the degree of extension of residue fields $f(\mathfrak{P}|p)=[\mathcal{O}_L/\mathfrak{P}:\mathcal{O}_K/p]$

$\Rightarrow \underbrace{\sum e_if_i}_{=[L:K]}=3$ for each P_j fixed place

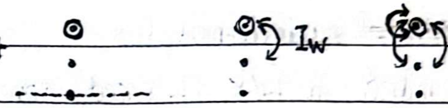
$\operatorname{Gal}(L/K)\curvearrowright\mathcal{O}_L$, we have, at each place w of L, with $\mathfrak{P}$ over p

$$1\to \underset{e_w}{I_w}\to \underset{e_wf_w}{G_w}\to \underset{f_w}{\operatorname{Gal}\big((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/p)\big)}\to 1$$
($\operatorname{Gal}(L/K)$ act trivially on residue field)

$I_w=\{\sigma\in\operatorname{Gal}(L/K)\mid \sigma(\alpha)\equiv\alpha \pmod{\mathfrak{P}},\ \forall\alpha\in\mathcal{O}_L\}$

$\trianglelefteq\{\sigma\in\operatorname{Gal}(L/K)\mid\sigma(\mathfrak{P})=\mathfrak{P}\}=G_w$

For example, at P_4



I_w $\quad G_w$

From geometric pointview, I_w is more essential for the arithmetic action

Rk. For higher inertia group and ⋯, omitted, the length of ramification is crucial if we want to state a ramified version of GCFT's result on Artin map, but we omit it here.

PART II Motivation of CFT

- Generalize cyclotomic extension of $\mathbb{Q}$:

(Kronecker–Weber) $\mathbb{Q}^{ab}=\bigcup\mathbb{Q}(\zeta_n)$ ⇝ Structure of Abelian extension (Existence)

- Generalize quardric reciprocity law:

$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right)\cdot(-1)^{\frac{(p-1)(q-1)}{4}}=1$ ⇝ Hilbert reciprocity law

- Observation: $\mathbb{Q}$ has no unramified extension v.s. $\mathbb{Z}$ is PID

$\mathbb{Q}(\sqrt{-5})$ has only unramified extension v.s. $\mathbb{Z}[\sqrt{-5}]$ has unique not principal ideal $(2, 1+\sqrt{-5})$

$\mathbb{Q}(\sqrt{-5},\sqrt{-1})/\mathbb{Q}(\sqrt{-5})$

⇝ Existence of unramified extension v.s. $Cl(\mathcal{O}_K)$ ~~non~~trivial

⇝ Ramification v.s. Split primes (Artin map)

Rk. I don't know the history, but I think it's impossible to use the second reason to motivative CFT, it's hard to directly see this.

We're introducing the ideal-theortic result of GCFT, used most in application, equivalent to idele-theortic one.

By the third observation, we need to dominate the ramification, we say a modulus $m = \prod p_v^{e_v}$ a finite formal product, and if v is infinite / Archimeadean, then $\begin{cases} e_v = 0 \text{ or } 1 & \text{for real place} \\ e_v = 0 & \text{for complex place} \end{cases}$

Then m dominate at each place p_v, the ramification e_v, and we have K_m/K and $Cl_m(K) \cong Gal(K_m/K)$

Conductor is the ~~minimal~~ maximal modulus making K_m/K unramified in L/K, L fixed, denoted $f_{L/K}$

i.e. v ramified place $\Leftrightarrow v \mid f_{L/K}$

$\begin{cases} m=1 \text{ unramified} & Gal(K_1/K) \cong Cl_1(K) = Cl(K) \supseteq \\ m=\infty \text{ unramified except } \infty & Gal(K_\infty/K) \cong Cl_\infty(K) =: Cl^+(K) \end{cases}$

narrowed class group

K_1 is called Hilbert class field, K_∞ is narrowed ... one.

