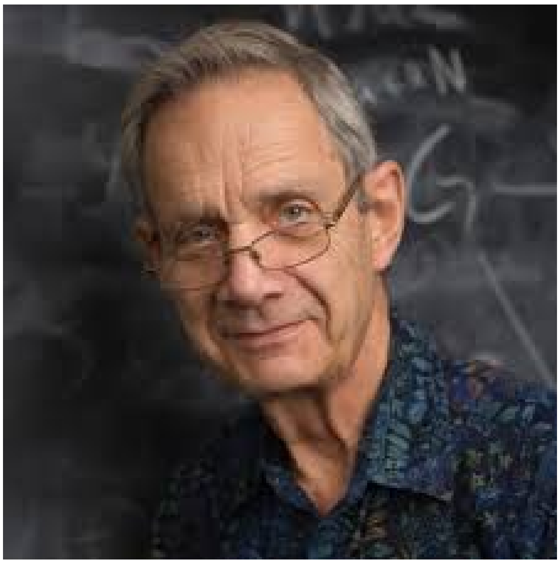
MATH621 - Algebraic Number Theory



Taught by Yihang Zhu
Notes taken by Haoran Li
2021 Spring

Department of Mathematics
University of Maryland

Contents

1 Overview

Class field theory(CFT)
Study of abelian extensions of global and local fields

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

Can understand abelian extensions of K in terms of an invariant of K
$C_K = \begin{cases} \mathbb{A}_k^\times/K^\times(ideleclassgroup, somegeneralizationofCl(O_K)), K \text{ global} K^\times, K \text{ local} \end{cases}$
Why do we care?

1. Quadratic reciproicty p, q distinct odd primes, $(p/q) = 1$ if p is a square mod q, -1 otherwise $(p/q)(q/p) = 1$ if one of $p, q \equiv 1 \bmod 4$, -1 if $p \equiv q \equiv 3 \bmod 4$

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
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 $p = P * \bar{P}$ splits in K and P is principle iff(by CFT) $p = P * \bar{P}$ 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 a formal symbol m = a formal product of powers of places of K. e.g. $K = \mathbb{Q}$
"ray class group": Cl_m = fractional ideals coprime to m/ principal ideals generated by $f \in K^\times, f \equiv 1 \bmod m$
i.e. if $m = v_1..v_k p^e 1..p^e l$
Fact: cl_m is always finite abelian
CFT: there is a finite abelian ext K_m/K called ray class field of m
whether prim p of K splits in K_m iff whether p has trivial image in Cl_m, for all p coprime to m
ex: $m = 1, K_m$ is the hilbert class field
K_m is uniquely characterized among finite ab ext over K by this
Generalized Kronecker-Weber theorem: Every finte ab ext E/K is contained in K_m/K for sufficiently large m one can choose m such that its members are precisely the places of K that ramify in E
e.g. 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 isomorphis $\Psi : Cl_m \to Gal(K_m/K)$ is iso has a concrete formula, $p \mapsto (p, K_m/K)$(well-definedness is nontrivial, called the Artin reciprocity). for ecery p coprime to m, know p is unramifed in K_m, recall in general, say E/K is a finite Galois ext of glocabl fields, suppose p is a prime of K that is unramifed in E, then $\forall B|p$, the frobenius $\sigma = (B, E/K)$ Artin symbol in $\mathrm{Gal}(E/K)$ characterized by σ stablizes B, the action of $\sigma on k(B)$ as $x \mapsto x^q, q = |k(p)|$
(B,E/K)|B runs through the primes of |p is a conjugacy class in Gal(E/K) called (p,E/K)
If 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 interms of $\mathbb{A}_k^\times/K^\times$ is cleaner. Easier to see functoriality in K

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

Application: Chebotarev density theorem
E/K is a finite Galois extesntion of number ifelds, $G = \mathrm{Gal}(E/K)$
forall p prim in K, unramified in E
(P,E/K) is the Frobenius element, the unique element σ that fix P if P|p, and acts on k(P) as $x \mapsto x^q, q = |k(p)|$ (p,E/K) is the conjugacy class

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 infiitely 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

Theorem 2.2 (Dirichlet theorem: primes in arithemetic progression)**.** if a,b∈Z, (a,b)=1, exists infi many primees p in the arithemetic progression a+bZ e.g. a=1,b=4, infi primes ≡1 mod 4

