Continuous Cohomology of $\mathbb{C}_K$

彭淏 1700010601@pku.edu.cn

1 Formal Groups

Def. (0.1.1). A **formal group law** of dimension n over a commutative ring R is a set of n power series $G = (G_1, \dots, G_n)$ in $K[[X_1, \dots, X_n, Y_1, \dots, Y_n]]$ that

$$G(X, 0) = G(0, X) = X, \quad G(G(X, Y), Z) = G(X, G(Y, Z)).$$

Note this immediately induce an inverse $\mathrm{inv}(X)$ that $G(X, \mathrm{inv}(X)) = G(\mathrm{inv}(X), X) = 0$. This can be constructed noticing $G(X, Y) = X + Y + o(X, Y)$.

A morphism of formal groups is a vector of power series $\varphi(X)$ that $\varphi(G(X, Y)) = H(\varphi(X), \varphi(Y))$.

A **formal R-module** is a formal group G over R together with a ring homomorphism $R \to \mathrm{End}_R(G)$ that $[a](X) = aX + \dots$.

Prop. (0.1.2) (Automorphisms). If $\alpha \in R^*$ and F_i are power series that the degree 1 term of (F_i) is invertible, then there are unique power series G_i that $G \circ F = \mathrm{id}$ and $F \circ G = \mathrm{id}$.

Proof: Use induction to find G that $F \circ G = id$. Then the degree 1 terms of G is also invertible, thus there are $G \circ H = \mathrm{id}$, now $F = H$ and the proof is finished. □

Prop. (0.1.3). $\mathbb{G}_a$ is the one-dimensional formal group with $\mathbb{G}_a(X, Y) = X + Y$, $\mathbb{G}_m$ is the one-dimensional formal group with $\mathbb{G}_m(X, Y) = X + Y + XY$. Over a $\mathbb{Q}$-algebra K, there is an isomorphism between $\mathbb{G}_a$ and $\mathbb{G}_m$ giving by $X \to \exp(X) - 1$.

1-dimensional Formal Groups

Def. (0.1.4). For a 1-dimensional formal group $\mathcal{F}$ over R, the **invariant differential** is a differential form $\omega = P(T)dT \in R[[T]]dT$ that $\omega \circ F(T, S) = \omega$. It is called **normalized** if $P(0) = 1$.

There exists uniquely an invariant differential, it is given by $F_X(0, T)^{-1}dT$.

Proof: We need to check $F_X(0, F(T, S))^{-1}F_X(T, S) = F_X(0, T)^{-1}$, and this is just $F(U, F(T, S)) = F(F(U, T), S)$ differentiated at U and let $U = 0$.

Conversely, if ω is an invariant differential, then $P(F(T, S))F_X(T, S) = P(T)$, let $T = 0$, then $P(S) = P(0)F_X(0, S)^{-1}$. □

Prop. (0.1.5). For a morphism $f : \mathcal{F} \to \mathcal{G}$ of 1-dimensional formal groups over R, $\omega_{\mathcal{G}} \circ f = f'(0)\omega_{\mathcal{F}}$.

Proof: We only need to show that $\omega_{\mathcal{G}} \circ f$ is an invariant differential for $\mathcal{F}$ and then compare their constant coefficients. For this, notice

$$\omega_{\mathcal{G}} \circ f(F(T, S)) = \omega_{\mathcal{G}}(G(f(T), f(S))) = \omega_{\mathcal{G}}(f(T)) = \omega_{\mathcal{G}} \circ f(T).$$

□

Def. (0.1.6). When R has characteristic 0, the **formal logarithm** $\log_{\mathcal{F}}$ for a 1-dimensional formal group is the integration of invariant differential $\int_0^T \omega_{\mathcal{F}} = T + c_1/2T^2 + \cdots$.

Then the **formal power exponential** is the the unique power series $\exp_{\mathcal{F}}$ that is the inverse of $\log_{\mathcal{F}}$. It exists uniquely by(0.1.2).

Prop. (0.1.7). For R char= 0 and an 1 dimensional formal group $\mathcal{F}$ over R, $\log_{\mathcal{F}} : \mathcal{F} \to \mathbb{G}_a$ is an isomorphism of formal groups over $R \otimes_{\mathbb{Z}} \mathbb{Q}$.

And if $\mathcal{F}$ is a formal R-module, then it is an isomorphism of R-modules, because from(0.1.5) that $\omega_{\mathcal{F}} \circ [a] = a\omega_{\mathcal{F}}$, thus $\log_{\mathcal{F}} \circ [a] = a \cdot \log_{\mathcal{F}}$.

Proof: From $\omega_{\mathcal{F}}(F(T,S)) = \omega_{\mathcal{F}}(T)$, we get that $\log_{\mathcal{F}}(F(T,S)) = \log_{\mathcal{F}}(S) + \log_{\mathcal{F}}(T)$. So it is a homomorphism. Now the inverse $\exp_{\mathcal{F}}$ is already given, so it is an isomorphism. □

Cor. (0.1.8). A 1-dimensional formal group over a ring R that has no torsion nilpotents is commutative.

Proof: We only prove for R torsion free, in this case $F(T,S) = \exp_{\mathcal{F}}(\log_{\mathcal{F}}(T) + \log_{\mathcal{F}}(S))$. □

Lubin-Tate Formal Group

Def. (0.1.9). For a p-adic number field K with a uniformizer π_K with residue field $\mathbb{F}_q$, a **Lubin-Tate power series** for π_K is a $\varphi(X) \in \mathcal{O}_K[[X]]$ that $\varphi(X) \equiv \pi_K X \mod X^2$ and $\varphi(X) \equiv X^q \mod \pi_K$.

