The p-adic Cyclotomic Character

Shubhrajit Bhattacharya
shubhrajit@cmi.ac.in

The Galois Representation Reading Group

Introduction

We wish to define a group homomorphism

$$\chi_p : G_{\mathbb{Q}} \longrightarrow \mathbb{Z}_p^*$$

where $\mathbb{Z}_p^*$ is the group of units of the ring $\mathbb{Z}_p$ of p-adic integers. The elements of $\mathbb{Z}_p$ can be identified with a Cauchy sequence $\{a_n\}_{n\geq 1}$ with $a_n \in \mathbb{Z}$ and satisfying the following conditions

1. $0 \leq a_n \leq p^n - 1 \quad \forall\, n \in \mathbb{N}$
2. $a_n \equiv a_{n+1} \pmod{p^n} \quad \forall\, n \in \mathbb{N}$

In fact, this representation is unique as a consequence of the following theorem

Theorem 1. *Every equivalence class $\boldsymbol{a}$ of Cauchy sequence sequences in $\mathbb{Q}_p$ exactly one representative Cauchy sequence $\{a_n\}_{n\geq 1}$ in $\mathbb{Q}$ satisfying the following properties*

1. $0 \leq a_n \leq p^n - 1 \quad \forall\, n \in \mathbb{N}$

2. $a_n \equiv a_{n+1} \pmod{p^n} \quad \forall\, n \in \mathbb{N}$

Proof. *Theorem 2* of §3 of chapter 1 in Neal Koblitz. □

Let $\sigma \in G_{\mathbb{Q}}$ and $K/\mathbb{Q}$ be a finite Galois extension. For any $\alpha \in K$, $\sigma(\alpha)$ is a root of the minimal polynomial of α since σ fixes $\mathbb{Q}$ point-wise. Therefore, normality of $K/\mathbb{Q}$ implies that $\sigma(\alpha) \in K$. Hence $\sigma(K) \subseteq K$. Thus σ restricts to K and gives an element $\sigma|_K$ of $\mathrm{Gal}(K/\mathbb{Q})$. Let $C_n = \mathbb{Q}(\zeta_{p^n})$ be the p^n-th *cyclotomic extension* of $\mathbb{Q}$, where

$$\zeta_{p^n} = \exp\left\{\frac{2\pi i}{p^n}\right\}$$

for $n \in \mathbb{N}$. Therefore σ restricts to $C_n/\mathbb{Q}$ and gives an element $\sigma_n := \sigma|_{C_n}$

$$\mathrm{Gal}(C_n/\mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}) \cong (\mathbb{Z}/p^n\mathbb{Z})^{\times}$$

Since $\sigma_n \in \mathrm{Gal}(C_n/\mathbb{Q})$, $\sigma_n(\zeta_{p^n})$ is also a p^n-th root of unity which is not 1 (σ_n is a field automorphism fixing $\mathbb{Q}$ point-wise, $1 \in \mathbb{Q}$ and $1 \neq \zeta_{p^n}$). Therefore, for each $n \in \mathbb{N}$, we get a $1 \leq z_n \leq p^n - 1$ such that

$$\sigma_n(\zeta_{p^n}) = \zeta_{p^n}^{z_n}$$

Observe that

$$\zeta_{p^{n+1}}^{p} = \exp\left\{\frac{2\pi i}{p^{n+1}}\right\}^{p} = \exp\left\{\frac{2p\pi i}{p^{n+1}}\right\} = \zeta_{p^n}$$

Therefore,

$$\zeta_{p^n}^{z_{n+1}} = \zeta_{p^{n+1}}^{pz_{n+1}} = (\sigma_{n+1}(\zeta_{p^{n+1}}))^p = \sigma_{n+1}(\zeta_{p^{n+1}}^{p}) = \sigma_{n+1}(\zeta_{p^n})$$

Since $\mathbb{Z}/p^n\mathbb{Z} \hookrightarrow \mathbb{Z}/p^{n+1}\mathbb{Z}$, $\sigma_{n+1}(\zeta_{p^n}) = \sigma_n(\zeta_{p^n})$. Therefore,

$$\zeta_{p^n}^{z_{n+1}} = \sigma_{n+1}(\zeta_{p^n}) = \sigma_n(\zeta_{p^n}) = \zeta_{p^n}^{z_n}$$

