V. Introduction to general CFT

24/8

V.1 norms

· Let $p \in \operatorname{Spec}(\mathbb{Z})$. For $\frac{a}{b} = p^n \frac{a'}{b'} \in \mathbb{Q}^*$, with a', b' coprime to p, define $\|\frac{a}{b}\|_p := p^{-n}$, $\|0\|_p := 0$.

54 **Prop**: $\|\ \|_p : \mathbb{Q} \to \mathbb{R}_{\geq 0}$ is a norm. Moreover, $\forall \alpha, \beta \in \mathbb{Q}$, $\|\alpha+\beta\|_p \leq \max\{\|\alpha\|_p, \|\beta\|_p\}$ (ultrametric property).

55 **Thm** (Ostrowski): Every norm in $\mathbb{Q}$ is equivalent to either the trivial one, the absolute value, or a p-adic norm.

Def: $\mathbb{Q}_p := \overline{\mathbb{Q}}^{\|\ \|_p}$. (The Banach closure of $\mathbb{Q}$).

$\mathbb{Z}_p := \{ z \in \mathbb{Q}_p \mid \|z\|_p \leq 1 \} = \{ \sum_{i=0}^{\infty} a_i p^i \mid 0 \leq a_i \leq p-1 \}$.

This is a local ring with maximal ideal $p\mathbb{Z}_p$.

obs: $\mathbb{Q}_p = \operatorname{frf}(\mathbb{Z}_p) = \{ \sum_{i \geq n_0} a_i p^i,\ n_0 \in \mathbb{Z},\ a_i \in \{0, \ldots, p-1\} \}$.

$\mathbb{Q}_p^{alg}$:= algebraic closure of $\mathbb{Q}_p$.

extension of norms: given $\alpha \in \mathbb{Q}_p^{alg}$, $\operatorname{Irr}(\alpha, \mathbb{Q}_p)$ of degree n, consider $\mathbb{Q}_p(\alpha) | \mathbb{Q}_p$, finite extension of degree n. Suppose $K = \mathbb{Q}_p(\alpha)$ Galois deg $n / \mathbb{Q}_p$. $\|\alpha\|_{p,/K} := \|N_{\mathbb{Q}_p(\alpha)|\mathbb{Q}}(\alpha)\|_p^{1/n}$ is a norm and $\forall \alpha \in \mathbb{Q}_p$, $\|\alpha\|_{p,/K} = \|\alpha^n\|_p^{1/n} = \|\alpha\|_p \leftarrow$ usual norm.

$\mathbb{C}_p := \overline{\mathbb{Q}_p^{alg}}^{\|\ \|_p}$.

Goal:
- local CFT: to describe abelian extensions of finite extensions of $\mathbb{Q}_p$. (Lubin-Tate)
- global CFT: to describe abelian extensions of finite extensions of $\mathbb{Q}$ (number fields)

Actually: local CFT $\rightsquigarrow$ global CFT (Chevalley).

Let $L|K$ be finite abelian, K number ~~theory~~ field. $G := Gal(L|K)$.

Def: A "prime" or a place of K is:

a) absolute value equivalent to some p-adic norm (non-archimedean or finite). Can be identified with a prime ideal $\mathfrak{p} \in Spec(\mathcal{O}_K)$:

$\mathfrak{p} \in Spec(\mathcal{O}_K)$, $\|x\|_\mathfrak{p} = N\mathfrak{p}^{-v_\mathfrak{p}(x)}$, $K_\mathfrak{p} \equiv$ p-adic completion,

$\mathcal{O}_{K,\mathfrak{p}}$ ring of integers, local, $\mathfrak{p}\mathcal{O}_{K,\mathfrak{p}} = (\pi)$.

b) absolute value equivalent to an embedding:

$\sigma: K \hookrightarrow \mathbb{R}$ real embedding, $\|x\|_\sigma = |\sigma(x)|$

$\sigma: K \hookrightarrow \mathbb{C} \setminus \mathbb{R}$ complex, $\sigma \in \{\sigma_1, \bar{\sigma}_1\}$, $\|x\|_\sigma = \sqrt{\sigma_1(x)\bar{\sigma}_1(x)} = \|\sigma_1(x)\|$.

(archimedean places)

I_K = group of fractional ideals.

$S \equiv$ denote a finite set of places (finite or/and real).