A **Lubin-Tate module** G over $\mathcal{O}_K$ is a formal $\mathcal{O}_K$-module that $[\pi_K](X)$ is a Lubin-Tate power series.

Prop. (0.1.10). Given a p-adic number field K with residue field $\mathbb{F}_q$, we consider the set ξ_π of all Lubin-Tate power series for π.

If $f, g \in \xi_\pi$ and $L(X) = \sum a_i X_i$ be a linear form, then there exists a unique power series $F(X)$ that $F(X) \equiv L(X)$ mod degree 2 and $f(F(X)) = F(g(X_1), \ldots, g(X_n))$.

Proof: Choose F consecutively, if $F_{r+1} = F_r + \Delta_r$, then must

$$\Delta \equiv \frac{f(F_r(X)) - F_r(g(X))}{\pi^{r+1} - \pi} \text{ mod degree } (r+2).$$

This has coefficient in $\mathcal{O}$ because $f \equiv g \equiv Z^q \mod \pi$. □

Cor. (0.1.11). If we let $f = g, L = X + Y$ to get F_f and $f, g, L = aX$ to get $a_{f,g}$, then

- $F_f(X,Y) = F_f(Y,X)$.
- $F_f(F_f(X,Y),Z) = F_f(X, F_f(Y,Z))$.
- $a_{f,g}(F_g(X,Y)) = F_f(a_{f,g}(X), a_{f,g}(Y))$.
- $a_f b_f(Z) = (ab)_f(Z)$.
- $(a+b)_f(Z) = F_f(a_f(Z), b_f(Z))$.
- $\pi_f(Z) = f(Z)$.

all follow from the unicity of the last proposition.

Cor. (0.1.12) (Existence of Lubin-Tate Module). We get a commutative formal $\mathcal{O}$-module F_f for every f. And this group can act on $\mathfrak{p}_L$ for an alg.ext L/K. The set of zeros $\Lambda_{f,n}$ of f^n in L, as the elements annihilated by π^n, is a submodule of $\mathfrak{p}_L^{(f)}$.

And $u_{g,f}$ for any unit $u \in \mathcal{O}$ defines an isomorphism between F_f and F_g, thus this formal group only depends on π, called F_π. Hence $L_{f,n} = K(\Lambda_{f,n})$ only depends on π, with Galois group $G_{\pi,n}$.

Prop. (0.1.13) (Different Uniformizers). Now consider different π, it is proven that F_π and $F_{\pi'}$ are isomorphic, but the coefficient in $\mathcal{O}_{\hat{T}}$ where T is the maximal unramified extension.

Thus $L_{\pi,n}$ and $L_{\pi',n}$ may not be isomorphic, but $T \cdot L_{\pi,n} = T \cdot L_{\pi',n}$ since $\hat{T} \cdot L_{\pi,n} = \hat{T} \cdot L_{\pi',n}$ and both of them is the algebraic closure of K in it.

Proof: Cf.[Neukirch CFT P105]. □

Lemma (0.1.14). The Newton polygon of $[\pi_K^n]/\pi_K^n$ has vertices $(1,0),(q,-1/e_K),(q^2,-2/e_K),\ldots$.

Proof: Notice $[\pi_K^n]$ has no infinite edge of negative slope because all its coefficient are in $\mathcal{O}_K$. Now look at its roots, it has a root 0, and $q-1$ roots of valuation $v_p(\pi_K)/(q-1)$, $q(q-1)$ roots of valuation $v_p(\pi_K)/q(q-1)$, and so on.

So by factor out these roots, $[\pi_K^n]/\pi_K^n$ is left with a power series whose Newton polygon is a single line with non-negative slope, which shows the desired result. □

Prop. (0.1.15). The formal logarithm of the Lubin-Tate formal group F_π satisfies:

$$\log_{\mathcal{F}_\pi}(T) = \varinjlim [\pi_{\mathcal{F}}^n]/\pi_{\mathcal{F}}^n.$$

Proof: By(0.1.7) we have

$$\log_{\mathcal{F}}(T) = \log_{\mathcal{F}}([\pi_{\mathcal{F}}^n])/\pi_{\mathcal{F}}^n = ([\pi_K^n] + a_2/2[\pi_K^n]^2 + \ldots)/\pi_K^n$$

and for any degree d, the valuation of coefficient of $[\pi_K^{2n}]/\pi_K^{2n}$ is bounded below by a constant $c(d)$ by the above lemma(0.1.14), so $[\pi_K^{2n}]/\pi_K^n$ converges to 0, thus the result. □

Cor. (0.1.16). The Newton polygon of $\log_{\mathcal{F}}(T)$ has vertices $(1,0),(q,-1/e_K),(q^2,-2/e_K),\ldots$.

Prop. (0.1.17). There is an isomorphism of $\mathcal{O}$-modules $\Lambda_{f,n} \cong \mathcal{O}/\pi^n\mathcal{O}$, Cf.[Neukirch CFT P101]. Thus the automorphism of $\Lambda_{f,n}$ is all of the form u_f for units, isomorphic to U_K/U_K^n.

So we can define a **Tate module** $TG = \varprojlim \operatorname{Ker}[\pi_K^n]$, it is a free $\mathcal{O}_K$-module of rank 1.

