CLASS FIELD THEORY OF $\mathbb{Q}$

This is addendum to Yihang's note on CFT theory for the special case when the base field K is the rational numbers $\mathbb{Q}$. In this case, CFT boils down to the theory of cyclotomic extensions which we will now review.

1. Cyclotomic extensions

Let F be a number field with ring of integers $\mathcal{O}_F$, N a positive integer and ζ_N a primitive N^{th} root of unity.. For a prime $\mathfrak{p}$ of F, we denote by $k_{\mathfrak{p}}$ the reside field of F at $\mathfrak{p}$, it is finite field and we let $q = \#k_{\mathfrak{p}}$ where q is a power of the prime $p \in \mathbb{Z}$.

The extension $F(\zeta_N)/F$ is Galois as it is the splitting field of $X^N - 1$, and we have an injection $\chi_N : \mathrm{Gal}(F(\zeta_N)/F) \hookrightarrow \mathbb{Z}/N\mathbb{Z}^\times$, which takes an element σ to the element m of $\mathbb{Z}/N\mathbb{Z}^\times$ for which $\sigma(\zeta_N) = \zeta_N^m$, so that the extension is also abelian.

Proposition 1.1. *1) Let N be coprime to $char\mathfrak{p}$, then $\mathfrak{p}$ is unramified in the extension $F(\zeta_N)/F$.*

2) $\chi_N(Frob_{\mathfrak{p}}) = q$

3) $\mathfrak{p}$ decomposes into a product of r primes in $F(\zeta_N)$ where $r := [F(\zeta_N) : F]/f$ where f is the order of q in $\mathbb{Z}/\mathfrak{N}\mathbb{Z}^\times$.

Proof. 1) Let $\mathfrak{p}'$ be a prime of $F(\zeta_N)$ above $\mathfrak{p}$ and let $D_{\mathfrak{p}}$ denote the decomposition group at $\mathfrak{p}$. Then if $\zeta_N \mapsto \zeta_N^i$ lies in the kernel of the map $D_{\mathfrak{p}} \to Gal(k_{\mathfrak{p}'}/k_{\mathfrak{p}})$, then $\zeta_N^i - \zeta_N \in \mathfrak{p}'$.

However if $f(X)$ is the polynomial $f(X) = 1 + X + ... + X^{N-1}$, we have that

$$\prod_{i=1}^{N-1}(1 - \zeta^i) = f(1) = N$$

and since N is coprime to p, we have that $\zeta^i - \zeta \in \mathfrak{p}'$ implies that $i = 1$.

2) $Frob_{\mathfrak{p}} \in D_{\mathfrak{p}}$ is characterised by the fact that it is mapped to the element $x \mapsto x^q$ in $Gal(k_{\mathfrak{p}'}/k_{\mathfrak{p}})$. Thus if $\overline{\zeta_N}$ denotes the image of ζ_N mod $\mathfrak{p}'$, it follows that

$$\overline{Frob_{\mathfrak{p}}(\zeta_N)} = \overline{\zeta}_N^q$$

However the reduction $1, \overline{\zeta_N}, ..., \overline{\zeta_N^{N-1}}$ are all distinct modulo $\mathfrak{p}$, hence $Frob_{\mathfrak{p}}(\zeta_N) = \zeta_N^q$.

3) Since $\mathfrak{p}$ is unramified in $F(\zeta_N)$, it decomposes as $\mathfrak{q}_1...\mathfrak{q}_r$ in $\mathcal{O}_{F(\zeta_N)}$, and $[F(\zeta_N) : F] = rf$ where f is the size of any residue extension $[k_{\mathfrak{q}_i} : k_{\mathfrak{p}}]$. But f is just the size of $Gal(k_{\mathfrak{p}}(\zeta_N)/k_{\mathfrak{p}})$, which is cyclic and generated by $Frob_{\mathfrak{p}}$, and hence is the order of q in $\mathbb{Z}/N\mathbb{Z}^\times$. □