Thus $z_n \equiv z_{n+1} \pmod{p^n}$. Therefore, $\{z_n\}_{n\geq 1}$ is a Cauchy sequence and uniquely represents an element of $\mathbb{Z}_p$. Since $z_1 \neq 0$, $\{z_n\}_{n\geq 1}$ represents an element of $\mathbb{Z}_p^*$. It can be easily verified that this assignment $\sigma \mapsto \{z_n\}_{n\geq 1}$ is actually a group homomorphism from $G_{\mathbb{Q}}$ to $\mathbb{Z}_p^*$. Now, $\mathbb{Z}_p^*$ sits inside $\mathbb{Q}_p^\times = \mathbb{Q}_p \setminus \{0\}$. Thus we actually have a group homomorphism

$$\chi_p : G_{\mathbb{Q}} \longrightarrow \mathbb{Q}_p^\times$$

each element $\boldsymbol{\alpha} \in \mathbb{Q}_p^\times$ gives rise to an invertible linear map $\boldsymbol{x} \mapsto \boldsymbol{\alpha x}$ for all $\boldsymbol{x} \in \mathbb{Q}_p$. Thus, we can identify $\mathbb{Q}_p$ as a 1-dimensional $\mathbb{Q}_p$ vector space and $\mathbb{Q}_p^\times$ with $\mathrm{GL}_1(\mathbb{Q}_p)$. Hence we get a 1-dimensional p-adic representation of the absolute Galois group of $\mathbb{Q}$

$$\chi_p : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_1(\mathbb{Q}_p)$$

This map χ_p is known as the *p-adic cyclotomic character*. This is also denoted by $\mathbb{Q}_p(1)$. This (1) in bracket is because there are related representations denoted by $\mathbb{Q}_p(n)$ for all non-zero integers. We will discuss them soon. Before that, we revisit some necessary facts from finite dimensional representations of a group G.

Some necessary facts on finite dimensional representations of a group G

We will mostly study finite dimensional representations of Galois groups (possibly infinite). Infinite Galois groups are topological groups (in fact any Galois group) with the *Krüll topology*.

The dual of a representation

Let V be $\mathbb{F}$-vector space of dimension $n \in \mathbb{N}$. Let G be a group and let ρ be a representation of G

$$\rho : G \longrightarrow \mathrm{GL}_{\mathbb{F}}(V)$$

We sometimes call that V *is a representation of* G. In this way of saying, we get that the dual space of V, *i.e.* $V^* = \mathrm{Hom}_{\mathbb{F}}(V, \mathbb{F})$ is also a representation of G. We want to define a group homomorphism

$$\rho^* : G \longrightarrow \mathrm{GL}_{\mathbb{F}}(V^*)$$

There is a natural *paring* $\langle \cdot\,, \cdot \rangle : V^* \times V \longrightarrow \mathbb{C}$, given by

$$\langle \varphi, \boldsymbol{v} \rangle \coloneqq \varphi(\boldsymbol{v}) \quad \forall\, \varphi \in V^*, \boldsymbol{v} \in V$$

We want that ρ and ρ^* preserves this *pairing* $\langle \cdot\,, \cdot \rangle$, *i.e.*

$$\langle \rho^*(g)(\varphi), \rho(g)(\boldsymbol{v}) \rangle = \langle \varphi, \boldsymbol{v} \rangle$$

for all $g \in G, \varphi \in V^*, \boldsymbol{v} \in V$. For any linear map $A \in \mathrm{GL}_{\mathbb{F}}(V)$, there is dual map $T^* \in \mathrm{GL}_{\mathbb{F}}(V^*)$, defined as follows

$$T^*(\varphi)(\boldsymbol{v}) = \varphi(T\boldsymbol{v}) \quad \forall\, \boldsymbol{v} \in V$$

We define $\rho^* : G \longrightarrow \mathrm{GL}_{\mathbb{F}}(V^*)$ as follows

$$\rho^*(g) \coloneqq (\rho(g^{-1}))^* \quad \forall\, g \in G$$

We first verify that this is indeed a group homomorphism.