Def. (0.1.18). As TG is a free $\mathcal{O}_G$-module of dimension 1, and G_K acts on TG, there can be attached a **Lubin-Tate character** $\chi_K : G_K \to \mathcal{O}_K^*$ by $g(\alpha) = [\chi_K(g)](\alpha)$, this depends on π_K, but its restriction on I_K doesn't depend on π_K, and is just the local CFT isomorphism composed with $x \to x^{-1}$.

Proof: $[\chi_K(g)]$ is, by definition, the morphism that is id on K^{ur} and g on L_π. So it equals g on all K^{ab} iff g is id on K^{ur}, that is, $g \in I_K$. So if $g \in I_K$, by local CFT(0.1.20), $(\chi(g))^{-1}$ corresponds to g, uniquely. □

Prop. (0.1.19). $G_{\pi,n} \cong \mathcal{O}_K^*/U_K^n$, thus we have $G_\pi \cong \mathcal{O}_K^*$. $L_{\pi,n}/K$ is Abelian totally ramified of degree $p^{n-1}(p-1)$ generated by a Eisenstein polynomial with constant coefficient π so π is in the norm group.

Proof: For this, first note Galois action induce an isomorphism on $\Lambda_{f,n}$, thus correspond to an element of U_K/U_K^n by(0.1.17), this is an injection because $\Lambda_{f,n}$ generate $L_{\pi,n}$. Then we use the canonical polynomial $f(Z) = \pi Z + Z^q$, $f^n = f^{n-1}\varphi(n)$, where $\varphi(n)$ is a Eisenstein polynomial, thus $L_{\pi,n}/K$ is totally ramifies with $|G_{\pi,n}| = q^{n-1}(q-1) = |U_K/U_K^n|$, thus the result. □

Prop. (0.1.20) (Explicit Local Norm Residue Symbol). Now we can write the universal residue symbol little bit more explicitly. For $a = u\pi^m$, (a, K) acts by φ^m on T and generated by the action $(u^{-1})_f$ on $\Lambda_{f,n}$ on $L_{\pi,n}$.

Thus the norm group of $L_{\pi,n}$ is just U^n by(0.1.19).

Proof: Cf.[Neukirch CFT P106]. □

Cor. (0.1.21). The norm groups of the totally ramified Abelian extension is precisely the groups that contains some $U_K^n \times (\pi)$ for some uniformizer π. And every totally ramified Abelian extension L/K is contained in some $L_{\pi,n}$.

Proof: For any totally ramified extension, choose a uniformizer, then its norm is a uniformizer π of K. And $N_{L/K}$ is open (as it contains $(K^*)^m$**??**.) Thus it contains some U^n. The rest follows from local CFT**??**. □

Cor. (0.1.22) (Maximal Abelian Extension of Local Fields). Let $L_\pi = \cup L_{\pi,n} = K(\Lambda_f)$, where $\Lambda_f = \cup\Lambda_{f,n}$, then $\underline{T \cdot L_\pi \text{ is the maximal extension of Abelian extension of } K}$. Hence $G_K^{ab} = G_{T,K} \times G_\pi$. This follows immediately from**??**.

Cor. (0.1.23) (Hasse-Arf). We can prove Hasse-Arf**??** in the case where K is a local field. This is because we already know the maximal Abelian extension, and $G(K^{ab}/T) \cong G(L_\pi/K) \cong \mathbb{O}_K^*$ for which we know the Galois action well(0.1.17)(0.1.19), so $i(\sigma) = v(\sigma(\alpha_n) - \alpha_n) = v([\sigma - 1](\alpha))$, which jumps at U_K^n(the same pattern as $K = \mathbb{Q}_p$**??**), thus the result.

Remark (0.1.24). There is a concrete example. When $K = \mathbb{Q}_p$, we can choose $f(Z) = (1+Z)^p - 1$, thus $L_{\pi,n}$ is just $\mathbb{Q}_p(\xi_{p^n})$. And we have $r_f = (1+Z)^r - 1$, thus we have

$$(a, \mathbb{Q}_p(\xi_{p^n})/\mathbb{Q}_p)\zeta = \zeta^r$$

where $a = up^m$, and $r \equiv u^{-1} \mod p^n$.

2 Cohomology of G_K action on $\mathbb{C}_p$

K is assumed to be a p-adic number field.

Lemma (0.2.1). Giving an $\sigma \in G(K/\mathbb{Q}_p)$, if $x, y \in \mathfrak{m}_{\mathbb{C}_p}$ that $x \equiv y \mod \pi_K^n$, then $[\pi_K]^\sigma(x) \equiv [\pi_K]^\sigma(y) \mod \pi_K^{n+1}$, where f^σ is given by action of σ on the coefficients.

Proof: This is because the coefficients of $[\pi_K]^\sigma$ are divisible by π_K except for degree q, where it is $x^q - y^q = (x-y)(x^{q-1} + x^{q-2}y + \ldots + y^{q-1})$ which is divisible by π_K^{n+1} because the residue field of K is of order q. □

Prop. (0.2.2). If we let the action of $\sigma \in G(K/\mathbb{Q}_p)$ on the residue field giving by $\overline{\sigma} : k_K \to \overline{\mathbb{F}}_p : x \mapsto x^{q_\sigma}$, where $q_\sigma = p^{n_\sigma}$ is a p-power, given an element $\eta = (\eta_0, \eta_1, \ldots) \in TG$, we have $\eta^{q_\sigma} \equiv [\pi_K]^\sigma(\eta_{n+1}^{q_\sigma}) \mod \pi_K$, hence the above lemma(0.2.1) shows that $[\pi_K^n]^\sigma\eta_n^{q_\sigma} \equiv [\pi_K^{n+1}]^\sigma(\eta_{n+1}^{q_\sigma}) \mod \pi_K^{n+1}$, so $[\pi_K^n]^\sigma(\eta_n^{q_\sigma})$ is a Cauchy sequence, converging to an element μ_σ(don't care about η).