V.II The Artin map

$\mathfrak{p} \in Spec(\mathcal{O}_K)$, $\mathfrak{P}|\mathfrak{p}$, $\mathfrak{P} \in Spec(\mathcal{O}_L)$ unramified:

$\varphi_\mathfrak{P} : D(\mathfrak{P}|\mathfrak{p}) \simeq Gal(\mathcal{O}_L/\mathfrak{P} \mid \mathcal{O}_K/\mathfrak{p}) = \langle \varphi_\mathfrak{P} : x \mapsto x^{N^K_\mathbb{Q}(\mathfrak{p})} \rangle$

Actually, since $L|K$ abelian, $\varphi_\mathfrak{P} = \varphi_\mathfrak{p} : Gal(L|K) \to Gal(\mathcal{O}_L/\mathfrak{P}|\mathcal{O}_K/\mathfrak{p})$

Def: Let $\mathfrak{c} \subseteq \mathcal{O}_K$ be an integral ideal divisible by all the primes of $\mathcal{O}_K$ which ramify at L. $I(\mathfrak{c})$ = frac. ideals coprime to $\mathfrak{c}$:

$(\cdot, L|K) : I(\mathfrak{c}) \to Gal(L|K)$

$\mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_r^{n_r} \mapsto \sigma_{\mathfrak{p}_1}^{n_1} \cdots \sigma_{\mathfrak{p}_r}^{n_r}$

Denote, sometimes $(\mathfrak{p}, L|K) = \left(\frac{\mathfrak{p}}{L|K}\right) = \sigma_\mathfrak{p}$.

56 **Thm** (weak Artin reciprocity) $\Rightarrow \exists \mathfrak{c}$, frac ideal,

Let $L|K$ be a finite abelian extension of number fields divisible by all the primes of K which ramify in L s.t.

$\mathfrak{c}_1 = (\mathfrak{c}_1 + \mathfrak{c}_2)\mathfrak{b}$ $\mathfrak{c}_2 = (\mathfrak{c}_1+\mathfrak{c}_2)\mathfrak{b}'$

$\forall \alpha \in K^* \mid \alpha \equiv 1 \bmod \mathfrak{c}$, $((\alpha), L|K) = 1$.

Notice: if this is true for $\mathfrak{c}_1, \mathfrak{c}_2 \Rightarrow$ also true for $\underset{\gcd}{\mathfrak{c}_1+\mathfrak{c}_2}$ $\Rightarrow$ $\exists$ the largest ideal $\mathfrak{c}$ for which this is true. It's denoted $\mathfrak{c}_{L|K}$ and called the conductor of the extension. (Rem V.3.8 Milne)

Def: ~~$P(\mathfrak{c}) = \{(\alpha) \mid \alpha \equiv 1 \ldots\} = \{\alpha \in K^* \mid$~~

$$P(\mathfrak{c}) = \{(\alpha) \mid \alpha \in K^*, \ \alpha \equiv 1 \bmod \mathfrak{c}\}$$

$$\Rightarrow \ P(\mathfrak{c}_{L|K}) \subseteq \mathrm{Ker}(\cdot, L|K).$$

Obs: $(\alpha) \in P(\mathfrak{c})$ not necessarily is $\alpha \equiv 1 \bmod \mathfrak{c}$, all we need is $\xi \in \mathcal{O}_K^* \mid \xi\alpha \equiv 1 \bmod \mathfrak{c}$.

More in general, following Milne, if S is a finite set of places,

$I^S :=$ subgroup of I_K generated by (finite) primes not in S, $\quad i(K^S) \supseteq P(\mathfrak{c})$

$K^S = \{\alpha \in K^* \mid (\alpha) \in I^S\} = \{\alpha \in K^* \mid v_{\mathfrak{p}}(\alpha) = 0 \ \forall \mathfrak{p} \in S \text{ finite}\}$

e.g. $K = \mathbb{Q}$, $S = \{p \mid n\}$, $I^S = \{(\frac{r}{s}) \mid (r,n) = (s,n) = 1\}$

$\mathbb{Q}^S = \{\frac{r}{s} \mid (r,n), (s,n) = 1\}$

$$1 \to \{\pm 1\} \to \mathbb{Q}^S \xrightarrow{i} I^S \to 1.$$
$$a \mapsto (a).$$

V.III Ray class fields and ray class groups

Def: Let $\mathfrak{c} \subseteq \mathcal{O}_K$ be an ideal. A ray class field (RCF) modulo $\mathfrak{c}$ is a finite abelian extn $K_{\mathfrak{c}}|K$ s.t. $\forall L|K$ finite abelian s.t. $\mathfrak{c}_{L|K} \nmid \mathfrak{c} \Rightarrow L \subseteq K_{\mathfrak{c}}$.