More appliecatino of CFT
Artin L funcitons: E/K fin Gal ext of fiels, ρ:Gal(E/K)→GL$_n(C), Sfinprimesincludingallramifiedprimesof Kd$
$0, CFT => meoromorphicexttoC$
Conjecture(Artin):..
Grumwold-Wang theorem: local-global behavior of fields. local-global principle for qudratic forms: A nondeg quadratic form over K=field rpere 0 over K(it=0 has sol over K) iff it rep 0 over K$_v forallplacesvofK$
CFT is the GL$_1 caseoftheLanglandsprogram$
CFT for $\mathbb{Q}$(given by cyclo ext of Q)
Review of cyclotomic extesions of Q
K=general feild,m≠0 in K is positive, the mth cyclo ext of K K$(\mu_m), \mu_m istherootsofunityin\bar{K}, allrootswouldbesimple, andisacyclicgroup \cong (Z/mZ)^\times undermultiplication, generatorisprimitivemthrootof1, denoted\zeta_m. K(\mu_m) = K(\zeta_m), bydefalsothesplittingfieldofx^m - 1overK, thusGaloisObeservation : Gal(K(\zeta_m)) embedsinto (Z/mZ)^\times, \sigma \mapsto a, \sigma(\zeta_m)\zeta_m^a, sotheextisabelian$
cyclo poly: $\Phi_m(x) = \prod_\zeta (x - \zeta) \in Z[x]\zeta runsprimitivemthrootsofunityinC$
$\Phi_1 = x - 1, \Phi_2 = x + 1, \cdots, \Phi_m = \frac{x^m - 1}{\prod_{d|m, d<m} \Phi_d(x)} K(\zeta_m)/Kisthesplitingfiledof\Phi_m \deg(_m) = \phi(m) = |(Z/mZ)^\times| \alpha : Gal(K/K) \to Z/mZ^\times isisoiff\Phi_m isirreducible$

Theorem 2.3 (Gauss)**.** Φ_m is irr in $\mathbb{Q}[x]$

Proof. Gauss's lemma reduce to factorization mod p ☐

Fact 2.4 (L washington sec2)**.**

1. O$_{Q(\zeta_m)} = Z[\zeta_m] \cong Z[x]/\Phi_m(x) assume$m≡2 mod 4$(ifm2 \bmod 4, then\phi(m) = \phi(m/2) => Q(zeta_m) = Q(zeta_m/2)) primepofQisunramifiedinQ(zeta_m) iffp \nmid m$
2. formula for $\mathbf{disc}\,$Q$(_m)$

Lemma 2.5. forall p∤m, p in Gal(Q(zeta$_m)/Q) is (p, Q(\zeta_m)/Q) theFrobeniuselement$

Proof. Only need to prove σfix P for P|p Recall: Suppose E/K is fin separable ext of fields, there is a way to explicitly factorize a prime p of K inside E(for almost all p), write E=K(α) such that α∈O$_E, O_K[\alpha] \subseteq O_E and O_k[\alpha] \otimes_{O_E} E = E(O_K[\alpha] isanorderinO_E). Conductor : f = \{x \in O_E | xO_E \subseteq O_K[\alpha]\}, largestidealofO_E thatliesinsdieO_K[\alpha] Fact : forpprimeofK, coprimetof, pO_E = \prod_{i=1}^g P_i^{e_i}, f(x) istheminimalpolyofainO_K[x], factorizeoverk(p) = O_K/p, \prod_{i=1}^g f_i^{e_i}, f_i irrink(p)[x], P_i = liftoff_i(\alpha)O_E + pO_E$
O$_E = Z[\zeta_m], min(zeta_m/Q) = \Phi_m, pO_E = \prod P_i^{e_i}, \Phi_m inF_p[x] factoras \prod f_i^{e_i}, P_i = liftoff_i(\zeta_m). SupposepsendsP_i toPj, i \neq j, butpsendP_i toliftoff_i(zeta_m^p) = h(zeta_p), h(\zeta_p) = (\tilde{f}(\zeta_m))^p inF_p impliesB_j \subseteq B_i, contradiction!$ ☐

Theorem 2.6. Recall: For Q, a moduls is a symbol m=$\infty \cdots morm = mforsomem \in Z_>0, Cl_m isthegroupoffractionalidealsofQcoprimetom/principleidealsgeneratedbyx \in Q^\times suchthatxcoprimetom, x \equiv 1 \bmod m, x > 0 ifm = \infty \cdot m$

Exercise 2.7. When m=∞·m, then we have an iso Z/mZ)$^\times \to Cl_m, forallp \nmid m, p \mapsto theclassoftheprimeideal(p) isoZ/mZ)^\times / \{$
$pm1 \to Cl_m, m = m, forallp \nmid m, p \mapsto theclassoftheprimeideal(p)$

References