If $g\in G_K$, then $g(\eta_n)=[\chi_K(g)](\eta_n)$, hence take q_σ-th power, $g(\eta_n^\sigma)\equiv[\chi_K(g)]^\sigma(\eta_n^{q_\sigma}) \mod \pi_K$, then

$$[\chi_K(g)]^\sigma[\pi_K^n]^\sigma(\eta_n^{q_\sigma})\equiv[\pi_K^n]^\sigma g(\eta_n^{q_\sigma})=g([\pi_K^n]^\sigma\eta_n^{q_\sigma}) \mod \pi_K.$$

hence by limiting, $g(\mu_\sigma)=[\chi_K(g)]^\sigma(\mu_\sigma)$.

Lemma (0.2.3).

$$v_p(\mu_\sigma)=\begin{cases}\frac{q_\sigma}{e_K(q-1)}+\frac{1}{e_K} & n(\sigma)\neq 0\\ \frac{1}{e_K(q-1)}+v_p(\sigma(\pi_K)-\pi_K) & n(\sigma)=0\end{cases}$$

Proof: By(0.1.14), we know the Newton polygon of $[\pi_K^n]^\sigma$. When $n(\sigma)\neq 0$, $v(\eta_1^{q_\sigma})=\frac{q_\sigma}{e_K(q-1)}>\frac{1}{e_K(q-1)}$, so the valuation of $[\pi_K]^\sigma(\eta_1^{q_\sigma})$ equals the valuation of its degree 1 term, which is $v(\pi_K\eta_1^{q_\sigma})=\frac{q_\sigma}{e_K(q-1)}+\frac{1}{e_K}$. Now we have by(0.2.2), we have $[\pi_K]^\sigma\eta^{q_\sigma}\equiv[\pi_K^2]^\sigma(\eta_2^{q_\sigma}) \mod \pi_K^2$, and $\frac{q_\sigma}{e_K(q-1)}+\frac{1}{e_K}<2/e_K$, so valuation already stable at degree 1, and $v(\mu_\sigma)=v([\pi_K]^\sigma(\eta_1^{q_\sigma}))$.

If $q_\sigma=1$, it's more delicate, because degree 1 and degree q term has the same minimal valuation, so they may jump to higher valuations. Notice $[\pi_K^n](\eta_n)=0$, so $[\pi_K^n]^\sigma(\eta_n)=([\pi_K^n]^\sigma-[\pi_K^n])(\eta_n)$. And we have by(0.3.1), for $x\in\mathcal{O}_K$, $v(\sigma(x)-x)\geq v(x)+v(\frac{\sigma(\pi_K)}{\pi_K}-1)+\delta_{v(x),0}v(\pi_K)$, with equality when $v_p(x)=q/e_K$. So by the Newton polygon, the minimum valuation of the coefficient of $[\pi_K^n]^\sigma-[\pi_K^n]$ appear at degree p^{n-1} and possibly p^n. The valuation of η_n is too small($\frac{1}{e_Kp^{n-1}(p-1)}$) that we don't need to consider other degrees but can assure that degree p^{n-1} is of minimum valuation, which is $v(\eta_n^{p^{n-1}})+v(\sigma(\pi_L)-\pi_L)=\frac{1}{e_K(q-1)}+v_p(\sigma(\pi_K)-\pi_K)$. □

Prop. (0.2.4). For any $\sigma\in G(K/\mathbb{Q}_p)\backslash\{\mathrm{id}\}$, there is an element $\alpha_\sigma\in\mathbb{C}_p^*$ that $\sigma\circ\chi_K(g)=g(\alpha_\sigma)/\alpha_\sigma$ for all $g\in G_K$, where χ_K is the Lubin-Tate character.

Proof: We let $\alpha_\sigma=\log^\sigma_{\mathcal{F}_\pi}(\mu_\sigma)$, by(0.2.3), $1/e_K<\mu_\sigma<\infty$, so by the Newton polygon analysis of $\log_{F_\pi}$(0.1.15), α_σ has the same valuation of μ_σ, in particular, $\alpha_\sigma\neq 0$. Then

$$g(\alpha_\sigma)=\log^\sigma_{\mathcal{F}_\pi}(g(\mu_\sigma))=(\log_{\mathcal{F}}\circ[\chi_K(g)])^\sigma(\mu_\sigma)=(\chi_K(g)\cdot\log_{\mathcal{F}_\pi})^\sigma(\mu_\sigma)=\sigma(\chi_K(g))\cdot\alpha_\sigma.$$

□

Cor. (0.2.5). $\log_p(\sigma(\chi_K(g)))=g(\log(\alpha_\sigma))-\log_p(\alpha_\sigma)$.

Def. (0.2.6). Let $\psi:G_K\to\Gamma_K\to\mathbb{Z}_p^*$ be a character factoring through Γ_K. Then we can form a representation $\mathbb{C}_p(\psi)$ of G_K on $\mathbb{C}_p$ that $\rho(\sigma)(x)=\psi(\sigma)\sigma(x)$. This is an action because G_K acts trivial on $\mathbb{Z}_p^*$.

