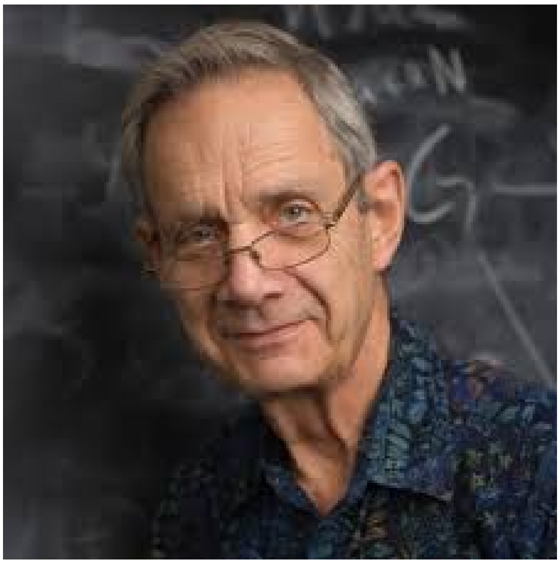
MATH621 - Algebraic Number Theory



Taught by Yihang Zhu
Notes taken by Haoran Li
2021 Spring

Department of Mathematics
University of Maryland

Contents

1 Overview

Class field theory(CFT) is the study of abelian extensions of global and local fields

Definition 1.1. A global field is a finite separable extension of $\mathbb{Q}$ or function field of a geometrically smooth curve over F_q. A local field is a finite extension of $\mathbb{Q}_p$ or function field of $F_q((t))$

we want to understand abelian extensions of K in terms of an invariant of K: the *idele class group*(some generalization of $\mathrm{Cl}(O_K)$)

$$C_K = \begin{cases} \mathbb{A}_k^\times/K^\times, K \text{ global} \\ K^\times, K \text{ local} \end{cases}$$

Why do we care?

Power reciprocity: The Legendre symbol $(n/p) = \begin{cases} 1 & n \text{ is a square } \bmod p \\ -1 & \text{otherwise} \end{cases}$

Quadratic reciprocity: For p, q distinct odd primes $(p/q)(q/p) = 1$ if one of $p, q \equiv 1 \bmod 4$, -1 if $p \equiv q \equiv 3 \bmod 4$, or more succinctly $(p/q)(q/p) = (-1)^{\frac{(p-1)(q-1)}{4}}$. Also $(-1/p) = (-1)^{\frac{p-1}{2}}$, $(2/p) = (-1)^{\frac{p^2-1}{8}}$

Class field theory is a vast and conceptual generalization of this, it put quadratic reciprocity into context. CFT $\Rightarrow$ higher power reciprocity, e.g. cubic reciprocity: 2,7 are not cubic powers mod 61

A classical problem: $p = x^2 + ny^2$, when a prime p can be written as above

If $n = 1$, this holds iff $p \equiv 1 \bmod 4$ or $p = 2$ iff p splits in $\mathbb{Q}(\sqrt{-1})$. CFT gives a complete solution to this for all n. See D. Cox "Primes of the form $x^2 + ny^2$"

If $n = 14$, then this holds iff $(-14/p) = 1$ and $(x^2 + 1)^2 - 8$ has root mod p

$K = \mathbb{Q}(\sqrt{-14})$, then this holds iff $p = \bar{P}P$ splits in K and P is principle iff(by CFT) $p = \bar{P}P$ splits in K and P splits in the Hilbert class field of K(H/K some specific finite abelian extension) iff p splits in H

"Reciprocity": whether a prime is principal is related to whether it splits in certain abelian extensions

"Class field": K is a number field, a modulus of K is a formal symbol $\mathfrak{m} = v_1^{e_1} \cdots v_k^{e_k}$. v_i's are places of K, and $e_i \in \mathbb{Z}_{\geq 0}$, satisfying: Complex places v don't appear in $\mathfrak{m}$, for real places v, $e_i = 0, 1$. e.g. $K = \mathbb{Q}$

Here a place is an equivalence class of absolute values, two absolute values are equivalent if they differ by a positive real power

The *ray class group* Cl_m is generated by fractional ideals coprime to $\mathfrak{m}$ modulo principal ideals generated by $f \in K^\times, f \equiv 1 \bmod \mathfrak{m}$. In the number field case, Cl_m is finite which is no longer true for global fields with char>0

The usual class group $\mathrm{Cl}(\mathcal{O}_K)$ is where $\mathfrak{m} = 1$

Fact: Cl_m is always finite abelian

The narrow class group, corresponds to $\mathfrak{m}$ is the product of all real places. This is the quotient group of all fractional ideals modulo those principal ideals generated $x \in K^\times$ such that $v(x) > 0$ for all real places v, i.e., the totally positive $x \in K^\times$

CFT: there is a finite abelian ext K_m/K called *ray class field* of $\mathfrak{m}$

Example: $m = 1, K_m$ is the hilbert class field

K_m is uniquely characterized among finite abelian(Galois) extension over K such that whether prime p of K splits in K_m iff whether p has trivial image in Cl_m, for all p coprime to m

