

**SHORT NOTES ON
GALOIS REPRESENTATIONS LENT 2010
(TU.TH.SA. 10AM, MR11)**

TERUYOSHI YOSHIDA

CONTENTS

Preface	2
Part 1. Introduction	3
Lecture 1. Introduction I: Algebraic number theory (Th. 14/1/10)	3
Lecture 2. Introduction II: Galois representations (Sa. 16/1/10)	3
Lecture 3. Introduction III: Automorphic representations (Tu. 19/1/10)	4
Lecture 4. Introduction IV: Motives (Th. 21/1/10)	4
Part 2. Class Field Theory of Hecke/ℓ-adic characters	5
Lecture 5. Class field theory of \mathbb{Q} : classical (Sa. 23/1/10)	5
Lecture 6. Class field theory of \mathbb{Q} : via adèles (Tu. 26/1/10)	6
Lecture 7. Global/local class field theory (Th. 28/1/10)	7
Lecture 8. Hecke characters and ℓ -adic characters (Sa. 30/1/10)	8
Part 3. Galois Representations	8

PREFACE

These are lecture notes I prepared for the Part III (Graduate level, non-examinable) course “Galois Representations” in Lent 2010. Meant to be completed as lectures proceed.

The topological groups are always Hausdorff.

Teruyoshi Yoshida
January 2010

Part 1. Introduction

LECTURE 1. INTRODUCTION I: ALGEBRAIC NUMBER THEORY (TH. 14/1/10)

LECTURE 2. INTRODUCTION II: GALOIS REPRESENTATIONS (SA. 16/1/10)

Definition 2.1. Let F be a field. We choose its separable closure \overline{F} . As all separable closures are isomorphic to each other by Steinitz' theorem, its Galois group $G_F := \text{Gal}(\overline{F}/F)$, called the *absolute Galois group* of F , is a well-defined group. It is a *profinite group*, because a natural isomorphism $G_F = \varprojlim_{F'} \text{Gal}(F'/F)$, where F' runs through all finite Galois subextensions of \overline{F}/F , gives a profinite structure on G_F . Thus it is a profinite topological group.

A *profinite structure* on a set (resp. group, ring) X is an isomorphism $X \cong \varprojlim_{\lambda} X_{\lambda}$, where $\{X_{\lambda}\}_{\lambda \in \Lambda}$ is an inverse system of *finite* sets (resp. groups, rings). Two such structures are *equivalent* when there is an isomorphism between their cofinal subsystems. An equivalence class of profinite structure defines a topology on X , namely an inverse limit topology where each X_{λ} is considered as a discrete set (resp. group, ring). This is called a *profinite topology* on X . As inverse limit topology is the subspace topology when considered as a closed subspace of $\prod_{\lambda} X_{\lambda}$, it is compact Hausdorff, and is *totally disconnected*, i.e. every connected component is a singleton. Conversely, every compact, Hausdorff, and totally disconnected topology is seen to be a profinite topology, by considering all possible continuous maps into discrete finite sets.

The *profinite completion* of \mathbb{Z} , defined as $\widehat{\mathbb{Z}} := \varprojlim_N \mathbb{Z}/(N)$, is an example of a profinite ring. The functor taking the group of units of rings commutes with inverse limits, thus we have $\widehat{\mathbb{Z}}^{\times} \cong \varprojlim_N (\mathbb{Z}/(N))^{\times}$, an example of a profinite abelian group.

Definition 2.2. For a field L , a *Galois representation* of F over L is a representation $R : G_F \rightarrow GL(V)$ of G_F on a finite dimensional vector space V over L . We always assume that R is continuous (the target $GL(V)$ can have any topology (e.g. discrete), but always Hausdorff).

