CLASS FIELD THEORY - THE BASICS

DYLAN COSTA

CONTENTS

Notes on the statements of Class Field Theory and the development and generalizations of certain concepts.

1. CLASS FIELD THEORY OVER **Q**

To begin we need to add some standard conventions. We let $\mathbf{Q}_m = \mathbf{Q}(\zeta_m)$ where m is a positive integer and $m \neq 2a$ for a an odd integer. This is simply to avoid having to add different cases since $\mathbf{Q}_{2a} = \mathbf{Q}_a$. Here is the first major theorem to help understand abelian extensions of $\mathbf{Q}$.

Theorem 1.1. *(Kronecker-Weber) Every abelian extension of the rational numbers* $\mathbf{Q}$ *is contained in a cyclotomic extension.*

Proof. Maybe □

With this tool, the study of ALL abelian extensions of $\mathbf{Q}$ has been reduced to the study of cyclotomic extensions. This becomes very helpful for us since the Galois group of any cyclotomic extension is well known.

Definition 1.2. Let L be an abelian extension of $\mathbf{Q}$, then $L \subset \mathbf{Q}_m$ for some m by the theorem above, we call any such m a *defining modulus* of L.

Notice there is no statement of uniqueness of defining moduli of L, and for good reason.

Example 1.3. Let $L = \mathbf{Q}(\sqrt{5})$. Then $L \subset \mathbf{Q}_5 \subset \mathbf{Q}_{15} \subset \mathbf{Q}_{20}$. So $5, 10, 20$ are all defining moduli for L.

We make the distinction of the smallest such defining modulus by calling it the *conductor* of L, denoted f_L. By definition, $\mathbf{Q}_m$ has conductor $f_{\mathbf{Q}_m} = m$. We have the following theorem which gives the formula for the conductor of a quadratic extension:

Theorem 1.4. *Let* $L = \mathbf{Q}(\sqrt{d})$ *for squarefree* d*. Then*

$$f_L = \begin{cases} |d| & \text{if } d \equiv 1 \bmod 4 \\ |4d| & \text{if } d \equiv 2, 3 \bmod 4. \end{cases}$$

A natural question that comes to mind is: does the conductor have any relation to the discriminant of a number field? The theorem above shows that (up to absolute value) the conductor of a nontrivial quadratic extension takes the same value as the discriminant. However, in the cyclotomic field cases, we see they do not have to be equal all the time. After all, given $L = \mathbf{Q}(\zeta_m + \zeta_m^{-1})$ the conductor is well known to be m as well. Pushing forward with conductors, we see

Theorem 1.5. *If m is a defining modulus of L then $f_L \mid m$.*

Proof. We know that for positive integers m_1 and m_2 we know $\mathbf{Q}_{m_1} \cap \mathbf{Q}_{m_2} = \mathbf{Q}_{\gcd(m_1,m_2)}$. By definition $L \subset \mathbf{Q}_{f_L}$ and $L \subset \mathbf{Q}_m$ so it must be in the intersection $L\mathbf{Q}_{\gcd(f_L,m)}$. The conductor is the smallest defining modulus so $d = \gcd(f_L, m)$ cannot be smaller than f_L and also cannot be larger than L (since it is a divisor). We conclude that

$$\mathbf{Q}_d = \mathbf{Q}_{f_L} \text{ meaning } \mathbf{Q}_{f_L} \subset \mathbf{Q}_m$$

which only occurs if $f_L \mid m$.

□

For simpler notation, we let $C_m = (\mathbf{Z}/m\mathbf{Z})^\times$ be the multiplicative group of integers (mod m) which are relatively prime to m. From Galois theory, we know for any defining modulus m, of L, we have $\mathrm{Gal}(\mathbf{Q}_m/\mathbf{Q}) = C_m$. So L is the fixed field for some subgroup of C_m which we will call $I_{L,m}$. This leads to the discussion of Artin's Law of Reciprocity

Theorem 1.6. *(Artin's Law of Reciprocity) If L is an abelian extension of $\mathbf{Q}$ with defining modulus m, then the following sequence is exact*

$$1 \to I_{L,m} \hookrightarrow C_m \to \mathrm{Gal}(L/\mathbf{Q}) \to 1.$$

where the map $(L/\ ) : C_m \to \mathrm{Gal}(L/\mathbf{Q})$ is the restriction of any automoprhism $\zeta \mapsto \zeta^a$ for any $a \in C_m$ to L.

