Talk 2: Abelian Class Field Theory & Frobenius Automorphisms

Ref: Part I Sections 1.1 – 1.4

§1.1 Galois groups

Def Number field is finite extension of $\mathbb{Q}$.

Def The degree of a field extension (of number fields) $K/\mathbb{Q}$ is its dimension over $\mathbb{Q}$ as a vector space:

$$[K:\mathbb{Q}] = \deg_{\mathbb{Q}} K := \dim_{\mathbb{Q}}(K)$$

For arbitrary field extensions $[K:F] = \dim_F(K)$

Ex 1 $\mathbb{Q}(i) = \{a+bi \mid a,b \in \mathbb{Q}\}$ obtained by adjoining roots of x^2+1

Ex 2 Cyclotomic fields $\mathbb{Q}(\zeta_N)$

$\deg_{\mathbb{Q}}(\mathbb{Q}(\zeta_N)) = \varphi(N)$

Def The Galois group of K/F is

$$\mathrm{Gal}(K/F) = \{\sigma \in \mathrm{Aut}(K) \mid \sigma_F = \mathrm{id}_F\}$$

Rem K' ext of K ext of $F \rightsquigarrow$

$\mathrm{Gal}(K'/F) \longrightarrow \mathrm{Gal}(K/F)$

with kernel $\mathrm{Gal}(K'/K)$

Ex $\mathrm{Gal}((\mathbb{Q}(\zeta_N)/\mathbb{Q}) \cong (\mathbb{Z}/N\mathbb{Z})^\times$

$= \{[\bar{n}] \in \mathbb{Z}/N\mathbb{Z} \mid \gcd(n,N)=1\}$

Identified by assigning $[n]$ to $\zeta_N \mapsto \zeta_N^n$

If we have M/N then $\mathbb{Q}(\zeta_M) \hookrightarrow \mathbb{Q}(\zeta_N)$

$\rightsquigarrow (\mathbb{Z}/N\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/M\mathbb{Z})^\times$ on Galois grps

Def The algebraic closure $\overline{F}$ of F is the field obtained by adjoining all roots of polynomials over F.

Number Thy: to describe the structure of $Gal(\overline{F}/F)$.

§1.2 Abelian Class Field Theory

Def The maximal abelian quotient of a gp G is $G/[G,G]$

Rem This can be identified with $Gal(F^{ab}/F)$ where F^{ab} maximal abelian extension

Thm [Kronecker-Weber] $\mathbb{Q}^{ab}$ is obtained by adjoining all roots of unity.

Cor
$$Gal(\mathbb{Q}^{ab}/\mathbb{Q}) \cong \varprojlim (\mathbb{Z}/N\mathbb{Z})^\times$$

where this inverse limit is the collection $(x_n)_{n\in\mathbb{N}}$ with $x_n \in (\mathbb{Z}/N\mathbb{Z})^\times$ such that $p(x_N) = x_M$ for $M|N \rightsquigarrow p: (\mathbb{Z}/N\mathbb{Z})^\times \to (\mathbb{Z}/M\mathbb{Z})^\times$

Def The field of p-adic numbers $\mathbb{Q}_p$ for p prime consists of the elements:

$$a_k p^k + a_{k+1} p^{k+1} + \dots \qquad (1.2)$$

where each $a_j \in \mathbb{Z}/p\mathbb{Z}$ and k: $a_k \neq 0$

Def The p-adic integers $\mathbb{Z}_p \subset \mathbb{Q}_p$ consist of those elements of the (1.2) where $k \geq 0$.

Rem $\mathbb{Z} \subset \mathbb{Z}_p$ as finite series elements $\rightsquigarrow \mathbb{Q} \hookrightarrow \mathbb{Q}_p$.

Rem $\mathbb{Z} \cong \mathbb{Z}_p$ as rings.

Rem $\mathbb{Q}_p$ is a completion of $\mathbb{Q}$ with respect to the norm $|\cdot|_p$

$$\left|\frac{a}{b}p^k\right|_p = p^{-k} \quad \text{where} \quad \begin{matrix}\gcd(a,p)=1\\ \gcd(b,p)=1\end{matrix}$$

Here the norm of an elt of the form $(1,2)$ is exactly p^{-k}.