Proposition 1. *The map $\rho^* : G \longrightarrow \mathrm{GL}_{\mathbb{F}}(V^*)$ is indeed a group homomorphim.*

Proof. We use the facts from linear algebra and group theory that for two linear maps $S, T \in \mathrm{GL}_{\mathbb{F}}(V)$, we have $(ST)^* = T^*S^*$ and for any two elements $a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$. Let $g, h \in G$. Then we get that

$$\begin{aligned} \rho^*(gh) &= (\rho((gh)^{-1}))^* \\ &= (\rho(h^{-1}g^{-1}))^* = (\rho(h^{-1})\rho(g^{-1}))^* \\ &\qquad \text{(since } \rho \text{ is a group homomorphism)} \\ &= (\rho(g^{-1}))^*(\rho(h^{-1}))^* = \rho^*(g)\rho^*(h) \end{aligned}$$

This completes the proof. □

Since V is finite dimensional, we can identify $\mathrm{GL}_{\mathbb{F}}(V) \cong \mathrm{GL}_n(\mathbb{F})$ with the space of $n \times n$ invertible matrices, we can also view the elements $\rho(g)$ (similarly) as matrices in $GL_n(\mathbb{F})$ by fixing some basis. Let use fix the standard bases $\mathcal{B} = \{\boldsymbol{e}_1, \boldsymbol{e}_1, \ldots, \boldsymbol{e}_n\}$ for V (identifying V with $\mathbb{F}^n$) and the corresponding $\mathcal{B}^* = \{\boldsymbol{e}_1^*, \boldsymbol{e}_1^*, \ldots, \boldsymbol{e}_n^*\}$ for the dual space V^* (identifying it with $\mathrm{Hom}_{\mathbb{F}}(\mathbb{F}^n, \mathbb{F})$). Here $\boldsymbol{e}_i^*$'s are defined as follows

$$\boldsymbol{e}_i^*(\boldsymbol{e}_j) = \delta_{ij} \quad \forall\, 1 \le i, j \le n$$

What is the relation between the matrices $\rho(g)$ and $\rho^*(g)$ with respect to the bases $\mathrm{B}, \mathcal{B}^*$ respectively? Let $A = [a_{ij}]_n$ be the matrix of $\rho(g)$. Then $\rho(g^{-1})$ has the matrix of $\rho(g)^{-1}$, *i.e.* A^{-1}. By definition, we get that $\rho^*(g)$ is nothing but the linear map $(\rho(g^{-1}))^*$. We prove that the matrix of $\rho^*(g)$ with respect to $\mathcal{B}^*$ is $(A^{-1})^T$ by the following lemma.

Lemma 1. *Let M be the matrix representation of a linear map $T : \mathbb{F}^n \longrightarrow \mathbb{F}^n$ with respect to $\mathcal{B}$. Then the the matrix representation of the dual map $T^* : \mathrm{Hom}_{\mathbb{F}}(\mathbb{F}^n, \mathbb{F}) \longrightarrow \mathrm{Hom}_{\mathbb{F}}(\mathbb{F}^n, \mathbb{F})$ with respect to $\mathcal{B}^*$ is M^T.*

Proof. Let $N = [N_{ij}]$ be the matrix representation of T^* and $M = [M_{ij}]$ be that of T with respect to $\mathcal{B}^*, \mathcal{B}$ respectively. Then

$$\begin{aligned} T^*(\boldsymbol{e}_i^*) &= \sum_{k=1}^{n} \boldsymbol{e}_k^* N_{kj} \\ \implies T^*(\boldsymbol{e}_i^*)(\boldsymbol{e}_j) &= \sum_{k=1}^{n} \boldsymbol{e}_k^*(\boldsymbol{e}_j) N_{kj} = N_{ij} \end{aligned}$$

Again,

$$
\begin{aligned}
T^*(\boldsymbol{e}_i^*)(\boldsymbol{e}_j) &= \boldsymbol{e}_i^*(T(\boldsymbol{e}_j)) \\
&= \boldsymbol{e}_i^*\left(\sum_{\ell=1}^{n} M_{j\ell}\boldsymbol{e}_\ell\right) = M_{ji}
\end{aligned}
$$

Therefore $M_{ij} = N_{ji}$ and hence the proof. $\square$

Tensor product of two representations

First we recall that what is the vector space $V \otimes_{\mathbb{F}} W$ for two $\mathbb{F}$-vector spaces V, W.