Define the fields

$$F^{cyc,p} = \bigcup_{(N,p)=1} F(\zeta_N)$$

$$F^{cyc} = \bigcup_{N} F(\zeta_N)$$

If we take inverse limits of the homomorphism

$$\chi_N : Gal(F(\zeta_N)/F) \to \mathbb{Z}/N\mathbb{Z}^\times$$

over all integers (resp. integers coprime to p) we obtain homomorphisms

$$\chi_F^p : Gal(F^{cyc,p}/F) \to \prod_{p' \neq p} \mathbb{Z}_{p'} := \hat{\mathbb{Z}}^p$$

$$\chi_F : Gal(F^{cyc}/F) \to \hat{\mathbb{Z}}$$

fitting into the commutative diagrams:

$$\begin{tikzcd}
\chi_F^p Gal(F^{cyc,p}/F) \arrow[r, hook] \arrow[d, equal] & \hat{\mathbb{Z}}^p \arrow[d, equal] \\
\lim_{\leftarrow (p,N)=1} Gal(F(\zeta_N)/F) \arrow[r, hook] & \lim_{\leftarrow (p,N)=1} \mathbb{Z}/N\mathbb{Z}^\times
\end{tikzcd}$$

$$\begin{tikzcd}
\chi_F : Gal(F^{cyc}/F) \arrow[r, hook] \arrow[d, equal] & \hat{\mathbb{Z}} \arrow[d, equal] \\
\lim_{\leftarrow N} Gal(F(\zeta_N)/F) \arrow[r, hook] & \lim_{\leftarrow N} \mathbb{Z}/N\mathbb{Z}^\times
\end{tikzcd}$$

χ_F is called the cyclotomic character associated to the field F.

As $F^{cyc,p}$ is a subfield of F^{cyc}, there is a natural projection

$$Gal(F^{cyc}/F) \to Gal(F^{cyc,p}/F)$$

which makes the following diagram commute:

$$\begin{tikzcd}
\chi_F : & Gal(F^{cyc}/F) \arrow[r] \arrow[d, two heads] & \hat{\mathbb{Z}} \arrow[d, two heads] \\
\chi_F^p : & Gal(F^{cyc,p}/F) \arrow[r] & \hat{\mathbb{Z}}^p
\end{tikzcd}$$

The previous proposition shows that $\chi_F^p(Frob_{\mathfrak{p}}) = q \in \hat{\mathbb{Z}}^p$.

2. Class field theory of $\mathbb{Q}$

When $F = \mathbb{Q}$, the Kronecker Weber theorem (which can be proved independently of CFT) tells us that $\mathbb{Q}^{ab} = \mathbb{Q}^{cyc}$, hence the class field theory of $\mathbb{Q}$ just follows from cyclotomic theory. In the following, the prime ideal $\mathfrak{p}$ is replaced with the rational prime generated by p.

Theorem 2.1. *(Class field theory of $\mathbb{Q}$)*

1) The injection $\chi_{\mathbb{Q}} : Gal(\mathbb{Q}^{ab}/\mathbb{Q}) \to \hat{\mathbb{Z}}$ is an isomorhism.

2) $\chi_{\mathbb{Q}}^p(Frob_p) = p \in \hat{\mathbb{Z}}^p$.

Proof. We have already seen part 2) from the above remark. Part 1) follows immediately from the irreducibiliy of cyclotomic polynomials, as this shows that χ_N is an isomorphism for all N. □

Our task now will be to translate the above into adelic language. It turns out the the group idele of classes has a very explicit description and that what is defined in Yihang's notes as the global Artin map is essentially just the inverse of the cyclotomic character $\chi_{\mathbb{Q}}$ defined above.

Remark 2.2. Actually with our conventions $\chi_{\mathbb{Q}}$ is the inverse of Art up to a sign. This comes about because we chose $Frob_p$ to be the "arithmetic Frobenius," had we instead chose it to be the "geometric Frobenius" (which is just the inverse of arithmetic Frobenius) the signs would work out. This sort of sign discrepancy occurs regularly in the literature so I chose this convention just to point it out.

3. Adelic reformulation

We refer to Yihang's notes for the definition of the ring of adeles $\mathbb{A}_F$ and the group of ideles $\mathbb{A}_F^*$. Our first aim will to prove that $\mathbb{A}_{\mathbb{Q}}^*$ is naturally isomorphic to the direct product $\hat{\mathbb{Z}}^* \times \mathbb{Q}^* \times \mathbb{R}_{>0}^*$.