Theorem 1.2 (Generalized Kronecker-Weber theorem)**.** Every finite abelian extension E/K is contained in K_m/K for sufficiently large $\mathfrak{m}$, one can choose $\mathfrak{m}$ such that its members are precisely the places of K that ramify in E

Example 1.3. If $v_1, \cdots, vk$ are the achmedian places of K that ramify in E, and $p_1 \cdots, p_k$ are unramified places, then $m = v_1, \cdots, v_k, p^{e_1}, \cdots, p_k^{e_k}$ for suff large $e_1, \cdots, e_k, E \subseteq K_m$

Artin isomorphism $\Psi : \mathrm{Cl}_m \to \mathsf{Gal}(K_m/K)$ has a concrete formula, $p \mapsto (p, K_m/K)$(well-definedness is nontrivial, called the Artin reciprocity). for every p coprime to m, know p is unramifed in K_m,
Recall: E/K is a finite Galois extension of global fields, suppose p is a prime of K that is unramifed in E, then $\forall P|p$, the arithmetic Frobenius element $\sigma = (P, E/K)$(Artin symbol) in $\mathsf{Gal}(E/K)$ is characterized by σ stablizes P, the action of $\sigma on k(P)$ as $x \mapsto x^q, q = |k(p)|$. $\{(P, E/K)|P\}$ runs through the primes of $P|p$ is a conjugacy class in $\mathsf{Gal}(E/K)$ called $(p, E/K)$. If $\mathsf{Gal}(E/K)$ is abelian, then $(p, E/K)$ is an element
Fact: For p of K unramified in E, $(p, E/K) = \{1\}$ iff p splits in E
The theory of ray CFT + Artin iso Ψ + K-W theorem gives the ideal theoretic formulation of global CFT
Adelic formulation in terms of $\mathbb{A}_k^\times/K^\times$ is cleaner. And it's easier to see functoriality in K that way

2 Class field theory over $\mathbb{Q}$

Application: Chebotarev density theorem
E/K is a finite Galois extension of number fields, $G = \mathrm{Gal}(E/K)$, forall p prime in K, unramified in E

Theorem 2.1. $\forall$ conjugacy classes C in G the set of p of K such that $(p, E/K) = C$ has density $|C|/|G|$ among all primes of K. In particular, there are infinitely many such primes p

applications in global Galois representation by density
consequence: p splits iff $(p, E/K) = \{1\}$, such primes constitute $1/|G|$ of all primes, thus infinitely many

Theorem 2.2 (Dirichlet theorem: primes in arithemetic progression)**.** if $a, b \in \mathbb{Z}$, $(a, b) = 1$, exists infinitely many primees p in the arithemetic progression $a + b\mathbb{Z}$, e.g. $a = 1, b = 4$, infinitely primes $\equiv 1 \bmod 4$

More application of CFT
Artin L funcitons: Let E/K be a finite Galois extension of number fields, $\rho : \mathrm{Gal}(E/K) \to GL_n(\mathbb{C})$, S finite primes including all ramified primes of K, define $L(\rho, s)$ for $\mathrm{re}(s) >> 0$, CFT $\Rightarrow$ meoromorphic extension to $\mathbb{C}$
Conjecture(Artin):..

Theorem 2.3 (Grumwold-Wang, local-global behavior of number fields, local-global principle for quadratic forms)**.** A non-degenerate quadratic form over a number field K represents 0 over K(it=0 has sol over K) iff it represents 0 over K_v for all places v of K

CFT is the GL_1 case of the Langlands program
CFT for $\mathbb{Q}$(given by cyclotomic extension of $\mathbb{Q}$)
Review of cyclotomic extesions of $\mathbb{Q}$
K is a general field, $m \in \mathbb{Z}_{>0}$, the m-th cyclotomic extension of K is $K(\mu_m)$, μ_m is the roots of unity in $\bar{K}$, all roots would be simple, and is a cyclic group $\cong (\mathbb{Z}/m)^\times$ under multiplication, generator is primitive m-th root of 1, denoted ζ_m. $K(\mu_m) = K(\zeta_m)$, by definition also the splitting field of $x^m - 1$ over K, thus Galois. Obeservation: $\mathrm{Gal}(K(\zeta_m))$ embeds into $(\mathbb{Z}/m\mathbb{Z})^\times$, $\sigma \mapsto a, \sigma(\zeta_m)\zeta_m^a$, so the extension is abelian. Cyclotomic polynomials are $\Phi_m(x) = \prod_\zeta (x - \zeta) \in \mathbb{Z}[x]$, ζ runs primitive m-th roots of unity in $\mathbb{C}$
$\Phi_1 = x - 1$, $\Phi_2 = x + 1$, $\Phi_m = \frac{x^m - 1}{\prod_{d|m, d<m} \Phi_d(x)}$. $K(\zeta_m)/K$ is the spliting filed of Φ_m. $\deg(\Phi_m) = \phi(m) = |(\mathbb{Z}/m\mathbb{Z})^\times|$
$\alpha : \mathrm{Gal}(K(\zeta_m)/K) \to (\mathbb{Z}/m)^\times$ is an isomorphism iff Φ_m is irreducible