("maximal abelian extension of K unramified outside $\mathfrak{c}$")

Intuitively, the RCF ~~is~~ can be thought of the largest field with given conductor, however, the conductor of $K_{\mathfrak{c}}|K$ may not $= \mathfrak{c}$.

e.g. The RCF of $\mathbb{Q}(i)$ modulo (2) is $\mathbb{Q}(i) \Rightarrow \mathfrak{c}_{\mathbb{Q}(i)|\mathbb{Q}(i)} = (1)$.

(57) Thm: Let $L|K$ be a finite abelian extension of number fields, $\mathfrak{c} \subseteq \mathcal{O}_K$ an ideal $\Rightarrow$

$$I(\mathfrak{c}_{L|K}) \xrightarrow{(\cdot, L|K)} Gal(L|K) \to 1$$

a) $(\cdot, L|K)$ ~~$\to$~~ $I(\mathfrak{c}_{L|K}) \to Gal(L|K) \to 1$

b) $Ker(\cdot, L|K) = (N^L_K(I_L)) \cdot P(\mathfrak{c}_{L|K})$.

c) $\exists!$ RCF $K_{\mathfrak{c}}$ of K of conductor $\mathfrak{c}_{L|K} | \mathfrak{c}$ (mod. $\mathfrak{c}$)

d) $K_{\mathfrak{c}}$ is characterised by the property that it's an abelian (finite) extn of K s.t $\left\{ \begin{array}{l} \text{primes in } K \\ \text{totally split} \\ \text{in } K_{\mathfrak{c}} \end{array} \right\} = \left\{ \begin{array}{c} \text{primes in} \\ P(\mathfrak{c}) \end{array} \right\}$.

Def (the Hilbert class field): K number field. $\mathfrak{c} = (1) = \mathcal{O}_K$. The RCF of K modulo $\mathfrak{c}$ is the maximal abelian unramified extension of K. It's called Hilbert class field (HCF) of K.

Obs: $I(\mathfrak{c}_{H_K|K}) = I((1)) =$ frac. ideals. $\underset{a),b)}{\Longrightarrow}$ $(\cdot, H_K|K) : Cl(\mathcal{O}_K) \overset{2}{\downarrow} Gal(H_K|K)$

$P(\mathfrak{c}_{H_K|K}) = P((1)) =$ ppal ideals

Q: For $\mathfrak{c} \neq (1)$, can we see $K_{\mathfrak{c}}$ s.t $Gal(K_{\mathfrak{c}}|K)$ is "some kind of ideal class group"?

second part

• **ray class groups**

Recall: $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_K)$ unramified at L. Then $\mathfrak{p}$ is totally split $\Leftrightarrow$ the extension of residual fields has degree $f=1 \Leftrightarrow (\mathfrak{p}, L|K)=1$

$\Rightarrow \mathrm{Ker}(\cdot, L|K) \supseteq \{\mathfrak{p}$ prime ideals which totally split at $L\}$.

Lemma: $\forall S \subseteq \mathrm{Spec}(\mathcal{O}_K)$, finite, $\exists$ exact sequence

$$1 \to U_K \to K^S \xrightarrow{i} I^S \to C = Cl(\mathcal{O}_K) \to 1 \quad , \; U_K := \mathcal{O}_K^*.$$
$$a \mapsto a\mathcal{O}_K \qquad \mathfrak{a} \mapsto [\mathfrak{a}]$$

Proof: $I^S \to C \to 1$: $\forall [\mathfrak{a}] \in C$, $\mathfrak{a}$ is represented by an ideal in I^S. Indeed, $\mathfrak{a} = \mathfrak{b}\mathfrak{c}^{-1}$, $\mathfrak{b}, \mathfrak{c}$ integral. $\forall c \in \mathfrak{c}$, $\mathfrak{a}(c) = \mathfrak{b}\mathfrak{c}^{-1}(c) \subseteq \mathfrak{b}$ integral $\Rightarrow$

Suppose $\mathfrak{a}$ integral. $\forall \mathfrak{p} \in S$ take $\pi_\mathfrak{p} \in \mathfrak{p} \setminus \mathfrak{p}^2$ (i.e. $v_\mathfrak{p}(\pi_\mathfrak{p})=1$)

set $\mathfrak{a} = \prod_{\mathfrak{p}\in S} \mathfrak{p}^{n_\mathfrak{p}} \mathfrak{b}$, $\mathfrak{b} \in I^S$ and