Thm [Ostrowski] Any norm-completion of $\mathbb{Q}$ is isomorphic to either $\mathbb{Q}_p$ or $\mathbb{R}$.

If $N = \prod_p p^{m_p}$, then

$$\mathbb{Z}/N\mathbb{Z} \cong \prod_p \mathbb{Z}/p^{m_p}\mathbb{Z}$$

So let $\widehat{\mathbb{Z}} = \varprojlim \mathbb{Z}/N\mathbb{Z}$ with respect to natural surjections $\mathbb{Z}/N\mathbb{Z} \twoheadrightarrow \mathbb{Z}/M\mathbb{Z}$ for $M \mid N$, then

$$\widehat{\mathbb{Z}} \cong \prod_p \left(\varprojlim \mathbb{Z}/p^r\mathbb{Z}\right)$$

$$\cong \prod_p \mathbb{Z}_p$$

$$\xrightarrow{[\text{Kro-W}]} \mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q}) \cong \widehat{\mathbb{Z}}^\times \cong \prod_p \mathbb{Z}_p^\times$$

In general there is no analogue of [Kro-W] for arbitrary fields. Instead we have to use ACFT.

Thm [ACFT] $\mathrm{Gal}(F^{ab}/F)$ is isom. to the gp of coun. comp. of $F^\times \backslash \mathbb{A}_F^\times$ where $\mathbb{A}_F$ is the ring of adèles.

Ex Adèles over $\mathbb{Q}$. Form a subring of direct product of all completions of $\mathbb{Q}$, namely an adèle is an

Def $((f_p), f_\infty)$, $f_p \in \mathbb{Q}_p$, $f_\infty \in \mathbb{R}$ such that $f_p \in \mathbb{Z}_p$ for all but finitely many p.

In pat. $\mathbb{A}_{\mathbb{Q}} \cong \left(\hat{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{Q}\right) \times \mathbb{R}$

Topology: $\mathbb{Z} \hookrightarrow$ direct prod. top.
$\mathbb{Q} \hookrightarrow$ discrete topo.
$\mathbb{R} \hookrightarrow$ Euclidean top.

diagonal embd. $\mathbb{Q} \hookrightarrow \mathbb{A}_{\mathbb{Q}}$ with quotient: $\mathbb{Q}\backslash\mathbb{A}_{\mathbb{Q}} \cong \hat{\mathbb{Z}} \times (\mathbb{R}/\mathbb{Z})$

Compact

$\mathbb{A}_{\mathbb{Q}}^\times$ are the invertible elts ("idèles") also have diag. embd $\mathbb{Q}^\times \hookrightarrow \mathbb{A}_{\mathbb{Q}}^\times$

$$\mathbb{Q}^\times\backslash\mathbb{A}_{\mathbb{Q}}^\times \cong \prod_p \mathbb{Z}_p^\times \times \mathbb{R}_{>0}$$

$\Rightarrow$ 0p conn. comp. is isom $\prod_p \mathbb{Z}_p^\times$ ✓

How: Arb. fields $F \rightsquigarrow \mathbb{A}_F$

Fact For number field F, its non-archimedean completions are parametrized by prime ideals i.e. elts of $\mathcal{O}_F$ the ring of integers of F

Def $\mathcal{O}_F = \{x \in F \mid x \text{ is root of monic poly. over } \mathbb{Z}\}$

Fact Each comp. of F with respect to a norm is either isomphic to fin ext. of $\mathbb{Q}_p$ or $\mathbb{R}$ or $\mathbb{C}$.

Each of these completions F_v, v is a norm, has its own ring of integers $\mathcal{O}_v$ $(\rightsquigarrow \mathbb{Z}_p \subset \mathbb{Q}_p)$

$\mathbb{A}_F$ is the <u>restricted</u> product of all F_v i.e. with only fin. many <u>not</u> in $\mathcal{O}_v$. $\mathbb{A}_{\mathbb{Q}} = \prod' \mathbb{Q}_p$

<u>Thm [ACFT]</u> $Gal(F^{ab}/F) \cong$ gp. conn. comp $F^\times \backslash \mathbb{A}_F^\times$