Theorem 2.4 (Gauss)**.** Φ_m is irreducible in $\mathbb{Q}[x]$

Proof. Gauss's lemma, reduce to factorization mod p □

Fact 2.5 (L washington sec2)**.**

1. $\mathcal{O}_{\mathbb{Q}(\zeta_m)} = \mathbb{Z}[\zeta_m] \cong \mathbb{Z}[x]/\Phi_m(x)$
2. assume $m \equiv 2 \bmod 4$(if $m \equiv 2 \bmod 4$, then $\phi(m) = \phi(m/2) \Rightarrow \mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_{m/2})$) prime p of $\mathbb{Q}$ is unramified in $\mathbb{Q}(\zeta_m)$ iff $p \nmid m$
3. formula for $\mathrm{disc}\,\mathbb{Q}(\zeta_m)$

Lemma 2.6. $\forall p \nmid m$, $p \in (\mathbb{Z}/m)^\times$ is $(p, \mathbb{Q}(\zeta_m)/\mathbb{Q})$ the Frobenius element in $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$

Proof. Only need to prove σ fix P for $P|p$
Recall: Suppose E/K is finite separable extension of number fields, there is a way to explicitly factorize a prime p of K inside E(for almost all p), write $E = K(\alpha)$ such that $\alpha \in \mathcal{O}_E$, $\mathcal{O}_K[\alpha] \subseteq \mathcal{O}_E$ and $\mathcal{O}_k[\alpha] \otimes_{\mathcal{O}_E} E = E(\mathcal{O}_K[\alpha]$ is an order in $\mathcal{O}_E$). Conductor: $f = \{x \in O_E | xO_E \subseteq O_K[\alpha]\}$, largest ideal of $\mathcal{O}_E$ that lies inside $\mathcal{O}_K[\alpha]$
Fact: for p prime of K, coprime to f, $p\mathcal{O}_E = \prod_{i=1}^g P_i^{e_i}$, $f(x)$ is the minimal polynomial of α in $\mathcal{O}_K[x]$, factorize over $k(p) = \mathcal{O}_K/p$, $\prod_{i=1}^g f_i^{e_i}$, f_i irreducible in $k(p)[x]$, P_i is a lift of $f_i(\alpha)\mathcal{O}_E + p\mathcal{O}_E$
$\mathcal{O}_E = \mathbb{Z}[\zeta_m]$, $\min(zeta_m/\mathbb{Q}) = \Phi_m$, $p\mathcal{O}_E = \prod P_i^{e_i}$, Φ_m in $F_p[x]$ factor as $\prod f_i^{e_i}$, P_i is a lift of $f_i(\zeta_m)$. Suppose p sends P_i to P_j, $i \neq j$, but p send P_i to lift of $f_i(\zeta_m^p) = h(\zeta_p)$, $h(\zeta_p) = (\tilde{f}(\zeta_m))^p$ in F_p implies $B_j \subseteq B_i$, contradiction! □

Theorem 2.7. For $\mathbb{Q}$, a modulus is a symbol $\mathfrak{m} = \infty m$ or $\mathfrak{m} = m$ for some $m \in \mathbb{Z}_{>0}$, $Cl_{\mathfrak{m}}$ is the group of fractional ideals of $\mathbb{Q}$ coprime to m/principle ideals generated by $x \in \mathbb{Q}^\times$ such that x coprime to m, $x \equiv 1 \bmod m$, $x > 0$ if $\mathfrak{m} = \infty \cdot m$

Exercise 2.8. When $\mathfrak{m} = \infty \cdot m$, then we have an iso $(\mathbb{Z}/m)^\times \to Cl_m$, $\forall p \nmid m$, the ray class group, $p \mapsto$ the class of the prime ideal (p) iso $(\mathbb{Z}/m)^\times/\{\pm 1\} \to Cl_m$, $\mathfrak{m} = m$, $\forall p \nmid m$, $p \mapsto$ the class of the prime ideal (p)