$\Rightarrow \exists a \in \mathcal{O}_K \mid a \equiv \pi_\mathfrak{p}^{n_\mathfrak{p}} \bmod \mathfrak{p}^{n_\mathfrak{p}+1} \; \forall \mathfrak{p} \in S \Rightarrow (a) \in \prod_{\mathfrak{p}\in S} \mathfrak{p}^{n_\mathfrak{p}} \mathfrak{b}'$, $\mathfrak{b}' \in I^S \Rightarrow$

$a^{-1}\mathfrak{a} \in I^S$ represents $[\mathfrak{a}]$. #

Def (moduli, see Milne)

A modulus for K is $m: \mathrm{Spec}(K) \to \mathbb{Z} \mid$ a) $m(\mathfrak{p}) \geq 0 \; \forall \mathfrak{p}$, $m(\mathfrak{p})=0$ for all but finitely many $\mathfrak{p}$, b) $\mathfrak{p}$ real $\Rightarrow m(\mathfrak{p}) \in \{0,1\}$, c) $\mathfrak{p}$ complex, $m(\mathfrak{p})=0$.

$m := \prod_\mathfrak{p} \mathfrak{p}^{m(\mathfrak{p})} = m_\infty \cdot m_0$; $m_\infty \equiv$ product of infinite primes, $m_0 \equiv$ of finite primes (an ideal).

If $m = m_\infty \cdot m_0$ is a modulus $K_{m,1} := \{a \in K^* \mid v_\mathfrak{p}(a-1) \geq m(\mathfrak{p}), \mathfrak{p} \mid m_0, a_\mathfrak{p} > 0, \mathfrak{p} \mid m_\infty$

obs: $v_\mathfrak{p}(a-1) \geq m(\mathfrak{p}) \Rightarrow a_\mathfrak{p} \equiv 1 \bmod \mathfrak{p}^{m(\mathfrak{p})} \Rightarrow a \in (\mathcal{O}_K/\mathfrak{p})^*$.

$S(m) \equiv$ support of $m = \{\mathfrak{p} \mid m\}$. If $a \in K_{m,1} \Rightarrow (a) \in I^{S(m)}$.

Def: (Ray class group modulo m) is $C_m := I^{S(m)} / i(K_{m,1})$.

Def: Let S be a finite set of primes of K. A homomorphism $\varphi: I^S \to G$ admits a modulus if $\exists$ modulus $\mathfrak{m}$ | $S(\mathfrak{m}) \supseteq S$, $\varphi(i(K_{\mathfrak{m},1})) = 1 \Leftrightarrow$

$$\begin{tikzcd} \varphi: I^S \arrow[r] \arrow[dr] & G \\ & I^S / i(K_{\mathfrak{m},1}) \cong C_{\mathfrak{m}} \arrow[u] \end{tikzcd}$$

Thm (Artin reciprocity law)

Let $L|K$ be a finite abelian extension of number fields, S = set of ramifying primes of K at $L \Rightarrow \varphi: I^S \to Gal(L|K)$ admits a modulus $\mathfrak{m}$ | $S(\mathfrak{m}) = S$ and defines

$$\boxed{I_K^{S(\mathfrak{m})} / i(K_{\mathfrak{m},1}).N_{L|K}(I_L^{S(\mathfrak{m})}) \cong Gal(L|K)}$$

Def: $H \leq I_K^{S(\mathfrak{m})}$ is a congruence subgroup modulo $\mathfrak{m}$ if $i(K_{\mathfrak{m},1}) \subseteq H \leq I_K^{S(\mathfrak{m})}$.

Thm (existence)

For every congruent subgroup mod. $\mathfrak{m}$, $\exists L|K$ finite abelian, unramified at primes not in $\mathfrak{m}$ | $H := i(K_{\mathfrak{m},1}).N_{L|K}(I_L^{S(\mathfrak{m})})$,

$$\boxed{I^{S(\mathfrak{m})}/H \cong Gal(L|K)}.$$

Cor: $\exists L_{\mathfrak{m}} \equiv$ the RCF modulo $\mathfrak{m}$, $C_{\mathfrak{m}} \cong Gal(L_{\mathfrak{m}}|K)$. ~~Moreover~~,
if $L \subseteq L_{\mathfrak{m}} \Rightarrow N(C_{L,\mathfrak{m}}) := i(K_{\mathfrak{m},1}) N(I_L^{S(\mathfrak{m})})$ mod $i(K_{\mathfrak{m},1})$.