K_m has very concrete definition by m, called ray class field, $Cl^+(K)$ is computed by {fractional ideals with positive generator} totally

(not compute K_∞ first, then balabala, it's hard)

E.g. Consider each place (p) of $\mathbb{Q}$ in $\mathbb{Q}(i)/\mathbb{Q}$:

$p=2$ (x^2+1) ramified / $\mathbb{F}_p$

$p \equiv 1 \boxed{(\text{mod } 4)}$ (x^2+1) split completely / $\mathbb{F}_p$

$p \equiv 3 \boxed{(\text{mod } 4)}$ (x^2+1) still irreducible / $\mathbb{F}_p$

v.s. $p\mathcal{O}_{\mathbb{Q}(i)} = p\mathbb{Z}[i]$'s split behaviour in $\mathbb{Z}[i]$:

$p=2$ $p\mathbb{Z}[i] = \mathfrak{P}^2$ ramified

$p=1 \boxed{(\text{mod } 4)}$ $p\mathbb{Z}[i] = \mathfrak{P}_1\mathfrak{P}_2$ split completely

$p=3 \boxed{(\text{mod } 4)}$ $p\mathbb{Z}[i]$ is prime inert

$\boxed{4 \text{ is the conductor}}$ of $\mathbb{Q}(i)/\mathbb{Q}$

日月光华 旦复旦兮

The statement of CFT in ideal-theortic language is same as idele-theortic, replace C_K by $Cl(K)$, but note that $Cl(K)$ is finite than profinite, the $Cl(K)$ is even more concrete to apply.

Application.

Split primes (seen above)

Chebetarev density thm (it's used to find density of split primes)

Artin L-function, Weber L-function..

Rk. L-function is a kind of invariant, for example, we compared L-function of automorphic forms and Galois rep, and indicated Langlands program.

Invariants are also helpful for original properties, it will be used in the proof of GCFT;

PART III Adelic formalism.

The idea is also collecting all places' data, and adelic is more direct and natural, I can say nothing interesting, I only give several remarks.

① We take the quotient $K^\times \backslash \mathbb{A}_K^\times$ the idele class group, because $K^\times$ has no contribuctation in any sense:

• $1 \to \boxed{K^\times} \to \mathbb{A}_K^\times \to C_K \to 1$ • $H^1(Gal(L/K), L^\times) = 0$

$1 \to \boxed{P_K} \to I_K \to Cl(K) \to 1$ (Hilbert 90);

send to principal ideals;

• Idele norm of $K^\times$ is $[L:K]$, and the invariant map (later we'll see):

$H^2 \to \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$ vanishes;

② $\mathbb{I}_K \to \mathbb{A}_K$ is continuous by not embedding, $\mathbb{I}_K$ has finer topology by $\mathbb{I}_K \hookrightarrow \mathbb{A}_K \times \mathbb{A}_K$, $x \mapsto (x, x^{-1})$;

③ The proof of almost all statement are base on the standard trick: $\mathbb{A}_K$ is metric space, each component given by valuation, how to justify each non-Archimeadean & Archimeadean places to control global is interesting.

日月光华 旦复旦兮

Application.

- Adelic Minkowski lattice thm: classical Minkowski thm only uses real embedding in infinity, but Adelic uses all places;
- Strong approximation (using Adelic Minkowski);
- Class number finite thm (using Adelic Minkowski);
- Automorphic forms: classical modular form only uses ~~real place in~~ infinity places, but automorphic uses all places, and general $\mathbb{Q}$ than $\mathbb{G}_m(K)\backslash\mathbb{G}_m(\mathbb{A}_K)$;

$\boxed{\text{PART IV}}$ Statement of CFT

Thm. ① (Artin Reciprocity)

$K^\times\backslash\mathbb{A}_K^\times \xrightarrow{\phi} \mathrm{Gal}(K^{ab}/K)$ has dense image and satisfying that:

(i) Let v unramified place, then $K_v^\times \hookrightarrow \mathbb{A}_K^\times \twoheadrightarrow K^\times\backslash\mathbb{A}_K^\times \xrightarrow{\phi} \mathrm{Gal}(K^{ab}/K)$

$\begin{cases} v \text{ nonArchimedean, } K_v \text{ is DVR, uniformer } \pi \mapsto \mathrm{Frob}_v \\ v \text{ Archimedean } (\mathbb{R}^\times \text{ or } \mathbb{C}^\times)\text{, it } -1 \mapsto i \end{cases}$