$E_m = \mathbb{Q}(\zeta_m)$, think of this as $Cl_{\infty m} \to \mathsf{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$
This means that $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ is the ray class field
Recall: this is also characterized by the following property: for almost all primes p, p splits in the ray class field iff p is trivial in the ray class group
for $p \nmid m$, p splits in m iff $(p, E_m/\mathbb{Q}) = 1$ iff p is trivial in $Cl_{\infty m}$
Note if $E \subseteq E_m$, then $E/\mathbb{Q}$ is again finte abelian extesion, and the composition $Cl_\infty m \to Gal(E_m/\mathbb{Q}) \xrightarrow{\text{restriction}} Gal(E/\mathbb{Q})$
Theorem[Kronecker-Weber, proof given by Hilbert, later simplified] Every finite abelian extension $E/\mathbb{Q}$ is over some $\mathbb{Q}(\zeta_m)$, can also choose m to be divisible only by those p that ramify in E
there is an elementary proof for the analogous result for $\mathbb{Q}_p$(local Kronecker-Weber, see Larry's book). Theorem true for all $\mathbb{Q}_p$ imply $\mathbb{Q}$(any non-trivial $E/\mathbb{Q}$ cannot be unramified everywhere)
CFT for $\mathbb{Q}$ is basically: Ψ and Kronecker-Weber theorem
Elegant proof for quadratic reciprocity: $p \neq q$ odd primes, and $q \equiv 1 \bmod 4$, then $(p/q) = (q/p)$ there is a unique index 2 subgroup of $(\mathbb{Z}/q)^\times$, i.e. there is a unique quadratic extension K of $\mathbb{Q}$ inside E_q, we know that q is the only finite prime that ramifies in E_q, thus q is the only finite prime that ramifies in K, thus $K = \mathbb{Q}(\sqrt{q})(K \neq Q(\sqrt{-q})$ since $q \equiv 1 \bmod 4, \mathsf{disc} = q$, not $4q$(2 also ramifies))
One can explicitly construct $\sqrt{q}$ inside $Q(\zeta_q)$(Gauss, see exercise in the notes). $(p/q) = 1$ iff p represents a square in $(\mathbb{Z}/q)^\times \cong \mathsf{Gal}(E_q/\mathbb{Q})$ iff p lies in the kernel of $\mathsf{Gal}(E_q/\mathbb{Q}) \to \mathsf{Gal}(K/\mathbb{Q})$ iff $(p, E_q/\mathbb{Q}) \to 1$ iff $(p, K/\mathbb{Q}) = 1$ iff p splits in K. $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{q}}{2}]$ contain $\mathbb{Z}[\sqrt{q}]$ with conductor $2\mathcal{O}_K$ iff $\mathrm{X}^1 - q$ splits mod p iff $(q/p) = 1$

Exercise 2.9. Try other cases: prove $(p/q) = -(q/p)$ if $p \equiv q \equiv 3 \bmod 4$

3 Ramification in $\mathbb{Q}(\zeta_m)$

$p \nmid m$ imply p unramified in $\mathbb{Q}(\zeta_m)$, $p\mathcal{O}_{\mathbb{Q}(\zeta_m)} = P_1^e \cdots P_g^e$, $f = [k(P_i) : k(p)]$, $efg = [\mathbb{Q}(\zeta_m), \mathbb{Q}] = \varphi(m)$. $e = 1$, f is the order of p in $(\mathbb{Z}/m\mathbb{Z})^\times$

Lemma 3.1. If $m = p^r$, $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ is totally unramified at p, i.e. $p\mathcal{O}_{\mathbb{Q}(\zeta_m)} = P^{[\mathbb{Q}(\zeta_m):\mathbb{Q}]}$

Proof. Modulo p, $\Phi_m(X) = \frac{X^{p^r}-1}{X^{p^{r-1}}-1} = \frac{(X-1)^{p^r}}{(X-1)^{p^{r-1}}} = (X-1)^{\varphi(m)}$, thus $p\mathcal{O}_{\mathbb{Q}(\zeta_m)} = P^{\varphi(m)}$ □

In general, $m = np^r$, $p \nmid n$, $\mathbb{Q}(\zeta_m)$ is the composite $\mathbb{Q}(\zeta_n)\mathbb{Q}(\zeta_{p^r})$, and $\mathbb{Q}(\zeta_n), \mathbb{Q}(\zeta_{p^r})$ are linearly disjoint over $\mathbb{Q}$ since $\varphi(m) = \varphi(n)\varphi(p^r)$
$p \nmid m$, $\mathbb{Q}(\zeta_m)_P/\mathbb{Q}_p \cong \mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p$, here $\mathbb{Q}(\zeta_m)_P = \mathbb{Q}_p(\zeta_m)$ is the composite $\mathbb{Q}_p\mathbb{Q}(\zeta_m)$
$D_P(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p)$, thus $\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p$ is unramified, and its degree is the order of p in $\mathbb{Z}/m\mathbb{Z}^\times$. Similarly, $m = p^r, \mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p$ is totally unramified, and its degree is $e = \varphi(p^r)$

Fact 3.2. K local field, $E/K, F/K$ two finite Galois extensions. If E/K is unramified of degree f and F/K is totally ramified of degree e, then E, F are linear disjoint over K, $[E : K] = ef$, e is ramification index, f is residue extension degree

$\mathbb{Q}_p(\zeta_m)$ is the composite $\mathbb{Q}_p(\zeta_n)\mathbb{Q}_p(\zeta_{p^r})$, $e = \varphi(p^r)$, f is the order of p in $\mathbb{Z}/m\mathbb{Z}^\times$. $[\mathbb{Q}_p(\zeta_m) : \mathbb{Q}_p] = ef$. The Galois group is the direct product

$$\begin{tikzcd}
\mathrm{Gal}(\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p) \arrow[r] & \mathrm{Gal}(\mathbb{Q}_p(\zeta_n)/\mathbb{Q}_p) \times \mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^r})/\mathbb{Q}_p) \\
(\mathbb{Z}/m)^\times \arrow[u, "\alpha_m"] \arrow[r] & (\mathbb{Z}/n)^\times \times (\mathbb{Z}/p^r)^\times \arrow[u]
\end{tikzcd}$$