Proof. As discussed previously, there is a natural embedding of $I_{L,m}$ into C_m since the very definition of $I_{L,m}$ comes from being a subgroup. Now consider the Artin Symbol map $(L/)$. This map is clearly surjective since $\mathrm{Gal}(L/\mathbf{Q})$ is isomorphic to $I_{L,m}$. In fact, the kernel of this map is exactly the set of $a \in C_m$ for which $\zeta \mapsto \zeta^a$ acts trivially on L. But to meet this condition is equivalent to saying that this automorphism is part of the subgroup of C_m for which L is the fixed field. We conclude $\ker(L/) = I_{L,m}$ creating a short exact sequence. □

A nice observation from this theorem is that the Galois group $\mathrm{Gal}(L/\mathbf{Q})$ is isomorphic to $C_m/I_{L,m}$. We will soon generalize these notions in the general setting. Assuming some knowledge of Algebraic Number Theory, we move to the following theorem:

Theorem 1.7. *(Conductor - Ramification Theorem) If L is an abelian extension of $\mathbf{Q}$, then p ramifies in L if and only if $p \mid f_L$.*

Teasing the reader with the idea that the conductor should naturally be related to the discriminant. After all, there is already a theorem about ramified primes in a general number field. That is, a prime is ramified if and only if it divides the discriminant.

Example 1.8. Continuing with Example 1.3, we know $f_L = 5$, and the only prime which ramifies is 5.

We finally arrive at the relationship between these two quantities that we have been looking at. First, we define a character (in the representation theory sense for readers who have some background knowledge.)

Definition 1.9. A *character* χ is a morphism $\chi : C_m \to \mathbf{C}^*$. We write $\hat{C_m}$ to denote the set of all characters on C_m.

Definition 1.10. A positive integer c is a *defining modulus of* $\chi \in \hat{C_m}$ if $a \equiv 1 \bmod c$ implies $\chi(a) = 1$.

We adopt the same notation as before: the conductor of a character is the smallest defining modulus of that character. Furthermore, for m a defining modulus of L we denote the *character group* of L to be the set

$$X_{L,m} = \{\chi \in \hat{C_m} : \chi(h) = 1 \text{ for all } h \in I_{L,m}\}.$$

This leads to the following:

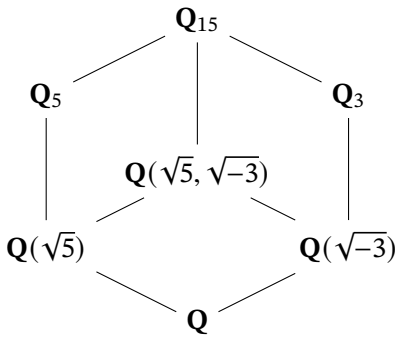
Theorem 1.11. *(Conductor-Discriminant Formula) Let m be a defining modulus of L. Then*

$$f_L = \text{lcm}\{f_\chi : \chi \in X_{L,m}\}$$

and

$$|\text{disc}(K)| = \prod_{\chi \in X_{L,m}} f_\chi.$$

Example 1.12. Let $L = \mathbf{Q}(\sqrt{5},)\sqrt{-3})$. We want to show $|\text{disc}(L)| = 5^2 \cdot 3^2$ and $f_L = 5 \cdot 3$. By Theorem 1.4 we have $f_{\mathbf{Q}(\sqrt{5})} = 5$ and $f_{\mathbf{Q}(\sqrt{-3})} = 3$. The following diagram follows



We know $\text{Gal}(\mathbf{Q}_5/\mathbf{Q}) \cong C_5$ and $\text{Gal}(\mathbf{Q}_3/\mathbf{Q}) \cong C_3$ which are both cyclic. Let a_1 be the generator of C_5 and a_2 be the generator of C_3. Since $\mathbf{Q}_{15} = \mathbf{Q}_5 \cdot \mathbf{Q}_3$ we have

$$\text{Gal}(\mathbf{Q}_{15}/\mathbf{Q}) \cong \text{Gal}(\mathbf{Q}_5/\mathbf{Q}) \times \text{Gal}(\mathbf{Q}_3/\mathbf{Q}) = \langle a_1 \rangle \times \langle a_2 \rangle.$$