Cor: For fixed $\mathfrak{m}$, the map $L \mapsto N_{L|K}(C_{L,\mathfrak{m}})$ is a bijection between the set of K-abelian (finite) extensions contained in $L_{\mathfrak{m}}$ and the set of subgroups of $C_{\mathfrak{m}}$. Moreover:

1) $L_1 \subseteq L_2 \Leftrightarrow N(C_{L_1,\mathfrak{m}_1}) \supseteq N(C_{L_2,\mathfrak{m}_2})$.
2) $N(C_{L_1L_2,\mathfrak{m}}) = N(C_{L_1,\mathfrak{m}}) \cap N(C_{L_2,\mathfrak{m}})$.
3) $N(C_{L_1 \cap L_2,\mathfrak{m}}) = N(C_{L_1,\mathfrak{m}}).N(C_{L_2,\mathfrak{m}})$

e.g. $K=\mathbb{Q}[\sqrt{m}]$ square-free. $S=$ primes of ramification $=$
$=\{p \mid m$ if $m\equiv 1 \bmod 4\}$ or $\{p\mid m, 2$ othw$\}$. $\Rightarrow \varphi_{K|\mathbb{Q}}: I^S \to Gal(K|\mathbb{Q})\cong\{\pm1\}$
$p\mapsto \left(\frac{m}{p}\right)$.

e.g. $L=\mathbb{Q}[\zeta_m]$, m odd or $4\mid m \Rightarrow S\supset\{p\mid m\}$.
$\varphi_{L|\mathbb{Q}}: I^S \to Gal(L|\mathbb{Q})\cong(\mathbb{Z}/m\mathbb{Z})^*$
$\left(\frac{r}{s}\right)\mapsto [r][s]^{-1}$.

e.g. $m=\ell$
$p^f\equiv 1 \bmod \ell \Rightarrow$
$p\mathcal{O}_L=\mathfrak{P}_1\dots\mathfrak{P}_r$ $\mathcal{O}_L/\mathfrak{P}_i$
$\mathbb{F}_p$ $x\mapsto x^p$

e.g. $m=(2)^3(17)^2(19)\infty$ in $\mathbb{Q}$,
$\mathbb{Q}_{m,1}=\{a\in\mathbb{Q}^* \mid v_2(a)\geq 3, v_{17}(a)\geq 2, v_{19}(a)\geq 1, a>0\}$.

Thm (to be proved in several steps in the exercises)
$\forall m$ modulus of K, there is an exact sequence

$$\boxed{1\to U/U_{m,1}\to K_m/K_{m,1}\to C_m\to C\to 1}$$

and a canonical isomorphism $K_m/K_{m,1}\cong\prod_{\mathfrak{p}\mid m_\infty}\{\pm\}\times\prod_{\mathfrak{p}\mid m_0}(\mathcal{O}_K/\mathfrak{p}^{m(\mathfrak{p})})^*$
$\cong\prod_{\mathfrak{p}\mid m_\infty}\{\pm1\}\times(\mathcal{O}_K/m_0)^*$, where $K_m=K^{S(m)}$, $U=\mathcal{O}_K^*$, $U_{m,1}=U\cap K_{m,1}$.

In particular, $\boxed{|C_m|=h_K\cdot(U_m:U_{m,1})^{-1}\cdot 2^{r_0}N(m_0)\prod_{\mathfrak{p}\mid m_0}\left(1-\frac{1}{N(\mathfrak{p})}\right)}$.

e.g. $m=1\Rightarrow C_m=C$.
e.g. $m=$ product of real primes $C_m=$ narrow class group $=$
$=I_K/\sim$: $\mathfrak{a}\sim\mathfrak{b}$ if $\mathfrak{a}\mathfrak{b}=(\alpha)$, $\alpha>>0$. Moreover:
$1\to U/U_+\to K^*/K_+\to C_m\to C\to 1$. $U_+=K_+\cap\mathcal{O}_K^*$.

$K^*/K_+\cong\prod_{\mathfrak{p}\mid m_\infty}\{\pm1\}$.
e.g. $K=\mathbb{Q}$, $m=(m)\Rightarrow 1\to\{\pm1\}\to(\mathbb{Z}/m\mathbb{Z})^*\to C_m\to 1$.
$m=(m)\infty$ $C_m\cong(\mathbb{Z}/m\mathbb{Z})^*$