$\alpha_n : \mathrm{Gal}(\mathbb{Q}_p(\zeta_n), \mathbb{Q}_p) \to (\mathbb{Z}/n)^\times$ sends Frobenius element to p, and the subgroup generated by Frobenius element to the subgroup generated by p
α_{p^r} is an isomorphism because $[\mathbb{Q}_p(\zeta_{p^r}) : \mathbb{Q}_p] = \varphi(p^r) = |(\mathbb{Z}/p^r)^\times|$
$\mathbb{Q}_p^\times = p^{\mathbb{Z}} \times \mathbb{Z}_p^\times$, $\mathbb{Z}_p^\times = \varprojlim_n (\mathbb{Z}/p^n)^\times$, $\mathbb{Z}_p^\times/(1 + p^r\mathbb{Z}_p) \cong (\mathbb{Z}/p^r)^\times$
Define a map $j_m : \mathbb{Q}_p^\times \to (\mathbb{Z}/m)^\times$

$$\begin{tikzcd}
\mathbb{Q}_p^\times \arrow[d, "j_m"'] & \cong & p^{\mathbb{Z}} \arrow[d, "p \mapsto p"] & \times & \mathbb{Z}_p^\times \arrow[d, "x \mapsto x^{-1} \mapsto \text{natural projection}"] \\
(\mathbb{Z}/m)^\times & \cong & (\mathbb{Z}/n)^\times & \times & (\mathbb{Z}/p^r)^\times
\end{tikzcd}$$

$$\begin{tikzcd}
\mathbb{Q}_p^\times \arrow[r] \arrow[rr, bend right, "\psi_m"'] & (\mathbb{Z}/m)^\times & \mathrm{Gal}(\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p) \arrow[l]
\end{tikzcd}$$

ψ_m is continuous and surjective
Suppose $m' \in \mathbb{Z}_{\geq 1}$ divisible by m, then $\mathbb{Q}_p(\zeta_m) \subseteq \mathbb{Q}_p(\zeta_{m'})$

$$\begin{tikzcd}
\mathbb{Q}_p^\times \arrow[r] \arrow[d, equal] & (\mathbb{Z}/m)^\times \arrow[d, twoheadleftarrow] & \mathrm{Gal}(\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p) \arrow[l] \arrow[d, twoheadleftarrow] \\
\mathbb{Q}_p^\times \arrow[r] & (\mathbb{Z}/m')^\times & \mathrm{Gal}(\mathbb{Q}_p(\zeta_{m'})/\mathbb{Q}_p) \arrow[l]
\end{tikzcd}$$

Take the inverse limit $\phi : \mathbb{Q}_p^\times \to \varprojlim_m \mathrm{Gal}(\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p) = \mathrm{Gal}(\cup\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p) = \mathrm{Gal}(\mathbb{Q}_p^{cyc}/\mathbb{Q}_p)$. The image is dense

Theorem 3.3 (local Kronecker-Weber theorem for $\mathbb{Q}_p$)**.** Every finite abelian ext of $\mathbb{Q}_p$ is contained in some $\mathbb{Q}_p(\zeta_m)$. $\mathbb{Q}_p^{cyc} = \mathbb{Q}_p^{ab}$ is the maximal abelian extension(which is the union of all finite abelian extension) of $\mathbb{Q}_p$ in $\overline{\mathbb{Q}_p}$

One of the main goals of local CFT is: for every local field K, to construct a map $K^\times \to \mathrm{Gal}(K^{ab}/K)$(local Artin map) and study its behaviour
e.g. If L/K is a finite abelian extension, if restrict to L/K(finite abelian extension, ψ_L/K), ϕ_L/K is surj and $\ker\psi_L/K = Im(N_L/K : L^\times \to K^\times)$
Can characterize which subgroups of $K^\times$ are of the form $\ker\psi_L/K$ for some L
Local-global relationship: We have local Artin map $\psi_p : \mathbb{Q}_p^\times \to \mathrm{Gal}(\mathbb{Q}_p^{ab}/\mathbb{Q}_p)$ and the global Artin map $\Psi_m : (\mathbb{Z}/m)^\times \to \mathrm{Gal}(\mathbb{Q}\zeta_m/\mathbb{Q})$

$$\begin{tikzcd}
(\mathbb{Z}/m)^\times \arrow[rr, "\Psi_m"] & & \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \\
\mathbb{Q}_p^\times \arrow[u, "j_{m,p}"] \arrow[r, "\psi_{p,m}"] & \mathrm{Gal}(\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p) = D_p(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \arrow[ur, hook]
\end{tikzcd}$$

Definition 3.4 (Chevalley(finite ideles)). $\mathbb{A}_f^\times = \{(x_p) \in \prod_p \mathbb{Q}_p^\times | x_p \in \mathbb{Z}_p^\times \text{ for almost all } p\}$, ideles is $\mathbb{A}^\times = \mathbb{R}^\times \times \mathbb{A}_f^\times$