(ii) Let v unramified place, $\mathcal{O}_v^\times$ vanishes under Artin map; in particular, if K^{ab}/K unramified, $K^\times\backslash\mathbb{A}_K^\times/\mathcal{O}_K^\times \hookrightarrow \mathrm{Gal}(K^{ab}/K)$ (almost isomorphic)

② (Relative version) L/K Abelian unramified,

$1 \to C_L \xrightarrow{N_{L/K}} C_K \xrightarrow[\text{dense}]{} \mathrm{Gal}(L/K)$, i.e. $C_K/N_{L/K}(C_L) \hookrightarrow \mathrm{Gal}(L/K)$ dense

③ For local field, replace C_K by $K^\times$, all same;

④ (Local-to-Global) $\forall v$,

$$\begin{array}{ccc} K_v^\times & \longrightarrow & \mathrm{Gal}(K_v^{ab}/K) \\ \downarrow & & \downarrow \\ K^\times\backslash\mathbb{A}_K^\times & \longrightarrow & \mathrm{Gal}(K^{ab}/K) \end{array}$$

⑤ (Weil group)

$$\begin{array}{ccccccccc} 0 & \to & \mathcal{O}_K^\times & \to & K^\times & \xrightarrow{\text{ord}} & \mathbb{Z} & \to & 0 \\ & & \downarrow\cong & & \downarrow\cong & & \| & & \\ 0 & \to & I_K & \to & W^{ab} & \xrightarrow{\text{dense}} & \mathbb{Z} & \to & 0 \\ & & \| & & \downarrow & & \downarrow & & \\ 0 & \to & I_K & \to & \mathrm{Gal}(K^{ab}/K) & \xrightarrow{\pi} & \hat{\mathbb{Z}} & \to & 0 \end{array}$$

} finite

$W^{ab} = \pi^{-1}(\mathbb{Z})$ as set

the dense Artin map factor through finite W^{ab}, $K^\times \xrightarrow{\sim} W^{ab}$ also called Artin map

⑥ (Existence) $\{H \le C_K \mid \text{finite index, open}\} \xleftrightarrow{1:1} \{L/K \mid L \subset K^{ab} \text{ Abelian}\}$ for local is same;

⑦ (Functoriality) The Norm and Ver functoriality, when we change base field K, induced by Res and Cor in group cohomology;

Rk. ① Here we first see the big coset $K^\times\backslash\mathbb{A}_K^\times/\mathcal{O}_K^\times$, generalized in Langlands program, and we interpret it as lattice maximal tori the Galois-Rep language:

$\{\text{character } \rho_1: K^\times\backslash\mathbb{A}_K^\times/\mathcal{O}_K^\times \to \overline{\mathbb{Q}}_\ell\} \xleftrightarrow{1:1} \{\text{character } \rho_2: \mathrm{Gal}(K^{ab}/K) \to \overline{\mathbb{Q}}_\ell\}$;

② $W^{ab} \to \mathrm{Gal}(K^{ab}/K)$ is injective but not close embedding, W^{ab} has finer topology than subspace topology;

③ When prove, we use finite extension to approximate; finite case L/K has isomorphism $C_K/N_{L/K}(C_L) \cong \mathrm{Gal}(L/K) \cong$ ideal-theoretic one

Application.

Hilbert Reciprocity: for local field $K_v \supset \mu_n$, we set the Hilbert symbol

$(-,-)_v: K_v^\times \times K_v^\times \to \mu_n$

$(a,b)_v := \dfrac{\phi(b)\sqrt[n]{a}}{\sqrt[n]{a}}$, as $\phi(b) \in \mathrm{Gal}(K_v^{ab}/K_v) \supset K_v^{ab} \supset (K_v^{ab})^\times$

Consider $n=2$, $a \in K_v^\times \Rightarrow \sqrt[n]{a} \in (K_v^{ab})^\times$

$\mu_2 = \{\pm 1\} \subset K_v^\times$ always holds

$\Rightarrow (a,b)_v = \begin{cases} 1; & ax^2+by^2=1 \text{ have solution} \\ -1; & \text{otherwise} \end{cases}$ (compare with Legendre symbol, if $v = b$ or $a \sim ax^2=1$ or $bx^2=1$)

