Computing CFT with Kummer Theory

Luke Askew

1 Introduction

Our goal will be to compute explicit polynomials for extensions of
Throughtout, let K be a number field and let $(\mathfrak{m}, C)$ be a congruence subgroup. The goal of this talk is to overview some ideas that come into explicitly computing the defining polynomial for the extension L/K corresponding to $(\mathfrak{m}, C)$ coming from the existence theorem of class field theory.

Our first simplification will be to just say that we can build up any abelian group from cyclic groups of prime order with the CRT, so we will restrict to this case.

We will take the Ray class number at C to be $h_{\mathfrak{m},C} = |Cl_{\mathfrak{m}}(K)/\overline{C}| = |I_{\mathfrak{m}}/C| = \ell$ for a prime ℓ, shich by class field theory will give us a desired extension L/K cyclic of degree ℓ.

2 Kummer Theory

Definition 2.0.1. *A field extension F/K is **Kummer** if it has abelian Galois group $G = \mathrm{Gal}(F/K)$ and K contains a primitive nth root of unity ζ_n where n is the exponent of G.*

We can use Kummer theory to find all cyclic degree n extensions of K if K contains ζ_n.

Set $G = \mathrm{Gal}(K^s/K)$.

$$1 \longrightarrow \mu_n(K) \longrightarrow K^s \xrightarrow{(-)^n} K^s \longrightarrow 1$$

and using that $\hom_{\mathbb{Z}}(G, -)$ is left exact (contravariant), we get the associated long exact sequence in cohomology.

$$1 \longrightarrow H^0(G, \mu_n(K)) \longrightarrow H^0(G, K^s) \xrightarrow{(-)^n} H^0(G, K^s) \longrightarrow H^1(G, \mu_n(K)) \longrightarrow H^1(G, K^s) \longrightarrow ...$$

Using that H^0 finds the G invariant elements, and Hilbert 90, we can find $H^1(G, \mu_n(K))$.

$$H^0(G, \mu_n(K)) \longrightarrow H^0(G, K^s) \xrightarrow{(-)^n} H^0(G, K^s) \longrightarrow H^1(G, \mu_n(K)) \longrightarrow H^1(G, K^s)$$

$$\mu_n(K) \longrightarrow K^\times \xrightarrow{(-)^n} K^\times \longrightarrow H^1(G, \mu_n(K)) \longrightarrow 1$$

so by the first isomorphism theorem, we have that $H^1(G, \mu_n(K)) \cong K^\times/(K^\times)^n$.

Further, we can say that because G acts trivially on $\mu_n(K)$ that there are no coboundaries to worry about, so in particular we have that

$$H^1(G, \mu_n(K)) \cong \mathrm{Hom}(G, \mu_n(K))$$

Theorem 2.1. *There is a bijection between*

$$\{\textit{cyclic subgroups of } K^\times/(K^\times)^n\}$$

and

$$\{\textit{cyclic extensions } L/K\}$$

Compare $K^\times/(K^\times)^n$ with the generators of cyclic subgroups in $\mathrm{Hom}(G, \mu_n(K))$. The kernels of these generators in G. By Galois theory, these kernels are associated to field extensions of K. Two generators for the same group will have isomorphic kernels.

Take a map $\phi : G \to \mu_n(K)$. The kernel will be a open normal subgroup, so will correspond to an extension L_ϕ.

Corollary 2.1.1. *An extension L/K is cyclic of degree n if and only if $L = K(\sqrt[n]{\alpha})$, where $\alpha \in K$ has order n in $K^\times/(K^\times)^n$.*

Proof. Following the isomorphism at the level of cocycles, we see that we get $\psi : K^\times/(K^\times)^n \to \mathrm{Hom}(G, \mu_n(K))$ via $\alpha \mapsto (g \mapsto \frac{g(\sqrt[n]{\alpha})}{\sqrt[n]{\alpha}})$.

The kernels of these maps is a fixed field $K(\sqrt[n]{\alpha})$.