We wrote $GL(V)$ for $\text{Aut}_L(V)$, which is isomorphic to $GL_n(L)$ whenever we choose a basis of V . We can consider Galois representations over arbitrary field F , but as G_F has a profinite topology, the theory is richest when L is *locally profinite* (see Lecture 6), i.e. when L is a finite extension of an ℓ -adic field \mathbb{Q}_{ℓ} for a prime ℓ . We call R an *ℓ -adic representation* of G_F when L is a subextension of $\overline{\mathbb{Q}_{\ell}}/\mathbb{Q}_{\ell}$ (we often let $L = \overline{\mathbb{Q}_{\ell}}$, but each representation turns out to have its image in $GL_n(L')$ for some finite extension L'/\mathbb{Q}_{ℓ}).

Preview: Let R be an n -dimensional Galois representations of F over $\overline{\mathbb{Q}_{\ell}}$, where F is a number field. For each place v of F , let F_v be the completion of F at v . Then G_{F_v} is identified with a subgroup of G_F , well-defined up to conjugacy. Thus a *restriction* R_v of R to G_{F_v} is well-defined up to isomorphism. When v is finite, then R_v is said to be *unramified* if it factors through the canonical surjection $G_{F_v} \rightarrow G_{k_v}$, where k_v is the residue field, a finite field. In this case $G_{k_v} \cong \widehat{\mathbb{Z}}$ is (topologically) generated by the Frobenius element, we have its eigenvalues (the *Frobenius eigenvalues*), an n -tuple of ℓ -adic numbers. When v divides ℓ , there is a class of ℓ -adic representations of G_{F_v} called *de Rham representations*, in which case an invariant called *Hodge-Tate weights*, an n -tuple of integers, is defined. We call R *algebraic* if (i) R_v is unramified for almost all v , and (ii) R_v is de Rham for all $v \mid \ell$. For an algebraic Galois representation R , we get the Frobenius eigenvalues at almost all v and the Hodge-Tate weights

at all $v \mid \ell$. As long as R is semisimple, the Frobenius eigenvalues at almost all v are enough to determine R uniquely by the *Chebotarev density theorem*.

LECTURE 3. INTRODUCTION III: AUTOMORPHIC REPRESENTATIONS (Tu. 19/1/10)

LECTURE 4. INTRODUCTION IV: MOTIVES (Th. 21/1/10)

Part 2. Class Field Theory of Hecke/ ℓ -adic characters

LECTURE 5. CLASS FIELD THEORY OF \mathbb{Q} : CLASSICAL (SA. 23/1/10)

We are interested in the *Galois representations* (see Lecture 2) of number fields F , and the *class field theory* is a theory of 1-dimensional Galois representations. When $F = \mathbb{Q}$, this has an explicit description by *cyclotomic fields*.

Definition 5.1. Let F be a field and \overline{F} its separable closure. Its *maximal abelian extension* F^{ab} is a union of all finite abelian subextensions of \overline{F}/F .

Its Galois group $G_F^{\text{ab}} := \text{Gal}(F^{\text{ab}}/F)$ is a profinite abelian group. As F^{ab} corresponds to the closure of commutators $\overline{[G_F, G_F]}$, the group G_F^{ab} is the *maximal abelian quotient* $G_F/\overline{[G_F, G_F]}$ of G_F . This means that all (continuous) characters of G_F factor through G_F^{ab} , i.e. considering characters of G_F^{ab} is equivalent to considering characters of G_F . Thus *class field theory* of F , which describes G_F^{ab} , is a theory of characters of G_F , i.e. 1-dimensional Galois representations.