If $\psi^k=\mathrm{id}$ for some k, then it is trivial on Γ_K^k. Γ_K is an open subgroup of $\mathbb{Z}_p$, so Γ_K^n is of finite index in Γ_K by**??**, hence also does its inverse image in G_K. So ψ comes from a finite extension L/K.

Prop. (0.2.7). $H^0(G_K,\mathbb{C}_p(\psi))=K$ if ψ is of finite order, and vanish if ψ is of infinite order.

Proof: Finite case: ψ factor through some G_L, so ψ corresponds to a continuous cocycle w.r.t the discrete topology of $\mathbb{C}_p$. So by(0.3.5) there is a $a\in\mathbb{C}_p^*$ that $\psi(\sigma)=\sigma(a)/a$, so $\mathbb{C}_p(\psi)\cong\mathbb{C}_p: x\mapsto ax$. And the result follows from Ax-Sen-Tate, as $K=\hat{K}$.

Infinite case: $H^0(G_K,\mathbb{C}_p(\psi))\subset H^0(H_K,\mathbb{C}_p(\psi))=\hat{K}_\infty(\psi)$ by Ax-Sen-Tate and the fact ψ is trivial on H_K. Then for the normalized trace R_n, which commutes with G_K, $g(R_n(x))=\psi^{-1}(g)R_n(x)$. But $G(K_n/K)$ is finite, so $R_n(x)=\psi^{-N}(g)R_n(x)$ for any g. So $R_n(x)=0$, otherwise ψ is of finite order. Now $R_n(x)\to x$, so $x=0$. □

Prop. (0.2.8). Now we compute $H^1(G_K, \mathbb{C}_p(\psi))$. There is a inf-res exact sequence

$$0 \to H^1(\Gamma_K, \hat{K}_\infty(\psi)) \to H^1(G_K, \mathbb{C}_p(\psi)) \to H^1(H_K, \mathbb{C}_p(\psi))$$

Then $H^1(H_K, \mathbb{C}_p(\psi)) = 0$. The first two vanish iff ψ is of infinite order, and is a K-vector space of dimension 1 if ψ is of finite order.

Proof: For the first assertion, ψ is trivial on H_K, so $\mathbb{C}_p(\psi) \cong \mathbb{C}_p$ as H_K-representation, so it suffice to show for $\psi = \mathrm{id}$. Let f be a cocycle, as H_K is compact, $f(H_K) \in p^{-k}\mathcal{O}_{\mathbb{C}_p}$ for some integer k. So the lemma below(0.2.9) shows that we can move f cohomologouly to higher valuation, i.e. $f(g) = \sum x_i - g(\sum x_i)$, so f is a coboundary.

For the second assertion, we assume $\Gamma_K \neq \mathbb{Z}_2^*$, for this case, see remark(0.2.10) below.

let γ be a topological generator of $\Gamma_K = 1 + p^k\mathbb{Z}_p^*$, $k \geq 0$, because $\mathbb{Z}_p^*$ are all topological cyclic groups except for $\mathbb{Z}_2^* \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}_2$, and γ_n be a topological generator of Γ_{F_n} which is also a power of γ. By(0.3.8) we know $H^1(\Gamma_K, \hat{K}_\infty(\psi)) = \hat{K}_\infty(\psi)/1-\gamma$.

For n large, we have a decomposition $\hat{K}_\infty(\psi) = K_n(\psi) \oplus X_n(\psi)$ by(0.3.11), and $1-\gamma_n$ is invertible on $X_n(\psi)$. Now $1 - \gamma_n = (1-\gamma)(1 + \gamma + \ldots + \gamma^{k-1})$, so $1-\gamma$ is also invertible in $X_n(\psi)$. And on $K_n(\psi)$, if ψ is of infinite order, then $1-\gamma$ is injective, otherwise $x = \psi(\gamma)^N\gamma^N(x) = \psi(\gamma)^N x$. So it is also surjective because it is a K-linear mapping of K_n. So $\hat{K}_\infty(\psi)/1-\gamma = 0$. If ψ is of finite order then $K_n(\psi) \cong K_n$ as Γ_K-module when n is large enough that γ factors through Γ_{K_n}, by(0.3.6). So $K_n/1-\gamma = K_n/\operatorname{Ker}(\mathrm{tr}_{K_n/K}) = K$. □

Lemma (0.2.9). If $f : H_K \to p^n\mathcal{O}_{\mathbb{C}_p}$ is a continuous cocycle, then there exists a $x \in p^{n-1}\mathcal{O}_{\mathbb{C}_p}$ that the cohomologous cocycle $g \mapsto f(g) - (x - g(x))$ has values in $p^{n+1}\mathcal{O}_{\mathbb{C}_p}$.

Proof: $p^{n+2}\mathcal{O}_{\mathbb{C}_p}$ is open in $p^n\mathcal{O}_{\mathbb{C}_p}$, so there is a finite extension L/K that $f(H_L) \in p^{n+2}\mathcal{O}_{\mathbb{C}_p}$. By(0.3.10), there is a z that $\mathrm{tr}_{L_\infty/K_\infty}(z) = p$, so there is a $y \in p^{-1}\mathcal{O}_{L_\infty}$ that $\mathrm{tr}_{L_\infty/K_\infty}(y) = 1$.