Definition 1 (**Tensor product**). *Let $\mathbb{F}$ be a field and V, W be two $\mathbb{F}$-vector spaces. Then the tensor product $V \otimes_{\mathbb{F}} W$ is an $\mathbb{F}$-vector space together with a universal bilinear map*

$$(u, v) \mapsto u \otimes v \quad \forall\, (u, v) \in V \times W$$

such that for any bilinear map $\beta : V \times W \longrightarrow U$, where any $\mathbb{F}$-vector space U, there is a unique linear map $T : V \otimes_{\mathbb{F}} W \longrightarrow U$ such that the following diagram commutes

$$
\begin{tikzcd}
V \times W \arrow[r, "(u,v)\mapsto u\otimes v"] \arrow[d, "\beta"'] & V \otimes_{\mathbb{F}} W \arrow[dl, dashed, "T"] \\
U &
\end{tikzcd}
$$

Figure 1

Two representations (V, ρ) and (W, ρ') of a group G induces a representation on the vector space $V \otimes_{\mathbb{F}} W$, which is given the following natural action of G on $V \otimes_{\mathbb{F}} W$

$$g(u \otimes v) \coloneqq gu \otimes gv$$

This representation is the tensor product of the two representation V, W. By induction, we can define the tensor product of m $\mathbb{F}$-vector spaces $V_1, V_2, \ldots, V_m$

$$V_1 \otimes V_2 \otimes \cdots \otimes V_m$$

and hence any m representations of G (in the same base field $\mathbb{F}$) induces a representation on $V_1 \otimes V_2 \otimes \cdots \otimes V_m$. For any representation V, we denote the n-fold tensor product $V \otimes V \otimes \cdots \otimes V$ by $V^{\otimes n}$.

We define $\mathbb{Q}_p(-1)$ to be the *dual representation* of $\mathbb{Q}_p(1)$. Then for any $m \geq 1$, we define $\mathbb{Q}_p(m)$ to be the power $\mathbb{Q}_p(1)^{\otimes m}$ and $\mathbb{Q}_p(-m)$ to be the power $Q_p(-1)^{\otimes m}$.

Definition 2 (**Tate twist**). *Let V be a finite dimensional vector space over $\mathbb{Q}_p$ and $\rho : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_{\mathbb{Q}_p}(V)$ be any p-adic representation of $G_{\mathbb{Q}}$. Then the m^{th} Tate twist $V(m)$ of V is defined as the following representation*

$$V(m) \coloneqq V \otimes \mathbb{Q}_p(m) \qquad \forall\, m \in \mathbb{Z}$$

Algebraicity and purity-the notion of motivic weight

Let K be a number field and V be a p-adic representation of $G_K = \mathrm{Gal}(\overline{K}/K)$, the absolute Galois group of K, which is unramified at all but finitely many places of K. Let Σ denote that finite set of places outside which V is unramified.

Definition 3 (**Algebraicity**). *Let Σ' be a finite set of places of K containing Σ. A p-adic representation V of G_K is said to be algebraic (or Σ'-algebraic, to be precise) if for each place $v \notin \Sigma'$, the characteristic polynomial of* Frob_v (Frob_v *is the Frobenius element of G_K at v and it acts on V) has coefficients in $\overline{\mathbb{Q}}$.*

Definition 4 (**Purity**). *Let w be an integer. A p-adic representation V of G_K is said to be* pure of weight w, *if there exists a finite set Σ' of places of K containing Σ, such that V is Σ'-algebraic and all the roots of the characteristic polynomial of* Frob_v *has complex absolute value $q_v^{-w/2}$ for all $v \notin \Sigma'$, where q_v is the cardinality of the finite residue field of K_v, i.e. the completion of K at v.*

This w is called the *motivic weight* of V. For example, we show that $\mathbb{Q}_p(1)$ is algebraic and pure of weight -2.