Defining characters on $\langle a_1 \rangle \times \langle a_2 \rangle$ comes down to realizing the order of both generators. We want χ_1 and χ_2 to be characters (i.e. morphisms into $\mathbf{C}$.) In order to do this, we need a_1 to map to an element with order 4 and a_2 to map to an element with order 2. Thus, the options for a generic character χ are

$$\chi(a_1) = 1 \text{ or } i, \chi(a_2) = \pm 1.$$

So we define $\chi_1(a_1) = i, \chi_1(a_2) = 1$ and $\chi_2(a_1) = 1, \chi_2(a_2) = -1$ so that the character group of C_{15} is given by

$$\langle \chi_1 \rangle \times \langle \chi_2 \rangle$$

Now we look into the relative Galois groups. Considering $\mathbf{Q}_3 = \mathbf{Q}(\sqrt{-3})$ then $\text{Gal}(\mathbf{Q}_3/\mathbf{Q}(\sqrt{-3})) = \{1\}$. We also know $\mathbf{Q}_5$ is a degree 4 extension over $\mathbf{Q}$. So $\text{Gal}(\mathbf{Q}_5/\mathbf{Q}(\sqrt{5}))$ must be an index 2 subgroup since the two fields are not equal. We get $\text{Gal}(\mathbf{Q}_5/\mathbf{Q}(\sqrt{5})) = \langle a_1^2 \rangle$. Putting everything together we can compute the character group

$$X_{L,15} = \langle \chi_1^2 \rangle \times \langle \chi_2 \rangle.$$

To continue further in this example, we need a little extra machinery.

Proposition 1. *The defining moduli of $\chi \in \hat{C_m}$ are precisely the multiples of f_χ.*

We omit the proof for the sake of demonstrating this example. Since 5 is a defining modulus for χ_1^2 then $f_{\chi_1} = 1$ or 5. But 1 is definitely not a defining modulus of χ_1^2 so it must be the case that $f_{\chi_1} = 5$. Similarly, 3 is a defining modulus for χ_2 we get $f_{\chi_2} = 3$.

To find a modulus for $\chi_1^2\chi_2$ we notice that

$$\chi_1(a_1)^2 = -1 \text{ and } \chi_2(a_2) = -1.$$

Thus, the condition requiring such a c where $a \equiv 1 \bmod c$ implies $\chi_1^2\chi_2(a) = 1$ is equivalent to $c \equiv 1 \bmod 5$ and mod 3. By the Chinese Remainder Theorem, this is equivalent to $c \equiv 1 \bmod 15$. so 15 is a defining modulus. By the previous proposition, $f_{\chi_1^2\chi_2} = 1, 3, 5, 15$. But by the requirements above, one can reason that it must be 15. Thus, by the Conductor-Discriminant Formula, $|\text{disc}(L)| = 1 \cdot 3 \cdot 5 \cdot 15 = 3^2 \cdot 5^2$ and $f_L = 3 \cdot 5$. Notice the added 1 when computing the discriminant. This takes into account the trivial character which sends everything to 1. This completes the example.

Example 1.13. We will show that for $L = \mathbf{Q}(\sqrt{2}, \sqrt{5})$ we have $|\text{disc}(L)| = 1600$ and $f_L = 40$.

Theorem 1.14. *(Decomposition Theorem) Let m be a defining modulus of L. If $p \nmid m$ then the order of $pI_{L,m}$ in $C_m/I_{L,m}$ is f, the residue class degree of p.*

This makes sense considering if $p \nmid m$ then p is unramified in L. Why is this so interesting? Well if we let $m = f_L$ and we know $efg = n = [L : \mathbf{Q}]$ then we can make statements about not only unramified primes but those which split completely in Galois extensions of $\mathbf{Q}$. We define $\text{Spl}(L)$ to be the set of all primes that split completely in L. Then $p \in \text{Spl}(L)$ if and only if $p \nmid f_L$ and $p \in I_{L,f_L}$ which is equivalent to p being congruent to integers mod f_L which are relatively prime. This is a finite set, so $p \in \text{Spl}(L)$ can be given by a finite number of congruence conditions.