Now for a set of representatives Q of H_K/H_L, denote $x_Q = \sum_{h\in Q} h(y)f(h)$, then for $g \in H_K$, $g(Q)$ is also a set of representative, and $g(x_Q) = \sum_{h\in Q} gh(y)gf(h) = \sum_{h\in Q} gh(y)(f(gh) - f(g)) = x_{g(Q)} - f(g)$, as $\mathrm{tr}(y) = 1$. So $f(g) - (x_Q - g(x_Q)) = x_{g(Q)} - x_Q$. The RHS is in $p^{n+1}\mathcal{O}_{\mathbb{C}_p}$, because: if we let $gh_i = h_{g(i)}a_i$, where $a_i \in H_L$, then $x_{g(Q)} - x_Q = \sum h_{g(i)}(y)f(h_{g(i)}a_i) - \sum h_{g(i)}(y)f(h_{g(i)}) = \sum h_{g(i)}(y)h_{g(i)}(f(a_i))$, which is in p^{n+1} because $h_{g(i)}(y) \in p^{-1}\mathcal{O}_{\mathbb{C}_p}$ and $f(a_i) \in p^{n+2}\mathcal{O}_{\mathbb{C}_p}$ by the choice of L. □

Remark (0.2.10). In case $\Gamma_K = \mathbb{Z}_2^*$,

$$0 \to H^1(\{\pm 1\}, K(\psi)) \to H^1(\mathbb{Z}_2^*, \hat{K}_\infty(\psi)) \to H^1(1 + 2\mathbb{Z}_2^*, \mathbb{C}_p(\psi))$$

$H^1(\{\pm 1\}, K(\psi)) = 0$ whether $\psi(-1) = 1$ or -1. And by the same proof as above, possibly replace X_n with X_{n+1}, to remedy the singularity of $p = 2$, $H^1(1 + 2\mathbb{Z}_2^*, \mathbb{C}_p(\psi)) = K$, with generator $[g \mapsto \frac{\chi(g)-1}{\gamma-1}(a)]$ for some a. This cocycle extends to a cocycle of $\mathbb{Z}_2^*$, so the map is surjective.

Prop. (0.2.11). The 1-dimensional K-vector space $H^1(G_K, \mathbb{C}_p)$ is generated by the cocycle $[g \mapsto \log_p \chi(g)]$.

Proof: By the proof of(0.2.8), we know that $K = K/1-\gamma \subset K_n/1-\gamma \xrightarrow{f} H^1(G_K, \mathbb{C}_p)$ is an isomorphism. for $\alpha \in K$, if $\chi(g) = \gamma^k$, then $f(\alpha)(g) = (1 + \gamma + \ldots + \gamma^{k-1})(\alpha) = k\alpha = \alpha \cdot \log_p(\chi(g))/\log_p(\gamma)$. So by continuity, f is a multiple of $[g \mapsto \log_p(\chi(g))]$. □

Lemma (0.2.12). Any $f \in \mathrm{Hom}(I_K^{ab}, \mathbb{Q}_p)$ is of the form $f(g) = \mathrm{tr}_{K/\mathbb{Q}_p}(\beta_f \log_p \chi_K(g))$ for some $\beta_f \in K$.

Proof: By(0.1.18), χ_K is a canonical isomorphism $I_K^{ab} \cong \mathcal{O}_K^*$. Any $f \in \mathrm{Hom}(\mathcal{O}_K^*, \mathbb{Q}_p)$ is of the form $f(y) = \mathrm{tr}_{K/\mathbb{Q}_p}(\beta_f \log_p(y))$ for some $\beta_f \in K$, because: by**??**, when n is large, $\log_p$ is a bijection between U_K^n and $\pi_K^n \mathcal{O}_K$.

$\pi_K^n \mathcal{O}_K \to \mathbb{Q}_p$ can be extended to a map $K \to \mathbb{Q}_p$ as $\mathbb{Q}_p$ is divisible. Now trace is a invertible bilinear form on K, so the assertion is true on U_K^n for some n, and because U_K^n is of finite index in $\mathcal{O}_K^*$ and $\mathbb{Q}_p$ is of char 0, this is true for all $\mathcal{O}_K^*$. □

Prop. (0.2.13). The map $H^1(G_K, \mathbb{Q}_p) \to H^1(G_K, \mathbb{C}_p)$ is given as follows: as $f \in H^1(G_K, \mathbb{Q}_p)$ must factor through G_K^{ab}, if the restriction of f to I_K^{ab} corresponds to β_f, then f maps to $\beta_f[g \mapsto \log_p \chi(g)]$.

Proof: $f(g) = \mathrm{tr}_{K/\mathbb{Q}_p}(\beta_f \log_p \chi_K(g))$ on I_K, but this map extends to map on G_K. So $f(g) = \mathrm{tr}_{K/\mathbb{Q}_p}(\beta_f \log_p \chi_K(g)) + c(g)$ for a unramified map c on G_K.