$\mathbb{Q}^\times$ diagonally sits in $\mathbb{A}^\times$, i.e. $x \mapsto (x_\infty, x_2, x_3, x_5, \cdots)$. Idelic global Artin map $\Psi_m : \mathbb{A}_f^\times \to Gal(\mathbb{Q}(\zeta_m)/\mathbb{Q}), (x_p) \mapsto \psi_{\infty,p}\prod\psi_{p,m}(x_p)$ which is a finite product since $\mathbb{Z}_p^\times$ elements go to 0
Here $\psi_{\infty,p}(x)$ is identity if x is positive, and σ_∞ which is $-1 \in \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) = (\mathbb{Z}/m)^\times$ if x is negative. So

$$(x_\infty, x_f) \mapsto \begin{cases} \Psi(x_f) & x_\infty > 0 \\ \sigma_\infty \Psi(x_f) & x_\infty < 0 \end{cases}$$

Exercise 3.5. This is actually a map $A^\times/\mathbb{Q}^\times \to \mathrm{Gal}(\mathbb{Q}^{cyc}/\mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q})$

Global CFT: For any global field K, Artin map $\Psi : A_K^\times/K^\times \to \mathrm{Gal}(K^{ab}/K)$
Future plan:
review of profinite groups: allows us to talk about infinite Galois theory
State the main theorems in local CFT after reviewing some basics about local fields
Lubin-Tate theory: analogue of the local cyclotomic extensions, gives an explicit construction of K^{ab} for a local field K
Group cohomology
Use Group cohomology to fully prove local CFT
Global CFT

4 Profinite groups

Example of direct system:

1. $(\mathbb{N}, \geq)$
2. $(\mathbb{N}, |)$
3. G is a (topological)group, $I = \{$finite index(open) normal subgrps of $G\}$, $N \geq N'$ if $N \subseteq N'$
4. Fix a field extension E/K, $I = \{L/K$ finite Galois$\}$, $L \geq L'$ if $L \supseteq L'$. If L, L' are both finite Galois, then so is their composite

Let C be a category(sets, groups, rings, top groups, top spaces, top rings). A profinite group is a topological group isomorphic to a inverse limit of finite groups. A profinite group is Hausdorff and compact

Theorem 4.1 (Tychonoff's theorem)**.** A product of compact spaces is compact

Theorem 4.2. G is a topological group, G is profinite iff it is Hausdorff compact and $1 \in G$ has a neighborhood basis consisting of open subgroups of G

Proof. $\Leftarrow$: Suppose $G = \varprojlim G_i$, $\forall i \in I$, $N_i = \ker(G \to G_i)$ give such a basis
$\Rightarrow$: □

Remark 4.3. In a topological group, every open subgroup is closed(being the complement of the union of its other cosets). In a compact group, a closed subgroup is open iff it's of finite index(conjugates cover G, then by compactness), and every open subgroup is closed hence compact

Example 4.4. $\mathbb{Z}_p$ with topology given by the p-adic value, $p^n\mathbb{Z}_p$ form a neighborhood basis of 0 in $\mathbb{Z}_p$ consisting of open subgroups. $\mathbb{Z}_p^\times = \varprojlim_n (\mathbb{Z}/m\mathbb{Z})^\times$ has $1 + p^n\mathbb{Z}_p$ as an open neighborhood basis of 0

Remark 4.5. A topological group is called locally profinte it's locally compact and Hausdorff and 1 has a neighborhood basis consisting of open subgroups. Equivalently, G has an open subgroup which is profinite

Example 4.6. $Q_p \overset{\text{open}}{\supseteq} Z_p$ is locally profinite since its not compact

Fact: A topological group is (locally) profinite iff it is Hausdorff, (locally compact) and totally disconnected
G is a topological group, I is the set of open normal finite index subgroups(Note: quotient top on G/N_i is discrete), so $\hat{G} = \varprojlim G/N_i$ defines a profinite group, called the profinite completion, and a natural continuous map $G \to \hat{G}$, it is an isomorphism iff G is profinite. For every continuous $G \to H$, where H is profinite, the it factors through $\hat{G} \to H$
Exercise: $\hat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$
Infinite Galois theory: E/K Galois(separable and normal), I is the subset consists of L/K which are finite Galois
Fact(easy): As abstract groups, $\mathrm{Gal}(E/K) = \varprojlim \mathrm{Gal}(L/K)$, define Krull topology on $\mathrm{Gal}(E/K)$ by profinite topology given by the right hand side

Theorem 4.7 (Galois correspondence)**.** Sub-extensions L/K corresponds to closed subgroups of $\mathrm{Gal}(E/K)$, $L \mapsto \mathrm{Gal}(E/L)$, $H \mapsto E^H$, $E^H = E^{\bar{H}}$, finite extensions are in bijective correspondence to open subgroups, Galois extensions are in bijective correspondence to normal subgroups. If L/K is Galois, then $\mathrm{Gal}(E/L)$ is normal in $\mathrm{Gal}(E/K)$, and $\mathrm{Gal}(L/K) \cong \mathrm{Gal}(E/K)/\mathrm{Gal}(E/L)$ as topological groups