Definition 5.2. For $N \in \mathbb{Z}_{>0}$, the *cyclotomic field* $F(\boldsymbol{\mu}_N)$ is a splitting field of $X^N - 1$ over F , and $\boldsymbol{\mu}_N$ is the set of roots of $X^N - 1$ in $F(\boldsymbol{\mu}_N)$. If $M \mid N$ then $F(\boldsymbol{\mu}_M) \subset F(\boldsymbol{\mu}_N)$, and their union $F(\boldsymbol{\mu}_\infty) := \bigcup_N F(\boldsymbol{\mu}_N)$ inside F^{ab} is the *maximal cyclotomic extension* of F . We have the following canonical injections of groups:

$$\begin{aligned} \varphi_N : \text{Gal}(F(\boldsymbol{\mu}_N)/F) &\ni (\zeta \mapsto \zeta^i, \forall \zeta \in \boldsymbol{\mu}_N) \longmapsto i \bmod N \in (\mathbb{Z}/(N))^\times, \\ \varphi &:= \varprojlim_N \varphi_N : \text{Gal}(F(\boldsymbol{\mu}_\infty)/F) \longrightarrow \widehat{\mathbb{Z}}^\times = \varprojlim_N (\mathbb{Z}/(N))^\times. \end{aligned}$$

Thus for an arbitrary field F , we have a surjection $G_F^{\text{ab}} \rightarrow \text{Gal}(F(\boldsymbol{\mu}_\infty)/F)$, followed by an injection $\varphi : \text{Gal}(F(\boldsymbol{\mu}_\infty)/F) \rightarrow \widehat{\mathbb{Z}}^\times$. The class field theory of \mathbb{Q} tells us that they are both isomorphisms when $F = \mathbb{Q}$ (the map φ is rarely an isomorphism in general).

Theorem 5.3. (Class field theory of \mathbb{Q}) *Let $F = \mathbb{Q}$ and $N \in \mathbb{Z}_{>0}$.*

- (i) (Irreducibility of cyclotomic polynomials) *The injections φ_N are isomorphisms. Hence φ is also an isomorphism.*
- (ii) (Kronecker-Weber theorem) *We have $\mathbb{Q}(\boldsymbol{\mu}_\infty) = \mathbb{Q}^{\text{ab}}$.*
- (iii) (Reciprocity law) *Let $K = \mathbb{Q}(\boldsymbol{\mu}_N)$. For a prime p not dividing N , let $\text{Fr}_p \in \text{Gal}(K/\mathbb{Q})$ be the arithmetic Frobenius, i.e. the unique element satisfying $\text{Fr}_p(x) \equiv x^p \pmod{p}$ for all $x \in \mathcal{O}_K$. Then $\varphi_N(\text{Fr}_p) = p \bmod N \in (\mathbb{Z}/(N))^\times$.*

LECTURE 6. CLASS FIELD THEORY OF \mathbb{Q} : VIA ADELES (TU. 26/1/10)

Definition 6.1. The *ring of finite adeles* is $\mathbb{A}^\infty := \mathbb{Q} \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}}$. This is a \mathbb{Q} -algebra. The *ring of adeles* is $\mathbb{A} := \mathbb{A}^\infty \times \mathbb{R}$, a direct product of \mathbb{Q} -algebras.

We are interested in its group of units $\mathbb{A}^\times = (\mathbb{A}^\infty)^\times \times \mathbb{R}^\times$ (which is called the *group of ideles* and came before adeles – “adele” was a shorthand of *additive idele*). We can view the components $(\mathbb{A}^\infty)^\times, \mathbb{R}^\times$ as subgroups of \mathbb{A}^\times , and they respectively have subgroups $\widehat{\mathbb{Z}}^\times, \mathbb{R}_{>0}^\times$. On the other hand, the structure morphism $\mathbb{Q} \rightarrow \mathbb{A}$ of the \mathbb{Q} -algebra \mathbb{A} gives an injective group homomorphism $\mathbb{Q}^\times \rightarrow \mathbb{A}^\times$, by which we consider \mathbb{Q}^\times as a subgroup.