□

Corollary 2.1.2. *Two field extensions $L_i = K(\sqrt[n]{\alpha_i})$ are isomorphic if and only if $a_2 = a_1^i\gamma^n$ with $\gamma \in K\times$. In this case, α_1 and α_2 are said to be **Kummer conjugate**.*

3 ℓ-Selmer Groups

Definition 3.0.1. *$\gamma \in K^*$ is a ℓ-**virtual unit** provided there exists an ideal $\mathfrak{q}$ having $\mathfrak{q}^\ell = \gamma\mathbb{Z}_K$.*

We will require the class group $Cl(K) = \bigoplus_{1\leq i\leq g}(\mathbb{Z}/d_i\mathbb{Z})\overline{\mathfrak{a}_i}$ where the $\overline{\mathfrak{a}_i}$

Lemma 3.0.1. *γ is a ℓ-virtual unit with exponent if and only if it belongs to the group generated by the units $\mathfrak{a}_i^\ell$.*

Definition 3.0.2. *Denote by $V_\ell(K)$ the ℓ-virtual units of K. This is a group under multiplication.*

Denote by $\mathrm{Sel}_\ell(K)$ the group $V_\ell(K)/(K^*)^\ell$.

Lemma 3.0.2. *The following sequence of $\mathbb{F}_\ell$ modules is exact:*

$$1 \longrightarrow \mathbb{Z}_K^\times/(\mathbb{Z}_K^\times)^\ell \longrightarrow \mathrm{Sel}_\ell(K) \xrightarrow{\phi} Cl(K)[\ell] \longrightarrow 1$$

Corollary 3.0.1. *Suppose K contains ζ_ℓ and has r_1 real places and r_2 complex places, then*

$$\dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell(K) = r_1 + r_2 + \dim_{\mathbb{F}_\ell} Cl(K)[\ell]$$

Proof. By Dirichlet's unit theorem, we have $\mathbb{Z}_K^* \cong \mathbb{Z}_{K,tors} \oplus \mathbb{Z}^{r_1+r_2-1}$ where the torsion is congruent to $\mu(K)$. As $\zeta_\ell \in K$, we have $\mu(K) \cong \mathbb{Z}/\ell\mathbb{Z}$.

This gives $\mathbb{Z}_K^\times/(\mathbb{Z}_K^\times)^\ell \cong (\mathbb{Z}/\ell\mathbb{Z})^{r_1+r_2}$, and we apply rank nullity.

□

Cohen keeps track of the actual basis elements in terms of the class group and unit group for computations. Call this basis v_i.

4 Polynomial for $\zeta_\ell \in K$

This section will be handwavey - I recommend anyone interested to look at Cohen's book.

To actually find α that will give us the desired conductor, there is a theorem of Hecke we can use with 12 conditions that relates ramification information and the prime ℓ.

Write $Cl(k)/(Cl(k))^\ell$ as $\oplus(\mathbb{Z}/\ell\mathbb{Z})a_i$ for some equivalence classes represented by ideals a_i.

For primes $p|m$ and either $p \nmid l$ or $v_p(m) < \ell\frac{e(p/\ell)}{\ell-1} + 1$ (this condition controls that $\ell \nmid \nu_p(\alpha)$) we can factor the primes into the form

$$p = \beta_p q_p^\ell \prod a_i^{x_i}$$

with x_i maximal and this defines some elements β_i. We're removing the parts of these ideals which are ℓth powers and ideals which are principal when we take ℓth powers since we want to control those with the ℓ-selmer group.