Example 4.8. $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q) \cong \varprojlim_n \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \cong \varprojlim_n \mathbb{Z}/n\mathbb{Z}$, $\mathbb{Z} \to \hat{\mathbb{Z}}$, $1 \mapsto 1$ is the Frobenius element

remark: G = profinite, S is dense iff image of S in each G_i is G_i, since G_i is discrete
$(\mathbb{Z}/m\mathbb{Z})^\times \cong \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$, thus $\hat{\mathbb{Z}}^\times \cong \mathrm{Gal}(\mathbb{Q}^{cyc}/\mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q})$ But $\mathbb{Q}_p^\times \to \mathrm{Gal}(\mathbb{Q}_p^{ab}/\mathbb{Q}_p)$ only has dense image

Exercise 4.9. G is locally profinite, and $\phi : G \to G'$ is continuous, G' is profinite, ϕ has dense image, then $\hat{G} \cong G'$

5 Local fields

A discrete valued field (K, v) is a surjective(normalized and exclude trivial valuations) function $v : K \to \mathbb{Z} \cup \{+\infty\}$ satisfying

1. $v(x) = +\infty \iff x = 0$
2. $v(xy) = v(x) + v(y)$ is a group homomorphism $K^\times \to \mathbb{Z}$
3. $v(x + y) \geq \min(v(x), v(y))$

Subring $\mathcal{O}_K = \{x \in K | v(x) \geq 0\}$ of K with $\mathrm{Frac}(\mathcal{O}_K) = K$ and that it is a valuation ring(in fact a DVR, i.e. a PID with unique non-zero prime ideal), with the unique non-zero prime ideal $m_K = \{x \in K | v(x) > 0\}$, generated by the uniformizer π such that $v(\pi) = 1$. $\mathcal{O}_K^\times = \{x \in K | v(x) = 0\}$. For any $x \in K$, there is a unique n such that $\pi^{-n}x \in \mathcal{O}_K^\times$, $n = v(x)$, i.e. v can be recovered from $\mathcal{O}_K$, in fact, all discrete valuations v on K corresponds to DVR's $\mathcal{O} \subseteq K$ whose fraction field is K. $k = \mathcal{O}_K/m$ is the residue field, then is a natural topology on K, pick $\alpha \in \mathbb{R}$, $0 < \alpha < 1$, define absolute value on K, $K^\times \to \mathbb{R}_{>0}$, $x \mapsto \alpha^{v(x)} = |x|$. Discrete valuations correspond to non-Archimedean absolute values whose image is a discrete subgroup of $\mathbb{R}^\times/\sim$, making K into a metric space, whose topology is independent of α. In fact, $\mathcal{O}_K$ is open, and m^n, $n \geq 1$ form an open neighborhood basis of 0

Ostrowski's theorem

Theorem 5.1 (Ostrowski's theorem)**.** Every non-trivial absolute value on $\mathbb{Q}$ is equivalent to either the real absolute value $||_\infty$ or p-adic absolute values $||_p$. A field that is complete with respect to an Archimedean absolute value is(topologically and algebraically) $\mathbb{R}$ or $\mathbb{C}$

Note. An absolute value is a norm with $|xy| = |x||y|$. Two absolute values $||, ||_*$ are equivalent if $||_* = ||^c$ for some $c > 0$. The trivial absolute value is $|0| = \infty$ and 0 otherwise

Example 5.2. $K = \mathbb{Q}, v = v_p, \mathcal{O}_K = \mathbb{Z}_{(p)}, m = p\mathbb{Z}_{(p)}$ is locally profinite. $K = \mathbb{Q}_p, v = v_p, \mathcal{O}_K = Z_p$ is profinite

Definition 5.3. (R, m) is a local ring, its completion $\hat{R} = \varprojlim_n R/m^n$. $\hat{R}$ is also local with unique max ideal $\hat{m} = \ker(\hat{R} \to R/m)$, $R \to \hat{R}$ is a natural local ring homomorphism, induce $R/m^n \cong \hat{R}/\hat{m}^n$, thus $\hat{\hat{R}} \cong \hat{R}$

We call (K, v) complete if $\mathcal{O}_K$ is complete as a local ring. and this is true iff K is complete in the metric sense

Definition 5.4. A non-archimedean local field is a discrete valued field (K, v) which is complete and has finite residue field. Archimedean local fields are $\mathbb{Q}, \mathbb{C}$ by Theorem 5.1

We use local fields to mean just non-archimedean local fields. In this case, $\mathcal{O}_K/m^n$ are discrete by exact sequences, so $\mathcal{O}_K$ is profinite, thus compact, K is locally profinite. Conversely, if (K, v) is a discrete valued field such that K is locally profinite(suffices to show that K is locally compact), then (K, v) is a local field
(K, v) is a discretely valued field, we have $\hat{\mathcal{O}_K}$ as a DVR with π again as the uniformizer, let $\hat{K}$ to be the field of fractions with a natural valuation $\hat{v}$, and K has dense image in $\hat{K}$. So if (K, v) has finite residue field, the completion is a local field