Proposition 6.2. *The group \mathbb{A}^\times is a direct product of its subgroups $\mathbb{Q}^\times, \widehat{\mathbb{Z}}^\times$, and $\mathbb{R}_{>0}^\times$.*

The proof is a straightforward exercise using the fact that \mathbb{Z} is a UFD (the class number of \mathbb{Q} is 1) and that $\mathbb{Z}^\times = \{\pm 1\}$ (hence *inside* $(\mathbb{A}^\infty)^\times$, we have $\mathbb{Q}^\times \cap \widehat{\mathbb{Z}}^\times = \mathbb{Z}^\times = \{\pm 1\}$ and $\mathbb{Q}_{>0}^\times \cap \widehat{\mathbb{Z}}^\times = \{1\}$). Now we wrote $\widehat{\mathbb{Z}}^\times$ as a quotient of \mathbb{A}^\times . The composite

$$\text{Art}_{\mathbb{Q}} : \mathbb{A}^\times \rightarrow \mathbb{Q}^\times \backslash \mathbb{A}^\times / \mathbb{R}_{>0}^\times \cong \widehat{\mathbb{Z}}^\times \cong G_{\mathbb{Q}}^{\text{ab}}$$

(the last map is φ^{-1}) is called the *global Artin map of \mathbb{Q}* . The quotient group $\mathbb{Q}^\times \backslash \mathbb{A}^\times \cong \widehat{\mathbb{Z}}^\times \times \mathbb{R}_{>0}^\times$ is what has been called the *idele class group* of \mathbb{Q} , and its characters are called *Hecke characters* — these are nothing other than the *automorphic representations of $GL_1(\mathbb{A})$* — and if it factors through $\widehat{\mathbb{Z}}^\times$, *Dirichlet characters*. (The reason we use the left quotient notation becomes clear when we get to the non-abelian case.)

The group \mathbb{A}^\times as a restricted product. The *Chinese remainder theorem* says $\mathbb{Z}/(N) \cong \prod_{p|N} \mathbb{Z}/(p^m)$ when p^m is the exact power of p dividing N , and as the inverse limits commute with direct products, we have:

$$\widehat{\mathbb{Z}} \cong \prod_p \mathbb{Z}_p, \quad \mathbb{Z}_p := \varprojlim_m \mathbb{Z}/p^m \quad (\text{the ring of } p\text{-adic integers}).$$

Tensoring \mathbb{Q} does not commute with the (infinite) direct product, but at least gives a \mathbb{Q} -algebra homomorphism (as $\mathbb{Q} \otimes_{\mathbb{Z}} -$ is a functor):

$$\mathbb{A}^\infty \longrightarrow \prod_p \mathbb{Q}_p, \quad \mathbb{Q}_p = \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}_p \quad (\text{the } p\text{-adic field}).$$

which is seen to be an injection, and we identify \mathbb{A}^∞ with its image subring of $\prod_p \mathbb{Q}_p$ (the *restricted product*), and similarly for $(\mathbb{A}^\infty)^\times$:

$$\begin{aligned} \mathbb{A}^\infty &= \left\{ (x_p) \in \prod_p \mathbb{Q}_p \mid x_p \in \mathbb{Z}_p \text{ for almost all } p \right\}, \text{ and} \\ (\mathbb{A}^\infty)^\times &= \left\{ (x_p) \in \prod_p \mathbb{Q}_p^\times \mid x_p \in \mathbb{Z}_p^\times \text{ for almost all } p \right\}, \end{aligned}$$

where *almost all p* means “except for finitely many p ”. We obtain the inclusion $\mathbb{Q}_p^\times \ni x_p \mapsto (1, \dots, 1, x_p, 1, \dots) \in (\mathbb{A}^\infty)^\times \subset \mathbb{A}^\times$. Thus under the composition

$$\mathbb{Q}_p^\times \rightarrow \mathbb{A}^\times \xrightarrow{\text{Art}_{\mathbb{Q}}} G_{\mathbb{Q}}^{\text{ab}} \rightarrow \text{Gal}(\mathbb{Q}(\boldsymbol{\mu}_\infty^p)/\mathbb{Q}),$$

where $\mathbb{Q}(\boldsymbol{\mu}_\infty^p) := \bigcup_{(p,N)=1} \mathbb{Q}(\zeta_N)$, the prime element $p \in \mathbb{Q}_p^\times$ (hence any uniformizer) is mapped to the *geometric Frobenius* $\text{Frob}_p := \text{Fr}_p^{-1}$ (the *reciprocity law*).