Proposition 2. *The p-adic cyclotomic character $\mathbb{Q}_p(1)$ is algebraic and pure of weight -2.*

Proof. The p-adic cyclotomic character is an 1-dimensional p-adic representation of $G_{\mathbb{Q}}$ given by the map described earlier

$$\chi_p : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_1(\mathbb{Q}_p)$$

In fact, for any $\sigma \in G_{\mathbb{Q}}$, $\chi_p(\sigma) \in \mathbb{Z}_p^*$. Let $\ell \neq p$ be a prime. We recall that χ_p maps $\sigma \in G_{\mathbb{Q}}$ to a unique representative $\{z_n\}_{n\geq 1}$ satisfying the properties

1. $\sigma(\zeta_{p^n}) = \zeta_{p^n}^{z_n}$
2. $z_n \equiv z_{n+1} \pmod{p^n}$

We first show that for any prime $\ell \neq p$, $\mathbb{Q}_p(1)$ is unramified at ℓ, *i.e.*, the inertia subgroup I_ℓ of G_K at the prime ℓ acts trivially. The map χ_p factors as follows, for each $n \in \mathbb{N}$

$$\begin{tikzcd} G_{\mathbb{Q}} \arrow[rr, "\chi_p"] \arrow[d, two heads, "\sigma \mapsto \sigma|_{\mathbb{Q}(\zeta_{p^n})}"'] & & \mathrm{GL}_1(\mathbb{Q}_p) \\ \mathrm{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}) \arrow[urr, "\chi_p'"'] & & \end{tikzcd}$$

Figure 4

This restriction map $\sigma \longmapsto \sigma|_{\mathbb{Q}(\zeta_{p^n})}$ takes I_ℓ to the inertia subgroup

$$I_{(\ell_n|\ell)} \leq \mathrm{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q})$$

where ℓ_n is some prime of $\mathbb{Q}(\zeta_{p^n})$ lying above ℓ. We know that $\mathcal{O}_K = \mathbb{Z}[\zeta_m]$ for $K = \mathbb{Q}(\zeta_m)$ (cf. Marcus §2 *theorem 10*). Therefore

$$\mathrm{disc}(\mathbb{Z}[\zeta_m]) = \mathrm{disc}(\zeta_m) = \frac{(-1)^{\frac{\varphi(m)}{2}} m^{\varphi(m)}}{\prod_{p|m} p^{\frac{\varphi(m)}{p-1}}}$$

When $m = p^n$, we have that $\ell \nmid \operatorname{disc}(\mathbb{Z}[\zeta_m])$. By *theorem 24, §3, Number Fields*, ℓ is unramified and hence $I_{(\ell_n|\ell)}$ is trivial. Thus I_ℓ acts trivially on $\mathbb{Q}_p$ (since I_ℓ is inverse limit of I_{ℓ_n}). Therefore χ_p is unramified outside $\{p\}$. We get that, for all n,

$$\mathrm{Frob}_\ell|_{\mathbb{Q}(\zeta_{p^n})}(x) \equiv x^\ell \pmod{\ell_n}$$

By uniqueness of the Frobenius element, $\mathrm{Frob}_\ell|_{\mathbb{Q}(\zeta_{p^n})}$ is same as $x \mapsto x^\ell$. Therefore $z_n = \ell$ for all sufficiently large n. Thus the sequence $\{z_n\}_{n\geq 1}$ converges to the image of $\ell \in \mathbb{Z}$ in $\mathbb{Q}_p$. Since $\ell \not\equiv 0 \pmod{p}$, we get that $z_1 \neq 0$. This shows that $\chi_p(\mathrm{Frob}_\ell) = \ell$, $\ell \in \mathbb{Z}_p^*$ and hence represents the 1×1 matrix $[\ell]$ in $\mathrm{GL}_1(\mathbb{Q}_p)$. This shows that the characteristic polynomial of Frob_ℓ is $\det(TI_1 - \chi_p(\mathrm{Frob}_\ell)) = T - \ell$. Therefore we can take $\Sigma' = \Sigma = \{p\}$ and the characteristic polynomial of Frob_ℓ has coefficients in $\overline{\mathbb{Q}}$ and its only root has complex absolute value $\ell = \ell^{-\frac{-2}{2}}$ for all $\ell \neq p$ and also the cardinality of the residue field of $\mathbb{Q}$ at ℓ, *i.e.*, $\mathbb{F}_\ell = \mathbb{Z}/\ell\mathbb{Z}$, is ℓ. Hence $\mathbb{Q}_p(1)$ is algebraic and pure of weight -2. □

References

[1] Jean-Marc Fontaine & Yi Ouyang, *Theory of p-adic Galois Representations*

[2] Jürgen Neukirch, *Algebraic Number Theory*

[3] Neal Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta-Functions*

[4] Willian Fultom & Joe Harris, *Representation Theory: A First Course*

[5] Daniel A. Marcus, *Number Fields*, Second Edition (2018)