Recall that $\mathbb{A}_{\mathbb{Q}}$ defined to be the restricted direct product over all places of $\mathbb{Q}$ of the completions of $\mathbb{Q}$ at each place, with respect to the compact open subgroups $\mathbb{Z}_p$ at each finite place. It is straightforward to show that $\mathbb{A}_{\mathbb{Q}}^*$ is then naturally the restricted direct product of the of the completions $\mathbb{Q}_v^*$ at all places of v of $\mathbb{Q}$ with respect to the compact open subgroups $\mathbb{Z}_p^*$ for all finite places p.

Conceretely an element of $\mathbb{A}_{\mathbb{Q}}^*$ consists of a sequence $(x_v)_v$ where v runs over places of $\mathbb{Q}$, such that for almost all finite places v corresponding to a prime p, $x_v \in \mathbb{Z}_p^*$. The only places v of $\mathbb{Q}$ are either finite, so corresponds to a prime p, or the embedding $\infty : \mathbb{Q} \to \mathbb{R}$. Thus an element of $\mathbb{A}_{\mathbb{Q}}^*$ can be considered as pair $((x_p)_{p \text{ prime}}, x_\infty)$ where $x_p \in \mathbb{Q}_p^*$, and $x_p \in \mathbb{Z}_p^*$ for almost all p and $x_\infty \in \mathbb{R}^*$.

This gives a natural decomposition

$$\mathbb{A}_{\mathbb{Q}}^* = \mathbb{A}_{\mathbb{Q}}^{f*} \times \mathbb{R}^*$$

where $\mathbb{A}_{\mathbb{Q}}^{f*}$ is the group of finite ideles given by the restricted direct product over all $\mathbb{Q}_p^*$ with respect to the compact open subgroups $\mathbb{Z}_p^*$.

By the chinese remainder theorem $\hat{\mathbb{Z}}$ decomposes as the product $\hat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$, and hence there is a natural inclusion

$$\hat{Z}^* \hookrightarrow \mathbb{A}_{\mathbb{Q}}^*$$

We thus have three natural subgroups of $\mathbb{A}_{\mathbb{Q}}^*$:

$$\mathbb{Q}^* \hookrightarrow \mathbb{A}_{\mathbb{Q}}^*,\ x \mapsto (x, x)$$

$$\hat{\mathbb{Z}}^* \hookrightarrow \mathbb{A}_{\mathbb{Q}}^*,\ u \mapsto (u, 1)$$

$$\mathbb{R}_> 0^* \hookrightarrow \mathbb{A}_{\mathbb{Q}}^*,\ y \mapsto (1, y)$$

Since the group $\mathbb{A}_{\mathbb{Q}}^*$ is abelian it suffices to show that any element of $\mathbb{A}_{\mathbb{Q}}^*$ can be written uniquel as a product of images of elements under the above embeddings.

Given $((x_p)_p, x_\infty)$, consider the element $x = \pm p^{v_p(x_p)} \in \mathbb{Q}$, where the sign of x matches x_∞ (this uses the fact that $\mathbb{Z}$ is PID). Then multiplying by x^{-1}, we see the element $((x^{-1}x_p)_p, x^{-1}x_\infty)$, satisfies $v_p(x^{-1}x_p) = 0$ and $x^{-1}x_\infty > 0$. Therefore $(x^{-1}x_p)_p \in \mathbb{Z}_p^*$ and $x^{-1}x_\infty \in \mathbb{R}_{>0}^*$. This gives us the decomposition $((x_p)_p, x_\infty) = xuy$ as above and it is clearly unique.

We thus obtain $\mathbb{Q}^* \backslash \mathbb{A}_{\mathbb{Q}}^* \cong \hat{\mathbb{Z}}^* \times \mathbb{R}_{>0}^*$.