Example 5.5. $\mathbb{F}_q(t)$, v_t valuation, with residue field $\mathbb{F}_q$, valuation ring $\mathbb{F}_q[t]$, and max ideal $t\mathbb{F}_q[t]$, the completion is the Laurent series in t, v_t gives the order of zero or pole, with valuation ring $\mathbb{F}[[t]]$

K is a local field
Structure of $(K, +)$ and $(K^\times, \times)$
$K^\times \cong \mathbb{Z} \times \mathcal{O}_K^\times$ as topological groups, $\mathbb{Z}$ with discrete topology
$U = \mathcal{O}_K^\times$, $U_n = 1 + m_K^n$, then $U \supseteq U_1 \supseteq \cdots$ form an open subgroup neighborhood basis of 1, $U/U_1 \cong k^\times$, $U_n/U_{n+1} \cong m_K^n/m_K^{n+1} \cong k$, $x \mapsto x - 1$
U_1 is the unique pro-p Sylow subgroup of U since $|U_n/U_{n+1}| = p$ and $|U/U_1| = p - 1$ is coprime to p
U is profinite since U is compact(closed in $\mathcal{O}_K$)

Remark 5.6. If K is a local field of characteristic 0, then for sufficiently large n(so that the series converge), $m_K^n \cong U_n$, $x \mapsto e^x$

Corollary 5.7. In this case, every finite index subgroup of $K^\times$ is open

Proof. Suppose H is of finite index j in $K^\times$, then $(K^\times)^j \subseteq H$. Fix uniformizer π, $(K^\times)^j \cong \pi^{j\mathbb{Z}} \times U^j$. $U^j \supseteq U_1^j \supseteq \cdots$, only need to show U_n^j is open for some n, for n large enough, $U_n \cong m_K^n \cong \mathcal{O}_K$, so $U_n^j \cong j\mathcal{O}_K \overset{open}{\subseteq} \mathcal{O}_K$ □

Teichmuller lift:

Fact 5.8. The surjective homomrophism $\mathcal{O}_K^\times \to k^\times$($k$ is the residue field which is finite) has a unique multiplicative section $[] : k^\times \to \mathcal{O}_K^\times$. Moreover, $[x] = \varinjlim_n y_n^{p^n}$, $y_n \in \mathcal{O}_K^\times$ is an arbitrary lift of $\sqrt{p^n} x \in k^\times$

Example 5.9. $K = \mathbb{Q}_5$, $[\bar{4}] = -1 \in \mathcal{O}_K^\times = \mathbb{Z}_5^\times$

Fact 5.10. $\forall x \in K^\times$, $\exists_1 (a_n)_{n \geq v(x)}$ such that $a_n \in \{0\} \cup [k^\times]$, $x = \sum_{n \geq v(x)} \pi^n a_n$

Warning: $x = sum\pi^n a_n$, $y = sum\pi^n b_n$, $x + y = x = sum\pi^n(a_n + b_n)$ is not the canonical choice
Finite extensions of local fields

Theorem 5.11 (Serre II.2)**.** (K, v) is a complete discretely valued field, E/K is a separable field extension, $\exists_1 w$ on E and $\exists_1 e \in \mathbb{Z}_{\geq 1}$ such that $\forall x \in K$(e is the ramification index), $w(x) = ev(x)$. Moreover, (E, w) is complete, k_E/k_K is a finite extension of degree $f = [E : K]/e$

Remark 5.12. $w(y) = v(N_{E/K}(y))/f$, $\forall y \in E$

$\Rightarrow$ Every finite extension of a local field has canonical structure of a local field itself. In the future, when we talk about finite extensions of local fields E/K, it's always assumed that the local field structure on E is obtained from K in this way

Fact 5.13. Every local field is either a finite extension of $\mathbb{Q}_p$ or $\mathbb{F}_q([t])$, Laurent series

6 Galois theory for local fields

Definition 6.1. A finite separable extension E/K is called unramified if $e(E/K) = 1$

Fact 6.2. If E/K is unramified, then it's Galois. $\mathrm{Gal}(E/K) \to \mathrm{Gal}(k_E/k_F)$ is an isomorphism

Fact 6.3. E/K finite unramified, L/K finite extension, $\mathrm{Hom}_K(E, L) \to \mathrm{Hom}_{k_K}(k)(k_E, k_L)$ is a bijection

Thus we have

$$\{K \subsetneq E \subsetneq L, E/K \text{ unramified}\} \leftrightarrow \{\text{subextension } of k_L/k_K\}$$

K^s/K is the separable closure. $\forall n \in \mathbb{Z}_{\geq 1}$, $\exists_1 K \subsetneq K_n \subsetneq K^s$ such that K_n/K is unramified and of degree n. $K^{un} = \bigcup_{n\geq 1} K_n$, K^{un}/K is a Galois field extension and contains all possible finite unramified extensions of K inside K^s(all are of the form K_n)

References

Index