Now by(0.3.7), $H^1(G, \hat{\mathbb{Q}}_p^{ur}/\mathbb{Q}_p)$ vanish because $H^1(G, \overline{\mathbb{F}}_p)$ vanish(0.3.6), so there is a $z \in \hat{\mathbb{Q}}_p^{ur}$ that $c(g) = g(z) - z$. And

$$\mathrm{tr}_{K/\mathbb{Q}_p}(\beta_f \log_p \chi_K(g)) = \sum_\sigma \sigma(\beta_f \log_p \chi_K(g)) = \beta_f \,\mathrm{tr}_{K/\mathbb{Q}_p}(\log_p \chi_K(g)) + \sum_\sigma (\sigma(\beta_f) - \beta_f)\sigma(\log_p \chi_K(g)).$$

Notice(0.2.4) gives a β_σ that $\sigma(\log_p \chi_K(g)) = g(\beta_\sigma) - \beta_\sigma$, and $\mathrm{tr}_{K/\mathbb{Q}_p}(\log_p \chi_K(g)) = \log_p \chi(g)$ because $(N_{K/\mathbb{Q}_p}\chi_K(g))^{-1} = (\chi(g))^{-1}$, as they both correspond via local CFT to the element in G_K^{ab} which acts by g on L_π and id on K^{ur}. Thus the result. □

Cor. (0.2.14). If $\eta : G_K \to \mathbb{Z}_p^*$ is a character and there is $y \in \mathbb{C}_p^*$ that $\eta(g) = g(y)/y$, then there exists a finite extension L of K that $\eta|_{G_L}$ is unramified, i.e. η is **potentially unramified**.

Proof: Apply $\log_p$, then the image of $f = \log_p \eta$ in $H^1(G_K, \mathbb{C}_p)$ is trivial, so the above proposition shows $\beta_f = 0$, so $\log_p \eta$ is trivial on I_K, so I_K is mapped by η into the μ_p, so $\eta((I_K^{ab})^{p-1}) = 1$.

$I_K^{ab} \cong \mathcal{O}_K^*$, so $(I^{ab})^{p-1}$ is of finite index in I_K^{ab}, so correspond to a finite Abelian extension E/K^{ur} that η is trivial on G_E. Now choose a primitive element β of E/K^{ur}, then $E \subset K(\beta) \cdot K^{ur} = (K(\beta))^{ur}$, so $\eta|_{G_{K(\beta)}}$ is unramified. □

Prop. (0.2.15). If $G_K \to GL_d(\mathbb{Q}_p)$ is such $\rho(g) = g(M)M^{-1}$ for $M \in GL_d(\mathbb{C}_p)$, then ρ is potentially unramified.

Proof: Cf.[Sen Continuous Cohomology and p-adic Galois representations]. □

3 Auxiliaries

__**Higher Ramification Groups**__

Prop. (0.3.1). For local fields L/K, if σ is in the inertia group, then

$$v_L(\frac{\sigma(x)}{x} - 1) \geq v_L(\frac{\sigma(\pi_L)}{\pi_L} - 1) + \delta_{v_L(x),0}$$

for any $x \in \mathcal{O}_L$ and a uniformizer π_L. Equality holds when $v_L(x) = 1$.

Proof: if L has residue field $\mathbb{F}_q$, then any element of $\mathcal{L}$ can be written as $\sum \xi_n \pi_L^n$, where ξ_n are all $q-1$-th roots of unity. And because σ is inertia group, all $q-1$-th roots of unity are preserved, so $\sigma(\xi_n \pi_L^n) - \xi_n \pi_L^n = \xi_n \pi_L(\frac{\sigma(\pi_L)}{\pi_L} - 1)(\sigma(\pi_L)^{n-1} + \sigma(\pi_L)^{n-2}\pi_L + \ldots + \pi_L^{n-1})$ has valuation$\geq$ $v(\frac{\sigma(\pi_L)}{\pi_L} - 1) + n$. Thus the result. □

Different and Discriminant

Prop. (0.3.2). If L/K is a finite extension and if I is an ideal of $\mathcal{O}_L$, then $v_K(\mathrm{tr}_{L/K}(I)) = \lfloor v_K(I\cdot\mathcal{D}_{L/K})\rfloor$.

Proof: By definition, $\mathrm{tr}_{L/K}(x\mathcal{O}_L)\subset\mathcal{O}_K$ iff $x\in\mathcal{D}_{L/K}^{-1}$, thus $\mathrm{tr}_{L/K}(I)\subset J$ iff $I\subset\mathcal{D}_{L/K}^{-1}J$, i.e. $\mathrm{tr}_{L/K}(I)$ is the smallest ideal J of $\mathcal{O}_K$ that contains $I\cdot\mathcal{D}_{L/K}$, thus the result. □

Galois Cohomology

Prop. (0.3.3). There is an exact sequence of pointed sets:

$$0\to H^1(G/H,M^H)\xrightarrow{inf}H^1(G,M)\xrightarrow{res}H^1(H,M)^{G/H}.$$

Proof: First $\mathrm{res}(H^1(G,M))\subset H^1(H,M)^{G/H}$ because $g(c)(h)=c(g)^{-1}c(h)h(c(g))$ is checked so $g(c)$ is cohomologous to c.

$\mathrm{res}\circ inf=0$ is easy, if $\mathrm{res}(c)=0$, then c is trivial on H, hence $c(gh)=c(g)$ and $h(c(g))=c(hg)=c(g\cdot g^{-1}hg)=c(g)$, so c is inflated from $H^1(G/H,M^H)$.

For the injectivity of inf. If $c(\overline{g})=g^{-1}g(a)$, then $a\in M^H$, so it is a coboundary in $H^1(G/H,M^H)$. □

Prop. (0.3.4). For L/K a Galois extension, $H^1(G(L/K),GL_n(L))=1$, where L is equipped with the discrete topology.

Proof: We prove any cocycle is a coboundary, for this, notice any cocycle factor through a finite quotient, and the images of it is contained in a finite extension of K, hence it reduce to the case of L/K finite.