Now we can define a map

$$Art_{\mathbb{Q}} : \mathbb{Q}^* \backslash \mathbb{A}_{\mathbb{Q}}^* \to Gal(\mathbb{Q}^{ab}/\mathbb{Q})$$

to be given by the composition

$$Art_{\mathbb{Q}} : \mathbb{Q}^* \backslash \mathbb{A}_{\mathbb{Q}}^* \longrightarrow \hat{\mathbb{Z}}^* \times \mathbb{R}_{>0}^* \twoheadrightarrow \hat{\mathbb{Z}}^* \xrightarrow{\chi_{\mathbb{Q}}^{-1}} Gal(\mathbb{Q}^{ab}/\mathbb{Q})$$

The adelic version of class field theory can then be stated as

Theorem 3.1. *1) There exists a unique continuous homomorphism $Art_{\mathbb{Q}} : \mathbb{Q}^* \backslash \mathbb{A}_{\mathbb{Q}}^* \to Gal(\mathbb{Q}^{ab}/\mathbb{Q})$ satisfying the follow properties:*

i) Let $\varpi \in \mathbb{A}_{\mathbb{Q}}^*$ denote the element $\varpi = (1, ..., p, ..., 1)$ where the p occurs in the p^{th} component. Then $Art_{\mathbb{Q}}(\varpi)|_{\mathbb{Q}^{cyc,p}} = Frob_{\mathfrak{p}}^{-1}$

ii) The restriction of $Art_{\mathbb{Q}}$ to $\mathbb{R}^*$ under the natural map $\mathbb{R} \hookrightarrow \mathbb{Q}^* \backslash \mathbb{A}_{\mathbb{Q}}^*$ is trivial on $\mathbb{R}_{>0}^*$ and takes -1 to complex conjugation.

2) $Art_{\mathbb{Q}}$ induces an isomorphism $\mathbb{Q}^* \backslash \mathbb{A}_{\mathbb{Q}}^* / \mathbb{R}_{>0}^* \cong Gal(\mathbb{Q}^{ab}/\mathbb{Q})$

Proof. Everything apart from uniqueness of $Art_{\mathbb{Q}}$ is immediate from above. The proof of uniqueness is not worth mentioning here.

As a sanity check, let's trace through the proof of property i) in the above. We may multpily the element ϖ by $p^{-1} \in \mathbb{Q}$ to obtain the element $(p^{-1}, ..., 1, ...p^{-1})$ which lies in $\hat{\mathbb{Z}}^*$ since p is invertible in $\mathbb{Z}_p'$ for $p' \neq p$. Let N be coprime to p, then we have the diagram:

$$\begin{tikzcd}
\hat{\mathbb{Z}}^* \arrow[r, "\chi_{\mathbb{Q}}^{-1}"] \arrow[d, two heads] & Gal(\mathbb{Q}^{ab}/\mathbb{Q}) \arrow[d, two heads] \\
\mathbb{Z}/N\mathbb{Z}^{\times} \arrow[r, "\chi_N{}^{-1}"] & Gal(\mathbb{Q}(\zeta_N/\mathbb{Q}))
\end{tikzcd}$$

The image of ϖ in $\mathbb{Z}/N\mathbb{Z}^{\times}$ is then just p^{-1} and so corresponds to $Frob_p^{-1}$ under χ_N. Taking the limit over N coprime to p we obtain the result. This point also explains the source of the sign discrepancy with the usual definition. □

Thus in the case of $\mathbb{Q}$, the Artin map really is completely explicit. From this description we can deduce the result that we needed in lectures, namely that if $x = ((x_p)_p, x_\infty)$ was an idele such that $x_p \equiv 1 \text{mod } N$, and r was the integer such that $r = \pm p^{v_p}(x_p)$ and sgn r = sgn x_∞, then $Art_{\mathbb{Q}}(x)(\zeta_N) = \zeta_N^{-r}$ (note the sign discrepancy).

For p dividing r we let ϖ_p denote the element of $(1, ..., p, ..., 1) \in \mathbb{A}_{\mathbb{Q}}^*$. Then let $\omega = \prod_{p|r} \varpi_p^{v_p(r)} \text{sgn } r$. It follows from property i) and ii) of the Theorem that $Art(\omega)$ acts on ζ_N via $\zeta_N \mapsto \zeta_N^r$.

Now $\omega^{-1}x \in \hat{\mathbb{Z}}^* \times \mathbf{R}_{>}^* 0$ and its projection to $\mathbb{Z}/N\mathbb{Z}^{\times}$ is 1 by the assumption $x_p \equiv 1 \text{mod } N$. There $\omega^{-1}x$ acts trivially on ζ_N and so x acts via $\zeta_N \mapsto \zeta_N$.