LECTURE 7. GLOBAL/LOCAL CLASS FIELD THEORY (TH. 28/1/10)

The reciprocity law was formulated for unramified primes — indeed the prime decomposition (behaviour of Frobenius) at almost all p is enough to determine a number field (Chebotarev density theorem; we'll come back to this later). In the adelic formulation we had to look at the uniformizers of \mathbb{Q}_p^\times modulo \mathbb{Z}_p^\times , and on the Galois side went down to $\mathbb{Q}(\mu_\infty^p)$, the maximal abelian extension where p is unramified. But the \mathbb{Z}_p^\times exactly corresponds to the ramification of p , and this is cleanly expressed as the compatibility of global and local class field theory.

We formulate the *local class field theory* for arbitrary local field, i.e. a finite extension K of \mathbb{Q}_p . Let $\mathcal{O}, \mathfrak{p}$ be the ring of integers and its maximal ideal, and $k = \mathcal{O}/\mathfrak{p} \cong \mathbb{F}_q$ be the residue field. The *normalized valuation* is denoted by $v : K^\times \rightarrow \mathbb{Z}$, sending uniformizers to 1. Then its *maximal unramified extension* $K^{\text{ur}} := K(\mu_\infty^p) = \bigcup_{(p,N)=1} K(\mu_N)$ is a DVF with the ring of integers \mathcal{O}^{ur} and the residue field $\mathcal{O}^{\text{ur}}/\mathfrak{p} \cong \bar{k}$, and the *Hensel's lemma* gives an isomorphism

$$\text{Gal}(K^{\text{ur}}/K) \ni \sigma \xrightarrow{\cong} \sigma|_{\mathcal{O}^{\text{ur}}} \bmod \mathfrak{p} \in \text{Gal}(\bar{k}/k).$$

The *geometric Frobenius* $\text{Frob}_K \in \text{Gal}(K^{\text{ur}}/K)$ is defined as the element mapping to $(x \mapsto x^q)^{-1} \in \text{Gal}(\bar{k}/k)$. For an algebraic extension L/K containing K^{ur} , we define its *Weil group* by

$$W(L/K) := \{\sigma \in \text{Gal}(L/K) \mid \sigma|_{K^{\text{ur}}} \in \text{Frob}_K^{\mathbb{Z}}\}.$$

We define the *valuation* $v : W(L/K) \rightarrow \mathbb{Z}$ by $\sigma|_{K^{\text{ur}}} = \text{Frob}_K^{v(\sigma)}$. The *Weil group* of K is $W_K := W(\bar{K}/K)$, and we have $W_K^{\text{ab}} = W(K^{\text{ab}}/K)$. If K'/K is finite, then $W_{K'} \subset W_K$.

Theorem 7.1. (Local class field theory) *We have a unique group homomorphism (the local Artin map) $\text{Art}_K^{-1} : W_K \rightarrow K^\times$, such that:*

- (i) (normalisation) $v \circ \text{Art}_K^{-1} = v$.
- (ii) (base change) *If K'/K is finite abelian, then $\text{Art}_K^{-1}(W_{K'}) = N_{K'/K}(K'^\times)$.*

Moreover, it induces $W_K^{\text{ab}} \cong K^\times$ (thus $\text{Art}_K : K^\times \xrightarrow{\cong} W_K^{\text{ab}}$), and for every finite K'/K , we have $N_{K'/K} \circ \text{Art}_{K'} = \text{Art}_K$ on $W_{K'}$ (the local base change for GL_1).