For some $a\in H^1(G,GL_n(L))$, for a vector $x\in L^n$, let $P(x)=\sum a(\sigma)\sigma(x)$, then $\{P(x)\}$ generate L^n, because if f is a linear functional that vanish on it, then

$$0=f(P(\lambda x))=\sum f(a(\sigma)\sigma x)\sigma\lambda.$$

But automorphisms are linearly independent over L, hence $f(a(\sigma)\sigma(x))=0$ for all σ, so $f=0$ as $a(\sigma)\in GL_n(L)$

Now let $\{P(x_i)\}$ generate L^n, then let T be the matrix with x_i as rows, then $P=\sum a(\sigma)\sigma(T)$ is invertible. Now $a(\sigma)=P\cdot\sigma(P)^{-1}$ is a cocycle. □

Cor. (0.3.5) (Hilbert's Multiplicative Satz 90). $H^1(G_{L/K},L^*)=0$ for Galois extension L/K, where L is equipped with the discrete topology

Prop. (0.3.6) (Hilbert's Additive Satz 90). For L/K a Galois extension, $H^1(G(L/K),L)=1$, where L is equipped with the discrete topology.

Proof: Form the normal basis theorem**??**, for finite Galois extension L/K, L is an induced module over K, thus $H^*(G,L)=H_*(G,L)=0$ for $*\neq 0$ and $H_T^*(G,L)=0$ by**??**.

Hence the same is true, for arbitrary Galois extension, when L is equipped with the discrete topology, the same as in the proof of(0.3.4). □

Prop. (0.3.7). Let π be a topologically nilpotent element of A which is complete in the π-adic topology and π is not a zero-divisor, let $R=A/\pi A$ equipped with discrete topology. Let G be a group which acts continuously on A and fix π, then if $H^1(G,R)$ is trivial, then $H^1(G,A)$ is trivial, and if moreover $H^1(G,GL_n(R))$ is trivial, then $H^1(G,GL_n(A))$ is trivial.

Proof: Cf.[Galois Representations Berger P15]. □

Prop. (0.3.8) (Cyclic Case). if G is a topological cyclic group $\overline{\langle g\rangle}$, then the map $H^1(G,M)\to M/(1-g)$ is well-defined and injective. And when M is profinite, p-adically complete, then the map is also surjective.

Proof: The surjection: there is only one choice: $c(g^i)=(1+g+\ldots+g^{i-1})(m)$. And we need to verify that it is continuous. The case of p-adic can be deduced from profinite case, because $c(\gamma)\in p^{-k}M$ for some k, and $p^{-k}M$ is then profinite. For any finite quotient N of M, there is a k that $kM=0$, and a n that $g^n=\mathrm{id}$ on N, so $c(g^{rkn})=0$ on N, which shows c is continuous. □

Ramification of Cyclotomic Fields

Prop. (0.3.9). $p^n v_p(\mathcal{D}_{K_n/F_n})$ is bounded and eventually constant. In particular $v_p(\mathcal{D}_{K_n/F_n})$ converges to 0.

Proof: Cf.[Galois representation Berger P20]. □

Cor. (0.3.10). If L/K is a finite extension, then $\mathrm{tr}_{L_\infty/K_\infty}(\mathfrak{m}_{L_\infty})=\mathfrak{m}_{K_\infty}$.

Proof: By(0.3.2) and the fact $G(L_\infty/K_\infty)\cong G(L_n/K_n)$ for n large by**??**, we have $\mathrm{tr}_{L_\infty/K_\infty}(\mathfrak{m}_{L_n})=\mathfrak{m}_{K_n}^{c_n}$, where $c_n=\lfloor v_{K_n}(\mathfrak{m}_{L_n}\mathcal{D}_{L_n/K_n})\rfloor$. By the above proposition, c_n is bounded by a c. But if $x\in\mathfrak{m}_{K_\infty}$, $x\in\mathfrak{m}_{K_n}^c$ for n large, so $x\in\mathrm{tr}_{L_\infty/K_\infty}(\mathfrak{m}_{L_\infty})$. □

Prop. (0.3.11). There is a decomposition of $\hat{K}_\infty=X_n\oplus X_n$, where $X_n=\mathrm{Ker}\,R_n$. If $\delta>0$, then for n large, $\alpha\in\mathbb{Z}_p^*$ and γ_n that $\chi(\gamma_n)$ is a topological generator Γ_{F_n}, $1-\alpha\gamma_n:X_n\to X_n$ (because γ commutes with R_n) is invertible and $v_p((1-\alpha\gamma_n)^{-1}x)\geq v_p(x)-1/(p-1)-\delta$, unless $\alpha=-1$ and $p=2$, in which case it is only invertible on X_{n+1}.

Proof: As usual, x_i is a basis of $\mathcal{O}_{K_n/F_n}$, then $x=\sum x_ie_i^*$, $x_i=\mathrm{tr}_{K_\infty/F_\infty}(xe_i)\in\hat{F}_\infty$, and $R_n(x)=0$. Then $(1-\alpha\gamma_n)$ acts on x_i, so it reduce to the case $K=\mathbb{Q}_p$, if one notices**??** and(0.3.9).

Injectivity: If $\alpha=1$, this is Ax-Sen-Tate. In other situations, $(1-\alpha\gamma_n)(R_{n+k}(x))=0$ for all $k\geq 0$, so $R_{n+k}(x)=\alpha^{p^k}\gamma_n^{p^k}(R_{n+k}(X))=\alpha^{p^k}R_{n+k}(X)$, so $R_{n+k}(x)=0$, hence $x=0$.

Surjectivity: Cf.[Galois representation Berger P23]. □