Definition 1.15. If p is an odd prime, $a \in \mathbf{Z}$, and $p \nmid a$ the *Legendre Symbol* $(\frac{a}{p})$ is given by

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } x^2 \equiv a \bmod p \text{ has a solution} \\ -1 & \text{if } x^2 \equiv a \bmod p \text{ has no solution.} \end{cases}$$

and if b is an odd positive integer where $b = p_1^{e_1} \cdots p_g^{e_g}$ the *Jacobi Symbol* is given by

$$\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right)^{e_1} \cdots \left(\frac{a}{p_g}\right)^{e_g}.$$

In the coming section we will being to get a notion of this in the general case, for now, we move back to the previous Example 1.12 to see how we can turn $p \in \text{Spl}(L)$ into a set of congruences.

Example 1.16. Let $L = \mathbf{Q}(\sqrt{5}, \sqrt{-3})$ as before. Then we have the isomorphism

$$\text{Gal}(\mathbf{Q}_{15}/\mathbf{Q}) \cong \langle a_1 \rangle \times \langle a_2 \rangle$$

where a_1, a_2 are the generators for $(\mathbf{Z}/5\mathbf{Z})^\times$ and $(\mathbf{Z}/3\mathbf{Z})^\times$ respectively. If we pick explicit generators, say 3 mod 5 and 2 mod 3 Then

$$\text{Gal}(\mathbf{Q}_{15}/\mathbf{Q}) \cong \langle 3 \bmod 5 \rangle \times \langle 2 \bmod 3 \rangle.$$

Using the Chinese Remainder Theorem, we arrive at the stunning result

$$\begin{aligned} \text{Gal}(\mathbf{Q}_{15}/L) &\cong \langle 3^2 \bmod 5 \rangle \times \langle 1 \bmod 3 \rangle \\ &\cong \langle 4 \bmod 15 \rangle. \end{aligned}$$

So primes that split completely in L are EXACTLY those that are 4 or 1 mod 15.

Proof. See [1, p. 123]. □

2. Global Class Field Theory

It is officially the time to begin generalizing the ideas over $\mathbf{Q}$ to an arbitrary ground field. We immediately run into the problem that the Kroncker-Weber Theorem does not hold when the ground field is not $\mathbf{Q}$. To rectify this we will construct a field that holds all the "nice" properties we want to hold from before. We first generalize a defining modulus.

Definition 2.1. When σ is a totally real embedding of K into $\mathbf{C}$ we associate a formal symbol $\mathfrak{p}_\sigma$ to denote a *real infinite $K-$prime.*

Definition 2.2. A *modulus* of K (number field), denoted $\mathfrak{m}$ is a formal product of an ideal in O_K and a set of real infinite primes $K-$primes. So

$$\mathfrak{m} = \mathfrak{m}_0 \cdot \text{ some infinite } K - \text{primes.}$$

where $\mathfrak{m}_0 \subset O_K$.

Let $A_\mathfrak{m}$ be the set of all fractional ideals $\mathfrak{a} \in A = A_K$ such that unique factorization of $\mathfrak{a}$ and $\mathfrak{m}$ into $K-$primes contain no $K-$primes in common. In essence, we are demanding that $\mathfrak{a}$ and $\mathfrak{m}$ are relatively prime as fractional ideals in O_K. To generalize the notion of congruence we need to understand the set $A_\mathfrak{m}$. We start with the following Proposition.

Proposition 2. *Let $K^* = K - \{0\}$. If $\alpha \in K$, let (α) be the principal ideal αO_K. If $(\alpha) \in A_\mathfrak{m}$ then $\alpha = \frac{a}{b}$ where $a, b \in O_K$ **AND** $(a), (b) \in A_\mathfrak{m}$!*

This result is not a triviality at all and the proof must be handled with some care.

Proof. □

With this Proposition, we can extend the notion of congruence to an arbitrary ground field.

Definition 2.3. Let $(\alpha) \in A_\mathfrak{m}$. Then $\alpha \equiv 1 \bmod \mathfrak{m}$ means $a \equiv b \bmod \mathfrak{m}_0$ where $\alpha = a/b$ are as above and $\sigma(\alpha) > 0$ for each infinite $K-$prime $\mathfrak{p}_\sigma$ occuring in $\mathfrak{m}$.

References

[1] N. Bourbaki, *Commutative Algebra*, Springer-Verlag, New York, 1989.
[2] F. Lindemann, "Über die Zahl π," *Math. Annalen* **20** (1882), 213–225. URL https://eudml.org/doc/ 157031.
[3] S. Lang, *Algebraic Number Theory*, 3rd ed., Springer-Verlag, New York, 1994.