$\Rightarrow$ Let $K=\mathbb{Q} \Rightarrow (p,q)_2 = (-1)^{\frac{(p-1)(q-1)}{4}}$

$(p,q)_p = \left(\frac{q}{p}\right)$, $(p,q)_q = \left(\frac{p}{q}\right)$

$(p,q)_v = 1$ otherwise

$\Rightarrow \prod_v (p,q)_v = 1$ is quadratic reciprocity.

generally, $\prod_v (a,b)_v = 1$ is Hilbert reciprocity (for higher also)

thus Hilbert reciprocity $\Rightarrow$ quadratic reciprocity ▨

PART V Group cohomology and Tate cohomology, Pf of CFT

Fundamental: Group cohomology $H^i(G,M)$ is by derive the functor $(-)^G$, homology is similiar;

What's good?

- It has standard resolution by the simplicial resolution;
- It has dimension shift trick: $0 \to M \to \mathrm{Ind}_1^G M \to M' \to 0$

Induced module has trivial cohomology, LES gives $H^{n+1}(M) = H^n(M')$ to cut dimension down to 0, then we can prove properties easily;

- $H^i(G) = H^i(BG)$ related with topological theory, explained by the simplicial construction of BG directly;
- Good functoriality when changing groups, e.g. Shapiro Lemma $H(G, \mathrm{Ind}_H^G M) = H(H, M)$ ($\Leftarrow$ derive $(\mathrm{Ind}_H^G M)^G = M^H$)

What's bad?

- The computation uses inhomogenous cycles to simplify, just as the computation of Hoschild cohomology, is very complicated;
- The functoriality is not complete, Res/Inf survive in cohomology, Cor/Conf survive in homology, the extension uses strange definition, and the adjoint relations are not full (Frobenius Reciprocity);

$\Rightarrow$ The broken of the last one motivates Tate cohomology, following the insight of Grothendieck's six functor formalism, we glue cohomology and homology (and extending operations such as cup product):

$$\begin{cases} \mathrm{Res}, \mathrm{Cor}\ (f^*, f_*) & \text{Projection formula } \checkmark \\ \mathrm{Inf}, \mathrm{Conf}\ (f^!, f_!) & \rightsquigarrow \text{Exact triangle/Excision sequence } \checkmark \\ \mathrm{Ind}, \mathrm{ind}\ (\mathrm{Hom}, \otimes) & \text{Duality/Adjoint } \checkmark \end{cases}$$

Some of them only survive in homological-level, just as geometric case.

(The excision sequence is $\xrightarrow{+1} H^i(G/H, A^H) \xrightarrow{\mathrm{Inf}} H^i(G,A) \xrightarrow{\mathrm{Res}} H^i(H,A) \xrightarrow{+1}$)

Rk. Normal basis thm $\Rightarrow$ Hilbert 90:

Normal basis thm $\Leftrightarrow L = \mathrm{Ind}_1^G K$, $G = \mathrm{Gal}(L/K)$ is induced module

$\overset{\text{Shapiro}}{\Rightarrow} H^i(G, L) = 0$ for $i \geq 1$

$\Rightarrow H^1(G, L) = 0$ is Hilbert 90 ▨ (additive)

For G is Galois group (profinite) in CFT, we proceed by reducing:

G profinite $\underset{\lim}{\rightsquigarrow}$ G finite $\xrightarrow[\text{Sylow}]{\text{Tate-Nakayama}}$ G cyclic p-group

- G cyclic case is always easy, take complete resolution and we find it has period 2, only compute $\hat{H}^{-1}(G,M)$ and $\hat{H}^0(G,M)$ by definition
- Tate-Nakayama is an generalization of Hilbert 90:

We call L/K is a class formation if $G = \mathrm{Gal}(L/K)$ finite satisfy $H^1(G_p, M) = 0$, $H^2(G_p, A) = \mathbb{Z}/p^r\mathbb{Z}$ for $G_p \leq G$ p^r-order p-subgroup, then $(-\cup \chi): \hat{H}^n(H,N) \to \hat{H}^{n+2}(H, N \otimes M)$ is isomorphism for $\forall H \leq G$ and $\forall$ torsion free M-module N

where $\chi \in \hat{H}^2(H,M)$ is generator of $\mathbb{Z}/p^r\mathbb{Z}$

holds for all finite G

Pf of CFT (sketch): L/K finite local

$$\begin{array}{ccc} C_K/N_{L/K}(C_L) & \longleftarrow & \mathrm{Gal}(L/K)^{ab} \\ \| & & \| \\ \hat{H}^0(\mathrm{Gal}(L/K), L^\times) & & H_1(\mathrm{Gal}(L/K), \mathbb{Q}) \\ & \nwarrow^{(-\cup\chi)} & \| \\ & & \hat{H}^{-2}(\mathrm{Gal}(L/K), \mathbb{Q}) \end{array}$$

$\chi \in \hat{H}^2(\mathrm{Gal}(L/K), L^\times) =: \mathrm{Br}(L/K) \underset{\cong}{\xrightarrow{\mathrm{ord}}} H^2(\mathrm{Gal}(L/K), \mathbb{Z})$

$\xrightarrow[\cong]{\delta^{-1}} H^1(\mathrm{Gal}(L/K), \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z})$ (space of characters)

$\xrightarrow{\mathrm{inv}_{L/K}}$ $\cong \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$

induced by $0 \to O_L^\times \to L^\times \xrightarrow{\mathrm{ord}} \mathbb{Z} \to 0$ and $0 \to \mathbb{Z} \to \frac{1}{[L:K]}\mathbb{Z} \to \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z} \to 0$

$\Rightarrow (-\cup\chi)^{-1} =: \phi$ is desired Artin map, and taking limit of L ▨

For Global field, it's much more complicated and tricky, roughly, we have $0 \to \mathrm{Br}(K) \to \bigoplus_v \mathrm{Br}(K_v) \to \mathbb{Q}/\mathbb{Z} \to 0$ ($\frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z} \hookrightarrow \mathbb{Q}/\mathbb{Z}$) and we compute idèle module Galois cohomology ▨

For existence via group cohomology, it's also tricky task, a more computable plan is by Lubin-Tate theory, see comments below $\blacksquare$

Rk. ① The $\mathrm{inv}_{L/K}: Br(L/K) \to \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$, called Hasse invariant, named by the central simple algebra interpretation of $Br(L/K)$, it associate each algebra a number, thus called "invariant";

② How this proof is motivated? Tate said he aimed imitating the Hilbert 90. If the Galois cohomology governs some deformation problem, then both Hilbert 90 and Tate-Nakayama are considering some "rigid Galois representation character", the couple with the obstruction class induce the isomorphism;

③ Lubin-Tate theory is based on the imitation of Kronecker-Weber which adding all ζ_n to extend to Abelian envelope, here Lubin-Tate is by adding all p-power torsion point of formal group law $/K$

Q. Is the deformation of formal group law the deformation problem parameterized by Tate cohomology in CFT?

E.g. ($p = x^2 + ny^2$)

Consider extensions

$$\begin{array}{l} \mathbb{Q}(\sqrt{-14}, \sqrt{2\sqrt{2}-1}) \\ \quad \big| \; 4:1, \text{unramified (unique one)}, (x^2+1)^2 - 8 = 0 \\ \mathbb{Q}(\sqrt{-14}) \\ \quad \big| \; 2:1, \; x^2 + 14 = 0 \\ \mathbb{Q} \end{array}$$

For $p \neq 7$, $\exists x, y \in \mathbb{Z}$,

$$\begin{array}{ccc} p = x^2 + 14y^2 & \Longleftrightarrow & (p) = (x+\sqrt{-14}y)(x-\sqrt{-14}y) \\ \Updownarrow & & \Updownarrow \text{GCFT} \\ x^2 \equiv -14 \pmod p & & \\ (x^2+1)^2 \equiv 8 \pmod p & \Longleftrightarrow & \text{unramified extension at place } \mathfrak{p} \end{array}$$

$\blacksquare$