Now we compare the local and global Galois groups. For a number field F , a *finite place* v is an isomorphism class of field homomorphism $F \rightarrow K$ with dense image, where K is a local field (they correspond bijectively to the prime ideals of \mathcal{O}_F). We write $K = F_v$, the *completion* of F at v . Then $F \rightarrow F_v$ extends to $\bar{F} \rightarrow \bar{F}_v$ by Steinitz' theorem, and this gives $G_{F_v} \rightarrow G_F$, well defined up to conjugation, and injective (by the density of \bar{F} in \bar{F}_v ; Krasner's lemma and weak approximation). Thus we have well defined subgroups $W_{F_v}^{\text{ab}} \subset G_{F_v}^{\text{ab}} \subset G_F$. Back to the class field theory of \mathbb{Q} —

Proposition 7.2. (Global/local compatibility for class field theory of \mathbb{Q}) *The restriction of $\text{Art}_{\mathbb{Q}} : \mathbb{A}^\times \rightarrow G_{\mathbb{Q}}^{\text{ab}}$ to \mathbb{Q}_p^\times gives $\text{Art}_{\mathbb{Q}_p} : \mathbb{Q}_p^\times \xrightarrow{\cong} W_{\mathbb{Q}_p}^{\text{ab}}$.*

LECTURE 8. HECKE CHARACTERS AND ℓ -ADIC CHARACTERS (SA. 30/1/10)

Locally profinite groups and the topology of \mathbb{A}^\times . In general, for an algebraic group G over \mathbb{Q} , we have an *adelic group*

$$G(\mathbb{A}) = G(\mathbb{A}^\infty) \times G(\mathbb{R}),$$

and the group of ideles is special case when $G = GL_1$. If G is defined over \mathbb{Z} as in the case $G = GL_n$, then $G(\mathbb{A}^\infty)$ is a *locally profinite* group (which we explain in a minute), whose topology is defined by the profinite subgroup $G(\widehat{\mathbb{Z}}) = \varprojlim_N G(\mathbb{Z}/(N))$. A topological group G

is called *locally profinite* if it has an open subgroup U such that the subspace topology on U is a profinite topology (see Lecture 2). Because $G = \coprod_{g \in G/U} gU$ as a topological space, the topology of G is determined by the topology of U and the group structure. Thus, when a group G has a subgroup U with a profinite structure, we can give a locally profinite topology on G by declaring that U is an open subgroup. This is how we topologised $G(\mathbb{A}^\infty)$ above (we will see another example later, the topology of local *Weil groups*). For example when $G = \mathbb{G}_a$ (the additive group), we have a locally profinite topology on \mathbb{A}^∞ by $\widehat{\mathbb{Z}} \subset \mathbb{A}^\infty$, and this makes \mathbb{A}^∞ into a topological ring. When $G = GL_1$, we get the topology of $(\mathbb{A}^\infty)^\times$. But we haste to remark that this is *not* the subspace topology induced from that of \mathbb{A}^∞ . In $\mathbb{A}^\times = (\mathbb{A}^\infty)^\times \times \mathbb{R}^\times$, the subgroups $\widehat{\mathbb{Z}}^\times, \mathbb{R}_{>0}^\times$ are open subgroups of the components $(\mathbb{A}^\infty)^\times, \mathbb{R}^\times$. As $(\mathbb{A}^\infty)^\times$ is totally disconnected and $\mathbb{R}_{>0}^\times$ is the connected component of 1 in \mathbb{R}^\times , the connected component of 1 in \mathbb{A}^\times is $\mathbb{R}_{>0}^\times$. Thus $\widehat{\mathbb{Z}}^\times \mathbb{R}_{>0}^\times$ is an open subgroup of \mathbb{A}^\times . The other part \mathbb{Q}^\times is very different.

Proposition 8.1. *The subgroup \mathbb{Q}^\times is discrete in \mathbb{A}^\times .*

Part 3. Galois Representations