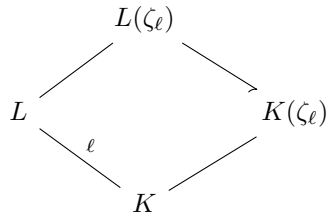
Theorem 4.1. *Let K be with $\zeta_\ell \in K$, L/K be cyclic of degree ℓ and conductor $\mathfrak{m}$. Then $L = K(\sqrt[\ell]{\alpha})$ for*

$$\alpha = \prod_B \beta_{\mathfrak{p}}^{x_{\mathfrak{p}}} \prod v_i$$

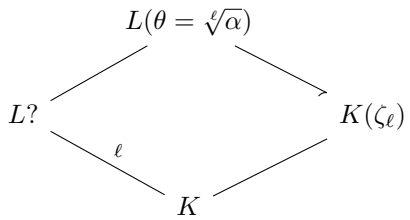
5 Descent when $\zeta_\ell \notin K$

When $\zeta_\ell \notin K$, we need to extend to a field that has a primitive ℓth root to use Kummer theory.

Here's our setup assuming we have L:



and we can close into it by taking Kummer extensions of K_z:



Using Galois theory on the following, we have that $\mathbb{Q}(\zeta_\ell)/\mathbb{Q}$ cyclic implies K_z/K is a normal extension.

So the Galois group $\mathrm{Gal}(K_z/K)$ is generated by some subgroup of a cyclic Galois group of order

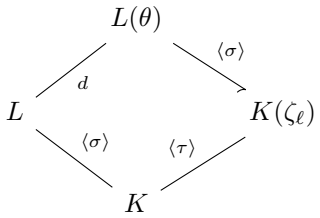
$$d|\ell - 1$$

, and will be defined by

$$\langle \tau \rangle = \mathrm{Gal}(K_z/K)$$

with

$$\tau(\zeta_\ell) = \zeta_\ell^g$$



Consider an extension of τ to L_z. We can see how these actions interact.

We will give a sketch of why this should be morally true. By Galois theory, we have the following short exact sequence of abelian groups:

$$1 \longrightarrow \mathrm{Gal}(F/K) \longrightarrow \mathrm{Gal}(F_z/K) \longrightarrow \mathrm{Gal}(K_z/K) \longrightarrow 1$$

$$1 \longrightarrow \mathbb{Z}/\ell\mathbb{Z} = \langle\sigma\rangle \longrightarrow \langle\sigma\rangle \oplus \langle\tau\rangle \longrightarrow \mathbb{Z}/d\mathbb{Z} = \langle\tau\rangle \longrightarrow 1$$

So we get a unique field automorphism for L_z fixing K for any two field automorphisms on K_z and L fixing K.

Abuse notation so that τ and σ are the lifts to L_z when paired with the identity.

Lemma 5.0.1. *τ and σ commute.*

We have that

$$\tau(\theta) = \zeta_\ell^r \theta$$

since τ is cyclic with prime order on K_z and fixes L.

$$\tau(\theta), \tau^{-1}(\theta) \in L_z$$

which gives

$$K_z(\tau(\theta)) = L_z$$

so $\tau(\theta)$ and θ are kummer conjugate

$$\tau(\theta) = \theta^i \gamma^\ell$$

with $(i, \ell) = 1$.

Both σ and τ act additively on ζ_ℓ and multiply by something in K, so they commute.

Theorem 5.1. *Given the prior setup, we get that $L = K(\eta)$ where*

$$\eta = Tr_{L_z/L}(\theta) = \sum_{i=0}^{d} \tau^i(\sigma)$$

We can do this by showing that $\eta \notin K$ since clearly $\eta \in L$ and because the extension is cyclic.

Proof. Suppose $\eta \in K$. Then $\sigma^k(\eta) = \eta$ for all k. Applying σ to both sides of the trace gives

$$\eta = \sigma^k(\eta) = \sum_{i=0}^{d} \tau^i(\sigma^k(\theta)) = \sum_{i=0}^{d} \tau^i(\zeta_\ell^{kr}\theta) = \sum_{i=0}^{d} \zeta_\ell^{kr}\tau^i(\theta)$$

These conditions show that $\tau^i(\theta) \in K_z$, so in particular $\theta \in K_z$ but $L_z = K_z(\theta)$. □